

MA132/138: FOUNDATIONS/SETS AND NUMBERS, SHARED LECTURE NOTES

SAUL SCHLEIMER

Here we discuss some of the foundational material that will be assumed in many other mathematics modules at Warwick. All exercises in these notes have solutions (in Appendix A). There is also a short glossary (Appendix B), an index of notation, and a list of references.

While the material is old, its presentation here is new. In particular these lecture notes have not been previously used. So, please inform me via the anonymous form (<https://forms.gle/wAsUQUMo79BKubHk6>) or via an email (s.schleimer@warwick.ac.uk) of any errors (or of possible improvements).

Acknowledgements. I thank the many teachers, colleagues, and students without whom this work would not exist. In particular: John W. Addison Jr. taught me logic and set theory before I knew what those were. His course introduced me to Halmos' book [6] which continues to be a valuable resource. Simon Thomas mentored me (and explained all of the tricky bits) the first time I taught logic and set theory. Oleg Kozlovski, Christopher Lazda, David Wood, and Robert Kropholler were/are my fellow-lecturers in MA132/138 in years previous and present; I thank them for their good humour, gentle corrections, and patience.

1. SETS AND SUBSETS

1.1. Sets. A *set* contains its *elements*. We do not give a more formal definition; instead we understand sets by their properties – that is, by the axioms they satisfy.

Notation 1.2. Suppose that X is a set. Then we may write X as a sequence of elements, preceded and succeeded by curly braces. \diamond

Notation 1.3. We take \mathbb{N} to be the set of natural numbers (including zero). Then we may write

$$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$$

This is pronounced as “the natural numbers equals the set of zero, one, two, three, four, and so on.” The three dots (an *ellipsis*) indicate that the sequence is to be completed in the “usual way”.¹ \diamond

Here we include zero as a natural number. Throughout these notes we will assume some knowledge of the order on \mathbb{N} as well as the arithmetic operations (addition, multiplication, and subtraction and division where defined) and their basic properties (commutativity, associativity, distributivity, and cancellativity).

As a simpler example of a set, suppose that X is the set containing exactly the natural numbers 0, 1, and 2. Then we may write

$$X = \{0, 1, 2\}$$

Notation 1.4. Suppose that X is a set. Suppose that x is an element of X . Then we may denote this by writing $x \in X$. Suppose that y is not an element of X . Then we may denote this by writing $y \notin X$. \diamond

For example, we have $0 \in \mathbb{N}$ while $1/2 \notin \mathbb{N}$. The former is pronounced as “zero is an element of the natural numbers” and the latter is pronounced “one-half is not an element of the natural numbers”. We now state our first axiom.

Axiom 1.5 (Extension). *Suppose that X and Y are sets. Suppose that for any $x \in X$ we have $x \in Y$. Suppose also that for any $y \in Y$ we have $y \in X$. Then $X = Y$.* \square

From this axiom we deduce the following equalities of sets.

$$\{0, 1, 2\} = \{0, 2, 1\} = \{1, 2, 0\} = \{0, 0, 0, 1, 2\}$$

That is: neither the order of the elements nor the number of times they appear within the braces effects the identity of the set. Thus a set is quite different from a *list*: that is, an ordered collection of elements, each of which may appear more than once. We give a more formal treatment of lists in Definition 4.18.

We finish this section by introducing a special set.

Definition 1.6. If X contains no elements then X is an *empty set*. \diamond

Exercise 1.7. Suppose that X and Y are empty sets. Prove that $X = Y$. \diamond

Thus there is at most one empty set. To obtain at least one, we require another axiom.

Axiom 1.8 (Empty set). *There is an empty set, denoted \emptyset .* \square

¹There are various formal definitions of the natural numbers: for example see [6, page 44].

1.9. Subsets.

Definition 1.10. Suppose that X and Y are sets. Suppose that for any $x \in X$ we have $x \in Y$. Then we say that X is a *subset* of Y . We may denote this by writing $X \subset Y$.

If X is a subset of Y , and not equal to Y , then we say that X is a *proper subset* of Y . \diamond

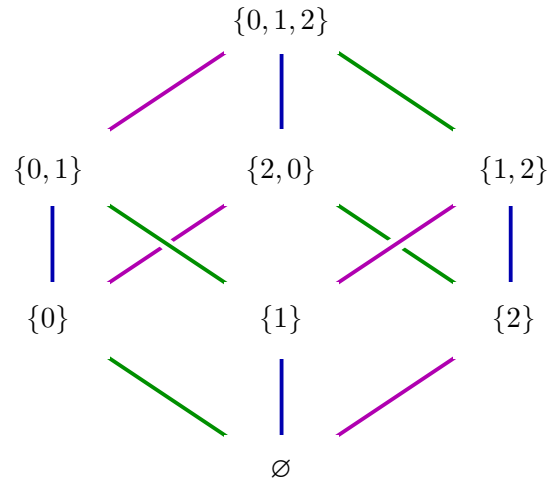


FIGURE 1.11. The subsets of $X = \llbracket 3 \rrbracket = \{0, 1, 2\}$. In this *Hasse diagram* we connect a subset A to a subset B by an ascending arc if $A \subset B$ and B has exactly one more element than A .

Exercise 1.12. Suppose that X is a set.

- (1) Prove that the empty set \emptyset is a subset of X .
- (2) Prove that X is a subset of X .

\diamond

Notation 1.13. For any natural number n , we define

$$\llbracket n \rrbracket = \{0, 1, 2, 3, \dots, n-1\} = \{k \in \mathbb{N} \mid k < n\}$$

That is, $\llbracket n \rrbracket$ is the subset of the natural numbers which are less than n . \diamond

For example, $\llbracket 0 \rrbracket$ is another name for the empty set. Also the set $X = \{0, 1, 2\}$ mentioned in Section 1.1 is equal to $\llbracket 3 \rrbracket$. We display all eight subsets of X in Figure 1.11.

Exercise 1.14. Sketch a proof that $\llbracket n \rrbracket$ has 2^n subsets. \diamond

Definition 1.15. Suppose that X is a set with exactly one element. Then we call X a *singleton* set. \diamond

For example, among the subsets of $\llbracket 3 \rrbracket$ there are exactly three singleton sets, namely $\{0\}$, $\{1\}$, and $\{2\}$.

We now state a useful lemma.

Lemma 1.16. *Suppose that X and Y are sets. Then the following are equivalent.*

- $X = Y$.
- $X \subset Y$ and $Y \subset X$.

Proof. Suppose that $X = Y$. By the second part of Exercise 1.12 we have $X \subset X$. Thus $X \subset Y$ and $Y \subset X$.

Suppose that $X \subset Y$ and $Y \subset X$. Then every element of X belongs to Y and every element of Y belongs to X . Thus $X = Y$ by the axiom of extension. \square

2. POWER SETS, SPECIFICATION, AND FUNCTIONS

2.1. Power sets. Exercise 1.14 leads us to the following.

Axiom 2.2 (Power set). *Suppose that X is a set. Then there exists a set whose elements are exactly the subsets of X .* \square

The set given by the axiom is called the *power set* of X . We may denote this set by $\mathcal{P}(X)$. Power sets grow frighteningly quickly. For example, by Exercise 1.14, the number of elements in $\mathcal{P}(\mathcal{P}(\llbracket n \rrbracket))$ is 2^{2^n} .

2.3. Specification. Recall that in Notation 1.13 we wrote

$$\llbracket n \rrbracket = \{k \in \mathbb{N} \mid k < n\}$$

and asserted that $\llbracket n \rrbracket$ is a set. To justify this, we need the following.

Axiom 2.4 (Specification). *Suppose that X is a set. Suppose that $S(x)$ is a property² which may or may not hold for elements of X . Then there is a subset $Y \subset X$ whose elements are exactly those elements x of X for which $S(x)$ holds.* \square

Note in the above the requirement to “specify” the containing set X .

Notation 2.5. Suppose that X is a set. Suppose that $S(x)$ is a property. Then we may write

$$\{x \in X \mid S(x)\}$$

to denote the subset given by Axiom 2.4. \diamond

²The precise definition of *property* belongs to a first course in set theory.

So, for example, in the notation $\llbracket 3 \rrbracket$ the containing set is \mathbb{N} and the property $S(k)$ is $(k < 3)$.

Remark 2.6. Building sets in this way is so common that we typically will not invoke the axiom of specification explicitly. \diamond

2.7. Functions. Here is our first, slightly informal, definition of *function*.

Definition 2.8. A *function* $f: X \rightarrow Y$ consists of the following.

- A set X , called the *domain*.
- A set Y , called the *codomain*.
- A *rule* f which, for every $x \in X$, gives an element $f(x) \in Y$. \diamond

We do not give a precise meaning to the word “rule”; in Definition 4.16 we give a more formal definition of functions. For two functions to be equal, they must have the same domains, codomains, and rules.

The notation $f: X \rightarrow Y$ is pronounced “ f is a function from X to Y ”. If $X = Y$ then we may say that “ f is a function on X ”.³

Here is the simplest kind of function.

Definition 2.9. Suppose that X is a set. The *identity function*

$$\text{Id}_X: X \rightarrow X$$

is defined by the rule $\text{Id}_X(x) = x$. \diamond

Non-identity functions are required to actually “do something”. One way to record this is as follows.

Definition 2.10. Suppose that X and Y are sets. Suppose that $f: X \rightarrow Y$ is a function. Suppose that $x \in X$ and $y \in Y$ are elements so that $y = f(x)$. Then we say that y is the *image* of x under f . \diamond

For the next example we take \mathbb{R} to be the set of real numbers and $\mathbb{R}_{\geq 0}$ to be the set of non-negative real numbers.

Example 2.11. Consider the following functions.

- (1) $f: \mathbb{R} \rightarrow \mathbb{R}$ where $f(x) = x^2$
- (2) $g: \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}$ where $g(x) = x^2$
- (3) $h: \mathbb{R} \rightarrow \mathbb{R}_{\geq 0}$ where $h(x) = x^2$
- (4) $k: \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ where $k(x) = x^2$

These functions have differing domains or codomains (or both). Thus all four functions are distinct. \diamond

The next example shows that the rule for a function need not be algebraic.

³Some authors instead say that $f: X \rightarrow X$ is a “function from X to itself”.

Lemma 2.12. *Suppose that $X = \{0, 1, 2\}$. Then there are 27 functions on X .*

Proof. Suppose that f is a function on X . Thus the domain and codomain are both equal to X . We can specify the rule for f by listing, in order, the elements $f(0)$, $f(1)$, and $f(2)$. There are three possibilities for each, and no other restrictions. Thus the number of possible rules is $3 \times 3 \times 3 = 27$. \square

Exercise 2.13.

- (1) Explicitly list all functions on $\llbracket 2 \rrbracket$.
- (2) For any $n \in \mathbb{N}$, count the number of functions on $\llbracket n \rrbracket$. Give a proof that your answer is correct in the style of Lemma 2.12. \diamond

3. TYPES OF FUNCTIONS, CARDINALITY AND COUNTING, CANTOR'S THEOREM AND RUSSELL'S PARADOX

3.1. Injections, surjections, bijections. For the next three definitions we suppose that X and Y are sets and that $f: X \rightarrow Y$ is a function.

Definition 3.2. Suppose that f has the following property:

- For every x and x' in X , if $f(x) = f(x')$ then $x = x'$.

Then we call f *injective*. \diamond

Definition 3.3. Suppose that f has the following property:

- For every y in Y , there is some x in X with $f(x) = y$.

Then we call f *surjective*. \diamond

Definition 3.4. Suppose that f is both injective and surjective. Then we call f *bijective*. \diamond

For example, the identity function Id_X is bijective. As shown by the next exercise, the status of a function – injective, surjective, both, or neither – depends not only on its rule but also on its domain and codomain.

Exercise 3.5. For each of the functions in Example 2.11, determine if it is injective, surjective, both, or neither. Give short justifications of your answers. \diamond

Definition 3.6. Suppose that $f: X \rightarrow X$ is bijective. Then we also call f a *permutation* of X . \diamond

Exercise 3.7. Suppose that n is a natural number. Count, with proof, the number of permutations of $\llbracket n \rrbracket$. \diamond

3.8. Cardinality. We have already done some counting in the exercises. We now give the formal terminology.

Definition 3.9. Suppose that X and Y are sets. Suppose that there is some bijection $f: X \rightarrow Y$. Then we say that X and Y have the same *cardinality*. When this happens we may write $|X| = |Y|$. \diamond

Definition 3.10. Suppose that X is a set. We say that X is *finite* if it has the same cardinality as $\llbracket n \rrbracket$ for some $n \in \mathbb{N}$. In this case we will write $|X| = n$ and say that X has cardinality equal to n . \diamond

In the above definition we asked only for the existence of *some* $n \in \mathbb{N}$ with $\llbracket n \rrbracket$ in bijection with X . This leaves open the possibility that there are many such natural numbers. However, using the pigeonhole principle (Corollary 17.11) we show that this does not happen; that is, when X is finite it has exactly one cardinality.

3.11. Cantor's theorem. We now state and prove our first theorem.

Theorem 3.12 (Cantor's theorem). *Suppose that X is a set. Suppose that $\mathcal{P}(X)$ is its power set. Suppose that $f: X \rightarrow \mathcal{P}(X)$ is a function. Then f is not a surjection.*

Proof. For a contradiction, suppose that f is a surjection. That is, for all $A \in \mathcal{P}(X)$ there is some $a \in X$ so that $f(a) = A$. We use f , and the axiom of specification, to build a subset of X . Define

$$B = \{x \in X \mid x \notin f(x)\}$$

That is, B is the subset of X consisting of those elements x which do not lie in the subset $f(x)$. Since f is surjective, there is some element of X , call it b , so that $f(b) = B$. There are now two possibilities⁴: either b is an element of B , or it is not.

Suppose that b is an element of B . Thus, by the defining property of B , we have that $b \notin f(b)$. Since $f(b) = B$, we deduce that $b \notin B$, a contradiction.

Suppose instead that $b \notin B$. Since $f(b) = B$ we deduce that $b \in f(b)$. Thus, by the defining property of B , we have that $b \in B$, another contradiction.

As both possibilities lead to contradiction, we deduce that our original assumption (the surjectivity of f) was incorrect. This completes the proof. \square

Exercise 3.13. Suppose that X is a set. Suppose that $\mathcal{P}(X)$ is its power set. Prove that there is no injection $g: \mathcal{P}(X) \rightarrow X$. \diamond

⁴Here we use the *law of the excluded middle*.

As a consequence of Theorem 3.12, we have that if X is a set, then there is no bijection from X to $\mathcal{P}(X)$. One often abbreviates Cantor's theorem by saying that, for each set X is “smaller than” its power set. This is an intuitive notion for finite sets, as $n < 2^n$ for all natural numbers. However sets which are not finite are more difficult to understand.

Definition 3.14. Suppose that X is a set. We say that X is *infinite* if it is not finite. That is, X does not have the same cardinality as any set $\llbracket n \rrbracket$, for any $n \in \mathbb{N}$. \diamond

For example, \mathbb{N} is infinite; this follows from the *pigeonhole principle*. See Exercise 17.10(3).

Remark 3.15. From Cantor's theorem we have that no set X is in bijection with its power set. This also applies when X is infinite. For example, \mathbb{N} is not in bijection with $\mathcal{P}(\mathbb{N})$. The latter power set is infinite; its singletons are in bijection with \mathbb{N} . However, Cantor tells us that $\mathcal{P}(\mathbb{N})$ is not in bijection with (and also does not inject into) \mathbb{N} . Thus $\mathcal{P}(\mathbb{N})$ is “larger” than \mathbb{N} . From this we deduce that there are “different sizes of infinities”. \diamond

3.16. Russell's paradox. This section is not examinable. The axiom of specification (Axiom 2.4) is sometimes called the axiom of “restricted comprehension”. This is because it was historically preceded by (what is now called) the axiom of “unrestricted comprehension”.

Axiom 3.17 (Unrestricted comprehension). *Suppose that $S(x)$ is a property. Then there is a set Y whose elements are exactly those x for which $S(x)$ holds.* \square

Unrestricted comprehension is much more powerful than specification; it eliminates the pesky requirement to “specify” the containing set X in advance. It therefore allows us to make many more sets. In fact, too many.

Theorem 3.18 (Russell's paradox). *The axiom of unrestricted comprehension leads to contradiction.*

Proof. We consider the property $S(X)$ which states that X is not an element of itself. In symbols we have $S(X) = (X \notin X)$.

The axiom of unrestricted comprehension now gives us the set $R = \{X \mid X \notin X\}$. That is, R is the set of sets which do not contain themselves (as elements). Since R is itself a set, it either contains itself (as an element) or it does not.

Suppose that R contains itself as an element. Then, by the definition of R , we have that $S(R)$ holds. Thus $R \notin R$. Thus R does not contain itself as an element. This is a contradiction.

