8. Equivalence relations and congruence classes

8.1. Equivalence relations and equivalence classes.

Definition. Let X be a set. A relation on X is a subset R of $X \times X$ (where $X \times X = \{(x, y) : x, y \in X\}$ is the Cartesian product of X is itself). If R is a relation on X, and $x, y \in X$, we write xRy if and only if $(x, y) \in R$.

A slightly less formal but more intuitive way to think about relations is as follows. We say that R is a relation on a set X if for every $x, y \in X$ we can form an expression xRy and declare it to be either true or false (depending on x and y). This is how familiar relations like $<$ (less than) or $|$ (divisibility) on $X = \mathbb{Z}$ are defined. If a relation R on X is defined in such a way, the corresponding subset of $X \times X$ (also denoted by R) is the set of all pairs (x, y) for which xRy is true.

Definition. Let R be a relation on X. We say that R is an equivalence relation if it satisfies the following conditions:

(i) xRx for all $x \in X$ (reflexivity)
(ii) If xRy for some $x, y \in X$, then yRx (symmetry)
(iii) If xRy and yRz for some $x, y, z \in X$, then xRz (transitivity)

While R is a standard notation for a general relation, equivalence relations are typically denoted by the symbol $\sim$. If $\sim$ is an equivalence relation on a set X, we often say that elements $x, y \in X$ are equivalent if $x \sim y$.

The relations $<$ and $|$ on $\mathbb{Z}$ mentioned above are not equivalence relations (neither is symmetric and $<$ is also not reflexive). An example of equivalence relation which will be very important for us is *congruence mod n* (where $n \geq 2$ is a fixed integer); in other words, we set $X = \mathbb{Z}$, fix $n \geq 2$ and define the relation $\sim$ on X by $x \sim y \iff x \equiv y \mod n$. Note that we already checked that such $\sim$ is an equivalence relation (see Theorem 6.1 from class).

Definition. Let $\sim$ be an equivalence relation on a set X. Given $x \in X$, we define the equivalence class of x to be the set

$$[x] = \{y \in X : y \sim x\}.$$

In other words, $[x]$ is the set of all elements of X which are equivalent to x. By AN equivalence class (with respect to $\sim$) we will mean the equivalence class of some element $x \in X$.

Example 1. *Let $X = \mathbb{R}^2$ (the Euclidean plane) and define the relation $\sim$ on X by $(x_1, y_1) \sim (x_2, y_2)$ if and only if $x_1^2 + y_1^2 = x_2^2 + y_2^2$.*

It is straightforward to check that $\sim$ is an equivalence relation. Given $(a, b) \in \mathbb{R}^2$, its equivalence class is the set $[(a, b)] = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = a^2 + b^2\}$. Clearly, $[(a, b)]$ is the circle of radius $\sqrt{a^2 + b^2}$ centered at $(0, 0)$ (note that the circle "degenerates" into a point if $a = b = 0$).

Thus, in this example equivalence classes are circles centered at the origin and the origin itself. Observe that in our example the equivalence classes of any two elements are either the same or are disjoint (have empty intersection) and, moreover, the union of all equivalence classes is the entire set X. These properties are true for equivalence classes with respect to any equivalence relation.

Proposition 8.1. *Let $\sim$ be an equivalence relation on a set X. Then for any $u, v \in X$ either $[u] = [v]$ or $[u] \cap [v] = \emptyset$. Moreover, $\bigcup\limits_{u \in X} [u] = X$.*

The first assertion of this proposition is left as a homework exercise. The second assertion holds simply because by reflexivity any element lies in its own equivalence class ($u \in [u]$ for every $u \in X$).

In Example 1 we were able to describe equivalence classes directly based on the definition, but if the formula describing the equivalence relation was more complicated, we would not be able to do this. The following "algorithm" can be used to compute all equivalence classes, at least when the number of equivalence classes is finite. Take some element $x \in X$ and compute its equivalence class $[x]$. If $[x] = X$, we are done (there is just one equivalence class); if not, we can choose some $y \in X \setminus [x]$ and compute its equivalence class $[y]$. If $[x] \cup [y] = X$, we are done (there are two equivalence classes); if not, choose $z \in X \setminus ([x] \cup [y])$, compute its equivalence classes and keep going until the union of the equivalence classes we explicitly computed is the entire set X.

Example 2. *Let us now compute the equivalence classes with respect to relation $\equiv \mod n$ on $\mathbb{Z}$ (where $n \geq 2$ is a fixed integer).*

Using the above algorithm, we start with the equivalence class of 0 and add classes one at a time until we exhaust all the integers. We get

$$\begin{array}{ccccc}
[0] & = & \{x \in \mathbb{Z} : x \equiv 0 \mod n\} & = & \{\ldots, -n, 0, n, 2n, \ldots\} \\
[1] & = & \{x \in \mathbb{Z} : x \equiv 1 \mod n\} & = & \{\ldots, 1-n, 1, n+1, 2n+1, \ldots\} \\
 & & & \ldots & \\
[n-1] & = & \{x \in \mathbb{Z} : x \equiv n-1 \mod n\} & = & \{\ldots, -1, n-1, 2n-1, 3n-1, \ldots\}
\end{array}$$

Thus, based on the above calculation, there are n (distinct) equivalence classes with respect to $\equiv \mod n$ relation, namely $[0], [1], \ldots, [n-1]$. To formally justify this claim we need to prove that

(i) the classes $[0], [1], \ldots, [n-1]$ are distinct and

(ii) for any $x \in \mathbb{Z}$ the class $[x]$ is equal to one of $[0], [1], \ldots, [n-1]$.

