TUESDAY WEEK 3 NOTES

SUDESH KALYANSWAMY

1. Equivalence Relations

1.1. **Definition and Examples.** We now turn our attention to a very specific type of relation, known as an equivalence relation. This concept comes up repeatedly in math classes in every area of math, so we devote an entire section to it.

Definition. A relation R on a set X is called an *equivalence relation* if R is reflexive, symmetric, and transitive.

Since equivalence relations are important, we will look at several examples.

Example. Let R be the relation on $\mathbb{R}$ defined by $x \sim y$ if $x - y \in \mathbb{Z}$. To check this is an equivalence relation, we need to check the three properties:

(1) *Reflexive*: Let $x \in \mathbb{R}$. Then $x - x = 0 \in \mathbb{Z}$, meaning $x \sim x$, which is what we wanted. Therefore, R is reflexive.
(2) *Symmetric*: Let $x, y \in \mathbb{R}$ with $x \sim y$. We want to show $y \sim x$. Since $x \sim y$, we know $x - y = k \in \mathbb{Z}$. But then $y - x = -k \in \mathbb{Z}$. Therefore, $y \sim x$, and R is symmetric.
(3) *Transitive*: Let $x, y, z \in \mathbb{R}$ with $x \sim y$ and $y \sim z$. We want to show $x \sim z$. Since $x \sim y$, we know $x - y = k \in \mathbb{Z}$, and since $y \sim z$, we know $y - z = l \in \mathbb{Z}$. But then
$$x - z = (x - y) + (y - z) = k + l \in \mathbb{Z}.$$
Thus, $x \sim z$, and R is transitive.

Therefore, R is an equivalence relation.

Example. Fix a positive integer n. We define a relation R on $\mathbb{Z}$ by saying $a \sim b$ if $n|(a - b)$. We saw in the previous section (with $n = 3$) that this relation is reflexive, symmetric, and transitive. There was nothing special about 3 in those examples. Replace the 3 by an n and the same work shows this is an equivalence relation for any $n \in \mathbb{Z}$.

Example. Let S and T be sets, and let $f : S \to T$ be a function. Define a relation R on S by saying $x_1 \sim x_2$ if $f(x_1) = f(x_2)$. This relation is clearly reflexive and symmetric. If $x_1 \sim x_2$ and $x_2 \sim x_3$, then $f(x_1) = f(x_2)$, and $f(x_2) = f(x_3)$, and therefore $f(x_1) = f(x_3)$, meaning $x_1 \sim x_3$. Thus, R is transitive, making it an equivalence relation.

1.2. **Equivalence Classes.**

Definition. Let R be an equivalence relation on a set X. For $a \in X$, define the *equivalence class* of a to be the set of all elements equivalent to a. It is denoted $[a]$. In other words,
$$[a] = \{x \in X : x \sim a\}.$$

Example. In the first example above, we have
$$[0] = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} = \mathbb{Z},$$
$$[2] = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} = \mathbb{Z},$$
$$[1.1] = \{\ldots, -3.9, -2.9, -1.9, -.9, .1, 1.1, 2.1, \ldots\}.$$
How do we get these? So see what $[0]$ is, we need to see which elements are equivalent to zero. We know $x \sim 0$ if and only if $x - 0 \in \mathbb{Z}$, but this just means $x \in \mathbb{Z}$. This is why $[0] = \mathbb{Z}$.

For the second one, we have that $x \sim 2$ precisely when $x - 2 \in \mathbb{Z}$. But if $x - 2 \in \mathbb{Z}$, then $x \in \mathbb{Z}$ as

well, which explains the second class.

Lastly, $x \sim 1.1$ if $x - 1.1 \in \mathbb{Z}$. This means $x = 1.1 + k$ for $k \in \mathbb{Z}$. This is how we get the last set.

Example. If $n = 3$ in the second example, how can we describe $[2]$? Well,

$$[2] = \{\ldots, -1, 2, 5, 8, 11, \ldots\}.$$

Taking a closer look, we see that $[2]$ is just the set of integers which have a remainder of 2 when divided by 3. More generally, $[a]$ will be the set of integers which have the same remainder as a when divided by 3. If n is just an arbitrary integer, then $[a]$ will be the set of integers which share the same remainder as a when divided by n.

Taking an even closer look at the relation on $\mathbb{R}$ given by $x \sim y$ if $x - y \in \mathbb{Z}$, observe $[0] = [2]$. Why is that? It happened because $0 \sim 2$ under R, so that anything equivalent to 2 is equivalent to 0 (by transitivity), and vice versa. This is a more general fact.

Lemma. If R is an equivalence relation on a set S, then for any $a, b \in S$, $[a] = [b]$ if and only if $a \sim b$.

Proof. Let $a, b \in S$. If $[a] = [b]$, then as $a \in [a]$, we know $a \in [b]$, and thus $a \sim b$.

