1 The Well-Ordering Principle, Induction, and Equivalence Relations

The set of natural numbers is the set

\[ N = \{1, 2, 3, \ldots \} . \]

(Some authors also include the number 0 in the natural numbers, but number theorists usually do not.)

The set of integers is the set

\[ Z = \{0, 1, -1, 2, -2, 3, -3, \ldots \} . \]

1.1 The Well-Ordering Principle

Every non-empty subset of the set of natural numbers has a smallest member.

Another way to state this is:

If \( S \subseteq N \) and \( S \neq \emptyset \), then there exists a number \( m \in S \) such that \( m \leq n \) for all \( n \in S \).

1.1.1 Example

Let \( S = \{ n \in N \mid n^2 > 15 \} \). Explain why \( S \) must have a smallest member and find this smallest member.

**Solution** First note that \( S \subseteq N \) and that \( S \neq \emptyset \) (because, for example, \( 10 \in S \)). Therefore \( S \) must have a smallest member. It is easy to see that this smallest member is \( m = 4 \). In fact, \( S = \{4, 5, 6, \ldots \} \).

1.1.2 Example

Let \( S = \{ n \in N \mid n > e^{1000} \} \). Explain why \( S \) must have a smallest member.

**Solution** Clearly \( S \subseteq N \). Also, since \( 3^{1000} \in S \), we see that \( S \neq \emptyset \). Therefore \( S \) has a smallest member. It’s not easy to determine what this smallest member is though.
1.2 The General Well-Ordering Principle

A more general version of the Well-Ordering Principle is

Suppose that \( S \) is some non-empty subset of the integers (\( \mathbb{Z} \)) and suppose that there is some integer \( n_0 \) such that every member of \( S \) is greater than or equal to \( n_0 \). Then \( S \) has a smallest member.

1.2.1 Example

Let \( S = \{ n \in \mathbb{Z} \mid |n| < 63 \} \). Explain why \( S \) must have a smallest member.

Solution

First note that \( S \subseteq \mathbb{Z} \) and that \( S \neq \emptyset \) (because, for example, 0 \( \in S \)). Also, every member of \( S \) is greater than or equal to \( n_0 = -63 \), because \(|-64| = 64 \neq 63.3\), \(|-65| = 65 \neq 63.3\), etc. By the General Well-Ordering Principle, \( S \) must have a smallest member. It is in fact easy to see here that the smallest member of \( S \) is \(-63\). In fact, the set \( S \) is the set of all integers that lie between \(-63\) and \(63\) (including \(-63\) and \(63\)).

1.3 The Principle of Induction

1.3.1 The Principle of Induction Stated in Terms of Sets

If

1. \( S \subseteq \mathbb{N} \),
2. \( 1 \in S \), and
3. \( n \in S \) implies that \( n + 1 \in S \),
then \( S = \mathbb{N} \).

1.3.2 The Principle of Induction Stated in Terms of Propositions

If

1. For each \( n \in \mathbb{N} \), \( P(n) \) is a statement that can be judged to be either true or false,
2. \( P(1) \) is true, and
3. the truth of \( P(n) \) implies the truth of \( P(n + 1) \),
then \( P(n) \) is true for all \( n \in \mathbb{N} \).
1.3.3 Example

Use induction to prove that if \( n \) is any natural number, then \( n^5 - n \) is divisible by 5.

**Proof** For each \( n \in N \), let \( P(n) \) be the statement “\( n^5 - n \) is divisible by 5”.

Then \( P(1) \) is the statement “\( 1^5 - 1 = 0 \) and 0 is divisible by 5.

Now for some general \( n \), let us consider the statements

\[
P(n) : n^5 - n \text{ is divisible by 5}
\]

and

\[
P(n + 1) : (n + 1)^5 - (n + 1) \text{ is divisible by 5}.
\]

Since

\[
(n + 1)^5 - (n + 1) = n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1 - (n + 1)
\]

\[
= (n^5 - n) + (5n^4 + 10n^3 + 10n^2 + 5n)
\]

\[
= (n^5 - n) + 5\left(n^4 + 2n^3 + 2n^2 + n\right),
\]

we see that if \( P(n) \) is true then \( P(n + 1) \) must also be true.

We conclude that \( P(n) \) must be true for all \( n \in N \).

1.4 The Strong Principle of Induction

If \( n_0 \) is some integer and:

1. For each \( n \geq n_0 \), \( P(n) \) is a statement that can be judged to be either true or false,

2. \( P(n_0) \) is true, and

3. the truth of \( P(x) \) for all \( x \) such that \( n_0 \leq x < n \) implies the truth of \( P(n) \),

then \( P(n) \) is true for all \( n \geq n_0 \).
1.4.1 Example

A *prime number* is a natural number that is greater than 1 and whose only positive divisors are itself and 1. (The first few prime numbers are 2, 3, 5, 7, 11, 13, 17.)

