MEETING 15 - RELATIONS

In this lecture we will study binary relations in general but mostly equivalence relations and partial order relations.

Binary relations

We will start with a defintion of what a binary relation actually is:

Definition: Let A and B be sets. A subset R of the cartesian product $A \times B$ is called a *binary relation* from A to B. If two elements $x \in A$ and $y \in B$ also have $(x, y) \in R$ we say that x and y are *related* and we write this xRy.

As we write this, we are introducting relations on just about anything we can form sets of. Since we can form sets of anything, we are, in effect, introducting a way of describing relations between anything. This level of abstraction can be confusing, so let us look at a few concrete examples.

Example: Let A be the set of 4 human beings, say $\{Charles, Linda, Muhammad, Sahar\}$ and let B be the set of professions $\{Carpenter, Doctor, Engineer, Teacher\}$. We can now define a relation from A to B by saying that x (one of the humans in A) is related to y (one of the professions in B) if and only if x has the profession B. We could then write "Charles is a carpenter" as $CharlesRCarpenter$. This would then set-theoretically mean that $(Charles, Carpenter) \in R$. It is also possible for a person to have two professions, if Sahar is both a doctor and a teacher we write $SaharRDoctor \wedge SaharRTeacher$, which can also be written $(Sahar, Doctor) \in R \wedge (Sahar, Teacher) \in R$.

Of course this is exactly the basis for a relational database management system (RDBMS) which is such a successful computer technical application of a concept in discrete mathematics. Let us look at a more mathematical example.

Example: Let us look at a numerical example. Let both A and B be the set of real numbers. Say that xRy if and only if $x^2 + y^2 = 1$. This defines a subset of the plane which we recognize as a circle of radius 1. And two real values x and y are related if and only if the corrsponding point (x, y) lies on the circle, that is $(x, y) \in R$ if we denote the circle with R. For example the points $(1, 0)$, $(0, 1)$, $(-1, 0)$, $(0, -1)$ are all on the circle, therefore we have $0R1$, $1R0$, $0R-1$, and $-1R0$. Since none of the points $(1, 1)$ and $(-1, -1)$ ar eon the circle, we do *not* have $1R1$ or $-1R-1$ though.

Binary relations have certain properties that makes them behave in special ways. In particular they are very interesting when they relate elements of the same set. In the two examples above, the first example did not relate elements of the sameset. The set of the four humans are not the set of professions (A was not B), whereas the second example was an example of a relation that related elements from the same set, that is the set A was the set B. We say that such a relation is defined *on* a set A. We formulate the most important properties in a definition:

Definition: Let R be a relation on a set A. Then:

(a) R is called *reflexive* $\Leftrightarrow \forall x \in A : xRx$, this means that each element in A is related to itself.
(b) R is called *symmetric* $\Leftrightarrow \forall x, y \in A : xRy \leftrightarrow yRx$, this means that we always have xRy and yRx at the same time, there can never be xRy unless we also have yRx.
(c) R is called *antisymmetric* $\Leftrightarrow \forall x, y \in A : xRy \wedge yRx \rightarrow x = y$. We will describe the meaning of this later on.
(d) R is called *transitive* $\Leftrightarrow \forall x, y, x \in A : xRy \wedge yRz \rightarrow xRz$, this means that if x is related to y and y in turn is related to z, then x is also related to z. The relation transcends y, or "carries over". We will see better what this means later on.

We will now study various examples of all these properties.

