Equivalence relations

1. Binary relations

Definition 1.1 (Relation between two sets). If $X$ and $Y$ are sets, a relation between $X$ and $Y$ is a subset $R \subseteq X \times Y$. For a relation $R \subseteq X \times Y$ and $x \in X, y \in Y$ if $(x, y) \in R$, we write $xRy$ and if $(x, y) \notin R$, we write $x \not\sim y$.

If $xRy$, we say that $x$ is $R$-related to $y$ and if $x \not\sim y$, we say that $x$ is not $R$-related to $y$.

Definition 1.2 (Binary relation on a set). A binary relation on a set $X$ is a relation $R$ between $X$ and $X$, that is, a subset $R \subseteq X \times X$.

Example 1.3.

1. For any set $X$, $\emptyset$ is a binary relation on $X$.
2. For any set $X \neq \emptyset$, the set $X \times X$ is a binary relation on $X$.
3. For any set $X \neq \emptyset$, the set $\text{diag}(X) := \{(x, x) : x \in X\}$ is a binary relation on $X$.
4. If $X \neq \emptyset$ is a set and $f : X \to X$ is a function, then $\text{graph}(f) = \{(x, y) \in X \times X : x \in X, y = f(x)\}$ is a binary relation on $X$.
5. For $X = \mathbb{R}$ the set $\{(x, y) \in \mathbb{R} \times \mathbb{R} : x \leq y\}$ is a binary relation on $\mathbb{R}$.
6. For $X = \mathbb{R}$ the set $\{(x, y) \in \mathbb{R} \times \mathbb{R} : x < y\}$ is a binary relation on $\mathbb{R}$.
7. For $X = \mathbb{R}$ the set $\{(x, y) \in \mathbb{R} \times \mathbb{R} : x - y \in \mathbb{Z}\}$ is a binary relation on $\mathbb{R}$.
8. For $X = \mathbb{Z}$ the set $\{(m, n) \in \mathbb{Z} \times \mathbb{Z} : m - n \text{ is divisible by 3}\}$ is a binary relation on $\mathbb{Z}$. We denote this relation by $\equiv_3$. Thus for $m, n \in \mathbb{Z}$ we have $m \equiv_3 n$ if and only if $m - n$ is divisible by 3.
9. For $X = \mathbb{R}^2$ let $R$ be the set of all $(p, q) \in \mathbb{R}^2 \times \mathbb{R}^2$ such that the distance from $p$ to the origin is equal to the distance from $q$ to the origin. Then $R$ is a binary relation on $\mathbb{R}^2$.

Definition 1.4 (Properties of relations). Let $R$ be a binary relation on a set $X$.

1. The relation $R$ is called reflexive if for every $x \in X$ we have $xRx$.
2. The relation $R$ is called symmetric if for all $x, y \in X$ we have $xRy \iff yRx$.
3. The relation $R$ is called transitive if whenever $x, y, z \in X$ are such that $xRy$ and $yRz$ then $xRz$.
4. The relation $R$ is called anti-symmetric if whenever $x, y \in X$ are such that $xRy$ and $yRx$ then $x = y$.

Example 1.5. Using the relations given in Example 1.3 we have:

- The relation given in part (1) of Example 1.3 is symmetric, anti-symmetric and transitive; if $X$ is nonempty then this relation is not reflexive.
- The relation given in part (2) of Example 1.3 is reflexive, symmetric, and transitive.
- The relation given in part (3) of Example 1.3 is reflexive, symmetric, anti-symmetric and transitive.
• The relation given in part (5) of Example 1.3 is reflexive, anti-symmetric and transitive, but it is not symmetric.
• The relation given in part (6) of Example 1.3 is anti-symmetric and transitive, but it is not symmetric and not reflexive.
• The relation given in part (7) of Example 1.3 is reflexive, symmetric, and transitive but not anti-symmetric.
• The relation given in part (8) of Example 1.3 is reflexive, symmetric, and transitive but not anti-symmetric.
• The relation given in part (9) of Example 1.3 is reflexive, symmetric, and transitive but not anti-symmetric.