Suppose instead that R does not contain itself as an element. Then $S(R)$ holds. So by the definition of R it contains R as an element. This is also a contradiction, and completes the proof. \square

At the heart of both Cantor's theorem and Russell's paradox there is a kind of "self-reference" or "iteration". Such ideas appear usefully in various parts of mathematics.

4. ORDERED PAIRS, CARTESIAN PRODUCTS, GRAPHICAL RELATIONS, LISTS AND STRINGS

We now turn to the problem of giving a more formal definition of functions. Recall that the issue with Definition 2.8 was that the term “rule” was undefined.

4.1. Ordered pairs and cartesian products. We first discuss unordered pairs.

Axiom 4.2 (Pair). *Suppose that X and Y are sets. Then there is a set whose elements are exactly X and Y .* \square

This set is written as $\{X, Y\}$. We may call this the *unordered pair* of X and Y .

Definition 4.3. Suppose that X and Y are sets. Suppose that $x, x' \in X$ and $y, y' \in Y$ are elements. Then an *ordered pair* (x, y) contains x and y , in that order.⁵ Two ordered pairs (x, y) and (x', y') are equal if and only if $x = x'$ and $y = y'$. \diamond

If (x, y) is an ordered pair then we may call x its first *entry* and y its second *entry*.

Axiom 4.4 (Ordered pairs). *Suppose that X and Y are sets. Suppose that $x \in X$ and $y \in Y$. Then the ordered pair (x, y) exists.*⁶ \square

Remark 4.5. To obtain ordered triples, or quadruples, or higher, we could add further axioms. Or, we could define $(x, y, z) = ((x, y), z)$. Or, we could define $(x, y, z) = (x, (y, z))$.

We will not make a choice here. Instead we boldly assert that the choice of formalisation is not important. Hopefully our intuition will carry us through any difficulties. \diamond

Definition 4.6. Suppose that X and Y are sets. Then the collection of all ordered pairs with first entry from X and second from Y is

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}$$

⁵Informally, ordered pairs are identical to lists of length two. However, if we allowed this in our formal definitions, then we would have a circularity. Namely, lists are defined in terms of functions (Definition 4.18), functions are defined in terms of ordered pairs (Definition 4.16), and finally ordered pairs are lists.

At a basic level it seems that there are three kinds of definitional scheme: unfounded, circular, or by infinite regress. Mathematicians have a strong preference for unfounded definitions, which they dignify with the name “axiomatic”. Whether we can so avoid paradox remains to be seen.

⁶There are various constructions of ordered pairs as sets. Perhaps the most common is due to Kuratowski [1921]. He takes $(x, y) = \{\{x\}, \{x, y\}\}$. Note that this definition of ordered pair relies on Axiom 4.2.

and is called the *cartesian product* of X and Y . \diamond

Axiom 4.7. Suppose that X and Y are sets. Then the cartesian product $X \times Y$ is a set.⁷ \square

The notation $X \times Y$ is very similar to the multiplicative notation for numbers. Here is one justification of that similarity.

Exercise 4.8. Sketch a proof that $\llbracket m \rrbracket \times \llbracket n \rrbracket$ has cardinality $m \times n$. \diamond

There is a special case of the cartesian product when $X = Y$. Here we use the notation X^2 for $X \times X$. This notation is again justified by Exercise 4.8.

Remark 4.9. For example, addition and multiplication of natural numbers give functions from \mathbb{N}^2 to \mathbb{N} . \diamond

Exercise 4.10. Suppose that X is a set. Show that $X \times \emptyset = \emptyset \times X = \emptyset$. \diamond

4.11. Graphical relations and functions.

Definition 4.12. A *relation* R from X to Y consists of the following.

- A set X , called the *domain*.
- A set Y , called the *codomain*.
- A subset of $X \times Y$. \diamond

If $X = Y$ then we say that R is “a relation on X ”. If (x, y) is an element of R we may denote this by writing xRy .

The empty set is a subset of $X \times Y$; this gives the *empty relation*. Likewise $X \times Y$ is a subset of itself; this gives the *universal relation*. When $X = Y$ then the set

$$\{(x, y) \in X^2 \mid x = y\}$$

gives the *identity relation* on X . Here is a more interesting example.

Example 4.13. Taking $X = Y = \mathbb{R}$ we have $X \times Y = \mathbb{R}^2$. Then unit circle is

$$C = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$$

Since C is a subset of \mathbb{R}^2 it is also a relation on \mathbb{R} . \diamond

Definition 4.14. Suppose that X and Y are sets. A relation G from X to Y is *graphical* if for every $x \in X$ there is exactly one $y \in Y$ so that (x, y) lies in G . \diamond

⁷If we rely on the Kuratowski constructions of ordered pairs then the existence of $X \times Y$ follows from the axioms of union and power set.

If $X = Y = \mathbb{R}$ then $X \times Y = \mathbb{R}^2$ is the usual plane. In this case there is a pictorial interpretation of Definition 4.14; namely, a relation $G \subset \mathbb{R}^2$ on \mathbb{R} is graphical if and only if every vertical line in \mathbb{R}^2 meets G in exactly one point.

Example 4.15. For example, of the following relations

$$P = \{(x, y) \in \mathbb{R}^2 \mid x^2 = y\} \quad Q = \{(x, y) \in \mathbb{R}^2 \mid x = y^2\}$$

the first is graphical and the second is not. \diamond

Definition 4.16. A *function* $f: X \rightarrow Y$ is a relation G , from X to Y , which is graphical. If (x, y) lies in G then we may write $f(x) = y$. \diamond

Note that in this definition the function f again has a domain and a codomain (which it inherits from the underlying relation G).

As an example, the “upwards parabola” P of Example 4.15 gives the function $f: \mathbb{R} \rightarrow \mathbb{R}$ with underlying relation $\{(x, x^2) \mid x \in \mathbb{R}\}$. On the other hand the “sideways parabola” Q of Example 4.15 and the circle C of Example 4.13 are not graphical and so do not give functions.

4.17. Lists.

Definition 4.18. Suppose that \mathcal{A} is a set. Suppose that n is a natural number. A *list* L is a function $L: \llbracket n \rrbracket \rightarrow \mathcal{A}$. We call n the *length* of the list L . We also say that the elements of L are *taken from* \mathcal{A} . \diamond

Since lists are functions, two lists are equal if and only if they

- have the same length,
- have elements taken from the same set, and
- have the same elements in the same order.

Notation 4.19. Suppose that C is a list of length n taken from the set \mathcal{A} . Then we may write either $C = (a_k)_{k=0}^{n-1}$ or

$$C = (a_0, a_1, a_2, \dots, a_{n-1})$$

That is, we may write C as a sequence of elements of \mathcal{A} , preceded and succeeded by parentheses. \diamond

Accordingly, the following lists are all distinct.

$$(0, 1, 2) \quad (0, 2, 1) \quad (1, 2, 0) \quad (0, 0, 0, 1, 2)$$

The first three lists are distinguished by having different last elements. Also, the last list has length five while the others have length three.

Lists of real numbers are often called *vectors*. According to Definition 4.18, the length of a list is always some natural number. In other treatments “infinite” lists – that is, functions from \mathbb{N} – are allowed. These infinite lists are often called *sequences*.

4.20. Strings. Suppose that \mathcal{A} is a set, here called an *alphabet*. The elements of \mathcal{A} are called *letters* (or *characters*). A list $C = (a_i)$, consisting of letters from \mathcal{A} , is often called a *string* (or a *word*) over \mathcal{A} . When elements of the alphabet \mathcal{A} are represented by single symbols, then the representation of the string w may omit the parentheses, the commas, and the spaces. Since strings are lists, they have a length: that is, the number of letters in the word.

Definition 4.21. Over any alphabet \mathcal{A} there is a unique string $\epsilon_{\mathcal{A}}$ of length zero; this is called the *empty string*. \diamond

Definition 4.22. Suppose that $\mathcal{B} = \{0, 1\}$ is our alphabet. We call the elements of \mathcal{B} *bits*. Strings over \mathcal{B} are called *binary strings*. \diamond

As examples of binary strings we have $\epsilon_{\mathcal{B}}$ (of length zero), 00 (of length two), 0101010001 (of length ten), and so on.

Exercise 4.23.

- (1) Determine the number of binary strings of length five.
- (2) Determine the number of binary strings of length n .
- (3) Determine the number of binary strings of length n having exactly one bit which is 1.
- (4) Determine the number of binary strings of length n having exactly two bits which are 1. \diamond

5. NEW SETS FROM OLD

5.1. The mathematicians' "and" and "or". In informal mathematical proofs, we are somewhat free in our usage of natural language. For example if P and Q are sentences, then as usual we have that " P and Q " holds if and only if both P and Q hold.

However when writing proofs, even informally, in our use of the word "or" we will depart somewhat from natural language. We will assume that " P or Q " holds if and only if *at least* one of P and Q hold. In particular we do *not* require that exactly one of P and Q holds.

As an example consider the following sentences.

$$P = (0 < 1 \text{ as natural numbers}), \quad Q = (0 = 1 \text{ as natural numbers})$$

So P holds and Q does not. Thus " P and Q " does not hold while " P or Q " does hold. Also, both " P and P " and " P or P " hold while neither " Q and Q " nor " Q or Q " holds.

In the above (and everywhere in mathematics) we necessarily define and discuss our mathematical language in terms of natural language. Thus we have defined the mathematical "and" and "or" partly in terms

of their meanings in natural language. This is unavoidable; the feeling of circularity so produced also appears to be unavoidable.

5.2. Union.

Axiom 5.3. *Suppose that \mathbb{X} is a set whose elements are again sets. Then the collection of all elements of elements of \mathbb{X} forms a set.* \square

This set is denoted

$$\bigcup_{X \in \mathbb{X}} X = \{z \mid z \in X \text{ for some } X \in \mathbb{X}\}$$

and is called the *union* over \mathbb{X} . We will concentrate on a special case of Axiom 5.3.

Notation 5.4. Suppose that X and Y are sets. Then we may form the union of X and Y as

$$X \cup Y = \{z \mid z \in X \text{ or } z \in Y\}$$

To see that this is a set we form $\mathbb{X} = \{X, Y\}$ using the axiom of pairing. We then take the union over \mathbb{X} using the axiom of unions. \diamond

Example 5.5.

- (1) If m and n are natural numbers then $\llbracket m \rrbracket \cup \llbracket n \rrbracket = \llbracket \max(m, n) \rrbracket$.
- (2) Suppose that $X = \{0, 1, 2\}$ and $Y = \{1, 2, 3\}$. Then $X \cup Y = \{0, 1, 2, 3\}$. \diamond

Lemma 5.6. *Suppose that X and Y are sets. Then $X \subset X \cup Y$.*

Proof. To prove that $X \subset X \cup Y$ we must show that every element of X is an element of $X \cup Y$. So fix any element $x \in X$. Then x lies in X or it lies in Y . Thus x lies in $X \cup Y$. Since this holds for every x in X we are done. \square

The following lemma likewise depends on the close connection between the union operator and the word “or”.

Lemma 5.7. *Suppose that X , Y , and Z are sets. Then we have the following.*

- (1) $X \cup \emptyset = X$ (*identity*)
- (2) $(X \cup Y) \cup Z = X \cup (Y \cup Z)$ (*associativity*)
- (3) $X \cup Y = Y \cup X$ (*commutativity*)
- (4) $X \subset Y$ if and only if $X \cup Y = Y$ (*absorption*)
- (5) $X \cup X = X$ (*idempotent*)

Exercise 5.8. Provide the proof of Lemma 5.7 \diamond

5.9. Intersection.

Definition 5.10. Suppose that \mathbb{X} is a set whose elements are again sets. The *intersection* over \mathbb{X} is the collection

$$\bigcap_{X \in \mathbb{X}} X = \{x \mid x \in X \text{ for every } X \in \mathbb{X}\}$$

In the special case where $\mathbb{X} = \{X, Y\}$ we instead write

$$X \cap Y = \{z \mid z \in X \text{ and } z \in Y\}$$

for the *intersection* of X and Y . \diamond

We could not prove that unions are sets directly; instead we needed a new axiom. The situation for intersections is simpler, because intersections are smaller than unions.

Lemma 5.11. *Suppose that \mathbb{X} is a set whose elements are again sets. Then the intersection over \mathbb{X} is a set.*

Proof. Let $\mathcal{X} = \bigcup_{X \in \mathbb{X}} X$ be the union over \mathbb{X} . We define the property $S(x)$ as follows:

$$S(x) = (\text{for every } X \in \mathbb{X}, \text{ we have } x \in X)$$

Then the intersection over \mathbb{X} equals $\{x \in \mathcal{X} \mid S(x)\}$. This is a set by the axiom of specification. \square

Notation 5.12. Suppose that X and Y are sets. Then we may form the intersection of X and Y as

$$X \cap Y = \{z \mid z \in X \text{ and } z \in Y\}$$

To see that this is a set we form $\mathbb{X} = \{X, Y\}$ using the axiom of pairing. We then take the intersection over \mathbb{X} using Lemma 5.11.

If $X \cap Y = \emptyset$ then we say that X and Y are *disjoint*. \diamond

There is a formal symmetry between union and intersection that mirrors the informal symmetry between the words “or” and “and”. Because of this, the proofs of the following lemmas are modelled, extremely closely, on those of Lemmas 5.6 and 5.7. We leave their writing out to the reader.

Lemma 5.13. *Suppose that X and Y are sets. Then $X \cap Y \subset X$. \square*

Lemma 5.14. *Suppose that X , Y , and Z are sets. Then we have the following.*

- (1) $X \cap \emptyset = \emptyset$ (*annihilator*)
- (2) $(X \cap Y) \cap Z = X \cap (Y \cap Z)$ (*associativity*)
- (3) $X \cap Y = Y \cap X$ (*commutativity*)
- (4) $X \subset Y$ if and only if $X \cap Y = X$ (*absorption*)
- (5) $X \cap X = X$ (*idempotent*) \square

5.15. Set difference.

Definition 5.16. Suppose that X and Y are sets. The collection

$$X - Y = \{x \in X \mid x \notin Y\}$$

is called the *set-theoretic difference* of X and Y . \diamond

$X - Y$ is also called, in some sources, the “relative complement of Y in X ”.

Lemma 5.17. *Suppose that X and Y are sets. Then $X - Y$ is a set.*

Proof. This follows from the axiom of specification, using X as the set and

$$S(x) = (x \notin Y)$$

as the property. \square

The proof of the next lemma is immediate from the definitions.

Lemma 5.18. *Suppose that X is a set. Then we have the following.*

- (1) $X - \emptyset = X$
- (2) $\emptyset - X = \emptyset$
- (3) $X - X = \emptyset$.

In particular, if X is not empty, then we have $X - \emptyset \neq \emptyset - X$. Thus, as with subtraction of numbers, set-theoretic difference is not commutative.

5.19. The boolean algebra of sets. The operations of union, intersection, and set-theoretic difference are related to each other in various ways. Here we mention only some of the best known.

Lemma 5.20 (Distributive laws). *Suppose that X , Y , and Z are sets. Then we have the following.*

- $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
- $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$

Exercise 5.21. Provide the proof of Lemma 5.20. \diamond

Lemma 5.22 (De Morgan’s laws). *Suppose that X , Y , and Z are sets. Then we have the following.*

- $X - (Y \cup Z) = (X - Y) \cap (X - Z)$
- $X - (Y \cap Z) = (X - Y) \cup (X - Z)$

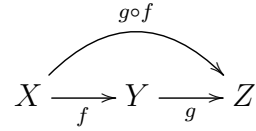
Exercise 5.23. Provide the proof of Lemma 5.22. \diamond

6. NEW FUNCTIONS FROM OLD

6.1. Composition.

Definition 6.2. Suppose that X , Y , and Z are sets. Suppose that $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are functions. Then we define the function $g \circ f: X \rightarrow Z$ by $(g \circ f)(x) = g(f(x))$. \diamond

The expression $g \circ f$ is pronounced as “ g composed with f ”. Here is a “diagram” representing the composition.



Lemma 6.3. [Composition is associative] Suppose that X , Y , Z , and W are sets. Suppose that $f: X \rightarrow Y$, $g: Y \rightarrow Z$, and $h: Z \rightarrow W$ are functions. Then we have

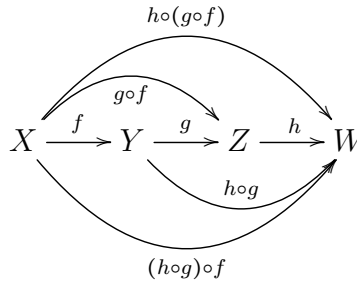
$$h \circ (g \circ f) = (h \circ g) \circ f$$

Proof. We note that $h \circ (g \circ f)$ and $(h \circ g) \circ f$ have the same domain (X) and codomain (W). Thus it only remains that they have the same rule. Suppose that x is any element of X . We compute as follows:

$$\begin{aligned} (h \circ (g \circ f))(x) &= h(g(f(x))) && \text{definition of } \circ \text{ twice} \\ &= ((h \circ g) \circ f)(x) && \text{definition of } \circ \text{ twice} \end{aligned}$$

Since this holds for all x in X , we deduce that $h \circ (g \circ f) = (h \circ g) \circ f$, as desired. \square

The above proof can be reproduced in a more diagrammatic form.