Example: Let the relation R on the integers be given by $xRy \Leftrightarrow \exists k \in \mathbb{Z} : x - y = 7 \cdot k$. In words we can say like this: the two integers x and y are related if they differ by a multiple of 7. (We express that multiple as $7 \cdot k$, where k is an integer.) This relation is reflexive. To see this we need to show that every integer x is related to itself. Is it a fact that there is an integer k such that $x - x = 7 \cdot k$? Sure! We can just pick $k = 0$. That concludes the proof that every x is related to itself because this argument does not depend on which x we are considering. Hence R is reflexive. We proceed to see that the relation is also symmetric. To see this we must show that $xRy \Leftrightarrow yRx$. Pick two arbitrary x and y which have xRy. Can we somehow also see that yRx? Well, if we study xRy in detail we see that it is the same thing as $x - y = 7 \cdot k$ for some $k \in \mathbb{Z}$. But this can also be written $y - x = 7 \cdot (-k)$ and since $-k$ is also an integer, we see indeed that also yRx. Again since x and y were chosen arbitrary we see that $xRy \Rightarrow yRx$. Letting the variables change roles also gives the reverse implication, that is $xRy \Leftarrow yRx$ so that in conclusion we have $xRy \Leftrightarrow yRx$. Again since the variables were arbitrarily chosen, the proof is complete. We now show transitivity and choose x, y, z arbitrarily and assume that xRy and yRz. This means that there are integers k and k' such that $x - y = 7 \cdot k$ and $y - z = 7 \cdot k'$. But then we can write $x - z = x - y + y - z = 7 \cdot k + 7 \cdot k' = 7 \cdot (k + k')$ and since both k and k' are integers, we conclude that x and z also differ by a multiple of 7, that is xRz and we have shown transitivity since the variables were arbitrarily chosen. The relation we are studying is not antisymmetric. To show this we must find some numbers that fail to meet the requirement for antisymmetry. Can we find two numbers x and y such that xRy and yRx but $x \neq y$? After some pondering, we find that yes, any two distinct numbers that differ by a multiple of 7 will do, for example $0R7$ and $7R0$ but $0 \neq 7$.

Can you recognize which relation this is? Well, it is just the congruence relation modulo 7.

The second relation described above (with the circle) is not reflexive, but it is symmetric. The proofs of these facts are left as exercises.

Example: We will now introduce a very important relation. Let x and y be integers and say that $xRy \Leftrightarrow \exists k \in \mathbb{Z} : y = kx$. That is x is related to y if y is a multiple of x. We sometimes say that x *divides* y or that y is *divisible* by x. We then write this relation like this

$$x|y.$$

This relation is reflexive since each integer x divides itself, because $x = 1 \cdot x$ so that $x = k \cdot x$ holds for $k = 1$. Similarly the relation is transitive, and we see this by again assuming $x|y$ and $y|z$ and showing that we also have $x|z$. Then, according to the definition, there exists integers k and k' such that $y = kx$ and $z = k'y$. Replacing y by kx in the last equation gives us $z = k'kx = \tilde{k}x$ for $\tilde{k} = k'k$, and since this is also an integer we have shown that $x|z$. Since x, y, z were arbitrary we have shown the transitivity. This relation is however not symmetric. To see this all we need to do is to find two numbers x and y such that $x|y$ but not $y|x$. After some pondering we realize that we can choose $x = 2$ and $y = 6$, then, certainly $2|6$ (since $6 = 3 \cdot 2$) but we cannot have $6|2$ (since if $2 = 6 \cdot k$, the k would not be an integer). If we restrict ourselves to positive integers we shall now see that the relation is antisymmetric and we see this by assuming $x|y$ and $y|x$ and showing that these numbers must be the same. This is true since $x|y$ and $y|x$ means that there are integers k and k' such that $x = ky$ and $y = k'x$. These relations show us that if one of x and y are 0, then both must be 0. We therefore assume that both of them are nonzero. Replacing x with ky in one of the equations gives us the new equation $y = k'ky$ and we may cancel y (since it is not z0) yielding the equation $1 = k'k$ where k' and k are integers. The question then is, which integers work? If we multiply together any integers that are not ± 1, we always get a number which has absolute value greater than 1, this means that the equation $1 = k'k$ can only have the solutions where both k' and k have absolute value 1, that is they must both be either -1 or $+1$. Since the product of them is 1, which is positive we alse see that they must either both be 1 or both be -1. If they are both 1, then obviously $x = y$. If they are both -1 we have the equations $x = -y$ and $y = -x$ but this is impossible when we are restricted to positive numbers. Hence the only option is $x = y$ and antisymmetry is shown.