Conversely, let $a \sim b$. Then $[a] \subseteq [b]$ because if $c \in [a]$, then $c \sim a$, and since $a \sim b$, we know by transitivity that $c \sim b$. Thus $c \in [b]$. The reverse inclusion is similar. Thus, $[a] = [b]$, as desired. □

Consider the relation on $\mathbb{Z}$ given by $a \sim b$ if $5|(b - a)$, an equivalence relation as above. Then we know $[2] = [7]$ since $2 \sim 7$, but $[2] \neq [1]$ as $2 \not\sim 1$.

Definition. Let R be an equivalence relation on a set S. If we consider the equivalence class $[a]$, then a is called a *representative* for the equivalence class.

Remark. All the work above shows that there could be many representatives for the same class. For example, if R on $\mathbb{R}$ is the relation $x \sim y$ if $x - y \in \mathbb{Z}$, then every equivalence class has infinitely many representatives. Take the class $[0]$. We know $[0] = [1]$, so 1 is a representative for the same class. In fact, any integer k can be a representative for the class, as $[0] = [k]$ for any $k \in \mathbb{Z}$. In this example, there are infinitely many possible representatives.

1.3. **Quotients.**

Definition. Let X be a set and R an equivalence relation on X. Then the set of equivalence classes under R is denoted X/R or $X/\sim$. We call this set X *modulo* R or the *quotient of* X *by* R.

Example. If R is the relation on $\mathbb{R}$ given by $x \sim y$ if $x - y \in \mathbb{Z}$, then what is $\mathbb{R}/\sim$? We know that two real numbers define the same equivalence class if they differ by an integer. Notice that every class has a representative which lies in the interval $[0, 1)$. For example, the class $[5.1234]$ is the same as the class $[.1234]$. Moreover, if $a, b \in [0, 1)$, then $[a] \neq [b]$, since there is no way a and b can differ by an integer (as they are less than distance 1 from one another). Thus,

$$\mathbb{R}/R = \{[c] : c \in [0, 1) \subset \mathbb{R}\}.$$

Example. Fix a positive integer n. Let R be the relation on $\mathbb{Z}$ given by $x \sim y$ if $n|(x - y)$. We typically denote $\mathbb{Z}/R$ by $\mathbb{Z}/n$ to emphasize that it depends on n. What is $\mathbb{Z}/n$? The claim is that

$$\mathbb{Z}/n = \{[0], [1], [2], \ldots, [n - 1]\}.$$

To see this, notice that every equivalence class has some representative between 0 and $n - 1$ (just take the remainder when divided by n). On the other hand, all these classes are inequivalent since the difference between any two of the representatives is less than n, and hence cannot be divisible by n.

1.4. **Equivalence Relations and Partitions.** We have the following proposition.

Proposition. Let X be a set and R an equivalence relation on X. Then every element of X belongs to a unique equivalence class.

Proof. Let $x \in X$. Then $x \in [x]$, so x belongs to some equivalence class. We want to show this class is unique. Suppose x belongs to another class $[y]$, i.e. $x \in [y]$. Then by definition, $x \sim y$. But then by the lemma proved above, we get $[x] = [y]$. Thus, the class is unique. □

What this proposition tells us is that equivalence classes divide our original set X into different disjoint pieces. We can make this precise with the following definition.

Definition. Let X be a set. A family $\mathcal{F}$ of subsets of X *partitions* X if every element of X belongs to exactly one member of $\mathcal{F}$.

Example. Let $X = \{1, 2, 3, 4\}$, and let $\mathcal{F} = \{\{1, 2\}, \{3\}, \{4\}\}$. Then $\mathcal{F}$ partitions X. On the other hand, if $\mathcal{G} = \{\{1, 2\}, \{1, 3, 4\}\}$, then $\mathcal{G}$ is not a partition of X because 1 belongs to two classes, not just one.

Given a set X and an equivalence relation R, then we get a partition of X by just considering the equivalence classes. That is, X/R partitions X. The converse is true as well.

Proposition. If $\mathcal{F}$ is a partition on X, then $\mathcal{F}$ determines an equivalence relation on X by declaring that $x \sim y$ if and only if $\exists A \in \mathcal{F}$ such that $x \in A$ and $y \in A$.

Proof. We show the three properties. First, take $x \in X$. Then $x \in A$ for some $A \in \mathcal{F}$ by definition of the partition. Thus, $x \sim x$, and the relation is reflexive.

Next, suppose $x \sim y$. Thus, $x \in A$ and $y \in A$ for some $A \in \mathcal{F}$. But this clearly means $y \sim x$ (conjunctions are symmetric). Thus, the relation is symmetric.

Finally, suppose $x \sim y$ and $y \sim z$ for elements $x, y, z \in X$. Then $x \in A$ and $y \in A$ for some $A \in \mathcal{F}$, and $y \in B$ and $z \in B$ for some $B \in \mathcal{F}$. However, by definition, y must belong to a unique member of $\mathcal{F}$, and thus $A = B$. Therefore, $x \sim z$, and the relation is transitive. □

1.5. **Functions and Quotient Spaces.** Defining functions when there are quotient spaces involved is not always the easiest thing to do. We do, however, have one natural function.

Definition. Let X be a set, and R an equivalence relation on X. Then there is a *natural projection* $p : X \to X/R$ given by $p(x) = [x]$.