Definition 6.4. Suppose that X and Y are sets. Suppose that $f: X \rightarrow Y$ and $g: Y \rightarrow X$ are functions. If $g \circ f = \text{Id}_X$ then we say that g is a *left inverse* for f . Similarly we say that f is a *right inverse* for g .

If $g \circ f = \text{Id}_X$ and $f \circ g = \text{Id}_Y$ then we say that g is an *inverse* for f . \diamond

Lemma 6.5. *Suppose that X and Y are non-empty sets. Suppose that $f: X \rightarrow Y$ is a function. Then we have the following.*

- (1) *f is injective if and only if f has a left inverse.*
- (2) *f is surjective if and only if f has a right inverse.*
- (3) *f is bijective if and only if f has an inverse. In this case the inverse is unique.*

Proof. We prove the forward and backwards directions of the first statement. The rest are left as exercises.

Suppose that f is injective. Since X is non-empty, we can fix some x_0 in X . We now define $g: Y \rightarrow X$ as follows.

$$g(y) = \begin{cases} x, & \text{if } f(x) = y \\ x_0, & \text{if there is no } x \in X \text{ with } f(x) = y \end{cases}$$

Suppose now that x is any element of X . Set $y = f(x)$. We compute as follows:

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) && \text{definition of } \circ \\ &= g(y) && \text{definition of } y \\ &= x && \text{first line of definition of } g \\ &= \text{Id}_X(x) && \text{definition of } \text{Id}_X \end{aligned}$$

Since this holds for all x in X , we deduce that $g \circ f = \text{Id}_X$, as desired.

Suppose that g is a left inverse for f . Suppose that x and x' are any elements of X . Suppose that $f(x) = f(x')$. We now compute as follows:

$$\begin{aligned} x &= \text{Id}_X(x) && \text{definition of } \text{Id}_X \\ &= (g \circ f)(x) && g \text{ is a left inverse for } f \\ &= g(f(x)) && \text{definition of } \circ \\ &= g(f(x')) && \text{because } f(x) = f(x') \\ &= (g \circ f)(x') && \text{definition of } \circ \\ &= \text{Id}_X(x') && g \text{ is a left inverse for } f \\ &= x' && \text{definition of } \text{Id}_X \end{aligned}$$

Since this holds for all x and x' , we deduce that f is injective, as desired. \square

Exercise 6.6. Provide the rest of the proof of Lemma 6.5. \diamond

Lemma 6.7. *Suppose that X , Y , and Z are sets. Suppose that $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are functions. Then we have the following.*

- (1) *If f and g are injective then so is $g \circ f$.*

(2) If f and g are surjective then so is $g \circ f$.

Exercise 6.8. Provide the proof of Lemma 6.7. \diamond

6.9. Iteration and orbits. There is an important special case of function composition.

Definition 6.10. Suppose that X is a set. Suppose that $f: X \rightarrow X$ is a function. Then we define

- (1) $f^{(0)} = \text{Id}_X$ and
- (2) for any $n \in \mathbb{N}$ we define $f^{(n+1)} = f \circ f^{(n)}$.

We say that $f^{(n)}$ is the n^{th} iterate of f . \diamond

Definition 6.11. Suppose that X is a set. Suppose that $f: X \rightarrow X$ is a function. Suppose that $x \in X$ is an element. Then we define

$$\mathcal{O}_f(x) = \{f^{(n)}(x) \mid n \in \mathbb{N}\}$$

We say that $\mathcal{O}_f(x)$ is the *forward orbit* of x under f . \diamond

In Definition 6.11 we used a new notation for sets. Here are the formalities.

Definition 6.12. Suppose that X and Y are sets. Suppose that $f: X \rightarrow Y$ is a function. Suppose that $Z \subset X$ is a subset. Then we may write

$$f(Z) = \{f(z) \mid z \in Z\}$$

to denote the set

$$\{y \in Y \mid \text{there is some } x \in Z \text{ so that } f(x) = y\}$$

The set $f(Z)$ is called the *image* of Z under f . \diamond

To complement images we have the following.

Definition 6.13. Suppose that X and Y are sets. Suppose that $f: X \rightarrow Y$ is a function. Suppose that $W \subset Y$ is a subset. Then

$$f^{-1}(W) = \{x \in X \mid f(x) \in W\}$$

is the *preimage* of W under f . \diamond

6.14. Cantor–Schoerder–Bernstein.

Theorem 6.15. Suppose that X and Y are sets. Suppose that $f: X \rightarrow Y$ and $g: Y \rightarrow X$ are injections. Then there is a bijection $h: X \rightarrow Y$. \square

The proof, while elementary, is beyond the scope of this module. As a hint of the ideas involved, define $h = g \circ f$ and $k = f \circ g$. Both of these are injections by Lemma 6.7. We then divide each of X and Y into three pieces using the structure of orbits of h and of k . We then assemble these pieces to find the desired bijection $F: X \rightarrow Y$.

7. REFLEXIVE, SYMMETRIC, AND TRANSITIVE RELATIONS, EQUIVALENCE RELATIONS, ORDER RELATIONS

7.1. Reflexive, symmetric, and transitive relations.

Definition 7.2. Suppose that X is a set. Suppose that $R \subset X^2$ is a relation on X .

- Suppose that, for all $x \in X$, we have xRx . Then we say that R is *reflexive*.
- Suppose that, for all $x, y \in X$, we have that xRy implies yRx . Then we say that R is *symmetric*.
- Suppose that, for all $x, y, z \in X$, we have that xRy and yRz implies xRz . Then we say that R is *transitive*. \diamond

Example 7.3. All of the following are relations on \mathbb{N} .

- The identity relation is reflexive, symmetric, and transitive.
- The empty relation is symmetric and transitive, but not reflexive.
- The relation of less than or equal ($x \leq y$) is reflexive and transitive, but not symmetric.
- The relation ($|x - y| \leq 1$) is reflexive and symmetric, but not transitive.
- The relation ($x = y$ or $x + 1 = y$) is reflexive, but not symmetric or transitive.
- The relation of inequality ($x \neq y$) is symmetric but not reflexive or transitive.
- The relation of less than ($x < y$) is transitive, but not reflexive or symmetric.
- The relation ($x + 1 = y$) is not reflexive, symmetric, or transitive. \diamond

Exercise 7.4. For each of the following relations on \mathbb{N} determine if it is reflexive, symmetric, or transitive.

- (1) xPy if $x + y = 2$
- (2) xQy if $x - y \leq 2$
- (3) xRy if $|x - y| \leq 2$ \diamond

7.5. Equivalence relations.

Definition 7.6. Suppose that X is a set. A relation on X is an *equivalence relation* if it is reflexive, symmetric, and transitive. \diamond

Remark 7.7. This definition is modelled on the properties of equality. So one is tempted to call equality of sets an equivalence relation. However this is not the case, because the collection of all sets is not a set. \diamond

Here is a simple-sounding exercise that still gives a real feel for the nature of equivalence relations.

Exercise 7.8. Suppose that $X = \llbracket 4 \rrbracket$. List all equivalence relations on X . Verify that your list is *complete* (all equivalence relations appear) and *irredundant* (no equivalence relation appears twice). \diamond

The same exercise, but with $X = \llbracket 5 \rrbracket$, is even more challenging. We leave this to the reader, together with the hint to look at sequence A000110 at the Online Encyclopedia of Integer Sequences [9].

The difficulty of these enumerations suggest that we require a more efficient way to think about equivalence relations. This will be provided in Section 8.

7.9. Partial orders.

Definition 7.10. Suppose that X is a set. Suppose that R is a relation on X . Then R is *antisymmetric* if, for all x and y in X we have

- if xRy and yRx then $x = y$. \diamond

For example, the relation \leq on \mathbb{N} is antisymmetric.

Definition 7.11. Suppose that X is a set. Suppose that R is a relation on X . If R is reflexive, antisymmetric, and transitive, then R is a *partial order*. \diamond

The identity relation on X is one example. Another is the relation of \leq on \mathbb{N} . A third is the relation of divisibility on positive natural numbers. Here is an example which is closely related to that.

Example 7.12. Suppose that X is a set. Suppose that $\mathcal{P}(X)$ is the power set of X . The relation $P \subset Q$ on $\mathcal{P}(X)$ is reflexive and transitive by Definition 1.10. It is antisymmetric by Lemma 1.16. Thus it is a partial order. We may call the pair $(\mathcal{P}(X), \subset)$ the *boolean poset* on X . \diamond

The word “poset” stands for “partially ordered set”.

7.13. Total orders.

Definition 7.14. Suppose that X is a set. Suppose that R is a relation on X . We may say that R is a *total relation* if, for all x and y we have xRy or yRx . \diamond

Definition 7.15. Suppose that X is a set. Suppose that R is a relation on X . We may say that R is a *total order* if it is reflexive, antisymmetric, transitive, and total. \diamond

That is, a total order is a partial order which is, additionally, total. Examples of total orders include “less than or equal” on the natural numbers (as well as the integers, the rationals, and the reals).

8. PARTITIONS, EQUIVALENCE CLASSES, AND QUOTIENTS

We now begin to explain a much more convenient technique for dealing with equivalence relations.

8.1. Partitions.

Definition 8.2. Suppose that X is a set. Suppose that $\mathbb{P} \subset \mathcal{P}(X)$ has the following properties:

- If $P \in \mathbb{P}$ then P is non-empty.
- $X = \bigcup_{P \in \mathbb{P}} P$.
- If $P, Q \in \mathbb{P}$ then either $P = Q$ or $P \cap Q = \emptyset$.

Then we call \mathbb{P} a *partition* of X . The elements $P \in \mathbb{P}$ are called the *parts* of the partition. \diamond

Any non-empty set X has two special partitions. These are

- The partition into singletons: $\mathbb{I} = \{\{x\} \mid x \in X\}$.
- The partition with one part: $\mathbb{U} = \{X\}$.

Here are the five partitions of $\llbracket 3 \rrbracket$:

$$\{\{0\}, \{1\}, \{2\}\} \quad \{\{0, 1\}, \{2\}\} \quad \{\{0, 2\}, \{1\}\} \quad \{\{0\}, \{1, 2\}\} \quad \{\{0, 1, 2\}\}$$

The notation here, while correct, interferes with understanding. So we give the same information in a more efficient way.

$$0|1|2 \quad 01|2 \quad 02|1 \quad 0|12 \quad 012$$

Here we place a vertical bar “|” between parts. We list partitions with smaller parts before those with larger parts. As a consequence of this we list partitions with more parts before those with fewer parts. Since a part is a subset, inside a part we list its elements in terms of size. This is only for convenience; for example the partitions $01|23$ and $10|32$ of $\llbracket 4 \rrbracket$ are equal.

Exercise 8.3.

- (1) Count the number of partitions of the set $X = \llbracket 4 \rrbracket$.
- (2) Sketch a proof that the set $X = \llbracket n \rrbracket$ has at least $2^{n-1} - 1$ partitions.

\diamond

8.4. Equivalence classes.

Definition 8.5. Suppose that X is a set. Suppose that E is an equivalence relation on X . Suppose that x lies in X . We define the set

$$[x]_E = \{y \in X \mid xEy\}$$

to be the *equivalence class* of x . \diamond

We have two trivial examples. In the identity relation on X equivalence classes are singletons. In the universal relation on X there is only one equivalence class, namely X .

Exercise 8.6. Compute the equivalence classes for each of the equivalence relations you found in Exercise 7.8. \diamond

Exercise 8.7. Here is a slightly non-mathematical problem. Suppose that X is the set of living people. We define an equivalence relation B on X where $xB y$ if x and y are born in the same month. Count the number of equivalence classes for B . \diamond

Notation 8.8. Suppose that X is a set. Suppose that E is an equivalence relation on X . Then we may denote the set of equivalence classes by⁸

$$X/E = \{[x]_E \mid x \in X\}$$

We call X/E the *quotient* of X by E . We also write $q_E: X \rightarrow X/E$ for the function $q_E(x) = [x]_E$. We call q_E the *quotient map* given by E . \diamond

Lemma 8.9. Suppose that X is a set. Suppose that E is an equivalence relation on X . Then the quotient X/E is a partition of X .

Proof. We must verify that $\{[x]_E \mid x \in X\}$ is a partition of X .

Since E is reflexive we have that x lies in $[x]_E$. Thus $[x]_E$ is non-empty. Also, since this holds for all x we have that $X = \bigcup_{x \in X} [x]_E$.

Suppose that x and y lie in X . If $[x]_E$ is disjoint from $[y]_E$ then there is nothing left to show. So suppose that z lies in $[x]_E \cap [y]_E$. Thus xEz and yEz . By symmetry we have zEy . By transitivity we have xEy . Suppose now that w is any element in $[y]_E$. Thus yEw . Since xEy , by transitivity we have xEw . Thus $[y]_E \subset [x]_E$.

The same argument, swapping x and y throughout, proves that $[x]_E \subset [y]_E$. From Lemma 1.16 implies $[x]_E = [y]_E$, as desired. \square

⁸It is more correct here to write

$$X/E = \{P \in \mathcal{P}(X) \mid \text{there is some } x \in X \text{ so that } P = [x]_E\}$$

However the notation in 8.8 is much more common.

As a temporary piece of notation, we use $\Pi_X(E) = X/E$ to denote the function that takes equivalence relations on X to partitions of X . Lemma 8.9 can now be sharpened, as follows.

Corollary 8.10. *Suppose that X is a set. Then the function Π is a bijection.*

Proof. Suppose that \mathbb{P} is a partition of X . We define a relation $Q = Q_{\mathbb{P}}$ on X where xQy if x and y lie in the same part of \mathbb{P} . Note that Q is reflexive, symmetric, and transitive, so Q is an equivalence relation. This gives a function $\Sigma(\mathbb{P}) = Q_{\mathbb{P}}$ from partitions to equivalence relations.

Suppose that E is an equivalence relation. Then $Q = \Sigma(\Pi(E))$ is also equivalence relation. By construction Q and E have the same equivalence classes. Thus xEy if and only if xQy . Thus $E = Q$. It follows that Σ is a left inverse for Π .

Suppose that \mathbb{P} is a partition. Then $\mathbb{Q} = \Pi(\Sigma(\mathbb{P}))$ is also a partition. So the parts of \mathbb{Q} are the equivalence classes of $\Sigma(\mathbb{P})$. But these are, by construction, the parts of \mathbb{P} . So $\mathbb{P} = \mathbb{Q}$. It follows that Σ is a right inverse for Π . By Lemma 6.5 we have that Π is a bijection. \square

8.11. Integers. The construction of quotients is one of the jewels of modern mathematics: a natural way to construct new things out of old. Here we lay out our first example; it will not be the last.

Definition 8.12. Suppose that $X = \mathbb{N}^2$. We define a relation $E \subset X^2 = (\mathbb{N}^2 \times \mathbb{N}^2)$ by

$$(p, q)E(r, s) \quad \text{if and only if} \quad p + s = r + q$$

Here the additions make sense because p , q , r , and s are natural numbers. \diamond

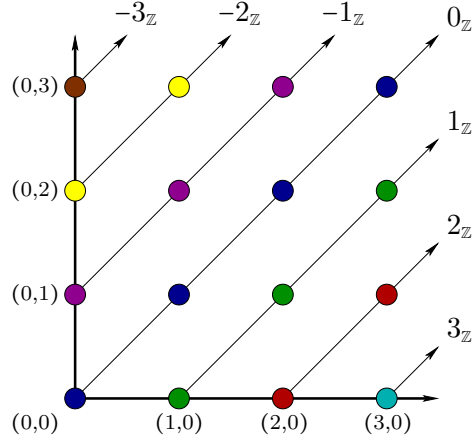
Exercise 8.13. Prove that E , as given by Definition 8.12, is an equivalence relation. \diamond

With Exercise 8.13 in hand we may explore the equivalence classes of E . Suppose that p lies in \mathbb{N} . Then we have

$$[(p, 0)]_E = \{(p + k, k) \in \mathbb{N}^2 \mid k \in \mathbb{N}\} \quad [(0, p)]_E = \{(k, p + k) \in \mathbb{N}^2 \mid k \in \mathbb{N}\}$$

To “see” this, we draw \mathbb{N}^2 as a quarter plane, with x - and y -axis being the first and second copies of \mathbb{N} . The points of the equivalence class $[(p, q)]_E$ lie along a line with slope one, running through (p, q) . See Figure 8.14.