**Definition 1.6** (Equivalence relation). An *equivalence relation* on a set $X$ is a binary relation $R$ on $X$ such that $R$ is reflexive, symmetric and transitive.

**Example 1.7.** In Example 1.3, parts (2), (3), (7), (8), (9) give equivalence relation and relations given in parts (5), (6) are not equivalence relations. The relation in part (1) is not an equivalence relation when $X$ is a nonempty set and it is an equivalence relation when $X$ is the empty set. The relation in part (4) is an equivalence relation if and only if $f : X \to X$ is the identity map.

2. Equivalence classes

**Definition 2.1** (Equivalence classes and the quotient set). Let $\sim$ be an equivalence relation on $X$. For $x \in X$ we put
\[
[x]_\sim := \{ y \in X : x \sim y \}
\]
and call $[x]_\sim$ the *equivalence class of $x$ with respect to $\sim$* or the $\sim$-equivalence class of $x$. Sometimes, for brevity, we will also denote $[x]_\sim$ by just $[x]$.

We put $X/\sim := \{ [x]_\sim : x \in X \}$ and call $X/\sim$ the *quotient set of $X$ by $\sim$*.

**Proposition 2.2.** Let $\sim$ be an equivalence relation on $X$. Then
\begin{enumerate}
  
  \item If $x, y \in X$ are such that $x \sim y$ then $[x]_\sim = [y]_\sim$.
  \item If $x, y \in X$ are such that $x \not\sim y$ then $[x]_\sim \cap [y]_\sim = \emptyset$.
  \item For any $x \in X$ we have $x \in [x]_\sim$.
\end{enumerate}

**Example 2.3.** In Example 1.3 we have:
\begin{itemize}
  
  \item For the equivalence relation $R = X \times X$ given in part (2), for every $x \in X$ we have $[x] = X$ and $X/R = \{X\}$.
  
  \item For the equivalence relation $R = \text{diag}(X)$ given in part (3), for every $x \in X$ we have $[x] = \{x\}$ and $X/R = \{\{x\} : x \in X\}$.
  
  \item For the equivalence relation $R$ on $X = \mathbb{R}$ given in part (7), for every $x \in \mathbb{R}$ we have $[x] = \{x + n : n \in \mathbb{Z}\}$.
  
  \item For the equivalence relation $\equiv_3$ on $\mathbb{Z}$ given by part (8), for any $m \in \mathbb{Z}$ the equivalence class $[m]$ consists of all $n \in \mathbb{Z}$ such that $n$ has the same remainder mod 3 as $m$. Thus, for example, $[1] = \{1 + 3k : k \in \mathbb{Z}\} = \{\ldots, -8, -5, -2, 1, 4, 7, 10, 13, 16, \ldots\}$. There are exactly 3 distinct equivalence classes, $[0], [1]$ and $[2]$ and $\mathbb{Z}/\equiv_3 = \{[0], [1][2]\}$.
  
  \item For the equivalence relation $R$ on $\mathbb{R}^2$ given by part (9), the equivalence class of the origin $O = (0, 0) \in \mathbb{R}^2$ is $[O] = \{O\}$. For any $p \in \mathbb{R}^2, p \neq O$, the equivalence class $[p]$ of $p$ is the circle around the origin of radius equal to the distance from $p$ to $O$.
\end{itemize}
Definition 2.4 (Quotient map). Let \( X \neq \emptyset \) be a set and let \(~\) be an equivalence relation on \( X \). We define the quotient map \( \pi : X \to X/\sim \) by the formula \( \pi(x) := [x] \) for \( x \in X \).

It is easy to see that if \(~\) is an equivalence relation on \( X \) then the quotient map \( \pi : X \to X/\sim \) is surjective. Moreover, in some sense, every surjective map from one set to another arises in this way.

Definition 2.5 (Descent of functions). Let \(~\) be an equivalence relation on \( X \) and let \( \pi : X \to X/\sim \) be the quotient map.

