7 Equivalence Relations

An important fundamental concept in algebra is the notion of an equivalence relation. These arise in many instances. We’ll use the idea in the next section, where we introduce modular integer rings.

**Definition 7.1.** Let $X$ be a non-empty set. A relation on $X$ is a subset of $X \times X$.

**Example 7.1.** Let $X$ be the set of real numbers. Let $R$ be the relation defined by $(x, y) \in R$ iff $x \leq y$. $R$ contains elements such as $(1,1), (\pi, 4), \text{and } (-7/3, 0)$, but does not contain $(2,1)$, since $2 \nleq 1$. Note that $(x, x) \in R$ for each $x \in X$, so we say that $R$ is a reflexive relation. Also if $x \leq y$ and $y \leq z$ then $x \leq z$. In particular if $(x, y), (y, z) \in R$ then $(x, z) \in R$. We say that the relation $R$ is transitive. On the other hand, $(1, 2) \in R$, but $(2,1) \notin R$, so $R$ is not symmetric.

**Definition 7.2.** Let $X$ be a non-empty set. A relation $R$ on $X$ is called an equivalence relation if

(i) $(x, x) \in R$ for every $x \in X$ ($R$ is reflexive),

(ii) if $(x, y) \in R$ then $(y, x) \in R$ ($R$ is symmetric),

(iii) if $(x, y), (y, z) \in R$ then $(x, z) \in R$ ($R$ is transitive).

If $R$ is an equivalence relation on a set $X$ then the equivalence class of an element $x \in R$ is defined as the set of all elements in $X$ that are equivalent to $x$. We write

$$[x] = \{y \in X : (x, y) \in R\}.$$ 

**Example 7.2.** Let $R$ be the relation on $\mathbb{Z}$ defined by $(x, y) \in R$ iff $y - x$ is divisible by 6. Then $(x, x) \in R$ since $x - x = 0 = 6 \cdot 0$, and clearly if $y - x$ is divisible by 6 then so is $x - y$, so $R$ is symmetric. Finally, if $y - x = 6k_1$ and $z - y = 6k_2$ then $z - y + y - x = z - x = 6(k_1 + k_2)$, so $R$ is transitive. We deduce that $R$ is an equivalence relation on $\mathbb{Z}$.

The equivalence class of 7 wrt $R$ is $[7] = \{y \in \mathbb{Z} : 6| (y - 7)\}$. Note that $y - 7 = 6k$ for some $k$ iff $y = 7 + 6k = 1 + 6(k+1)$, which holds iff $y - 1 = 6(k+1)$. In particular $y$ is equivalent to 7 iff $y$ is equivalent to 1. So $[7] = [1]$ wrt $R$.

Observe that both 1 and 7 have the same equivalence class, and both give the same remainder upon division by 6. This is no coincidence. In fact in general if $(x, y) \in R$ then there is some $k$ such that $y = x + 6k$, so $x$ and $y$ have the same unique positive remainder in $\{0, 1, 2, 3, 4, 5\}$. This gives another way to describe the equivalence class of $x$ wrt $R$:

$$[x] = \{x + 6k : k \in \mathbb{Z}\}.$$ 

Let’s list the distinct equivalence classes of $R$. Note that since there are just six distinct remainders wrt 6, there must be exactly 6 distinct equivalence classes $[x]$, as $x$ runs over $\mathbb{Z}$.

$$[0] = \{6k : k \in \mathbb{Z}\}$$
$$[1] = \{6k + 1 : k \in \mathbb{Z}\}$$
$$[2] = \{6k + 2 : k \in \mathbb{Z}\}$$
$$[3] = \{6k + 3 : k \in \mathbb{Z}\}$$
$$[4] = \{6k + 4 : k \in \mathbb{Z}\}$$
$$[5] = \{6k + 5 : k \in \mathbb{Z}\}$$

Note that every integer $x$ gives some remainder in $\{0, ..., 6\}$, so this is the complete list of equivalence classes of $R$. Note also that the positive remainder produced in the application of the division algorithm to $x$ and 6 is unique, so every pair of distinct equivalence classes has empty intersection. We say that the set of equivalence classes of $R$ form a partition of $X$.