Consulting Figure 8.14, we find that the elements of a fixed equivalence class share a “mysterious” property; namely $(p, q)E(r, s)$ if and only if $p - q = r - s$. We this “mysterious” because subtraction is not

FIGURE 8.14. The equivalence classes of E (Definition 8.12).

defined for natural numbers. We enshrine this observation in our next piece of notation.

Notation 8.15. Let E be the equivalence relation on \mathbb{N} given in Definition 8.12. Then we may write

$$\mathbb{Z} = \mathbb{N}/E$$

If k is a natural number then we may write $k_{\mathbb{Z}} = [(k, 0)]_E$. We may call $k_{\mathbb{Z}}$ an *integer* and \mathbb{Z} the set of *integers*. \diamond

We usually omit the subscript \mathbb{Z} from our integers. Instead we use phrases like “Suppose that k is an integer” or “Fix $k \in \mathbb{Z}$ ”.

9. WELL-DEFINED FUNCTIONS AND INTEGER ARITHMETIC

9.1. Arithmetic in \mathbb{Z} . We now would like to be able to add and multiply integers. Moreover, and this is rather the point of integers, we would also like to negate and subtract them. There is a natural choice for all of these operations, as well as a certain problem to be overcome.

Definition 9.2. We call $0_{\mathbb{Z}}$ and $1_{\mathbb{Z}}$ the *zero* and *one* of \mathbb{Z} . Suppose that $k_{\mathbb{Z}} = [(p, q)]_E$ and $\ell_{\mathbb{Z}} = [(r, s)]_E$. We define the following operations on \mathbb{Z} .

- $k_{\mathbb{Z}} +_{\mathbb{Z}} \ell_{\mathbb{Z}} = [(p + r, q + s)]_E$ (addition)
- $k_{\mathbb{Z}} \times_{\mathbb{Z}} \ell_{\mathbb{Z}} = [(pr + qs, ps + qr)]_E$ (multiplication)
- $-k_{\mathbb{Z}} = [(q, p)]_E$ (negation)

\diamond

These definitions all operate in a similar fashion. They claim to define functions from \mathbb{Z}^2 to \mathbb{Z} , but in fact they are functions from $\mathbb{N}^2 \times \mathbb{N}^2$ to \mathbb{Z} . This is because they “look inside” the equivalence class, make a choice of an element, and compute with that. Only then do they form a new equivalence class.

As an example, suppose that we wish to compute $3_{\mathbb{Z}} +_{\mathbb{Z}} 4_{\mathbb{Z}}$. We might choose $(6, 3)$ and $(6, 2)$ to represent $3_{\mathbb{Z}}$ and $4_{\mathbb{Z}}$. We then form $[(12, 5)]_E$ and note that this is $7_{\mathbb{Z}}$, as desired. However, what if we instead had picked $(10, 7)$ and $(10, 6)$ to represent $3_{\mathbb{Z}}$ and $4_{\mathbb{Z}}$? In that case we get $[(20, 13)]_E$; luckily this is again equal to $7_{\mathbb{Z}}$. Being lucky is nice; however a more systematic method is available.

9.3. Well-defined functions.

Theorem 9.4. *Suppose that X and Y are sets. Suppose that E is an equivalence relation on X . Suppose that $f: X \rightarrow Y$ is a function. Suppose also that we have:*

(INVAR) *for all $x, x' \in X$, if xEx' then $f(x) = f(x')$.*

Then there is a unique function $f_E: X/E \rightarrow Y$ satisfying $f = f_E \circ q_E$.

This generalises to functions from $(X/E)^2$ and higher cartesian products.

When mathematicians use Theorem 9.4 – the “universal property of quotients” – they usually do not explicitly invoke it. Instead they

- (1) define f (while pretending to define f_E),
- (2) check the hypothesis (INVAR), and
- (3) then declare that f_E is *well-defined*.

After proving the theorem we shall do the same.

Proof of Theorem 9.4. We first build the function f_E and then prove it is unique.

Let Q be relation from X/E to Y which contains $([x]_E, y)$ exactly when

- there is some $x' \in X$ so that $f(x') = y$ and $x' \in [x]_E$.

Suppose that $[x]_E$ is any equivalence class. Note that $[x]_E$ is non-empty as it contains x . Let $y = f(x)$. Then $([x]_E, y)$ lies in Q .

Suppose that there is some $x \in X$ and $y', y'' \in Y$ so that $([x]_E, y')$ and $([x]_E, y'')$ lie in Q . By the defining property of Q there are x' and x'' in $[x]_E$ so that $f(x') = y'$ and $f(x'') = y''$. By the definition of $[x]_E$ we have xEx' and xEx'' . By the symmetry of E we have $x'E x$. By the transitivity of E we have $x'E x''$. By the hypothesis (INVAR) we have $f(x') = f(x'')$, and so $y' = y''$. Thus Q is graphical, as desired. Taking $f_E = Q$ completes the construction.

Suppose that x is an element of X . Thus $(f_E \circ q_E)(x) = f_E([x]_E) = f(x)$ and so we have $f = f_E \circ q_E$.

Suppose that $f'_E: X/E \rightarrow Y$ is another function satisfying $f = f'_E \circ q_E$. Suppose that $[x]_E$ is an element of X/E . Then $f_E([x]_E) = f(x)$. Also,

$f'_E([x]_E) = f'_E(q_E(x)) = f(x)$. Since f_E and f'_E have the same domain, codomain, and relation, they are equal. Thus f_E is unique. \square

9.5. Back to arithmetic.

Lemma 9.6. *The arithmetical operations in \mathbb{Z} , given in Definition 9.2, are well-defined.*

Proof. Suppose that (p, q) and (p', q') are elements of $k_{\mathbb{Z}}$. Suppose that (r, s) and (r', s') are elements of $\ell_{\mathbb{Z}}$. Swapping them as needed, we may assume that $p < p'$ and $r < r'$. Appealing to the solution to Exercise 8.13 we find that there are natural numbers P and R so that

$$(p + P, q + P) = (p', q') \quad \text{and} \quad (r + R, s + R) = (r', s')$$

To show that addition in \mathbb{Z} is well-defined we compute as follows:

$$\begin{aligned} (p' + r', q' + s') &= (p + P + r', q + P + s') \\ &= (p + P + r + R, q + P + s + R) \\ &= (p + r + P + R, q + s + P + R) \end{aligned}$$

By the solution to Exercise 8.13 this last lies in $[(p + r, q + s)]_E$, as desired.

To show that multiplication in \mathbb{Z} is well-defined we compute as follows:

$$\begin{aligned} (p'r' + q's', p's' + q'r') &= ((p + P)r' + (q + P)s', (p + P)s' + (q + P)r') \\ &= ((p + P)r' + (q + P)s', (p + P)s' + (q + P)r') \\ &= ((p + P)(r + R) + (q + P)(s + R), \\ &\quad (p + P)(s + R) + (q + P)(r + R)) \\ &= ((pr + qs + (p + q)R + (r + s)P + 2PR, \\ &\quad ps + qr + (p + q)R + (r + s)P + 2PR)) \end{aligned}$$

By the solution to Exercise 8.13 this last lies in $[(pr + qs, ps + qr)]_E$, as desired.

To show that negation in \mathbb{Z} is well-defined we compute as follows:

$$(q', p') = (q + P, p + P)$$

By the solution to Exercise 8.13 this last lies in $[(q, p)]_E$, as desired. \square

With the operations in place we can deduce their usual properties, as lemmas, rather than as axioms. We will focus on two which are mysterious in some presentations, but which are transparent here.

Corollary 9.7.

- $-0_{\mathbb{Z}} = 0_{\mathbb{Z}}$
- $(-1_{\mathbb{Z}}) \times_{\mathbb{Z}} (-1_{\mathbb{Z}}) = 1_{\mathbb{Z}}$

Proof. Recall that $0_{\mathbb{Z}} = [(0, 0)]_E$. We obtain $-0_{\mathbb{Z}}$ by reversing the order of $(0, 0)$. Since this does not change the ordered pair, we have $-0_{\mathbb{Z}} = 0_{\mathbb{Z}}$.

We now compute as follows:

$$\begin{aligned}
 (-1_{\mathbb{Z}}) \times_{\mathbb{Z}} (-1_{\mathbb{Z}}) &= (-[(1, 0)]_E) \times_{\mathbb{Z}} (-[(1, 0)]_E) && \text{definition of } 1_{\mathbb{Z}} \\
 &= ([(0, 1)]_E) \times_{\mathbb{Z}} ([(0, 1)]_E) && \text{definition of negation} \\
 &= ([(0 \times 0 + 1 \times 1, 0 \times 1 + 1 \times 0)]_E) && \text{definition of } \times_{\mathbb{Z}} \\
 &= ([(1, 0)]_E) && \text{arithmetic} \\
 &= 1_{\mathbb{Z}} && \text{definition of } 1_{\mathbb{Z}}
 \end{aligned}$$

and we are done. \square

Here is a final corollary.

Corollary 9.8. *The natural function $\mathbb{N} \rightarrow \mathbb{Z}$ taking $n \mapsto n_{\mathbb{Z}}$ is an injection. Furthermore, this function takes addition and multiplication in \mathbb{N} to the corresponding operations in \mathbb{Z} . \square*

With the integers safely defined, we return to thinking of individual integers as numbers, rather than as equivalence classes.

Challenge 9.9. Give a definition of \mathbb{Q} , the rational numbers, in the style of Definition 8.12. Use this to explain the claim that $1/2$ “equals” $2/4$. Use your definitions to prove that all non-zero elements of \mathbb{Q} have a multiplicative inverse. Finally, give a natural injection from \mathbb{Z} to \mathbb{Q} and prove that this function takes addition, multiplication, and negation in \mathbb{Z} to addition, multiplication and negation in \mathbb{Q} .

10. MODULAR ARITHMETIC

10.1. Multiples and divisors.

Definition 10.2. Suppose that m and n are integers. We say that m is a *multiple* of n if there is an integer k so that $m = k \times n$. If m is a multiple of n then we also say that n *divides* n . \diamond

Notation 10.3. Suppose that m and n are integers. Suppose that n divides m . Then we may write $n|m$. \diamond

Exercise 10.4. Show the following.

- (1) The relation of divides on \mathbb{Z} is reflexive and transitive, but not symmetric.
- (2) Plus and minus one divide all integers.
- (3) All integers divide zero.
- (4) Zero divides only itself. \diamond

10.5. Modulus n .

Definition 10.6. Suppose that a , b , and n are integers. We say that a and b are *congruent modulo n* if there is some integer k so that $a = b + kn$. That is, $a - b$ is a multiple of n . \diamond

Thus congruence modulo n gives a relation on \mathbb{Z} .

Notation 10.7. Suppose that a , b , and n are integers. If a and b are congruent modulo n then we may write $a \equiv b \pmod{n}$. We call n the *modulus* of the congruence. \diamond

Exercise 10.8. Prove that $a \equiv b \pmod{n}$ is an equivalence relation on \mathbb{Z} . \diamond

Notation 10.9. The equivalence classes of $a \equiv b \pmod{n}$ are often called *congruence classes*. If a is an integer then we may write $[a]_n$ for the congruence classes modulo n containing a . We also may write

$$\mathbb{Z}/n\mathbb{Z} = \{[a]_n \mid a \in \mathbb{Z}\}$$

for the set of equivalence classes.⁹ Finally we use $q_n: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ for the quotient map. \diamond

The notation $\mathbb{Z}/n\mathbb{Z}$ is pronounced “ \mathbb{Z} mod n \mathbb{Z} ” or “ \mathbb{Z} modulo n \mathbb{Z} ”.

Exercise 10.10. Prove the following.

- The equivalence classes of $\mathbb{Z}/0\mathbb{Z}$ are singletons.

⁹The notation $\mathbb{Z}/n\mathbb{Z}$ comes from algebra, where we may form a “quotient” of a *group* (or *ring*) by one of its *subgroups* (or *ideals*).

- The quotient $\mathbb{Z}/1\mathbb{Z}$ contains exactly one equivalence class.
- For any integer n we have $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(-n)\mathbb{Z}$. \diamond

We now count the number of elements of $\mathbb{Z}/n\mathbb{Z}$: that is, the number of equivalence classes of $a \equiv b \pmod{n}$.

Exercise 10.11. In light of Exercise 10.10 we may suppose that n is a positive integer.

- Suppose that m is an integer. Prove that $[m - n]_n = [m]_n = [m + n]_n$.
- Suppose that r and r' lie in $\llbracket n \rrbracket$. Prove that $r = r'$ if and only if $[r]_n = [r']_n$.
- Sketch a proof that $\mathbb{Z}/n\mathbb{Z}$ has exactly n elements: that is, $a \equiv b \pmod{n}$ has exactly n equivalence classes. \diamond

As a concrete example we explore the equivalence classes of the integers modulo $n = 6$. Suppose that a lies in \mathbb{Z} . Then we have

$$[a]_6 = \{a + 6k \in \mathbb{Z} \mid k \in \mathbb{Z}\}$$

To “see” this, we draw \mathbb{Z} along an logarithmic spiral in \mathbb{C} , the complex plane, as shown in Figure 10.12. The points of the equivalence class $[a]_6$ lie along the ray from the origin and through the point $\exp(a \frac{2\pi i}{6})$.

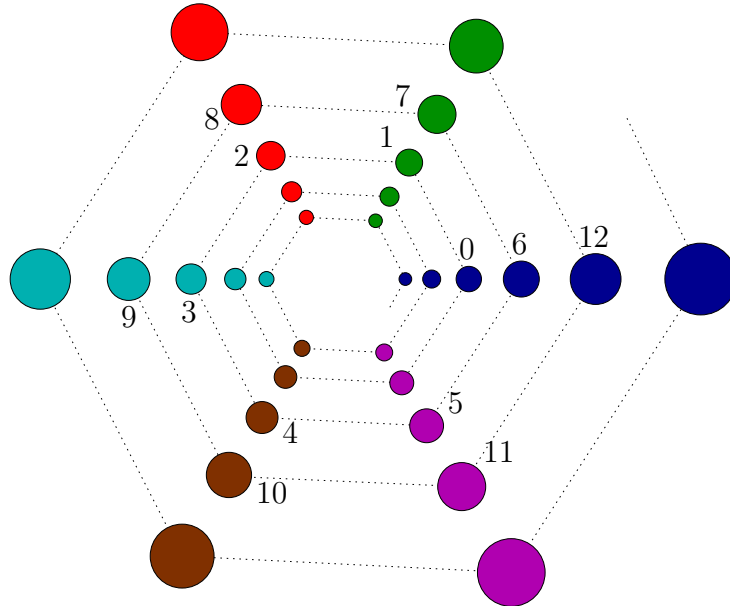


FIGURE 10.12. The equivalence classes of $a \equiv b \pmod{6}$ (Definition 10.6).

10.13. Modular addition, multiplication, and negation.

Definition 10.14. Suppose that n is an integer. We call $[0]_n$ and $[1]_n$ the *zero* and *one* of $\mathbb{Z}/n\mathbb{Z}$. Suppose that a and b are integers. We define the following operations on $\mathbb{Z}/n\mathbb{Z}$.

- $[a]_n +_n [b]_n = [a + b]_n$ (addition)
- $[a]_n \times_n [b]_n = [a \times b]_n$ (multiplication)
- $-_n[a]_n = [-a]_n$ (negation) ◇

Lemma 10.15. *The arithmetical operations in $\mathbb{Z}/n\mathbb{Z}$, given in Definition 10.14, are well-defined.* □

The proofs are similar to, but simpler than, those of Lemma 9.6 and we omit them.

Corollary 10.16. *The quotient function $q_n: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ takes addition, multiplication, and negation in \mathbb{Z} to the corresponding operations in $\mathbb{Z}/n\mathbb{Z}$.* □

Exercise 10.17.

- (1) Find the unique integer between zero and six (inclusive) congruent to $3^{20} \pmod{7}$.
- (2) Find the unique integer between zero and six (inclusive) congruent to $2^{111} \pmod{7}$.
- (3) Find the unique integer between zero and six (inclusive) congruent to $2^{3^{20}} \pmod{7}$. ◇

11. BOOLEANS AND THEIR OPERATORS

11.1. **Booleans.** We introduce two new symbols T and F.

Definition 11.2. A *boolean* is an element of the set $\mathcal{B} = \{T, F\}$. ◇

One common interpretation of the symbols T and F is “true” and “false”.

11.3. Boolean operators.

Definition 11.4. Suppose that n is a natural number. Suppose that $\mathcal{B} = \{T, F\}$. Recall that \mathcal{B}^n is the cartesian product of \mathcal{B} with itself, n times. We may call a function $f: \mathcal{B}^n \rightarrow \mathcal{B}$ a *boolean operator*. The number n is called the *arity* of f . ◇

For example, the identity $\text{Id}_{\mathcal{B}}$ is a boolean operator with arity one. There are two boolean operator with arity one which are *constant*; one always returns T and the other always returns F. Here is the final operator with arity one.