Here is a problem: Is there a relation which has *all* four properties, reflexivity, symmetry, antisymmetry, and transitivity?

Higher order relations: Study independently.

Equivalence relations

This deals with relations that have the three properties reflexivity, symmetry and transitivity. These relations are particularly interesting and they are called equivalence relations. We lay this down formally in a definition:

Definition: Let R be a relation on a set A. If R is reflexive, symmetric, and transitive, then R is called an *equivalence relation* on A.

We have seen one equivalnce relation, it wa the one above where $xRy \Leftrightarrow \exists k \in \mathbb{Z} : x - y = 7 \cdot k$. With our notation on divisibility we could rewrite this a

$$xRy \Leftrightarrow 7|x - y,$$

that is 7 divides $x - y$. We also noted that with out earlier concept of congruences, this could be written $x \equiv y \pmod 7$.

We will now dissect this relation a bit. Which integers are related to 0? To find this out we study these numbers as a set. The set of integers that are related to 0 can be denoted as

$$\{x \in \mathbb{Z}; 7|(x - 0)\} = \{x \in \mathbb{Z}; \exists k \in \mathbb{Z} : x = 7 \cdot k\}$$

But this is merely the set consisting of all multiples of 7, that is $\{0, \pm 7, \pm 2 \cdot 7, \pm 3 \cdot 7, \ldots\}$. One usually say that these are the numbers that give *remainder* 0 when we divide by 7. And, in our teminology of congruences, this is all numbers congruent to 0 modulo 7.

We continue our dissection of this relation and as which integers are related to 1? To find this out we again, as above, study these numbers as a set. The set of integers that are related to 1 can then be denoted as

$$\{x \in \mathbb{Z}; 7|(x - 1)\} = \{x \in \mathbb{Z}; \exists k \in \mathbb{Z} : x - 1 = 7 \cdot k\} = \{x \in \mathbb{Z}; \exists k \in \mathbb{Z} : x = 7 \cdot k + 1\}$$

But this is merely the set consisting of all multiples of 7 with 1 added, that is $\{0+1, \pm 7+1, \pm 2\cdot 7+1, \pm 3\cdot 7+1, \ldots\}$. And, similarly, we say that these are the numbers that give remainder 1 when we divide by 7. Again, in our terminology of congruences, this is the set of all numbers congruent to 1 modulo 7.

We can continue in exactly the same way and see that all numbers that are related to 2, 3, 4, 5, and 6, are the numbers that give the remainders 2, 3, 4, 5, and 6 when we divide by 7. All these sets can be written

$$\{0 + 2, \pm 7 + 2, \pm 2 \cdot 7 + 2, \ldots\}, \{0 + 3, \pm 7 + 3, \pm 2 \cdot 7 + 3, \ldots\}, \{0 + 4, \pm 7 + 4, \pm 2 \cdot 7 + 4, \ldots\},$$
$$\{0 + 5, \pm 7 + 5, \pm 2 \cdot 7 + 5, \ldots\}, \{0 + 6, \pm 7 + 6, \pm 2 \cdot 7 + 6, \ldots\}.$$

Now the interesting question is, what happens when we study all the numbers that are related to 7. Which are those? Well, 7 itself is a multiple of 7 so it is in $\{0, \pm 7, \pm 2 \cdot 7, \pm 3 \cdot 7, \ldots\}$, and if a number x is related to 7, it is also related to 0, by transitivity, but then it must be in $\{0, \pm 7, \pm 2 \cdot 7, \pm 3 \cdot 7, \ldots\}$ because this is the set of all numbers related to 0. We come back to 0, which is where we started. Similarly we find that all numbers related to 8 in fact again is the set $\{0 + 1, \pm 7 + 1, \pm 2 \cdot 7 + 1, \pm 3 \cdot 7 + 1, \ldots\}$ and so on. I turns out that there are no other sets of this type, the sets