If \( f : X \to Y \) is a function, we say that \( f \) descends or factors through to a function from \( X/\sim \to Y \) if there exists a function \( \bar{f} : X/\sim \to Y \) such that \( f = \bar{f} \circ \pi \).

Example 2.6. Consider the equivalence relation \( \equiv_3 \) on \( \mathbb{Z} \), defined in part (8) of Example 1.3, and denote \( \mathbb{Z}_3 := \mathbb{Z}/\equiv_3 \), the quotient set for this equivalence relation. Let \( \pi : \mathbb{Z} \to \mathbb{Z}_3 \) be the quotient map.

1. Verify that the function \( f : \mathbb{Z} \to \mathbb{Z}_3 \) given by \( f(n) = [5n + 1]_3 \), does descend to a function \( \bar{f} : \mathbb{Z}_3 \to \mathbb{Z}_3 \) and compute the function \( \bar{f} \).
2. Consider the function \( g : \mathbb{Z} \to \mathbb{Z} \) defined as \( g(n) = 1 \) for \( n \geq 0 \) and \( g(n) = -1 \) for \( n < 0 \). Verify that \( g \) does not descend to a function \( \bar{g} : \mathbb{Z}_3 \to \mathbb{Z} \).

Theorem 2.7. Let \(~\) be an equivalence relation on a set \( X \neq \emptyset \) and let \( f : X \to Y \) be a function. Then the following hold:

1. If \( f \) descends to a function \( \bar{f} : X/\sim \to Y \) then this function \( \bar{f} \) is unique. That is, if \( f \) descends to functions \( h,h' : X/\sim \to Y \) then \( h = h' \).
2. The function \( f \) descends to a function from \( X/\sim \to Y \) if and only if \( f \) is constant on each \( \sim \)-equivalence in \( f \), that is, if and only if for any \( x,x' \in X \) with \( x \sim x' \) we have \( f(x) = f(x') \).

Theorem 2.8 (First Isomorphism Theorem for sets). Let \( X,Y \) be nonempty set and let \( f : X \to Y \) be a surjective map.

Define a relation \(~\) on \( X \) as \( x \sim x' \) if and only if \( f(x) = f(x') \), where \( x,x' \in X \). Then

1. \(~\) is an equivalence relation on \( X \).
2. The function \( f \) descends to a bijection \( \bar{f} : X/\sim \to Y \), given by

\[
\bar{f}([x]_\sim) := f(x)
\]

for \( x \in X \).

3. Integers \( \text{mod } m \)

Definition 3.1 (Integers mod \( m \)). Let \( m \geq 2 \) be an integer. We define a relation \( \equiv_m \) on \( \mathbb{Z} \) by setting

\[
\equiv_m := \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : a - b = mk \text{ for some } k \in \mathbb{Z}\}.
\]

Then one can check that \( \equiv_m \) is an equivalence relation on \( \mathbb{Z} \) with exactly \( m \) distinct equivalence classes

\[
\mathbb{Z}/\equiv_m = \{[0],[1],\ldots,[m-1]\}
\]

We denote \( \mathbb{Z}/\equiv_m \) by \( \mathbb{Z}_m \) or, sometimes, by \( \mathbb{Z}/m\mathbb{Z} \). The elements of \( \mathbb{Z}_m \) are called congruence classes \( \text{mod } m \).

Note that in the above situation for \( a,b \in \mathbb{Z} \) we have \( a \equiv_m b \) if and only if \( a \) and \( b \) have the same remainder when divided with the remainder by \( m \). If we want to
explicitly indicate the value of $m$, for $a \in \mathbb{Z}$ we will also denote the $\equiv_m$-class of $a$ by $[a]_m$.

**Notation 3.2.** Let $m \geq 2$ be an integer.

For $a, b \in \mathbb{Z}$ we write

\[ a = b \pmod{m} \]

if $a \equiv_m b$ and we write

\[ a \not\equiv b \pmod{m} \]

if $a \not\equiv_m b$.