Definition 11.5. Suppose that P is a boolean. We define $(\neg P)$ via the following table.

P	$(\neg P)$
T	F
F	T

We call $(\neg P)$ the *negation* of P . It is pronounced “not P ”. \diamond

Definition 11.6. Suppose that P and Q are booleans. We define the following operators; all have arity two.

P	Q	$(P \vee Q)$	$(P \wedge Q)$	$(P \rightarrow Q)$	$(P \leftrightarrow Q)$
T	T	T	T	T	T
T	F	T	F	F	F
F	T	T	F	T	F
F	F	F	F	T	T

The operators \vee , \wedge , \rightarrow , and \leftrightarrow are called, respectively, the *disjunction*, the *conjunction*, the *implication*, and the *equivalence* operators. These are, in order, pronounced as “or”, “and”, “implies”, and “is equivalent to”. \diamond

Remark 11.7. There are twelve more boolean operators of arity two. It is an amusing exercise to list them all and give them their names. \diamond

We will call the operators \neg , \vee , \wedge , \rightarrow , and \leftrightarrow the *basic* boolean operators. We may compose these operators to obtain more complicated ones, with possibly higher arities.

Example 11.8. In these examples, the arity is two; this is because the arity counts the number of independent inputs to the operator.

- $((P \wedge P) \wedge (Q \wedge Q))$
- $((P \rightarrow (\neg P)) \rightarrow Q)$
- $((P \leftrightarrow (\neg P)) \leftrightarrow (Q \leftrightarrow (\neg Q)))$ \diamond

Suppose that f is a boolean operator. Any given composition of the basic operators, giving f , is called an *expression* for f . In an expression any sub-expression (beginning and ending with a pair of matching parentheses) is called a *clause*. A clause that does not contain parentheses is necessarily one of the basic operators. As an example, the expression

$$((P \wedge P) \wedge (P \vee P))$$

has three clauses of lengths five, five, and thirteen. This expression is a somewhat lengthy description of the operator $\text{Id}_{\mathcal{B}}$.

We note, but do not prove, that the five basic operators are a bit more than is strictly “needed”.

Theorem 11.9. *Any boolean operator can be written as a composition of the operators \neg and \vee .* \square

As a few very special cases of the theorem, we note the following equalities.

$$\begin{aligned}(P \wedge Q) &= (\neg((\neg P) \vee (\neg Q))) \\ (P \rightarrow Q) &= ((\neg P) \vee Q) \\ (P \leftrightarrow Q) &= ((P \rightarrow Q) \wedge (Q \rightarrow P))\end{aligned}$$

Using these we can express \leftrightarrow solely in terms of \neg and \vee .

Exercise 11.10. Simplify the compositions given in Example 11.8. Then write each in terms of \neg and \vee . \diamond

11.11. Boolean algebra. The boolean operators \vee and \wedge have many features in common with the operations \cup and \cap . The following are modelled on Lemmas 5.7, 5.14, 5.20, and 5.22

Lemma 11.12. *Suppose that P , Q , and R are booleans. Then we have the following.*

- (1) $(P \vee T) = T$ and $(P \vee F) = P$ (identity)
- (2) $((P \vee Q) \vee R) = (P \vee (Q \vee R))$ (associativity)
- (3) $(P \vee Q) = (Q \vee P)$ (commutativity)
- (4) $(P \rightarrow Q) = T$ if and only if $(P \vee Q) = Q$ (absorption)
- (5) $(P \vee P) = P$ (idempotent)

Exercise 11.13. Provide the proof of Lemma 11.12 \diamond

We omit the remaining proofs.

Lemma 11.14. *Suppose that P , Q , and R are booleans. Then we have the following.*

- (1) $(P \wedge T) = P$ and $(P \wedge F) = F$ (identity)
- (2) $((P \wedge Q) \wedge R) = (P \wedge (Q \wedge R))$ (associativity)
- (3) $(P \wedge Q) = (Q \wedge P)$ (commutativity)
- (4) $(P \rightarrow Q) = T$ if and only if $(P \wedge Q) = P$ (absorption)
- (5) $(P \wedge P) = P$ (idempotent)

\square

Lemma 11.15 (Distributive laws). *Suppose that P , Q , and R are booleans. Then we have the following.*

- $(P \wedge (Q \vee R)) = ((P \wedge Q) \vee (P \wedge R))$
- $(P \vee (Q \wedge R)) = ((P \vee Q) \wedge (P \vee R))$

\square

Lemma 11.16 (De Morgan's laws). *Suppose that P and Q are booleans. Then we have the following.*

- $(\neg(P \vee Q)) = ((\neg P) \wedge (\neg Q))$

$$\bullet (\neg(P \wedge Q)) = ((\neg P) \vee (\neg Q)) \quad \square$$

11.17. Tautologies.

Definition 11.18. Suppose that n is a natural number. Suppose that $\mathcal{B} = \{T, F\}$. Suppose that $f: \mathcal{B}^n \rightarrow \mathcal{B}$ is a boolean operator. We may call f a *tautology* if $f(x) = T$ for all $x \in \mathcal{B}^n$. We may call f an *antinomy* if $f(x) = F$ for all $x \in \mathcal{B}^n$. \diamond

For an example, consider $f(P) = (P \rightarrow P)$. This is a boolean operator of arity one. If $P = T$ then we obtain $f(T) = (T \rightarrow T) = T$, according to Definition 11.6. If $P = F$ then we obtain $f(F) = (F \rightarrow F) = T$. Thus f is a tautology. Similarly, $g(P) = (P \leftrightarrow (\neg P))$ is an antinomy.

Lemma 11.19. Suppose that f and g are boolean operators of the same arity. Then $(f \leftrightarrow g)$ is a tautology if and only if $f = g$. \square

In particular, if f and g are given as different compositions of the basic operators, then we may freely replace the one expression by the other. Thus tautologies give us ways to simplify boolean operators expressed as compositions.

We note that Lemma 11.19, added to the lemmas of Section 11.11, give us a large supply of tautologies. Here are a few more, that seem to arise in practice.

$$\begin{array}{ll} ((\neg(\neg P)) \leftrightarrow P) & \text{double negation} \\ ((P \rightarrow Q) \leftrightarrow ((\neg Q) \rightarrow (\neg P))) & \text{contraposition} \\ ((P \rightarrow Q) \leftrightarrow ((\neg P) \vee Q)) & \text{definition of implication} \\ ((P \leftrightarrow Q) \leftrightarrow ((P \rightarrow Q) \wedge (Q \rightarrow P))) & \text{definition of equivalence} \end{array}$$

And here are some of the tautologies graced with the name “rules of deduction”.

$$\begin{array}{ll} (P \vee (\neg P)) & \text{law of the excluded middle} \\ ((P \wedge (P \rightarrow Q)) \rightarrow Q) & \text{modus ponens} \\ (((P \rightarrow Q) \wedge (Q \rightarrow R)) \rightarrow (P \rightarrow R)) & \text{transitivity of implication} \\ (((\neg P) \rightarrow F) \rightarrow P) & \text{argument by contradiction} \end{array}$$

12. TRUTH TABLES

Here we discuss *truth tables*; an algorithmic method for dealing with boolean operators expressed as a composition of the basic operators. Before we do so, we require an ordering on the set of binary strings of a fixed length.

12.1. Ordering binary strings. Suppose that n is a natural number. Suppose that u and v are binary strings of length n . Suppose that u_i is the i^{th} bit of u ; we define v_i similarly.

We now say that $u \leq v$ if either

- $u = v$ or
- there is some k so that $u_i = v_i$ for $i < k$ and $u_k = 0$ while $v_k = 1$.

This is called the *lexicographic* order on binary strings of a fixed length. Said another way, $u \leq v$ if at the first position k where they disagree we have $u_k < v_k$.

Here is the lexicographic ordering of the binary strings of length three.

$$000 \leq 001 \leq 010 \leq 011 \leq 100 \leq 101 \leq 110 \leq 111$$

Here are a few examples in length five.

$$00111 \leq 01000 \quad 01000 \leq 01101 \quad 11110 \leq 11111$$

Exercise 12.2. Give the lexicographic order on binary strings of length four. \diamond

We may transfer this to obtain an ordering on the elements of $\{T, F\}^n$ by making an identification of T with zero and F with one. Here is the resulting lexicographic order on strings over $\{T, F\}$ of length three.

$$TTT \leq TTF \leq TFT \leq TFF \leq FTT \leq FTF \leq FFT \leq FFF$$

12.3. Lookup tables. The *lookup table* for a boolean operator f of arity n is

- the list of strings ω of length n over $\{T, F\}$ and
- next to each ω in the list the boolean $f(\omega)$.

Examples have almost already appeared in Definitions 11.5 and 11.6.

12.4. An algorithm to produce lookup tables. Suppose that f is a boolean operator of arity n . Suppose that f is given to us as a composition of the basis operators. To be concrete, we will use $f = ((P \vee Q) \rightarrow (Q \wedge P))$ as our running example. To form the lookup table for f we must compute $f(T, T)$, $f(T, F)$, $f(F, T)$, and $f(F, F)$ and record them, in that order. To save effort and space, we do not compute these one at a time. Instead we compute them together, in a *truth table*, as follows.

Algorithm 12.5.

- (1) We make a table with five ($= 1 + 2^n$) rows, with f in the first row. We leave all columns blank, except for the columns below

P and Q . Those we fill using the values for P and Q generated by lexicographic order.

$$\begin{array}{c} ((P \vee Q) \rightarrow (Q \wedge P)) \\ \hline \begin{array}{cccc} T & T & T & T \\ T & F & F & T \\ F & T & T & F \\ F & F & F & F \end{array} \end{array}$$

- (2) For each innermost clause (those that do not contain further parentheses), and for each row (so the values of P and Q are fixed), we use Definitions 11.5 and 11.6 to fill in the value of the clause.

$$\begin{array}{c} ((P \vee Q) \rightarrow (Q \wedge P)) \\ \hline \begin{array}{cccccc} T & \mathbf{T} & T & T & \mathbf{T} & T \\ T & \mathbf{T} & F & F & \mathbf{F} & T \\ F & \mathbf{T} & T & T & \mathbf{F} & F \\ F & \mathbf{F} & F & F & \mathbf{F} & F \end{array} \end{array}$$

The new entries in the table are in bold face.

- (3) We now repeat the process for the clauses only containing innermost clauses, using the computed values of the innermost.

$$\begin{array}{c} ((P \vee Q) \rightarrow (Q \wedge P)) \\ \hline \begin{array}{cccccc} T & T & T & \mathbf{T} & T & T & T \\ T & T & F & \mathbf{F} & F & F & T \\ F & T & T & \mathbf{F} & T & F & F \\ F & F & F & \mathbf{T} & F & F & F \end{array} \end{array}$$

Again, the new entries in the table are in bold face.

- (4) In general, we repeat the previous step; in its k^{th} iteration we assign values to clauses containing only clauses dealt with at step $k - 1$ or earlier.

This completes the algorithm.

Here then is the lookup table for our running example.

P	Q	$((P \vee Q) \rightarrow (Q \wedge P))$
T	T	T
T	F	F
F	T	F
F	F	T

We deduce that the boolean operator is equal to $(P \leftrightarrow Q)$.

Exercise 12.6. Use Algorithm 12.5 to prove that modus ponens

$$((P \wedge (P \rightarrow Q)) \rightarrow Q)$$

is a tautology.

◇

13. QUANTIFIERS AND THEIR LAWS

13.1. Quantifiers. Here we explore two kinds of statements: the *universal* and the *existential*.

We begin with a running example from Euclid’s *Elements* [4, Book 9, Proposition 20]. We give the statement in a slight nonstandard form.¹⁰

Theorem 14.2. *There are arbitrarily large primes.*

We postpone the proof. We rephrase Theorem 14.2 as follows:

(EUC) For every natural number n there exists a natural number p so that $p > n$ and p is prime.

We introduce a function $\text{PRIME}:\mathbb{N} \rightarrow \{\text{T}, \text{F}\}$ defined by $\text{PRIME}(n) = \text{T}$ exactly when n is prime. With this definition we can rewrite our condition as follows.

(EUC) For every natural number n there exists a natural number p so that $((p > n) \wedge \text{PRIME}(p))$.

To finish rewriting (EUC) we require a bit of notation and a definition.

Notation 13.2. Suppose that X is a set. We may abbreviate the phrase *for all* $x \in X$ as $\forall x \in X$. We may abbreviate the phrase *there exists* $x \in X$ as $\exists x \in X$.

In either case, if the set X is fixed throughout the discussion, we may simplify the notation to just $\forall x$ and $\exists x$. \diamond

Note that \forall is an upside-down “A” and \exists is a backwards “E”. These logical operators are called *quantifiers*. The fragment $\forall x$ may be pronounced as “for all x ”, “for every x ”, “for any x ”, “for each x ”, or similar. The fragment $\exists x$ may be pronounced as “there exists x ”, “for some x ”, “for at least one x ”, or similar.

Definition 13.3. Suppose that X is a set. Suppose that $S(x)$ is a property. Then the sentence $(\forall x \in X \ S(x))$ holds if and only if $S(x)$ holds for every x in X . On the other hand, the sentence $(\exists x \in X \ S(x))$ if and only if $S(x)$ holds for some x in X . \diamond

This definition justifies the names of the two quantifiers: \forall is the *universal* quantifier while \exists is the *existential* quantifier. We can now finish rewriting our condition (with the background set understood to be the natural numbers).

(EUC) $(\forall n (\exists p ((p > n) \wedge \text{PRIME}(p))))$

¹⁰This is because we wish to focus on quantifiers ranging over a fixed set (here the natural numbers) rather than quantifiers ranging over sets.

Thus do we replace clarity by concision. We justify this by noting that shorter expressions are far easier to manipulate formally.¹¹

Exercise 13.4. Translate the following sentences into English and determine whether or not they hold. For each one the background set is the natural numbers.

- $(\forall p (\exists n ((p > n) \wedge \text{PRIME}(p))))$
- $(\exists n (\forall p ((p > n) \wedge \text{PRIME}(p))))$
- $(\exists p (\forall n ((p > n) \wedge \text{PRIME}(p))))$ ◇

As the exercise shows, the order of quantifiers is a delicate matter. That is, the sentences

$$(\forall x (\exists y S(x, y))) \quad \text{and} \quad (\exists y (\forall x S(x, y)))$$

are only very rarely equivalent.

13.5. Negation and distribution for quantifiers. There is a duality between the universal and existential quantifiers, as follows.

Theorem 13.6. *Suppose that X is our background set. Suppose that $S(x)$ is a property. Then*

- $(\neg(\forall x S(x)))$ holds if and only if $(\exists x (\neg S(x)))$ holds.
- $(\neg(\exists x S(x)))$ holds if and only if $(\forall x (\neg S(x)))$ holds.

Proof. Suppose that $(\neg(\forall x S(x)))$ holds. Thus $(\forall x S(x))$ does not hold. So $S(x)$ does not hold for some x in X . Thus $(\neg S(x))$ does hold for some x in X . That is, $(\exists x (\neg S(x)))$ holds.

Each step of the above argument reverses; thus the first equivalence is proven.

To prove the second, negate both sentences and recall that $(\neg(\neg P))$ is equivalent to P . □

Theorem 13.7. *Suppose that X is our background set. Suppose that $R(x)$ and $S(x)$ are properties. Then*

- $(\forall x (R(x) \wedge S(x)))$ holds if and only if $((\forall x R(x)) \wedge (\forall x S(x)))$ holds.
- $(\exists x (R(x) \vee S(x)))$ holds if and only if $((\exists x R(x)) \vee (\exists x S(x)))$ holds.

On the other hand, there are no “distributive laws” for \forall over \vee or for \exists over \wedge . We omit the proofs.

¹¹To see the truth of this, try multiplying one hundred and twelve by eighty three *without* using some form of place notation.

Proof of Theorem 13.7. Suppose that $(\forall x (R(x) \wedge S(x)))$. Then for every x in X we have that $(R(x) \wedge S(x))$ holds. That is, for every x in X we have that $R(x)$ holds and $S(x)$ holds. So, for every x in X we have that $R(x)$ holds and, for every x in X , we also have that $S(x)$ holds. That is, $(\forall x R(x))$ holds as does $(\forall x S(x))$. Thus $((\forall x R(x)) \wedge (\forall x S(x)))$ holds.

Every step of the above argument reverses; thus the first equivalence is proven.

To prove the second, negate both sides, apply Theorem 13.6, and recall that $R(x)$ and $S(x)$ were arbitrary properties. \square

Exercise 13.8.