Assertion (i) is clear since the integers $0, 1, \ldots, n-1$ are pairwise non-congruent to each other (mod n), and (ii) is a consequence of the following claim.

Claim 8.2. *Let $a, b \in \mathbb{Z}$. Then $[a] = [b]$ if and only $a \equiv b \mod n$. In particular, if we are given any $x \in \mathbb{Z}$ and we divide x by n with remainder: $x = nq + r$ with $0 \leq r \leq n-1$, then $[x] = [r]$.*

Proof. If $[a] = [b]$, then $a \in [a] = [b]$, so by definition $a \equiv b \mod n$. Conversely, if $a \equiv b \mod n$, then $a \in [b]$, so $[a] \cap [b]$ is nonempty (as $a \in [a] \cap [b]$) whence $[a] = [b]$ by Proposition 8.1. □

8.2. **The ring of congruence classes $\mathbb{Z}_n$.** Fix an integer $n \geq 2$. The equivalence classes with respect to the relation $\equiv \mod n$ are called *congruence classes mod n*. We will denote the set of (distinct) congruence classes mod n by $\mathbb{Z}_n$. Thus, as we proved above, $\mathbb{Z}_n$ has n elements: $[0], [1], \ldots, [n-1]$.

Note that $[x]$ is a perfectly valid element of $\mathbb{Z}_n$ for ANY $x \in \mathbb{Z}$, not just for $x = 0, 1, \ldots, n-1$; it is just that taking x outside of the set $\{0, 1, \ldots, n-1\}$ will not yield any new elements. For instance, $[n] = [0]$, $[n+1] = [1]$, $[-1] = [n-1]$ etc.

We now define two binary operations $+$ and $\cdot$ on $\mathbb{Z}_n$ by setting

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

Note that in both formulas, $+$ and $\cdot$ on LHS are operations on $\mathbb{Z}_n$ we are defining while $+$ and $\cdot$ on RHS are the usual addition and multiplication of integers.

Theorem 8.3. *$\mathbb{Z}_n$ with these operations is a commutative ring with 1.*

Proof. Before verifying the axioms, we need to show that operations in $\mathbb{Z}_n$ are *well defined*. The following example shows what could go in principle go wrong with the way operations are defined. Consider, say, $n = 7$. Then $[1] = [8]$ and $[2] = [16]$ in $\mathbb{Z}_7$, so it should be true $[1] + [2] = [8] + [16]$ (as we are adding the same two elements of $\mathbb{Z}_7$ on both sides). However, from the way operations are defined it is not clear why $[1] + [2]$ and $[8] + [16]$ could not be different, as $[1]+[2]=[1+2]=[3]$ while $[8]+[16]=[24]$. There is no problem in this particular example as $7 \mid (24-3)$, so $[3]=[24]$ in $\mathbb{Z}_7$, but we need to make sure that things will work the same way if we pick different n and different elements of $\mathbb{Z}_n$ (and also that the same is true for multiplication).

So, in general, we need to show that if we are given any $a, b, a', b' \in \mathbb{Z}$ such that $[a]=[a']$ and $[b]=[b']$, then $[a+b]=[a'+b']$ and $[ab]=[a'b']$. This is done as follows: by definition $[a]=[a']$ and $[b]=[b']$ means that $a \equiv a' \mod n$ and $b \equiv b' \mod n$. By Theorem 6.3 we have $a+b \equiv a'+b' \mod n$ and $ab \equiv a'b' \mod n$ which, in turn, implies that $[a+b]=[a'+b']$ and $[ab]=[a'b']$. Thus, we checked that both $+$ and $\cdot$ on $\mathbb{Z}_n$ are well defined.

We proceed with axiom verification. First of all, (A0) and (G0) are clear from definition since $[x]$ is an element of $\mathbb{Z}_n$ for any integer x. Next we verify associativity of addition (A2). Axioms (A1), (M1), (M2) and (D1)-(D2) can be verified using the same general procedure.

For any $a, b, c \in \mathbb{Z}$ we need to show that $[a]+([b]+[c])=([a]+[b])+[c]$. We have

$$\begin{array}{cl}
[a]+([b]+[c]) & \text{LHS of (A2)} \\
=[a]+[b+c] & \text{Definition of addition in } \mathbb{Z}_n \\
=[a+(b+c)] & \text{Definition of addition in } \mathbb{Z}_n \\
=[(a+b)+c)] & \text{Associativity of addition in } \mathbb{Z} \\
=[a+b]+[c] & \text{Definition of addition in } \mathbb{Z}_n \\
=([a]+[b])+[c] & \text{Definition of addition in } \mathbb{Z}_n
\end{array}$$

Finally, to prove (A3), (A4) and (M3) observe that $[a]+[0]=[0]+[a]=[a]$, $[a]+[-a]=[0]$ and $[a]\cdot[1]=[1]\cdot[a]=[a]$ for all $a \in \mathbb{Z}$. Thus, (A3) holds with $0=[0]$, (A4) holds with $-[a]=[-a]$ and (M3) holds with $1=[1]$. In other words, the zero element of $\mathbb{Z}_n$ is the congruence class of 0; the unity (1) of $\mathbb{Z}_n$ is the congruence class of 1, and the additive inverse of the congruence class of a is the congruence class of the additive inverse of a. □

Below we compute the multiplication table for $\mathbb{Z}_6$:

$\odot$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Based on this table, $\mathbb{Z}_6$ is not a field since there is no $[1]$ in the rows labeled by $[2], [3]$ and $[4]$. Thus, the only invertible elements are $[1]$ and $[5] = -[1]$ and $[1]^{-1} = [1]$ and $[5]^2 = [1]$.