A *composite number* is a natural number that is greater than 1 and that is not prime. (The first few composite numbers are 4, 6, 8, 9, 10, 12, 14, 15, 16.)

(Note that the number 1 is the only natural number that is neither prime nor composite. Every other natural number is either prime or composite.)

Use the Strong Principle of Induction to prove that every natural number greater than 1 is either a prime number or is a product of prime numbers.

**Proof**  We want to prove that the statement

\[ P(n) : n \text{ is either a prime number or is a product of prime numbers} \]

is true for all \( n \geq 2 \).

First we observe that \( P(2) \) is certainly true because 2 is a prime number.

Also, given some \( n > 2 \) and supposing that \( P(x) \) is true for all \( x \) such that \( 2 \leq x < n \), can we conclude that \( P(n) \) must also be true? If \( n \) is a prime number, then \( P(n) \) is certainly true. If \( n \) is a composite number, then \( n \) has some divisor other than itself and 1 which means that \( n = st \) where \( s \) and \( t \) are natural numbers that are both greater than 1 and both less than \( n \). Due to our supposition that \( P(x) \) is true for all \( x \) such that \( 2 \leq x < n \), we see that \( P(s) \) and \( P(t) \) must both be true, meaning that both \( s \) and \( t \) must either be prime numbers or products of prime numbers. It follows that \( n \) must be a product of prime numbers (since \( n = st \)).

We have used the Strong Principle of Induction to prove that every natural number greater than 1 is either a prime number or is a product of prime numbers.

1.5 Remark

The Well–Ordering Principle, The Principle of Induction, and The Strong Principle of Induction are all *logically equivalent* to each other. This means that any one of these principles can be logically deduced from any other. We will not prove the logical equivalence of these principles in this course.
1.6 Relations

If $A$ is any non–empty set, then $A \times A$ is defined to be the set of all ordered pairs of elements of $A$. In other words,

$$A \times A = \{(x, y) \mid x \in A \text{ and } y \in A\}.$$  

For example, if $A = \{-3, 2, 6\}$, then

$$A \times A = \{(-3, -3), (-3, 2), (-3, 6), (2, -3), (2, 2), (2, 6), (6, -3), (6, 2), (6, 6)\}.$$

A relation, $R$, on a set $A$ is a subset of $A \times A$. If $(x, y) \in R$, then we say that “$x$ is related to $y$”.

1.6.1 Example

For the set $A = \{-3, 2, 6\}$, we can define the following relation $R$:

$$R = \{(-3, 2), (-3, 6), (2, 6), (6, -3), (6, 6)\}.$$  

For this relation, note that $-3$ is related to $6$ and $6$ is related to $-3$. Also $-3$ is related to $2$, but $2$ is not related to $-3$.

1.7 Equivalence Relations

A relation, $R$, on a set $A$ is said to be an equivalence relation if

1. $R$ is reflexive – meaning that $(x, x) \in R$ for all $x \in A$,

2. $R$ is symmetric – meaning that if $(x, y) \in R$, then $(y, x) \in R$, and

3. $R$ is transitive – meaning that if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$.

1.7.1 Example

For the set $A = \{-3, 2, 6\}$, the relation

$$R = \{(-3, 2), (-3, 6), (2, 6), (6, -3), (6, 6)\}$$

is not an equivalence relation. In fact $R$ satisfies none of the criteria of an equivalence relation!
1. $R$ is not reflexive because $(-3, -3) \notin R$.

2. $R$ is not symmetric because $(-3, 2) \in R$ but $(2, -3) \notin R$.

3. $R$ is not transitive because $(6, -3) \in R$ and $(-3, 2) \in R$ but $(6, 2) \notin R$.

1.7.2 Example
For the set $A = \{-3, 2, 6\}$, the relation

$$R = \{(-3, -3), (3, 6), (2, 2), (6, -3), (6, 6)\}$$

is an equivalence relation.

1.7.3 Example
Let $Z$ be the set of all integers and let the relation $R$ be defined on $Z$ by

$$R = \{(x, y) \in Z \times Z \mid y - x \text{ is a multiple of } 5\}.$$ 

Show that $R$ is an equivalence relation on $Z$.

**Proof**

1. Let $x \in Z$. Then $x - x = 0$ which is a multiple of 5 ($0 = 0 \cdot 5$). Thus $(x, x) \in R$. This shows that $R$ is reflexive.