- Prove that $(\forall x (R(x) \rightarrow S(x)))$ implies $((\forall x R(x)) \rightarrow (\forall x S(x)))$.
- Show by means of an example that the latter need not imply the former. \diamond

14. PROOF

14.1. An example.

Theorem 14.2. *There are arbitrarily large primes.*

The more usual statement is “There are infinitely many primes.” The original statement in Euclid’s *Elements* is “Prime numbers are more than any assigned multitude of prime numbers.” [4, Book 9, Proposition 20]. But actually that is false: the actual “original” statement was written in Greek, probably on papyrus, perhaps within a few decades of 300 BCE. No trace of it remains. The oldest surviving complete copy of Euclid’s *Elements* is instead written on parchment and dates to 888 CE [5].

Before giving the proof of Theorem 14.2, we require a definition and two preliminary results.

Definition 14.3. Suppose that p is a natural number greater than one. Then p is *prime* if it has exactly two positive divisors. \diamond

Since p is divisible by one, and by itself, these are all of its (positive) divisors. Here are the needed “helper” statements.

Lemma 17.12. *Suppose that X is a finite set. Suppose that Y is a subset of X . Then Y is finite.*

Proposition 16.12. *Suppose that n is a natural number greater than one. Then n is divisible by some prime.*

Proof of Theorem 14.2. Recalling the discussion of Section 13.1, we begin by fixing a natural number n . We now must find a prime p larger than n .

Let \mathcal{P} be the set of primes less than or equal to n . By Lemma 17.12, the set \mathcal{P} is finite. So let $(p_i)_{i=0}^k$ be the list of elements of \mathcal{P} , say in order of size. We define N to be one, plus the product of these primes. That is:

$$N = 1 + p_0 \cdot p_1 \cdot p_2 \cdots p_k$$

Suppose that p lies in \mathcal{P} . Thus N is congruent to one modulo p . In particular N is not divisible by p .

By Proposition 16.12, the natural number N is divisible by some prime, say q . We deduce that q does not lie in \mathcal{P} . From the definition of \mathcal{P} we deduce that q is greater than n . \square

There are several things to note about the proof.

- The overall plan of the proof follows the previous discussion in Section 13.1.
- The existence of \mathcal{P} follows from the axiom of specification applied to $\llbracket n + 1 \rrbracket$.
- The finiteness of \mathcal{P} depends on Lemma 17.12. Although this lemma is “obvious” we have not proved it yet.
- Likewise, the claim that N is divisible by a prime depends on Proposition 16.12. Again we have not proved this yet.

Each of these points is interesting in its own right. Taking them altogether, they suggest that different proofs of Theorem 14.2 can have very different levels of detail.

However it is *not* the case that writing down a proof is “merely” a matter of being “formal enough”. A proof may also require some act of imagination. As one piece of evidence for this we note that the definition of N , above, was a bit subtle. If this is not convincing enough, consider the following exercise.

Exercise 14.4. Prove that there are arbitrarily large primes that are congruent to 3 modulo four. \diamond

14.5. Proof, informally. With our example in hand, we attempt an informal definition.

Definition 14.6. A *proof* is a convincing argument. \diamond

This definition lays bare the central issue; for an argument to be convincing, there is some person that needs to be convinced. However, an argument that convinces one person may not convince another. In one respect this is obvious; somebody who does not read English will

not find the proof of Theorem 14.2, or indeed anything in these lecture notes, enlightening.

Next, there are rhetorical issues. For example, a writer may signal the difficulty of steps in a proof. Phrases such as “it is easy to see” or “a simple argument gives” are common. Less common, but still used are phrases like “it is a deep result that” or “the crucial step is”. However, there is a blurry area between helpful advice on the one hand and misleading propaganda on the other. Both may be convincing, but we should try to avoid the latter.

Finally, there are subtle problems of representation. While writing these notes I have assumed that you, the reader, has an excellent background at A-levels maths. But perhaps my conception of A-level maths is incorrect. Or perhaps your preparation is stronger in some areas and weaker in others; as a result some of the arguments here may be more or less convincing.

Taking the above definition seriously leads us to a somewhat awkward conclusion; that “proof” is a social construct that lives somewhere between the minds of the writer and the reader.

14.7. Formal proof. We now try to minimise the sociological nature of “proof”. (This section is not examinable.)

Definition 14.8. Suppose that \mathcal{A} is a list of axioms. Suppose that \mathcal{D} is a list of rules of deduction. Furthermore, suppose that there are algorithms that decide if a given statement lies in \mathcal{A} (or not) and if a given statement can be deduced, by a given rule in \mathcal{D} , from a given list of other statements.

Suppose now that S is a statement. Then a *proof of S from \mathcal{A} and \mathcal{D}* is a list $(S_i)_{i=0}^n$ of statements where:

- For each k , either
 - S_k is an axiom (lies in \mathcal{A}) or
 - S_k follows from the statements $(S_i)_{i < k}$ by one of the rules of deduction (from \mathcal{D}) and
- $S_n = S$. ◇

This more formal definition captures many features of mathematical practice. It is also a valuable tool in making proofs first-class mathematical objects. Done carefully, proofs written this way can be checked by computer, using tools such as *proof assistants*. Finally, and perhaps most significantly, Gödel started from the idea of formal proof and showed that (for very general \mathcal{A} and \mathcal{D}) there are statements that can neither be proven nor disproven.

Definition 14.8 is the model for how mathematicians think of proofs. However it is not, for the most part, what they actually *do*. Mathematicians use diagrams, draw pictures, collect evidence (by hand or via computer), make conjectures, stare into space, and argue with each other a lot, often waving their hands about. It is perhaps possible to restate some of these activities in terms of Definition 14.8. But that is not the end goal of most mathematicians.

15. PATTERNS OF PROOF

15.1. Direct proof of implications. Many mathematical statements are written in the form “if P then Q ” where again P and Q are mathematical statements.

Definition 15.2. The statement ‘if P then Q ’ is an the *implication* with *hypothesis* P and *conclusion* Q . \diamond

Here is an example.

Lemma 15.3. *If n is an even integer then n^2 is an even integer.*

One way to prove an implication is *directly*. That is, we assume P , make various deductions, and finally deduce Q .

Proof of Lemma 15.3. Suppose that n is an even integer. So there is some integer k with $n = 2k$. Thus $n^2 = 4k^2 = 2 \times 2k^2$. Thus n^2 is even, as desired. \square

Exercise 15.4. Give a direct proof of the implication “If n is an odd integer then n^2 is an odd integer.” \diamond

Definition 15.5. The *converse* of the implication “if P then Q ” is the implication “if Q then P ”. \diamond

In general if an implication holds, its converse may or may not hold.

Definition 15.6. We may say that P and Q are *equivalent*, and we may write “ P if and only if Q ” when P implies Q and Q implies P . \diamond

Note that to prove an equivalence we must prove a pair of implications.

Exercise 15.7. Give a direct proof of the following fragment of Lemma 5.14. Suppose that X and Y are sets. If $X \subset Y$ then $X \cap Y = X$. \diamond

Exercise 15.8. Give a direct proof of the following implication: Suppose that X , Y , and Z are sets. Suppose that $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are bijections. Then $g \circ f$ is a bijection. \diamond

15.9. Proof by contraposition.

Definition 15.10. The *contrapositive* of the implication “if P then Q ” is the implication “if not Q then not P ”. \diamond

As discussed in Section 11.17, the statement

$$((P \rightarrow Q) \leftrightarrow ((\neg Q) \rightarrow (\neg P)))$$

is a tautology. Thus to prove an implication it suffices to prove its contrapositive.

Suppose that k is an integer. We say that k is a *sum of two squares* if there are integers x and y so that $k = x^2 + y^2$.

Lemma 15.11. *Suppose that p is an integer. If $p \equiv 3 \pmod{4}$ then p is not a sum of two squares.*

Proof. We prove the contrapositive, directly. Suppose that p is a sum of two squares. So there are integers x and y so that $p = x^2 + y^2$. There are now several cases: either x and y are both even, both odd, or have opposite parity.

Suppose that x and y are both even. So we have integers z and w so that $x = 2z$ and $y = 2w$. Thus $x^2 = 4z^2$ and $y^2 = 4w^2$ are both divisible by four. That is $x^2 \equiv y^2 \equiv 0 \pmod{4}$. Thus $p \equiv x^2 + y^2 \equiv 0 \pmod{4}$.

Suppose that x and y are both odd. So we have integers z and w so that $x = 2z + 1$ and $y = 2w + 1$. Thus $x^2 = 4z^2 + 4z + 1$ and $y^2 = 4w^2 + 4w + 1$ are both congruent to one modulo four. Thus $p \equiv x^2 + y^2 \equiv 2 \pmod{4}$.

Finally suppose that x and y have opposite parity. Breaking the symmetry, we assume that x is even and y is odd. So we have integers z and w so that $x = 2z$ and $y = 2w + 1$. Using the same logic as above, we find that $p \equiv x^2 + y^2 \equiv 1 \pmod{4}$.

In all cases we have that p is not congruent to three modulo four. \square

Note that in the above proof the outermost pattern was a proof by contraposition. However, as an inner pattern we had a *proof by cases*. This is a way to organise work; we announce the complete list of cases and then dispose of each in order.

Exercise 15.12. Suppose that p is an integer. Prove that if $p \equiv 7 \pmod{8}$ then p is not a sum of three squares. [Hint: if $p = x^2 + y^2 + z^2$ then consider x modulo four.] \diamond

15.13. Proof by contradiction. We now have a result even older than Theorem 14.2. (This was known to the cult of Pythagoras [10]. However, it was likely also known a thousand years earlier [2].)

Theorem 15.14. *There is no rational number r so that $r^2 = 2$.*

This is a *non-existence statement*. To prove it, we use *proof by contradiction*. That is, we assume its negation and derive a contradiction. This is very similar to the tautology

$$(((\neg P) \rightarrow F) \rightarrow P)$$

Proof of Theorem 15.14. Suppose, for a contradiction, that there is some rational number r so that $r^2 = 2$. By definition, we have that $r = p/q$ where p and q are integers, with q positive. Since $r^2 = (-r)^2$ we may also assume that p is positive.

We now give a *proof by infinite descent*. Take $p_0 = p$ and $q_0 = q$. Square both sides to find $p_0^2/q_0^2 = r^2 = 2$. Thus $p_0^2 = 2q_0^2$. Since p_0^2 is even, by the contrapositive of Exercise 15.4 we have that p_0 is even. We write $p_0 = 2p_1$ and find that $4p_1^2 = 2q_0^2$. Thus $q_0^2 = 2p_1^2$ and, again by Exercise 15.4, we have that q_0 is even. We write $q_0 = 2q_1$ and find that $4q_1^2 = 2p_1^2$. Thus $p_1^2 = 2q_1^2$.

Repeating the argument, we obtain sets $\{p_k\}_{k \in \mathbb{N}}$ and $\{q_k\}_{k \in \mathbb{N}}$ so that

$$p_k^2 = 2q_k^2 \quad p_{k+1} = 2p_k \quad \text{and} \quad q_{k+1} = 2q_k$$

We deduce that $p_k > p_{k+1}$. Thus $\{p_k\}_{k \in \mathbb{N}}$ is a set of natural numbers with no least element. This contradicts the well-ordering principle (Theorem 16.11). \square

Exercise 15.15. Prove that there is no rational number r so that $r^2 = 3$. \diamond

Exercise 15.16. Prove that there is no rational number r so that $r^3 = 2$. \diamond

15.17. Proof by construction.

Lemma 15.18. *There is a prime greater than 200.*

This is an *existence statement*. Note that Theorem 14.2 implies this, but without giving an explicit prime. In a *proof by construction* we give an explicit example and verify that it has the desired properties.

Proof of Lemma 15.18. We claim that $N = 211$ is prime. Suppose not; then N factors as a product of, say, $k \geq 2$ primes. If all of these primes are greater than $\sqrt{N} \sim 14.5$ then we conclude that $N > (\sqrt{N})^k \geq N$, a contradiction. Thus to prove N is prime it suffices to check if any of the primes less than 15 divide N .

The list of primes less than 15 is $(2, 3, 5, 7, 11, 13)$. For each we give its largest multiple which is still less than N .

$$210 = 2 \times 105 \quad 210 = 3 \times 70 \quad 210 = 5 \times 42$$

$$210 = 7 \times 30 \quad 209 = 11 \times 19 \quad 208 = 13 \times 16$$

Thus 211 is congruent to one modulo two, three, five, and seven. Similarly 211 is congruent to two modulo eleven and congruent to three modulo thirteen. In particular 211 is not divisible by any of the given primes, so we are done. \square

The outermost pattern in the above is a proof by construction. However the inner steps are themselves proofs, using other patterns.

Exercise 15.19. Give a proof by construction of the following: there is a number less than 1000 having at least four distinct prime factors. \diamond

Exercise 15.20. Prove that there is an injection from \mathbb{Q} to \mathbb{N} . \diamond

16. INDUCTION AND RECURSION

16.1. **Induction.** We now state the *principle of induction*.¹²

Axiom 16.2. Suppose that $(P(n))_{n \in \mathbb{N}}$ is a sequence of sentences, one for each natural number. Suppose that

- (1) $P(0)$ holds and
- (2) for all $k \in \mathbb{N}$, if $P(k)$ holds then $P(k+1)$ holds.

Then $P(n)$ holds for all n . □

In the above definition, part (1) is often called *the base case*. Part (2) is often called the *induction step*; also, in part (2) the sentence $P(k)$ is often called the *induction hypothesis*.

Here is a simple example of *proof by induction*.

Lemma 16.3. Every natural number is either even or odd.

Proof. Suppose that n is a natural number. Let $P(n)$ be the sentence “ n is even or n is odd”.

We now deal with the base case, where $n = 0$. Since $0 = 2 \times 0$, the number zero is even. Thus $P(0)$ holds.

We now deal with the induction step. Suppose that k is a natural number which is even or odd. We must prove that $k+1$ is even or odd. There are two cases.

- Suppose that k is even. Thus there is a natural number ℓ so that $k = 2\ell$. So $k+1 = 2\ell+1$ is odd.
- Suppose that k is odd. Thus there is a natural number ℓ so that $k = 2\ell+1$. So $k+1 = 2\ell+2 = 2(\ell+1)$ is even.

Thus $P(k)$ implies $P(k+1)$, establishing the induction step.

Thus we are done by induction. □

Exercise 16.4. Prove that every natural number is congruent to at least one of zero, one, or two, modulo three. ◇

16.5. **Recursion.** We now give one version of the *recursion theorem*, sometimes called *weak* or *linear* recursion. There are others; see [6, page 48].

Theorem 16.6. Suppose that $F: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ is a function. Suppose that a is a natural number. Then there is a unique function $f: \mathbb{N} \rightarrow \mathbb{N}$ so that

- $f(0) = a$ and
- for all k we have $f(k+1) = F(k, f(k))$. □

¹²This can be proven from the axioms of set theory – for example, see [3, Theorem 4B].

Example 16.7. With notation as in Theorem 16.6, we take $F(k, \ell) = 2k + 1 + \ell$ and $a = 0$. The conclusion of the theorem gives a function $f: \mathbb{N} \rightarrow \mathbb{N}$ where

- $f(0) = 0$ and
- $f(n + 1) = 2n + 1 + f(n)$. ◇

We compute the first few values of f .

$$\begin{aligned}
 f(0) &= 0 \\
 f(1) &= 2 \times 0 + 1 + f(0) = 1 \\
 f(2) &= 2 \times 1 + 1 + f(1) = 3 + 1 = 4 \\
 f(3) &= 2 \times 2 + 1 + f(2) = 5 + 3 + 1 = 9 \\
 f(4) &= 2 \times 3 + 1 + f(3) = 7 + 5 + 3 + 1 = 16 \\
 f(5) &= 2 \times 4 + 1 + f(4) = 9 + 7 + 5 + 3 + 1 = 25
 \end{aligned}$$

This leads us to the following.

Lemma 16.8. *The sum of the first n odd numbers equals n^2 .*

Proof. The sum of the first $n + 1$ odd numbers is given by adding the first $n - 1$ odd numbers, and then adding $2n + 1$ to the result. Thus the sum is exactly $f(n)$, as given by Example 16.7. Since $f(n)$ is defined by recursion, we give a proof by induction.

In the base case we have $f(0) = 0 = 0^2$, as desired.

For the induction step, we suppose that $f(k) = k^2$. We now compute as follows.

$$\begin{aligned}
 f(k + 1) &= 2k + 1 + f(k) && \text{definition of } f \\
 &= 2k + 1 + k^2 && \text{induction hypothesis} \\
 &= (k + 1)^2 && \text{algebra}
 \end{aligned}$$

Since the base case and the induction step hold we are done by induction. □

Exercise 16.9. Define $g(n)$ to be the sum of the first n natural numbers. Give a definition using recursion, compute the first several values, guess a polynomial equalling g , and prove your conjecture using induction. ◇

16.10. The well-ordering principle. Suppose that S is a subset of \mathbb{N} . An element $s \in S$ is a *least* element if, for all $t \in S$, we have $s \leq t$.