**Theorem 3.3** (Addition and multiplication on $\mathbb{Z}_m$). Let $m \geq 2$ be an integer. For $a, b \in \mathbb{Z}$ put $[a]_m + [b]_m := [a + b]_m$ and $[a]_m \cdot [b]_m := [ab]_m$.

Then this produces well-defined binary operations $+$ and $\cdot$ on $\mathbb{Z}_m$.

**Proof.** Note that there is, in fact, something to check here.

Thus suppose $[a]_m = [a_1]_m$ and $[b]_m = [b_1]_m$. We need to verify that in this case $[a + b]_m = [a_1 + b_1]_m$ and $[ab]_m = [a_1 b_1]_m$. We will check the latter and leave the former as an exercise.

Since $[a]_m = [a_1]_m$ and $[b]_m = [b_1]_m$, we have $a_1 = a + km$ and $b_1 = b + qm$ for some $k, m \in \mathbb{Z}$. Then

\[ a_1 b_1 - ab = (a + km)(b + qm) - ab = kmb + aqm = (kb + aq)m \]

is divisible by $m$ and hence $[a_1 b_1]_m = [ab]_m$, as required.

\[ \square \]

4. **Polynomials mod $h$**

Let $h(x) \in \mathbb{R}[x]$. We define a relation $\equiv_h$ on $\mathbb{R}[x]$ by setting

\[ \equiv_h := \{ (f, g) \in \mathbb{R}[x] \times \mathbb{R}[x] : \text{there exists } q \in \mathbb{R}[x] \text{ such that } f - g = qh \} \]

**Proposition 4.1.** For any $h(x) \in \mathbb{R}[x]$, the relation $\equiv_h$ is an equivalence relation on $\mathbb{R}[x]$.

**Proof.** For any $f \in \mathbb{R}[x]$ we have $f - f = 0 = 0 \cdot h$, so that $f \equiv_h f$. Thus $\equiv_h$ is reflexive.

Suppose $f, g \in \mathbb{R}[x]$ are such that $f \equiv_h g$. Thus $f - g = qh$ for some $q \in \mathbb{R}[x]$. Hence $g - f = (-q)h$ and so $g \equiv_h f$. Thus $\equiv_h$ is symmetric.

Now suppose $f, g, p \in \mathbb{R}[x]$ are such that $f \equiv_h g$ and $g \equiv_h p$. Thus there exist $q, w \in \mathbb{R}[x]$ such that $g - f = qh$ and $p - g = wh$. Then

\[ p - f = p - g + g - f = wh + qh = (w + q)h \]

so that $p \equiv_h f$. Thus $\equiv_h$ is transitive, as required.

We have checked that $\equiv_h$ is reflexive, symmetric and transitive, and hence it is an equivalence relation on $\mathbb{R}[x]$.

\[ \square \]

For $h \in \mathbb{R}[x]$ we denote the quotient set $\mathbb{R}[x]/\equiv_h$ by $\mathbb{R}[x]/(h)$. For $f \in \mathbb{R}[x]$ we will sometimes denote the $\equiv_h$-equivalence class of $f$ by $[f]_h$.

Exactly the same argument as in the proof of Theorem 3.3 implies that the following holds:
Theorem 4.2. Let $h \in \mathbb{R}[x]$. For $f, g \in \mathbb{R}[x]$ put $[f]_h + [g]_h := [f + g]_h$ and $[f]_h \cdot [g]_h := [fg]_h$. Then this produces well-defined binary operations $+$ and $\cdot$ on $\mathbb{R}[x]/(h)$.

Example 4.3. Let $h = x^2 + 1 \in \mathbb{R}[x]$.
(1) Verify that in $\mathbb{R}[x]/(h)$ we have $[x]_h[x]_h + [1]_h = [0]_h$.
(2) Consider the function $\iota : \mathbb{R} \to \mathbb{R}[x]/(h)$ given by $\iota(a) = [a]_h$ for $a \in \mathbb{R}$. Is this function injective?
(3) Consider the map $u : \mathbb{C} \to \mathbb{R}[x]/(h)$ given by $u(a + ib) = [a + bx]_h$ where $a, b \in \mathbb{R}$. Is this map bijective?