$$\{0, \pm 7, \pm 2 \cdot 7, \pm 3 \cdot 7, \ldots\}, \{0 + 1, \pm 7 + 1, \pm 2 \cdot 7 + 1, \pm 3 \cdot 7 + 1, \ldots\}$$
$$\{0 + 2, \pm 7 + 2, \pm 2 \cdot 7 + 2, \ldots\}, \{0 + 3, \pm 7 + 3, \pm 2 \cdot 7 + 3, \ldots\}, \{0 + 4, \pm 7 + 4, \pm 2 \cdot 7 + 4, \ldots\},$$
$$\{0 + 5, \pm 7 + 5, \pm 2 \cdot 7 + 5, \ldots\}, \{0 + 6, \pm 7 + 6, \pm 2 \cdot 7 + 6, \ldots\}.$$

together contain all integers. We say that they form a *partition* of the set of integers, that is $\mathbb{Z}$. If two numbers x and y are related, they must therefore lie in the same set. This is a special type of equivalence on integers, and it has it's own name and we have encountered the name before but we restate the definition here in the context of binary relations:

If the two numbers x and y lie in the same set (that is, they are related) we say that x is *congruent* to y *modulo* 7.

Above we have worked with 7 and then the integers got partitioned into 7 sets. Of course this is no coincidence, since we base all calculations on 7. If we would have chosen 2 then we would have had two sets like this and the integers would then be partitioned into the sets

$$\{0, \pm 2, \pm 2 \cdot 2, \pm 2 \cdot 3, \ldots\}, \{0 + 1, \pm 2 + 1, \pm 2 \cdot 2 + 1, \pm 2 \cdot 3 + 1, \ldots\}$$

which are simply the even and odd numbers, and together they contain all integers. (When then talk about *congruence modulo 2.*)

This is a general property of an equivalence relation: it partitions the set it is defined on into disjoint sets and these sets together contain all the elements of the set. An equivalence relation thus introduces a structure on the set it is defined on. Structures of this type often have extremely good uses, the congruence relation for example led to the development of the RSA cryptosystem. Because this property of equivalence relations is so useful we will study it separately. We will do this by first introducing some terminology and some notation.

Notation: For an equivalence relation we often express the fact that two elements a and b are related by writing $a \sim b$. We very often refer to the relation itself by writing this symbol, and then we say "the relation $\sim$". The three characteristics of and equivalence relation can then be expressed that for every a, b, c in the underlying set A we must have the three conditions

reflexivity: $a \sim a$
symmetry: $a \sim b \Leftrightarrow b \sim a$
transitivity: $a \sim b \wedge b \sim c \Rightarrow a \sim c$

We continue by introducing some terminology:

Definition: Let $\sim$ be an equivalence relation defined on a set A and let a be any element in A. If an element $b \in A$ is related to a we ($a \sim b$) we say that a and b are *equivalent*. The set of all elements that are equivalent to a is called the *equivalence class* of a and it is written $\bar{a}$. The set of all equivalence classes is denoted $A/\sim$. (This is a set of sets!)

Example: When we study the congruence relation modulo 7 above, the equivalence classes of the numbers $0, 1, 2, 3, 4, 5, 6$ are the sets

$$\bar{0} = \{0, \pm 7, \pm 2 \cdot 7, \pm 3 \cdot 7, \ldots\}, \bar{1} = \{0 + 1, \pm 7 + 1, \pm 2 \cdot 7 + 1, \pm 3 \cdot 7 + 1, \ldots\}$$
$$\bar{2} = \{0 + 2, \pm 7 + 2, \pm 2 \cdot 7 + 2, \ldots\}, \bar{3} = \{0 + 3, \pm 7 + 3, \pm 2 \cdot 7 + 3, \ldots\}, \bar{4} = \{0 + 4, \pm 7 + 4, \pm 2 \cdot 7 + 4, \ldots\},$$
$$\bar{5} = \{0 + 5, \pm 7 + 5, \pm 2 \cdot 7 + 5, \ldots\}, \bar{6} = \{0 + 6, \pm 7 + 6, \pm 2 \cdot 7 + 6, \ldots\}.$$

and we have seen that these classes partition $\mathbb{Z}$. We will now prove that this is the case for any equivalence relation. We will formulate this as a theorem, but first we will state a very important property of an equivalence class:

Proposition: Let $\sim$ denote an equivalence relation on a set A. Let $a \in A$. Then for any $x \in A$ we have $x \sim a \Leftrightarrow \bar{x} = \bar{a}$.

