Sets and Logic, Dr. Block, Lecture Notes, 4-13-2020

We continue discussing equivalence relations and partitions. Please read Section 11.5 of the text and work on Exercises 1, 3, 5, and 7 on page 221 of the text.

Last time we saw that if you start with an equivalence relation on a set A, then the set equivalence classes forms a partition of A. of Our next theorem shows that if we start with a partition $\mathcal{F}$ of a set A, then from this partition we can get an equivalence relation on A. This theorem is given as an exercise in the text (Exercise 4 in section 11.4).

Here is an example to think about as you study the proof.

Consider the set $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and the partition of A given by

$$\mathcal{F} = \{\{1, 2, 3, 4\}, \{5, 6\}, \{7, 8, 9\}\}.$$

I have inserted some remarks at various points in the proof. The remarks should be omitted in the formal proof.

Theorem. Suppose that A is a set, and $\mathcal{F}$ is a partition of A. Then there is an equivalence relation R on A such that the set of equivalence classes is equal to $\mathcal{F}$.

Proof. Suppose that A is a set, and $\mathcal{F}$ is a partition of A. We define a relation R on A by declaring that xRy if and only if there exists some $B \in \mathcal{F}$ such that $x \in B$ and $y \in B$.

(Remark: We use the same variable B here to indicate that both x and y are in the same set of the partition. So, in the example given above, we have xRy if and only if $x, y \in \{1, 2, 3, 4\}$ or $x, y \in \{5, 6\}$ or $x, y \in \{7, 8, 9\}$.)

First, we prove that R is reflexive. Suppose that $x \in A$. Then, since $\mathcal{F}$ is a partition, there exists some $B \in \mathcal{F}$ such that $x \in B$. It follows by logical equivalence that $x \in B$ and $x \in B$. Therefore, xRx. It follows that R is reflexive.

(Remark: We used the equivalence, $P \equiv (P \wedge P)$.)

Second, we prove that R is symmetric. Suppose that $x, y \in A$ and xRy. Then for some $B \in \mathcal{F}$, we have $x \in B$ and $y \in B$. It follows by logical equivalence that $y \in B$ and $x \in B$. Therefore, yRx. It follows that R is symmetric.

(Remark: We used the equivalence, $(P \wedge Q) \equiv (Q \wedge P)$.)

Third, we prove that R is transitive. Suppose that $x, y, z \in A$. Suppose that xRy and yRz. Then, there is some set $B \in \mathcal{F}$ such that $x \in B$ and $y \in B$, and there is some set $D \in \mathcal{F}$ such that $y \in D$ and $z \in D$.

(Remark: We could not at this point call both of the sets B. If we did we would be assuming that the two sets are equal. We can not assume that. We have to prove it.)

Now, observe that $y \in B$ and $y \in D$. So, B and D are not disjoint. Since $B, D \in \mathcal{F}$ and $\mathcal{F}$ is a partition, it follows that $B = D$. Thus, $x \in B$ and $z \in B$. Therefore, xRz. It follows that R is transitve.

Since R is reflexive, symmetric, and transitive, we conclude that R is an equivalence relation.

Finally, we prove that for the relation R, the set of equivalence classes is equal to $\mathcal{F}$.

(Remark: We prove that the two sets are equal, by proving that each one is a subset of the other.)

First, suppose that X is an equivalence class. Then $X = [x]$ for some $x \in A$. Since $\mathcal{F}$ is a partition, there is some $B \in \mathcal{F}$ such that $x \in B$. It follows from how we defined the relation R that $X = [x] = B$. So $X \in \mathcal{F}$.

Second, suppose that $X \in \mathcal{F}$. Since $\mathcal{F}$ is a partition, there is some $x \in X$. It follows from how we defined the relation R that $X = [x]$. So X is an equivalence class.

We conclude that the set of equivalence classes is equal to $\mathcal{F}$.

□

Theorem. Let n be a positive integer. The relation R on $\mathbb{Z}$ given by xRy if and only if

$$x \equiv y \pmod{n}$$

is an equivalence relation on $\mathbb{Z}$. Moreover, there are exactly n distinct equivalence classes given by

$$[0], [1], \ldots, [n-1].$$

Proof. It is proved in the text on Page 208, that this relation R is reflexive, symmetric, and transitive. Hence, R is an equivalence relation.

We now prove two claims:

Claim 1. If $c, d \in \{0, 1, \ldots, n-1\}$ and $c \neq d$, then $[c] \neq [d]$.

We prove Claim 1. Suppose that $c, d \in \{0, 1, \ldots, n-1\}$ and $c \neq d$. Proceeding by contradiction, suppose that $[c] = [d]$. Then $c \in [d]$. So,

$$c \equiv d \pmod{n}.$$

It follows that for some integer j we have $c - d = jn$. Then $d - c = (-j)n$. Since $c \neq d$, either $c > d$ or $d > c$. We consider these two cases.

Case 1. $c > d$. Then $c - d$ is a positive integer which is less than n, and n divides $c - d$. This is a contradiction.

Case 2. $d > c$. Then $d - c$ is a positive integer which is less than n, and n divides $d - c$. This is a contradiction.

Since we obtained a contradiction in each case, this proves the Claim 1.

Claim 2. For every integer x there is an integer $r \in \{0, 1, \ldots, n-1\}$ such that $[x] = [r]$.

We prove Claim 2. Suppose that x is an integer. By the division algorithm there exist integers q and r such that $x = qn + r$. So $x - r = nq$. It follows that n divides $x - r$. Therefore,

$$x \equiv r \pmod{n}.$$

It follows that $[x] = [r]$. This proves Claim 2.

It follows from the two claims that there are exactly n distinct equivalence classes given by

$$[0], [1], \ldots, [n-1].$$

□

Definition. The relation R in the previous theorem is sometimes called the relation $\equiv \pmod{n}$. The set of equivalence classes for this relation is denoted by $\mathbb{Z}_n$. This set is sometimes called the integers modulo n.

The following theorem is important to keep in mind as you read Section 11.5 of the text.

Theorem. Let n be a positive integer. Suppose that $a, b, c, d \in \mathbb{Z}$ satisfy

$$a \equiv c \pmod{n} \text{ and } b \equiv d \pmod{n}.$$

Then $a + b \equiv c + d \pmod{n}$ and $ab \equiv cd \pmod{n}$.

Proof. Let n be a positive integer. Suppose that $a, b, c, d \in \mathbb{Z}$ satisfy

$$a \equiv c \pmod{n} \text{ and } b \equiv d \pmod{n}.$$

Then there are integers j and k such that $a - c = jn$ and $b - d = kn$. It follows that

$$(a + b) - (c + d) = (a - c) + (b - d) = jn + kn = (j + k)n.$$

Therefore, $a + b \equiv c + d \pmod{n}$.

It also follows that

$$ab - cd = ab - ad + ad - cd = a(b - d) + d(a - c) = akn + djn = (ak + dj)n.$$

Therefore, $ab \equiv cd \pmod{n}$.

□

Definition and Remark. We can define two operations, which we call addition and multiplication, on the set $\mathbb{Z}_n$ by

$$[a] + [b] = [a + b] \text{ and } [a] \cdot [b] = [a \cdot b].$$

This is well-defined in light of the previous theorem. This is discussed in Section 11.5 of the text.

□