5. Transversals

Definition 5.1 (Transversal). Let $\sim$ be an equivalence relation on a nonempty set $X$. A subset $T \subseteq X$ is called a transversal for $\sim$ if

1. For any $x, y \in T$ such that $x \neq y$ we have $x \not\sim y$; and
2. We have $X = \cup_{x \in T} [x]$.

In other words, a family $T$ of elements of $X$ is a transversal for $\sim$ if for every $x \in X$ there exists a unique $t \in T$ such that $x \sim t$.

Example 5.2.
- If $X$ is a nonempty set and $R = X \times X$ (as in part (2) of Example 1.3) then for any $x \in X$ the set $T = \{x\}$ is a transversal for $R$.
- If $X$ is a nonempty set and $R = \text{diag}(X)$ (as in part (3) of Example 1.3) then $T = X$ is a transversal for $R$.
- For the equivalence relation $\equiv_3$ on $\mathbb{Z}$, the sets $T_1 = \{0, 1, 2\}$ and $T_2 = \{-1, 3, 10\}$ are transversals.
- For the equivalence relation $R$ on $\mathbb{R}^2$ defined in part (9) of Example 1.3, any ray in $\mathbb{R}^2$ starting at the origin is a transversal. In particular, the set $\{(x, 0) : x \geq 0\}$ is a transversal for $R$.

Proposition 5.3. Let $\sim$ be an equivalence relation on a nonempty set $X$, and let $T \subseteq X$ is a transversal for $\sim$. Then there is a natural bijection $T \to X/\sim$ given by $t \mapsto [t]_\sim$, where $t \in T$.

The following fact is intuitively obvious but its formal proof requires a nontrivial tool from set theory called the “Axiom of Choice”:

Theorem 5.4. Let $X$ be a nonempty set, and let $\sim$ be an equivalence relation on $X$. Then there exists a transversal $T \subseteq X$ for $\sim$.

6. Partitions

Let $X$ be a set. Recall that $P(X)$ denotes the power set of $X$, that is $P(X) = \{Y \subseteq X\}$.

A partition of a nonempty set $X$ is a subset $\mathcal{Y} \subseteq P(X)$ such that the following conditions hold:

- Each $Y \in \mathcal{Y}$ is a nonempty subset of $X$.
- If $Y_1, Y_2 \in \mathcal{Y}$ are such that $Y_1 \neq Y_2$ then $Y_1 \cap Y_2 = \emptyset$.
- We have $\cup_{Y \in \mathcal{Y}} Y = X$. 

Thus one can think of a partition of $X$ as a way of decomposing $X$ into a union of nonempty pairwise disjoint pieces or "tiles".

Proposition 2.2 implies that if $\sim$ is an equivalence relation on a nonempty set $X$, then the equivalence classes for $\sim$ give a partition of $X$:

**Proposition 6.1.** Let $\sim$ be an equivalence relation on a nonempty set $X$. Then

$$X/\sim = \{[x]_\sim | x \in X\}$$

is a partition of $X$.

It turns out that a converse to the above statement also holds:

**Proposition 6.2.** Let $X \neq \emptyset$ and let $(Y_j)_{j \in J}$ be a partition of $X$. Then there exists a unique equivalence relation $\sim$ on $X$ such that $X/\sim = \{Y_j | j \in J\}$.

**Proof.** Define a binary relation $\sim$ on $X$ as follows. For $x, y \in X$ we say that $x \sim y$ if there is $j \in J$ such that $x, y \in Y_j$. It is not hard to check that $\sim$ is an equivalence relation and that for any $j \in Y_j$ and any $x \in Y_j$ we have $[x] = Y_j$, so that $X/\sim = \{Y_j | j \in J\}$. \qed