Proof: Suppose $\bar{x} = \bar{a}$. Since $x \sim x$ we have $x \in \bar{x}$, but since $\bar{x} = \bar{a}$ this also means that $x \in \bar{a}$. But this means exactly that $x \sim a$ which is what we wanted to prove. Supposed conversely that $x \sim a$. We now need to prove that $\bar{x} = \bar{a}$. Whenever we want that two sets S_1, S_2 are the same we often prove the two inclusions $S_1 \subseteq S_2$ and $S_1 \supseteq S_2$. We will do this with the sets $\bar{x}$ and $\bar{a}$, that is we will show that both $\bar{a} \subseteq \bar{x}$ and $\bar{x} \subseteq \bar{a}$. Suppose that $y \in \bar{x}$. Then $y \sim x$ and $x \sim a$ so $y \sim a$ by transitivity. Therefore $y \in \bar{a}$ so that $\bar{x} \subseteq \bar{a}$. Conversely suppose that $y \in \bar{a}$. Then $y \sim a$. Since we also have $a \sim x$ we have both $y \sim a$ and $a \sim x$. Again, by transitivity we get $y \sim x$ and hence $y \in \bar{x}$ so that $\bar{a} \subseteq \bar{x}$. In conclusion we have shown $\bar{a} = \bar{x}$.

This proposition has a very important consequence for equivalence classes: *We can choose any element of an equivalence class and it will determine the whole equivalence class.* We can therefore speak of a *representative* of an equivalence class, and a representative of an equivalence class is *simply any member of the equivalence class.* In the example above, as soon as we choose a number (say 15) this number has a certain remainder (1) when we divide by 7, and all the other numbers in the same equivalence class as this number (15) also have the same remainder when we divide them by 7. The same is of course true for any number. As an exercise formulate this for another divisor, what happen when we divide by 4? What happens when we divide by 10?

Now we are ready to state and prove the theorem mentioned above:

Theorem: The equivalence classes associated with an equivalence relation $\sim$ on a set A gives rise to a partition of A.

Proof: Every element $a \in A$ is in an equivalence class, namely $\bar{a}$ itself so we can be sure of that

$$A \subseteq \cup_{C \in A/\sim} C.$$

Here we denote the family of all equivalence classes of the relation by $A/\sim$. Conversely since all elements only come from A we must also have

$$A \supseteq \cup_{C \in A/\sim} C$$

and these two inclusions give

$$A = \cup_{C \in A/\sim} C.$$

This means that if we take together all the equivalence classes in a union, then they form the set A. To show that it is a partition of A we must show that two equivalence classes are either disjoint or they are equal. Assume that two equivalence classes C_1 and C_2 have one element a in common. Then we have $x \sim a$ for all $x \in C_1$ and $y \sim a$ for all $y \in C_2$. But this also means that a is a representative for both the equivalence class C_1 and C_2, but then they must be the same class. This means that all the different equivalence classes must either have all elements in common, that is they are the same class, or they must be disjoint. As their union is A this shows that they form a partition of A and the the proof is complete.

The notation for the set of equivalence classes above is used in many mathematical texts. As told above, the set of equivalence classes is denoted $A/\sim$ and this is a set of sets. It is called the *quotient set* of A *mod* $\sim$.