**Definition 7.3.** Let $X$ be a non-empty set. A partition of $X$ is a collection $\mathcal{P}$ of subsets of $X$ such that:

(i) $X$ is the union of the subsets $P \in \mathcal{P}$,
(ii) \( P \cap Q = \{\} \) unless \( P = Q \) for any pair of subsets of \( X \) contained in \( P \).

In other words, \( P \) is a partition of \( X \) if \( X \) is the disjoint union of the subsets of \( X \) contained in \( P \).

We have the following connection between partitions and equivalence relations of a set.

**Theorem 7.1.** Let \( X \) be a non-empty set. Then every partition of \( X \) induces an equivalence relation on \( X \), and every equivalence relation induces a partition of \( X \).

**Proof.** Let \( R \) be an equivalence relation on \( X \). Let \( P \) be the collection of distinct equivalence classes of \( X \) wrt \( R \):

\[
P = \{[x] : x \in X\}.
\]

It’s clear that the union of subsets \([x]\) of \( X \) in \( P \) is all of \( X \) as \( x \) ranges over \( X \). If \( z \in [x] \cap [y] \) then \((x, z), (y, z) \in R\), which, by symmetry and transitivity gives \((x, y) \in R\), so \([x] = [y]\). It follows that \( P \) is a partition of \( X \).

On the other hand if \( P \) is a partition of \( X \), define a relation \( R \) on \( X \) by \((x, y) \in R\) iff \( x \) and \( y \) belong to the same subset of \( X \) contained in \( P \). Clearly \( R \) is reflexive since the union of the subsets of \( X \) in \( P \) is \( X \). \( R \) is clearly symmetric, and finally if \( x, y \in P \) and \( y, z \in P \) then \( x, z \in P \), so \( R \) is transitive. \( \square \)

**Example 7.3.** Let \( X = \{1, 2, 3, 4, 5\} \). Then

\[
P = \{\{1, 2, 3\}, \{4\}, \{5\}\}
\]

is a partition of \( X \). It is routine to check that the relation

\[
\begin{align*}
(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), \\
(3, 3), (2, 1), (3, 1), (3, 2), (4, 4), (5, 5)
\end{align*}
\]

satisfies the axioms of an equivalence relation.

Recall the Division Algorithm in \( \mathbb{Z} \):

**Theorem 7.2.** Let \( a, b \in \mathbb{Z}, b \neq 0 \). Then there exist unique \( m, r \in \mathbb{Z} \) such that

\[
a = mb + r, r < |b|.
\]

We say that \( r \) is a reminder of \( a \) modulo \( b \), or that \( r \) is found by reducing \( a \) wrt \( b \), and write \( \text{rem}_b(a) = r \).

Given a positive integer \( n \), the relation \( R \) on \( \mathbb{Z} \) defined by \((x, y) \in R\) if \( x \) and \( y \) have the same remainder modulo \( n \) is an equivalence relation. The equivalence class of \( x \) wrt this relation is the set

\[
[x] = \{nm + x : m \in \mathbb{Z}\} = \{y \in \mathbb{Z} : \text{rem}_n(y) = \text{rem}_n(x)\}.
\]

Since there are exactly \( n \) remainders modulo \( n \), namely 0, 1, 2, ..., \( n-1 \), there are exactly \( n \) distinct equivalence classes in \( \mathbb{Z} \) wrt this relation.

\[
\begin{align*}
[0] & = \{nk : k \in \mathbb{Z}\} \\
[1] & = \{nk + 1 : k \in \mathbb{Z}\} \\
\vdots & = \vdots \\
[n-1] & = \{nk + (n-1) : k \in \mathbb{Z}\}
\end{align*}
\]

The set of all these classes forms a partition of \( \mathbb{Z} \):

\[
P = \{[0], [1], ..., [n-1]\}.
\]

In fact, as we’ll see in the next section, this set has a natural algebraic structure, forming a ring called the **ring of integers modulo** \( n \).
8 The Ring of Integers Modulo $n$

We consider an important class of finite rings, the ring of integers modulo $n$.