We are now in a position to pay off one of our debts. We prove the *well-ordering principle* by induction.

Theorem 16.11. *Suppose that S is a subset of \mathbb{N} . If S is non-empty, then S has a least element.*

Proof. We prove the contrapositive. So suppose that S has no least element.

We now proceed by induction. Let $P(n)$ be the sentence “ $S \cap \llbracket n \rrbracket = \emptyset$ ”.

We first deal with the base case. Since $\llbracket 0 \rrbracket = \emptyset$ we have that $P(0)$ holds.

We now turn to the induction step. We prove this by contradiction. Suppose that $S \cap \llbracket n \rrbracket$ is empty and $S \cap \llbracket n + 1 \rrbracket$ is non-empty. Thus n lies in S , and is a least element. This contradicts our assumption that S has no least element. This completes the induction step.

We deduce that $P(n)$ holds for all n . Thus S is empty, as desired. \square

It is *almost* the case that the well-ordering principle implies the principle of induction. For a detailed and elementary discussion, see [7].

We are now equipped to pay off another of our debts [4, Book 7, Proposition 31].

Proposition 16.12. *Suppose that n is a natural number greater than one. Then n is divisible by some prime.*

Proof. Suppose that n is a natural number, greater than one. Let S be the set of divisors of n which are greater than one. That is,

$$S = \{k \in \mathbb{N} \mid k > 1 \text{ and } k \text{ divides } n\}$$

Note that n lies in S , so S is not empty.

Applying the well-ordering principle, let s be a least element of S . If s is prime we are done. So, for a contradiction, suppose that s is not prime. So s is divisible by some natural number t strictly between one and s . Since divisibility is transitive, we deduce that t lies in S . So s was not a least element of S , a contradiction. \square

17. STRONG INDUCTION, RECURSION, FINITE SETS, AND THE PIGEONHOLE PRINCIPLE

17.1. Strong induction. In the usual form of induction we only allowed ourselves to “look back one step”. With the strong form we may look back as many steps as we like.

Axiom 17.2. *Suppose that $(P(n))_{n \in \mathbb{N}}$ is a sequence of sentences, one for each natural number. Suppose that*

- *for all $k \in \mathbb{N}$, if $P(\ell)$ holds for all $\ell < k$ then $P(k)$ holds.*

Then $P(n)$ holds for all n . \square

Despite the name, strong induction is very slightly *weaker* than weak induction. We again refer to [7] for a closely related discussion.

Strong induction gives us another “proof pattern”. Here is an important example.

Theorem 17.3. *Suppose that n is a natural number, greater than zero. Then n has a unique factorisation into primes.*

Proof. Suppose that n is a natural number greater than zero. If $n = 1$ then n has the empty factorisation. We now assume that $n \geq 2$ and proceed by strong induction.

We first prove that n has *at least one* prime factorisation. If n is prime then we are done. If n is not prime, then we may write $n = a \cdot b$ where a and b are natural numbers strictly between one and n . As a and b are less than n , by the induction hypothesis both a and b have unique prime factorisations. Multiplying these together we obtain a prime factorisation for n .

We now prove that n has *at most one* prime factorisation. Suppose that

$$n = p_1 \cdot p_2 \cdots p_k \quad \text{and} \quad n = q_1 \cdot q_2 \cdots q_\ell$$

are a pair of factorisations. We may assume that $p_i \leq p_{i+1}$ and $q_i \leq q_{i+1}$ for all i . If $p_1 = q_1$ then apply the induction hypothesis to n/p_1 to conclude that $p_i = q_i$ for all i .

Suppose, for a contradiction, that $p_1 < q_1$. Then we have

$$p_1(p_2 \cdots p_k - q_2 \cdots q_\ell) = (q_1 - p_1)q_2 \cdots q_\ell$$

Since $1 \leq q_1 - p_1 < n$ the induction hypothesis gives us a prime factorisation $r_1 \cdot r_2 \cdots r_m$. So the displayed number above factors as

$$r_1 \cdot r_2 \cdots r_m \cdot q_2 \cdots q_\ell$$

and this factorisation is unique. Note that p_1 divides this. However, since $p_1 < q_1$ we deduce that p_1 is not equal to any of the q_i . We deduce that p_1 equals one of the r_i . Thus p_1 divides $q_1 - p_1$. So p_1 divides q_1 , a contradiction.

The case where $q_1 < p_1$ is argued similarly and this completes the proof. \square

17.4. Strong recursion. Instead of giving a precise statement of “strong” recursion we give a very common example.

Example 17.5. We define $f: \mathbb{N} \rightarrow \mathbb{N}$ by

- $f(0) = 0$,
- $f(1) = 1$, and
- $f(k+2) = f(k+1) + f(k)$ for all $k \in \mathbb{N}$.

We may call $f(n)$ the n^{th} *Fibonacci number*. \diamond

Note that the definition of $f(n)$ requires knowing the previous two values. Here are the first ten values of f .

n	0	1	2	3	4	5	6	7	8	9
$f(n)$	0	1	1	2	3	5	8	13	21	34

Proving facts about the Fibonacci numbers will typically require strong induction.

Sets, like functions, may also be constructed recursively. Again, instead of giving formal definitions we content ourselves with a few examples.

Exercise 17.6.

- (1) Determine the number of binary strings of length n where no adjacent bits are equal.
- (2) [Hard.] Determine the number of binary strings of length n where no adjacent bits are both 0. \diamond

17.7. Finite sets and the pigeonhole principle. A *dovecote* is a structure intended to house pigeons or doves. Part of its interior is typically divided into small *pigeonholes* to allow the pigeons to nest separately or in pairs. The *pigeonhole principle* states that

- if there are more pigeons than pigeonholes and
- if every pigeon is in some pigeonhole

then some pigeonhole contains at least two pigeons. The origins of the principle are, of course, unclear [1].

We give a slightly non-standard proof, starting with the following.

Theorem 17.8. *Suppose that n is a natural number. Suppose that $f: \llbracket n \rrbracket \rightarrow \llbracket n+1 \rrbracket$ is a function. Then f is not a surjection.*

This statement is modelled on our version of Cantor's theorem (Theorem 3.12).

Proof of Theorem 17.8. We proceed by induction.

We begin with the base case. Here we must prove that there is no surjection from $\llbracket 0 \rrbracket$ to the singleton set $\llbracket 1 \rrbracket$. For a contradiction, suppose that there is some surjection $f: \llbracket 0 \rrbracket \rightarrow \llbracket 1 \rrbracket$. Thus there is some element a of $\llbracket 0 \rrbracket$ so that $f(a) = 0 \in \llbracket 1 \rrbracket$. However, by Notation 1.13 the set $\llbracket 0 \rrbracket$ is empty. Thus a does not exist, we have obtained a contradiction, and the base case is complete.

We now prove the contrapositive of the induction step. Suppose that $f: \llbracket n+1 \rrbracket \rightarrow \llbracket n+2 \rrbracket$ is a surjection. We now define a function

$g: \llbracket n \rrbracket \rightarrow \llbracket n+1 \rrbracket$.

$$g(k) = \begin{cases} f(k), & \text{if } f(k) < n+1 \\ f(n), & \text{if } f(k) = n+1 \text{ and } f(n) < n+1 \\ 0, & \text{if } f(k) = f(n) = n+1 \end{cases}$$

We now show that g is a surjection.

Suppose that ℓ is any element of $\llbracket n+1 \rrbracket$; so $\ell < n+1$ and thus is an element of $\llbracket n+2 \rrbracket$. Since f surjects $\llbracket n+2 \rrbracket$ there is some $k \in \llbracket n+1 \rrbracket$ so that $f(k) = \ell$. There are now two cases: either $k < n$ or $k = n$.

- (1) Suppose that $k < n$. Since $f(k) = \ell < n+1$, the first line of the definition of g applies. Thus $g(k) = f(k) = \ell$ and we are done.
- (2) Suppose that $k = n$. This does not lie in the domain of g . Instead, we again use the fact that f is surjective. So there is some $k' \in \llbracket n+1 \rrbracket$ so that $f(k') = n+1$. Note that $f(n) = \ell < n+1 = f(k')$. Since f is a function, we deduce that k' is not equal to n . Since $f(k') = n+1$ and $f(n) < n+1$, the second line of the definition of g applies. Thus $g(k') = f(n) = \ell$ and we are done.

Thus g is a surjection, as claimed. This completes the induction step, and thus the proof of the theorem. \square

Remark 17.9. In the proof above, the third line of the definition of g is only present to ensure that g is a function. The third line is not needed to show that g is a surjection. \diamond

Exercise 17.10. Give proofs of the following, using Theorem 17.8 as needed.

- (1) Suppose that n is a natural number. Prove that there is no injection $g: \llbracket n+1 \rrbracket \rightarrow \llbracket n \rrbracket$.
- (2) Suppose that m and n are natural numbers, with $m > n$. Prove that there is no injection $g: \llbracket m \rrbracket \rightarrow \llbracket n \rrbracket$.
- (3) Suppose that n is a natural number. Prove that there is no bijection $g: \mathbb{N} \rightarrow \llbracket n \rrbracket$. [That is, \mathbb{N} is infinite in the sense of Definition 3.14.]
- (4) Suppose that X is a finite set. Then it has a unique cardinality (as given in Definition 3.9).
- (5) Suppose that X is a finite set. Then a function $f: X \rightarrow X$ is an injection if and only if it is surjection. \diamond

From Exercise 17.10(4) we deduce the following.

Corollary 17.11. *Suppose that X and Y are finite sets with cardinalities m and n . Then there is a bijection from X to Y if and only if $m = n$.* \square

We finish with a final result about finite sets, paying off our final (?) debt.

Lemma 17.12. *Suppose that X is a finite set. Suppose that Y is a subset of X . Then Y is finite.*

Proof. Since X is finite, it is in bijection with $\llbracket n \rrbracket$ for some $n \in \mathbb{N}$. So we may simplify the remainder of the proof by assuming $X = \llbracket n \rrbracket$. This also allows us to assume that Y is a subset of \mathbb{N} .

We now build a function f by recursion. That is, we define a sequence of functions and take f equal to the last one.

In the base case we have $f_0: \llbracket 0 \rrbracket \rightarrow Y$, the unique function with domain $\llbracket 0 \rrbracket$ and codomain Y .

For the recursive step, we assume that $f_k: \llbracket k \rrbracket \rightarrow Y$ has already been defined. Let $Y_k = f_k(\llbracket k \rrbracket)$ be the image of $\llbracket k \rrbracket$ under f_k . There are two cases.

- If $Y_k = Y$ then $f = f_k$ and the construction is done.
- Otherwise, let $y_k \in Y - Y_k$ be the least element, obtained from the well-ordering principle. We now define $f_{k+1}: \llbracket k+1 \rrbracket \rightarrow Y$ by

$$f_{k+1}(\ell) = \begin{cases} f_k(\ell), & \text{if } \ell < k \\ y_k, & \text{if } \ell = k \end{cases}$$

This defines f_{k+1} and so completes the recursive step.

By induction each of the f_k is an injection. Thus by the pigeonhole principle (Exercise 17.10) the construction terminates after at most n steps, giving f . Since the construction terminates, f is surjective. Thus Y is finite. \square

APPENDIX A. SOLUTIONS TO EXERCISES

Solution 1.7. Suppose that X and Y are empty sets. Then every element of X (there are none) belongs to Y . Similarly, every element of Y (there are none) belongs to X . Thus, by the axiom of extension, $X = Y$. \square

Solution 1.12.

- (1) To prove that $\emptyset \subset X$ we must check, for every $x \in \emptyset$, that x lies in X . Since there are no elements of \emptyset , no checks can (or need to) be made. Thus all checks (again, there are none) are successful. Thus $\emptyset \subset X$, as desired. [Such a statement, where nothing needs to be checked, is said to hold *vacuously*.]
- (2) To prove that $X \subset X$ we must check, for every $x \in X$, that x lies in X . This holds, so we are done. \square

Solution 1.14. Suppose that Y is a subset of $\llbracket n \rrbracket$. For each $k < n$, either k is in Y or it is not. All of these possibilities are *independent*: that is, for any collection of n two-fold choices there is such a subset Y . Thus there are $2 \times 2 \times \cdots \times 2 = 2^n$ subsets of $\llbracket n \rrbracket$. \square

Solution 2.13.

- (1) Recall that

$$\llbracket n \rrbracket = \{0, 1, 2, \dots, n-1\}$$

is the set of the first n natural numbers. To represent a function $f: \llbracket 2 \rrbracket \rightarrow \llbracket 2 \rrbracket$ we list the images as lists of the form $(f(0), f(1))$. Here are all possibilities:

$$(0, 0) \quad (0, 1) \quad (1, 0) \quad (1, 1)$$

Note that there are two possibilities for the first entry, and two possibilities for the second, giving a total of $4 = 2 \times 2$ functions overall.

- (2) Suppose that f is a function on $\llbracket n \rrbracket$. We can specify the rule for f by listing, in order, the elements $f(0)$, $f(1)$, $f(2)$, and so on until $f(n-1)$.¹³ There are n possibilities for each, and no other restrictions. Thus the number of possible rules is n , multiplied by itself, n times. Thus the correct count is $n \times n \times n \times \cdots \times n = n^n$. \square

Solution 3.5.

¹³Any argument that mentions “and so on” in fact needs *induction*. We will discuss this more carefully in Section 16.

- (1) The function $f: \mathbb{R} \rightarrow \mathbb{R}$, where $f(x) = x^2$, is not injective because $f(1) = f(-1)$. It is not surjective because -1 is not a square of a real number.
- (2) The function $g: \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}$, where $g(x) = x^2$, is injective. For, suppose that x and y are non-negative reals. Suppose that $g(x) = g(y)$. Thus $x^2 = y^2$ and so $x^2 - y^2 = 0$. We factor and deduce that $(x + y)(x - y) = 0$. Note that, since x and y are non-negative, then $x + y = 0$ if and only if $x = y = 0$. In this case we are done. Suppose instead that $x + y > 0$. Dividing, we find that $x - y = 0$. Thus $x = y$, as desired.
On the other hand, g is not surjective because -1 is not a square of a positive real number.
- (3) The function $h: \mathbb{R} \rightarrow \mathbb{R}_{\geq 0}$, where $h(x) = x^2$, is not injective, because $h(-1) = h(1)$. It is surjective because every non-negative real number has a real square root. A careful proof of this requires the *completeness* property of the real numbers.
- (4) The function $k: \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$, where $k(x) = x^2$, is a bijection. It is injective for the same reason g is injective. It is surjective for the same reason h is surjective. \square

Solution 3.7. Recall that

$$n! = n \times (n-1) \times (n-2) \times \dots \times 2 \times 1$$

is the *factorial* of n . We claim that the number of permutations of $\llbracket n \rrbracket$ is $n!$ (pronounced “ n factorial”).

Suppose that $f: \llbracket n \rrbracket \rightarrow \llbracket n \rrbracket$ is a permutation. We may represent f as via the list $(f(0), f(1), \dots, f(n-1))$. There are n possibilities for $f(0)$. Since f is a bijection, it is an injection. Thus we know that $f(1) \neq f(0)$. Thus there are $n-1$ possibilities for $f(1)$. By the same logic, we have that $f(2) \neq f(1)$ and $f(2) \neq f(0)$. Thus there are $n-2$ possibilities for $f(2)$. Continuing in this way, we have $n-k$ possibilities for $f(k)$. Thus, when we reach $f(n-1)$ there is only one possibility for it. We deduce that there are $n! = n \times (n-1) \times (n-2) \times \dots \times 2 \times 1$ permutations of $\llbracket n \rrbracket$. \square

Solution 3.13. Suppose that X is a set. Suppose that $g: \mathcal{P}(X) \rightarrow X$ is an injection. We define a function $f: X \rightarrow \mathcal{P}(X)$ as follows.

Suppose that $a \in X$. Note that, as g is injective, there is at most one (and perhaps no) subset $A \subset X$ so that $g(A) = a$. That is, either $g(A) = a$ for some unique $A \subset X$ or there is no such A . In the former case we take $f(a) = A$. In the latter case we take $f(a) = \emptyset$. Since g is a function, we find that f is surjective. This contradicts Theorem 3.12. \square

Solution 4.8. A solution here relies on our definition of $m \times n$.

A geometric definition takes $m \times n$ to be the number of unit squares in a m -by- n rectangle. The squares are indexed by ordered pairs from $\llbracket m \rrbracket \times \llbracket n \rrbracket$. This gives a bijection from $\llbracket m \rrbracket \times \llbracket n \rrbracket$ to the set of squares, and we are done. [This proof relies on our intuitions about the plane \mathbb{R}^2 ; however this is one of the things we were hoping to understand using cartesian products.]

A recursive definition instead assumes (of \times) that for all m we have:

- (1) $m \times 0 = 0$ and
- (2) for all n , we have $m \times (n + 1) = m \times n + m$.