2. Suppose that $(x, y) \in R$. Then $y - x$ is a multiple of 5. This means that $y - x = 5t$ for some integer $t$. Now note that $x - y = -(y - x) = -5t = 5(-t)$. Since $-t$ is an integer, we see that $x - y$ is a multiple of 5. Therefore $(y, x) \in R$. This shows that $R$ is symmetric.

3. Suppose that $(x, y) \in R$ and $(y, z) \in R$. Then $y - x$ and $z - y$ are both multiples of 5. This means that there are integers $s$ and $t$ such that $y - x = 5s$ and $z - y = 5t$. Since

$$z - x = (z - y) + (y - x) = 5t + 5s = 5(t + s)$$

and $t + s$ is an integer, we see that $z - x$ is a multiple of 5. Thus $(x, z) \in R$. This shows that $R$ is transitive.
1.8 Equivalence Classes

Suppose that \( R \) is a relation on a set \( A \) and suppose that \( x \) is an element of \( A \). The equivalence class of \( x \) is denoted by \([x]\) and is defined to be the set of all elements of \( A \) that are related to \( x \). In other words,

\[
[x] = \{ y \in A \mid (x, y) \in R \}.
\]

1.8.1 Example

For the set \( A = \{-3, 2, 6\} \) and the equivalence relation

\[
R = \{(-3, -3), (-3, 6), (2, 2), (6, -3), (6, 6)\},
\]

note that

\[
[-3] = \{-3, 6\} \\
[2] = \{2\} \\
[6] = \{-3, 6\}.
\]

Note that \([-3] = [6]\).

1.8.2 Example

For the equivalence relation, \( R \), defined on the set, \( Z \), of all integers by

\[
R = \{(x, y) \in Z \times Z \mid y - x \text{ is a multiple of } 5\},
\]

find the equivalence class of 2. In general, find the equivalence class of \( x \).

**Solution** Since

\[
[2] = \{ y \in Z \mid (2, y) \in R \}
\]

we see that

\[
[2] = \{ y \in Z \mid y - 2 \text{ is a multiple of } 5\}.
\]

To say that \( y - 2 \) is a multiple of 5 is to say that there exists some integer \( t \) such that \( y - 2 = 5t \). Thus every element, \( y \), of \( Z \) that is related to 2 must be a number of the form \( y = 2 + 5t \) where \( t \) is an integer. Therefore

\[
[2] = \{ y \in Z \mid y = 2 + 5t \text{ for some integer } t \}.
\]
We can also list the members of \([2]\) as follows:
\[ [2] = \{2, 7, 12, 17, 22, \ldots \} \cup \{-3, -8, -13, -18, -23, \ldots \}. \]

It is actually quite easy to visualize the equivalence class \([2]\) on the number line. To graph \([2]\) on the number line, we just mark 2 and then begin measuring distances of 5 to the left and to the right of 2 and mark these points as we measure.

It should not be easy to see that the equivalence class of any \(x\) is
\[ [x] = \{y \in \mathbb{Z} \mid y = x + 5t \text{ for some integer } t\}. \]

For example,
\[ [3] = \{3, 8, 13, 18, 23, \ldots \} \cup \{-2, -7, -12, -17, -22, \ldots \}. \]

Note that, in fact, \(R\) has only five distinct equivalence classes. They are
\[
\begin{align*}
[0] &= \{0, 5, 10, 15, 20, \ldots \} \cup \{-5, -10, -15, -20, -25, \ldots \} \\
[1] &= \{1, 6, 11, 16, 21, \ldots \} \cup \{-4, -9, -14, -19, -24, \ldots \} \\
[2] &= \{2, 7, 12, 17, 22, \ldots \} \cup \{-3, -8, -13, -18, -23, \ldots \} \\
[3] &= \{3, 8, 13, 18, 23, \ldots \} \cup \{-2, -7, -12, -17, -22, \ldots \} \\
[4] &= \{4, 9, 14, 19, 24, \ldots \} \cup \{-1, -6, -11, -16, -21, \ldots \}. \\
\end{align*}
\]

Any equivalence class, \([x]\), is equal to one of the above five. For example \([-4] = [1]\) and \([37] = [2]\).

### 1.9 Partitions of Sets

If \(A\) is some non-empty set, then a partition of \(A\) is a set, \(C\), of non-empty subsets of \(A\) such that each element of \(A\) belongs to exactly one of these subsets of \(A\).