Recall Example 7.2. The set of distinct equivalence classes of $\mathbb{R}$ are given by

$$\{[0], [1], [2], [3], [4], [5]\}.$$  

We denote this set by $\mathbb{Z}_6$, or $\mathbb{Z}/6\mathbb{Z}$, and call these equivalence classes the congruence or residue classes of the integer 6. We write $a \equiv b \pmod{6}$ if $a$ and $b$ belong to the same congruence class of 6 and say that $a$ and $b$ are equal modulo 6.

We can define addition in $\mathbb{Z}_6$ as follows:

$$[a] + [b] = [a + b].$$


Similarly, we define multiplication in $\mathbb{Z}_6$ by

$$[a][b] = [ab].$$

So, for example $([3][4] + [2][5]) + [2] = ([0] + [4]) + [2] = [4] + [2] = [0]$.

All of these notions can be extended to the case of any positive integer $n$.

Let $n$ be a positive integer. We denote by $\mathbb{Z}_n$, or $\mathbb{Z}/n\mathbb{Z}$, the set of distinct congruence classes modulo $n$:

$$\mathbb{Z}_n = \{[0], [1], ..., [n-1]\}.$$  

As we’ve seen in the previous section, the congruence class of $x$ is given by

$$[x] = \{nk + x : k \in \mathbb{Z}\}$$

for each $x \in \mathbb{Z}$, and $[x]$ has a unique representation as $[r]$ where $r$ the remainder of $x$ modulo $n$.

We define addition and multiplication modulo $n$ as follows:

$$[a] + [b] = [a + b], \quad [a][b] = [ab].$$

It is straightforward to check that these are well-defined operations on $\mathbb{Z}_n$: If $[x] = [x']$, $[y] = [y']$ for some $x, x', y, y' \in \mathbb{Z}$, then there exist $k, t \in \mathbb{Z}$ such that

$$[x] + [y] = [x + y] = [(nk + x') + (nt + y')] = [n(k + t) + (x' + y')] = [x' + y'] = [x'] + [y'].$$

The proof that multiplication is well-defined as an operation on $\mathbb{Z}_n$ is similar.

Given any $a, b, c \in \mathbb{Z}$, associativity of addition in $\mathbb{Z}$ gives

$$( [a] + [b] ) + [c] = [(a + b) + c] = [a + (b + c)] = [a] + ([b] + [c]),$$

and

$$( [a][b] )[c] = [(ab)c] = [a(bc)] = [a][([b][c])],$$

so addition and multiplication modulo $n$ are associative on $\mathbb{Z}$.

The additive identity of $\mathbb{Z}$ is given by $[0]$, and as with associativity, the distributive laws hold in $\mathbb{Z}_n$ and are inherited from the distributivity of $\mathbb{Z}$:

$$( [a] + [b] )[c] = [(a + b)c] = [ac + bc] = [a][c] + [b][c],$$

and

$$[a]([b] + [c]) = [a(b + c)] = [ab + ac] = [a][b] + [a][c].$$

It follows that $\mathbb{Z}_n$ is a ring wrt the operations of addition and multiplication as defined here.

In fact multiplication is commutative in $\mathbb{Z}_n$ and $[1]$ is the multiplicative identity of $\mathbb{Z}_n$, so:
Theorem 8.1. Let \( n \) be a positive integer. The set of integers modulo \( n \) is a unital commutative ring.

We might now ask ourselves the question, "when, if ever, is \( \mathbb{Z}_n \) a field?".

Note that in \( \mathbb{Z}_6 \),

\[
[2][1] = [2], [2][3] = [0], [2][4] = [2], [2][5] = [4],
\]

so \([2]\) has no inverse in \( \mathbb{Z}_6 \). In fact, since \([2][3] = [0] \) in \( \mathbb{Z}_6 \), neither of \([2]\), or \([3]\) are units in \( \mathbb{Z}_6 \).