Example: Returning to the example above with congruences modulo 7, we saw earlier that

$$\bar{0} = \{0, \pm 7, \pm 2 \cdot 7, \pm 3 \cdot 7, \ldots\}, \bar{1} = \{0+1, \pm 7+1, \pm 2 \cdot 7+1, \pm 3 \cdot 7+1, \ldots\}$$

$$\bar{2} = \{0+2, \pm 7+2, \pm 2 \cdot 7+2, \ldots\}, \bar{3} = \{0+3, \pm 7+3, \pm 2 \cdot 7+3, \ldots\}, \bar{4} = \{0+4, \pm 7+4, \pm 2 \cdot 7+4, \ldots\},$$

$$\bar{5} = \{0+5, \pm 7+5, \pm 2 \cdot 7+5, \ldots\}, \bar{6} = \{0+6, \pm 7+6, \pm 2 \cdot 7+6, \ldots\}.$$

To further illustrate the theorem about partitions of the set A, in our example here we have $A = \mathbb{Z}$ and if we think about it, it is really a fact that

$$\mathbb{A} = \bar{0} \cup \bar{1} \cup \bar{2} \cup \bar{3} \cup \bar{4} \cup \bar{5} \cup \bar{6}$$

and since none of these sets have any elements in common, they are clearly a partition of $\mathbb{Z}$.

Partial orders

Equivalence relations is one very important form of binary relation. The other sort of very important binary relation is the *partial order*. A partial order has two requirements in common with the equivalence relations: reflexivity and transitivity, but instead of symmetry, a partial order is antisymmetric. We make a formal definition:

Definition: A *partial order* on a set A is a binary relation that is reflexive, antisymmetric, and transitive. A *partially ordered set*, *poset* for short, is a pair $(A, \preceq)$ where A is a set and $\preceq$ is a partial order defined on A. Two elements $a, b \in A$ are said to be *comparable* if either $a \preceq b$ or $b \preceq a$. If every two elements of A are comparable, then we call $(A, \preceq)$ a *totally ordered set* and $\preceq$ is then called a *total* order.

We will study some examples of partial and total orders.

Example: Of course an ordinary set of numbers together with the ususal less-than-or-equal relation is a partially ordered set. Indeed is is even a totally ordered set since for every two numbers a, b we have either $a \leq b$ or $b \leq b$ (or both if $a = b$).

Example: All positive integers together with the divides-relation, $|$, is a partially ordered set. Let us verify the requirements for this to be a partially ordered set:

> **Reflexivity:** As a positive integer x always divides itself (we have $x|x$ since $x = 1 \cdot x$), reflexivity is fulfilled for the relation $|$ on the set of positive integers.
>
> **Antisymmetry:** We saw above that $|$ was antisymmetric, that is we saw before that $x|y$ and $y|x$ leads to $x = y$ when we are restricted to positive integers.
>
> **Transitivity:** Likewise we also saw before that transitivity was satisfied.

These three properties makes $|$ into a partial order on the set of positive integers. What is the meaning of the word *partial*? The fact is that under the relation $|$ on the set of positive integers, we cannot compare all numbers with each other. This means that $|$ is not a total order on the set of all positive integers. For instance we do not have $5|7$ or $7|5$ this means that the numbers 5 and 7 are not comparable.

Draw some Hasse diagrams of partially ordered sets.

A partial order compares elements in a set. This means that we can form the notion of upper and lower bounds of sets. We make the following definition:

Definition: Let $(A, \preceq)$ be a partially ordered set. An element $a \in A$ is called *maximum* if and only if $b \preceq a$ for every $b \in A$. Conversely, an element $a \in A$ is called *minimum* if and only if $a \preceq b$ for every $b \in A$. An element $a \in A$ is called *maximal* if and only if

$$b \in A \wedge a \preceq b \Rightarow b = a$$

and *minimal* if

$$b \in A \wedge b \preceq a \Rightarow b = a.$$

Thus a **maximum** element is "bigger" (in the sense of $\preceq$) than all other elements in the set, while a (mere) **maximal** element is one that is at least not less than any other element.

Draw some Hasse diagrams of partially ordered sets with maximal elements and maximum.

We skip the parts about greatest lower bounds/smallest upper bounds and lattices