#### 1.9.1 Example

There are five possible ways to partition the set \(A = \{-3, 2, 6\}\). They are
\[
\begin{align*}
C_1 &= \{-3, 2, 6\} & (\text{a partition consisting of one subset of } A \text{ which is } A \text{ itself}). \\
C_2 &= \{-3\}, \{2\}, \{6\} & (\text{a partition consisting of three subsets of } A - \text{ all singleton sets}). \\
C_3 &= \{-3\}, \{2, 6\} & (\text{a partition consisting of two subsets of } A). \\
C_4 &= \{2\}, \{-3, 6\} & (\text{a partition consisting of two subsets of } A). \\
C_5 &= \{6\}, \{-3, 2\} & (\text{a partition consisting of two subsets of } A). \\
\end{align*}
\]
1.9.2 Example

There are infinitely many ways to partition the set of integers

\[ \mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\} . \]

One possible way that might come immediately to mind, using three subsets of \( \mathbb{Z} \) is

\[ C = \{\{0\}, \{1, 2, 3, \ldots\}, \{-1, -2, -3, \ldots\}\} . \]

Referring back to the example in which we considered the relation

\[ R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid y - x \text{ is a multiple of } 5\} , \]

which is an equivalence relation on \( \mathbb{Z} \), we observe that

\[ C = \{[0], [1], [2], [3], [4]\} \]

is also a partition of \( \mathbb{Z} \).

The following two theorems summarize the connection between equivalence relations and partitions.

1.10 Theorem: Equivalence Relations Give Rise to Partitions

If \( A \) is a non–empty set and \( R \) is an equivalence relation on \( A \), then the set of equivalence classes of elements of \( A \) form a partition of \( A \).

1.10.1 Proof

Let \( C \) be the set of equivalence classes of \( A \). That is, let

\[ C = \{[x] \mid x \in A\} . \]

In order to prove that \( C \) is a partition of \( A \), we must prove that each member of \( A \) belongs to exactly one of the subsets of \( A \) that comprise \( C \).

First, we observe that for any \( x \in A \), it must be true that \( x \in [x] \) because \( (x,x) \in R \) (due to the reflexivity of \( R \)). This shows that every member of \( A \) belongs to at least one of the subsets of \( A \) that comprise \( C \).

We will now show that it is not possible that some member, \( x \), of \( A \) belongs to more than one of the subsets of \( A \) that comprise \( C \). To do this, we will show that if \( x \in [y] \), then it must be the case that \( [y] = [x] \).
Suppose that \( x \in [y] \). Then \( x \) and \( y \) are related to each other, meaning that \( (x, y) \in R \) and \( (y, x) \in R \). We want to show that this implies that \([y] = [x]\). To do this, we must show that every member of \([y]\) is a member of \([x]\) and that every member of \([x]\) is a member of \([y]\) (in other words, we must show that \([y] \subseteq [x]\) and that \([x] \subseteq [y]\)). To this end, let \( t \in [y]\). Then, since \((t, y) \in R\) and \((y, x) \in R\) and \(R\) is transitive, it must be the case that \((t, x) \in R\). Hence \( t \in [x]\), and we have shown that \([y] \subseteq [x]\). The proof that \([x] \subseteq [y]\) is similar.

This completes the proof that \( C = \{[x] \mid x \in A\} \) is a partition of \( A \).

1.11 Theorem: Partitions Give Rise to Equivalence Relations

If \( A \) is a non–empty set and \( C \) is a partition of \( A \), then

\[
R = \{(x, y) \mid x \text{ and } y \text{ belong to the same member of } C\}
\]

is an equivalence relation on \( A \).

1.11.1 Proof

1. First we prove that \( R \) is reflexive: For any given \( x \in A \), since \( C \) is a partition of \( A \), it must be true that \( x \) belongs to exactly one of the members of \( C \). Thus \((x, x) \in R\). This shows that \( R \) is reflexive.

2. Next we prove that \( R \) is symmetric: If \((x, y) \in R\), then \( x \) and \( y \) belong to the same member of \( C \). However, it is obviously equivalent to say that \( y \) and \( x \) belong to the same member of \( C \). Thus \((y, x) \in R\). This proves that \( R \) is symmetric.

3. Finally we prove that \( R \) is transitive: If \((x, y) \in R\) and \((y, z) \in R\), then \( x \) and \( y \) belong to the same member of \( C \) and \( y \) and \( z \) belong to the same member of \( C \). However, since \( y \) can belong to only one member of \( C \) (because \( C \) is a partition), it must be the case then that \( x \) and \( z \) belong to this same member of \( C \). Thus \((x, z) \in R\).

We have shown that \( R \) is an equivalence relation on \( A \).
1.12 Homework

In the textbook, Chapter 1, Section 1 (page 7) - do exercises 1–5 and exercise 7. (These are mostly exercises involving induction.)