One question would be whether we could go the other way. Namely, is there a function $X/R \to X$ mapping $[x] \mapsto x$? We could certainly try to define a function this way, but we run into trouble. The problem is that this may not be a function. For example, consider the map $f : \mathbb{Z}/5 \to \mathbb{Z}$ mapping $[x] \to x$. This says $f([2]) = 2$, and $f([3]) = 3$. But it also means $f([7]) = 7$, which is bad since $[2] = [7]$. So $f([2]) = 2$ and 7, which contradicts the definition of a function.

The moral of the story is that when defining functions with some quotient space as the domain, we need to check it is *well-defined*, which means that it does not depend on the choice of representative. Let us look at an example.

Problem. Show that $f : \mathbb{Z}/5 \to \mathbb{Z}/5$ given by $f([x]) = [2x]$ is a well-defined function.

Solution. What we want to show is that if $[x] = [y]$, then $f([x]) = f([y])$. Well, if $[x] = [y]$, then $x \sim y$, so $5|(x - y)$. We want to show $[2x] = [2y]$, i.e. that $5|(2x - 2y)$. But notice that as $5|(x - y)$, there is an integer k such that $5k = x - y$. Then $5(2k) = 2x - 2y$, meaning $5|(2x - 2y)$, as desired. Thus, this function is well-defined.

Remark. The map $f : \mathbb{Z}/5 \to \mathbb{Z}$ given by $f([x]) = 2x$ is NOT well-defined. Notice $f([1]) = 2$, but if we change the representative to 6, then $f([6]) = 12 \neq 2$, which means this map depends on the choice of representative. Therefore, it is not a function.

1.6. **Problems.** Let us look at some problems.

Problem. Let S and T be sets, and let $f : S \to T$ be a function. Consider the relation R on S given by $s_1 \sim s_2$ if $f(s_1) = f(s_2)$. This is an equivalence relation. Define a map $g : S/\sim \to T$ given by $g([s]) = f(s)$.

(a) Show g is a well-defined function.

(b) Show that g is injective.

Solution. (a) Suppose $[s_1] = [s_2]$. We want to show $g([s_1]) = g([s_2])$. If $[s_1] = [s_2]$, then $s_1 \sim s_2$, meaning $f(s_1) = f(s_2)$. But then

$$g([s_1]) = f(s_1) = f(s_2) = g([s_2]),$$

meaning g is well-defined.

(b) Suppose $g([s_1]) = g([s_2])$. We want to show $[s_1] = [s_2]$. By definition of g, we know $f(s_1) = f(s_2)$, so $s_1 \sim s_2$. This implies $[s_1] = [s_2]$, as desired.

Problem. Consider the map $g : \mathbb{Z}/n \times \mathbb{Z}/n \to \mathbb{Z}/n$ given by $g([x], [y]) = [xy]$. Show that g is well-defined.

Solution. Suppose $[x] = [x']$ and $[y] = [y']$. We want to show $g([x], [y]) = g([x'], [y'])$. Since $x \equiv x' \bmod n$, there exists a k such that $x - x' = nk$. Similarly, there exists an l such that $y - y' = nl$. We want to show $n|(xy - x'y')$. It is not immediately clear how to do this, but we observe we can write

$$xy = (x' + nk)(y' + nl) = x'y' + n(lx' + ky') + n^2kl.$$

Thus, $xy - x'y' = n(lx' + ky' + nkl)$, which is what we needed. Therefore g is well-defined.

Remark. This gives us a way of multiplying modulo n: $[x] \cdot [y] = [xy]$, and this is well-defined by the above problem. In the HW, you will show addition is well-defined as well. Another way of writing what was shown above is that if $x \equiv x' \bmod n$ and $y \equiv y' \bmod n$, then $xy \equiv x'y' \bmod n$.

To show you the power of the above remark, consider the following problem:

Problem. Compute the remainder when 8^7 is divided by 3.

Solution. There are several approaches to this problem given what we've done. The first is to say that we are looking for 8^7 mod 3, i.e. $[8^7]$ in quotient space $\mathbb{Z}/3$. By the above, this is just $[8]^7$. We know $[8] = [2]$, so this is just $[2]^7$. We could just list out the powers of $[2]$ in $\mathbb{Z}/3$: $[2]^2 = [4] = [1]$, so $[2]^3 = [2]$, and $[2]^4 = [1]$, and so on. We end up with $[2]^7 = [2]$, and thus the remainder is 2.

We could also have noticed that $[8] = [-1]$, so $[8]^7 = [-1]^7 = [(-1)^7] = [-1] = [2]$, so the remainder is 2.

Problem. Is the well-defined function $f : \mathbb{Z}/6 \to \mathbb{Z}/6$ given by $f([x]) = [2x + 3]$ injective?

Solution. Since $\mathbb{Z}/6$ only has 6 elements, we should be able to just check it:

$$f([0]) = [3], \quad f([1]) = [5], \quad f([2]) = [1], \quad f([3]) = [3].$$

At this point we can stop since $f([0]) = f([3])$, which means f is not injective.