In general:

**Theorem 8.2.** Let \( R \) be a unital ring. If \( a \) is a zero divisor in \( R \) then \( a \) is not a unit in \( R \).

**Proof.** Let \( a \in R \) be a zero divisor. Then \( a \neq 0 \) and there exists nonzero \( b \in R \) such that \( ab = 0 \). If \( a \) is a unit in \( R \) then there exists \( c \in R \) such that \( ac = ca = 1 \). But then

\[
b = (ca)b = c(ab) = 0,
\]
giving a contradiction. It follows that \( a \) has no inverse in \( R \). \( \square \)

So no zero divisor of \( \mathbb{Z}_n \) has an inverse in \( \mathbb{Z}_n \) wrt multiplication. Indeed if \( n \) can be properly factorised as \( n = ab \) for \( 0 < a, b < n \), then \([a][b] = [n] = [0] \) in \( \mathbb{Z}_n \), so \([a]\), \([b]\) are neither \([0]\) nor invertible in \( \mathbb{Z}_n \) and hence \( \mathbb{Z}_n \) is not a field. This shows that if \( \mathbb{Z}_n \) is a field, then \( n \) must be prime.

In fact the converse to this statement is also true. We’ll use the fact that if \( d = \gcd(a, b) \) for a pair of nonzero integers \( a, b \) then there exist \( s, t \in \mathbb{Z} \) such that \( as + bt = d \).

**Theorem 8.3.** \( \mathbb{Z}_n \) is a field if and only if \( n \) is prime.

**Proof.** Let \( n \) be a positive integer. Then \( n \) is prime if and only if \( \gcd(n, m) = 1 \) for every nonzero integer \( m \) that is not a multiple of \( n \). Let \( m \in \mathbb{Z} \) such that \([m] \neq [0] \). Then \( n \) is prime if and only if there exist \( s, t \in \mathbb{Z} \) such that \( ns + mt = 1 \), which holds only if \([ns] = [mt] = [m][t] = [1] \), which is true if and only if \([t] = [m]^{-1} \) in \( \mathbb{Z}_n \).

On the other hand, if \([m][t] = [1] \) for some integer \( t \) then \( n \) divides \( 1 - mt \) in \( \mathbb{Z} \), so there exists \( s' \in \mathbb{Z} \) such that \( 1 = ns' + mt \), and \( \gcd(n, m) = 1 \). Since \([m] \neq [n] \) was arbitrarily chosen, we deduce that \( n \) is prime. \( \square \)

From the proof of Theorem 8.3, it is easy to see that the units of \( \mathbb{Z}_n \) are precisely the elements \([m] \in \mathbb{Z}_n \) such that \( m \) and \( n \) are relatively prime (have no factors in common). In particular, every element of \( \mathbb{Z}_n \) is either a unit or a zero divisor.

We denote by \( \mathcal{U}(\mathbb{Z}_n) \) the set of units of \( \mathbb{Z}_n \).

**Lemma 8.1.** \( \mathcal{U}(\mathbb{Z}_n) \) is a group wrt the operation of multiplication in \( \mathbb{Z}_n \).

**Proof.** If \([a], [b] \in \mathcal{U}(\mathbb{Z}_n) \) then there exist \([x], [y] \in \mathcal{U}(\mathbb{Z}_n) \) such that \([a][x] = [b][y] = [1] \). Then

\[
[ab][xy] = ([a][b])([x][y]) = ([a][x])([b][y]) = [1],
\]

so by commutativity in \( \mathbb{Z}_n \), \([xy]\) is the inverse of \([ab]\). This shows that multiplication is an operation on \( \mathbb{Z}_n \).

We’ve already seen that it is an associative operation, \([1]\) is the identity of \( \mathcal{U}(\mathbb{Z}_n) \) wrt multiplication, and every element of \( \mathcal{U}(\mathbb{Z}_n) \) is invertible in \( \mathcal{U}(\mathbb{Z}_n) \) by definition. \( \square \)

In general, \( \mathcal{U}(\mathbb{Z}_n) = \{[m] : \gcd(m, n) = 1\} \).