In addition, do the following exercises:

1.13 Exercises

1. Use the Well-Ordering Principle to explain why the set
   \[ S = \{37 + 5x \mid x \in \mathbb{Z} \text{ and } 37 + 5x > 0\} \]
   must have a smallest member. Find this smallest member.

2. Explain why the set
   \[ S = \{37 + 5x \mid x \in \mathbb{R} \text{ and } 37 + 5x > 0\} \]
   (where \( \mathbb{R} \) denotes the set of all real numbers) does not have a smallest member.

3. Use the Well-Ordering Principle to explain why the set
   \[ S = \{4x + 8y \mid x \in \mathbb{Z}, y \in \mathbb{Z}, \text{ and } 4x + 8y > 0\} \]
   has a smallest member. Try, by experimentation, to find this smallest member.

4. Use the Well-Ordering Principle to explain why the set
   \[ S = \{5x + 9y \mid x \in \mathbb{Z}, y \in \mathbb{Z}, \text{ and } 5x + 9y > 0\} \]
   has a smallest member. Try, by experimentation, to find this smallest member.

5. Prove by induction that if \( n \) is any natural number, then
   \[ 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n + 1)(2n + 1)}{6} . \]
   This formula, which you may remember from Calculus, can also be written using summation notation as
   \[ \sum_{k=1}^{n} k^2 = \frac{n(n + 1)(2n + 1)}{6} . \]
6. Use induction to prove that if $n$ is any natural number, then the number $n^3 - n$ is divisible by 3.

7. Let $Z$ be the set of all integers and define the relation $R$ on $Z$ by

$$ R = \{ (x, y) \mid y = x \}.$$

(Another way to describe this relation is $R = \{ (x, x) \mid x \in Z \}$.)

Is $R$ an equivalence relation? If so, then prove it. If not, then explain why not.

8. (Thinking back to Calculus). Let $X$ be the set of all differentiable functions $f : (-\infty, \infty) \to (-\infty, \infty)$ and define the relation $R$ on $X$ by

$$ R = \{ (f, g) \mid f'(x) = g'(x) \text{ for all } x \in (-\infty, \infty) \}.$$

In other words, we are defining two functions to be related to each other if the two functions have the same derivative.

Prove that $R$ is an equivalence relation. Also, give an example of two different functions, $f$ and $g$, that are related to each other via $R$.

9. (Another Calculus One). Let $X$ be the set of all continuous functions $f : [0, 1] \to [0, 1]$ and define the relation $R$ on $X$ by

$$ R = \left\{ (f, g) \mid \int_0^1 f(x) \, dx = \int_0^1 g(x) \, dx \right\}.$$

Prove that $R$ is an equivalence relation. Also, give an example of two different functions, $f$ and $g$, that are related to each other via $R$.

10. Let $A$ be the set

$$ A = \{ 2, 3, 4, 5, \ldots \}.$$

($A$ contains all natural numbers except 1.)

Let $C$ be the set of subsets of $A$

$$ C = \{ C_2, C_3, C_4, C_5, \ldots \}.$$
where

\[ C_2 \text{ is the set of all positive multiples of } 2 \]
\[ C_3 \text{ is the set of all positive multiples of } 3 \]
\[ C_4 \text{ is the set of all positive multiples of } 4 \]
\[ \vdots \]
\[ \text{etc.} \]

Is \( C \) a partition of \( A \)? Explain why or why not.

11. Let \( R = (-\infty, \infty) \) be the set of real numbers and let \( C \) be the set of subsets of \( R \)
\[ C = \{ Q, Q^\# \} \]
where \( Q \) is the set of rational numbers and \( Q^\# \) is the set of irrational numbers.

Is \( C \) a partition of \( A \)? Explain why or why not.

12. Let \( Z \) be the set of all integers and let the relation \( R \) be defined on \( Z \) by
\[ R = \{(x, y) \in Z \times Z \mid y - x \text{ is a multiple of } 4\} . \]

(a) Show that \( R \) is an equivalence relation on \( Z \).
(b) Find the equivalence classes of 0, 1, 2, and 3.
(c) Explain why there are no other distinct equivalence classes of \( R \) other than the ones that you found in part b. (Give some examples such as “\([-31] = [?]\)” and “\([14] = [?]\)”.)

13. How many different possible equivalence relations can be defined on the set \( A = \{1, 2\} \)?

14. How many different possible equivalence relations can be defined on the set \( A = \{1, 2, 3, 4\} \)? Hint: Recall that each equivalence relation on a set corresponds to a partition of the set.

15. Explain why if \( A \) is any non-empty set, \( A \times A \) is an equivalence relation on \( A \).