Now the proof that $\llbracket m \rrbracket \times \llbracket n \rrbracket$ has the correct cardinality requires induction, and the following lemma: If X and Y are disjoint finite sets then $|X \cup Y| = |X| + |Y|$. \square

Solution 4.10. The set $A \times B$ consists of all ordered pairs (a, b) where a lies in A and b lies in B . Suppose that A is the empty set. Then there are no such elements a . Thus there are no such ordered pairs.

The argument when B is empty is similar. \square

Solution 4.23.

- (1) Here are two binary strings of length five:

11001 01010

In general, if $b_0b_1b_2b_3b_4$ is a binary string, then there are two possibilities for each of the bits b_i . Thus the number of binary strings of length five is $2^5 = 32$.

- (2) The reasoning above generalises to any $n \in \mathbb{N}$; so there are 2^n binary strings of length n . In particular, there is exactly one binary string of length zero - the empty string $\epsilon_{\mathcal{B}}$.
- (3) Suppose that w is a binary string of length n having exactly one bit which is 1. Thus the other bits are all zeros. There are five such strings of length five.

10000 01000 00100 00010 00001

In general, the string w is completely determined by the position (also called the *index*) of the non-zero bit. There are n choices for this position, thus there are n such binary strings.

- (4) Suppose that w is a binary string of length n having exactly two bits which are 1. Thus the other bits are all zeros. There are ten such strings of length five.

11000 10100 10010 10001 01100
01010 01001 00110 00101 00011

As in the previous exercise, w is determined by the positions of the non-zero bits. Suppose that these positions are i and j . Since i is a position in w , we have $0 \leq i < n$, and similarly for j . If we swap the roles of i and j we obtain the same string. Thus, to avoid counting this string twice, we introduce the assumption that $i < j$.

We have reduced the problem to that of counting the pairs (i, j) so that $0 \leq i < j < n$. We note that, if i is fixed, then there are $n - i - 1$ possibilities for j . Thus the number of such pairs is

$$(n-1) + (n-2) + \cdots + 2 + 1 = \frac{n(n-1)}{2}$$

Checking our work with $n = 5$ we obtain $(5 \times 4)/2 = 10$. \square

Solution 5.8. Each proof relies (in a slightly different way) on the similarity between

- how the union operator acts on sets and
- how the word “or” acts on properties.

We will also use Lemma 1.16 repeatedly; that is, to prove an equality of sets it suffices to prove that each contains the other.

- (1) Taking $Y = \emptyset$ we apply Lemma 5.6 and deduce that $X \subset X \cup \emptyset$.

To prove the opposite inclusion, suppose that x lies in $X \cup \emptyset$. Thus x lies in X or the empty set. However, the empty set contains no elements (Definition 1.6) thus x lies in X . Thus $X \cup \emptyset \subset X$. By Lemma 1.16 we are done.

- (2) Suppose that x lies in $(X \cup Y) \cup Z$. Then x lies in X or Y , or in Z . We deduce that x lies in X , or in Y or Z . Thus x lies in $X \cup (Y \cup Z)$. Thus $(X \cup Y) \cup Z \subset X \cup (Y \cup Z)$.

For the opposite inclusion, suppose that x lies in $X \cup (Y \cup Z)$. Then x lies in X , or in Y or Z . We deduce that x lies in X or Y , or in Z . Thus x lies in $(X \cup Y) \cup Z$. Thus $X \cup (Y \cup Z) \subset (X \cup Y) \cup Z$. By Lemma 1.16 we are done.

- (3) Suppose that x lies in $X \cup Y$. Thus x lies in X or in Y . That is, x lies in X or x lies in Y . Thus x lies in Y or x lies in X . Thus x lies in $Y \cup X$. Thus $X \cup Y \subset Y \cup X$.

The opposite inclusion is proved in the same way, swapping the roles of X and Y .

- (4) Suppose that $X \subset Y$. Suppose that x lies in $X \cup Y$. Then x lies in X or in Y . Since $X \subset Y$ in either case x lies in Y . Thus $X \cup Y \subset Y$. The opposite inclusion follows from Lemma 5.6. From Lemma 1.16 we deduce that $X \cup Y = Y$.

Suppose that $X \cup Y = Y$. By Lemma 5.6 we have that $X \subset X \cup Y$. Since $X \cup Y = Y$ we deduce that $X \subset Y$.

(5) By Lemma 5.6 we have that $X \subset X \cup X$.

For the opposite inclusion, suppose that x lies in X or in X . That is, x lies in X or x lies in X . Thus x lies in X . We deduce that $X \cup X \subset X$. From Lemma 1.16 we deduce that $X \cup X = X$. \square

Solution 5.21. By Lemma 1.16 to prove an equality it suffices to check two inclusions.

Suppose that x lies in $X \cap (Y \cup Z)$. Thus x lies in X and x lies in Y or Z . Thus x lies in X and Y or x lies in X and Z . Thus x lies in $X \cap Y$ or x lies in $X \cap Z$. Thus x lies in $(X \cap Y) \cup (X \cap Z)$ as desired.

Suppose that x lies in $(X \cap Y) \cup (X \cap Z)$. Then we reverse the above steps to find that x lies in $X \cap (Y \cup Z)$, as desired.

The proof that union distributes over intersection is similar, and we omit it. \square

Solution 5.23. By Lemma 1.16 to prove an equality it suffices to check two inclusions.

Suppose that x lies in $X - (Y \cup Z)$. Thus x lies in X and does not lie in Y or in Z . Since x is not in Y or in Z we deduce that x is not in Y and x is not in Z . Thus x lies in X and not in Y and not in Z . Thus x lies in X and not in Y and lies in X and not in Z . Thus x lies in $X - Y$ and lies in $X - Z$. Thus x lies in $(X - Y) \cap (X - Z)$, as desired.

Suppose that x lies in $(X - Y) \cap (X - Z)$. Reversing the above steps shows that x lies in $X - (Y \cup Z)$, as desired.

The proof of the second equality is similar, and we omit it. \square

Solution 6.6. Suppose that f is surjective. Thus, for each $y \in Y$ there is some $x \in X$ so that $f(x) = y$. For each y we choose one such x and denote it $g(y)$.¹⁴ Thus $g: Y \rightarrow X$ is a function. We now compute as follows:

$$\begin{aligned} (f \circ g)(y) &= f(g(y)) && \text{definition of } \circ \\ &= y && \text{definition of } g(y) \\ &= \text{Id}_Y(y) && \text{definition of } \text{Id}_Y \end{aligned}$$

Since this holds for all y in Y , we deduce that $f \circ g = \text{Id}_Y$, as desired.

¹⁴When Y is infinite, picking the elements $g(y)$ requires the *axiom of choice*.

Suppose that g is a right inverse for f . Suppose that y is any element of Y . Let $x = g(y)$. We compute as follows:

$$\begin{aligned}
 y &= \text{Id}_Y(y) && \text{definition of } \text{Id}_Y \\
 &= (f \circ g)(y) && g \text{ is a right inverse for } f \\
 &= f(g(y)) && \text{definition of } \circ \\
 &= f(x) && \text{definition of } x
 \end{aligned}$$

Since this holds for all y in Y , we deduce that f is surjective, as desired.

Suppose that f is bijective. Thus f is injective and surjective. By the above, f has both a left inverse, say g , and a right inverse, say g' . Note that f is a right inverse for g and a left inverse for g' . Again applying the above, we deduce that g is surjective and g' is injective. Suppose that y is any element of Y . We compute as follows:

$$\begin{aligned}
 g(y) &= g(\text{Id}_Y(y)) && \text{definition of } \text{Id}_Y \\
 &= g((f \circ g')(y)) && g' \text{ is a right inverse for } f \\
 &= (g \circ (f \circ g'))(y) && \text{definition of } \circ \\
 &= ((g \circ f) \circ g')(y) && \text{associativity of } \circ \\
 &= (g \circ f)(g'(y)) && \text{definition of } \circ \\
 &= \text{Id}_X(g'(y)) && g \text{ is a left inverse for } f \\
 &= g'(y) && \text{definition of } \text{Id}_x
 \end{aligned}$$

Thus $g = g'$ is the desired inverse for f . Note also that if g'' is another inverse for f then the above computation (with g'' replacing g') shows that $g = g''$. Thus f has only one inverse, as desired.

Suppose that f has an inverse, say g . So g is both a right and left inverse for f . Thus by the above f is both injective and surjective. Thus f is bijective, as desired. \square

Solution 6.8. Suppose that f and g are both injective. Suppose that x and x' lie in X . Suppose that $(g \circ f)(x) = (g \circ f)(x')$. Since g is injective, we deduce that $f(x) = f(x')$. Since f is injective, we deduce that $x = x'$, as desired.

Suppose that f and g are both surjective. Suppose that z lies in Z . Since g is surjective, there is some y in Y so that $g(y) = z$. Since f is surjective, there is some x in X so that $f(x) = y$. Thus $(g \circ f)(x) = z$, as desired. \square

Solution 7.4.

(1) We list the solutions to $x + y = 2$ over \mathbb{N} . They are:

$$(0, 2), (1, 1), (2, 0)$$

These are all of the elements of P . Since $(0,0)$ is not in P , we have that P is not reflexive. Since the formula defining P is symmetric in x and y , we have that P is symmetric. (This can also be proved directly, by checking the ordered pairs.) Since $(0,2)$ and $(2,0)$ lie in P but $(0,0)$ does not, P is not transitive.

- (2) We list the solutions to $x - y \leq 2$ over \mathbb{N} . They are, for $n, k \in \mathbb{N}$:

$$(n+2, n), (n+1, n), (n, n), (n, n+1), \dots, (n, n+k), \dots$$

Since (n, n) lies in Q for all n , we have that Q is reflexive. Since $(0,3)$ lies in Q but $(3,0)$ does not, Q is not symmetric. Since $(4,2)$ and $(2,0)$ lie in Q but $(4,0)$ does not, Q is not transitive.

- (3) We list the solutions to $|x - y| \leq 2$ over \mathbb{N} . They are, for $n \in \mathbb{N}$:

$$(n+2, n), (n+1, n), (n, n), (n, n+1), (n, n+2)$$

Since (n, n) lies in R for all n , we have that R is reflexive. Since the formula defining R is symmetric in x and y , we have that R is symmetric. Since $(4,2)$ and $(2,0)$ lie in Q but $(4,0)$ does not, R is not transitive. \square

Solution 7.8. Recall that an equivalence relation E on X is a subset of X^2 . Since $X = \llbracket 4 \rrbracket$ we may visualise X^2 as a four-by-four grid of squares. We visualise E by filling in some of the squares of the grid – blank squares do not belong to E . Finally, we give each filled square a colour, and insist that filled squares in the same row or column receive the same colour. (The reason for this will be explained when we discuss *equivalence classes*.) All equivalence relations on $\llbracket 4 \rrbracket$, represented in this fashion, are drawn in Figure A.1. Each of the properties of an equivalence relation places a condition on the diagrams of Figure A.1.

- Since E is reflexive, the squares on the diagonal (running from the upper left to lower right in each diagram) are all filled.
- Since E is symmetric, each diagram has a reflection symmetry across the diagonal.
- Since E is transitive, there is a “Tetris” effect in the diagram. Suppose that the square (x, y) , in row x and column y , is filled. Then for every filled square in row y , say (y, z) , the corresponding square, here (x, z) , is filled in row x .

On the other hand, if a diagram follows these rules, then it encodes an equivalence relation. We now generate the diagrams as follows.

- (1) The diagonal gives the identity relation.
- (2) Given a diagram of an equivalence relation (say the identity) we can fill in a single additional square. We then use symmetry

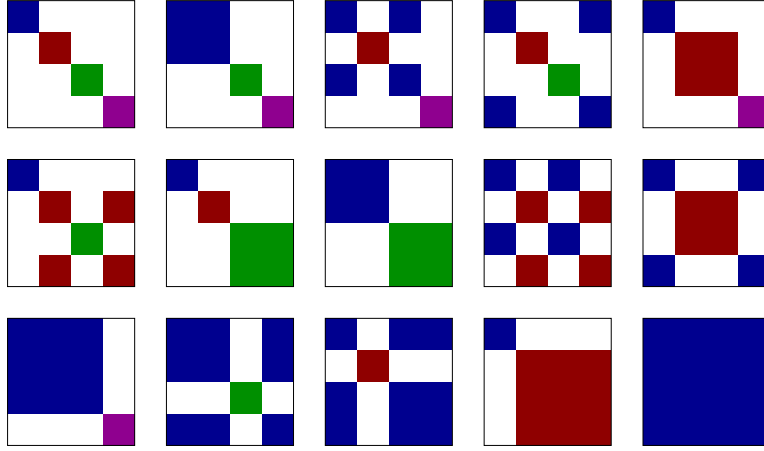


FIGURE A.1. Equivalence relations on $X = \llbracket 4 \rrbracket$. Drawing style inspired by Tilman Piesk [8] who presents the case of $X = \llbracket 5 \rrbracket$.

and transitivity to fill in the smallest number of squares needed to make the diagram that of an equivalence relation.

Starting with the identity relation the above procedure gives the next six diagrams. Starting with one of those, we obtain the next seven diagrams. Finally, starting with one of those we obtain the final diagram, of the universal relation.

Our list is complete because every equivalence is obtained from the identity relation by adding some number (perhaps zero) of squares. Our list is irredundant because all of the diagrams are distinct. \square

Solution 8.3.

- (1) We list the partitions of $X = \llbracket 4 \rrbracket$ by listing those with smaller parts before those with larger parts.

0|1|2|3 01|2|3 02|1|3 03|1|2 0|12|3

0|13|2 0|1|23 01|23 02|13 03|12

012|3 013|2 023|1 0|123 0123

If the largest part of a partition is a singleton, then all parts are singletons and we obtain 0|1|2|3. To obtain more partitions from this, we combine any two; there are six ways to do this. After this we consider the partitions with two parts of size two; there are three of these. Finally, there are four partitions with a part of size three and one partition with a single part. Thus there are 15 partitions of $\llbracket 4 \rrbracket$.

- (2) We count the partitions of $X = \llbracket n \rrbracket$ with exactly two parts, say P and Q . Note that $Q = X - P$ is determined by P . Thus it suffices to count the number of subsets of X which are non-empty and proper. There are $2^n - 2$ of these. However, these come in complementary pairs P and $X - P$. So dividing by two gives the desired lower bound. \square

Solution 8.6. Each colour in each diagram in Exercise 7.8 corresponds to one equivalence class. As a consequence,

- the equivalence classes of the equivalence relations in the solution to Exercise 7.8 are exactly
- the parts of the partitions given in the solution to Exercise 8.3(1). \square

Solution 8.7. There are twelve equivalence classes – one for every month of the year. (Note that this assumes that in each month there is at least one person born in that month.)

As a further exercise: Suppose that D is the equivalence relation on the set of people where $x Dy$ if x and y are born on the same day of the same month. Count the number of equivalence classes for D . \square

Solution 8.13. We recall that for $(p, q), (r, s) \in \mathbb{N}^2$ we have

$$(p, q)E(r, s) \quad \text{if and only if} \quad p + s = r + q$$

Since $p + q = p + q$ we deduce that E is reflexive. Since $p + s = r + q$ implies $r + q = p + s$ we deduce that E is symmetric.

Transitivity is more interesting. Suppose that $(p, q)E(r, s)$ and $(r, s)E(t, u)$. Thus $p + s = r + q$ and $r + u = t + s$. We add these equations to obtain

$$p + s + r + u = r + q + t + s$$

Addition in \mathbb{N} is *cancellative* – that is $x + y = x + z$ if and only if $y = z$. Thus in the equation above we may cancel the terms $(r$ and $s)$ appearing on both sides. This gives $p + u = t + q$, as desired. \square

Solution 10.4.

- (1) Suppose that m , n , and ℓ are integers.

Since $m = 1 \times m$ we have that $m|m$. Thus divides is reflexive.

Suppose that $\ell|n$ and $n|m$. So there are integers k and h so that $n = k \times \ell$ and $m = h \times n$. Substituting, we have that $m = (h \times k) \times \ell$. Thus $\ell|m$. So divides is transitive.

Note that $1|2$, but 2 does not divide 1. Thus divides is not symmetric.

- (2) Suppose that m is an integer. Then $m = m \times 1 = (-m) \times (-1)$. Thus 1 and -1 divide m .
- (3) Suppose that m is an integer. Then $0 = 0 \times m$. Thus m divides zero.
- (4) Suppose that m is an integer. Suppose that zero divides m . Thus there is some k so that $m = k \times 0$. Thus $m = 0$. Thus zero divides only itself. \square

Solution 10.8. Note that $a - a = 0 = 0 \times n$. Thus $a \equiv a \pmod{n}$. Thus the relation is reflexive.

Suppose that $a \equiv b \pmod{n}$. So n divides $a - b$. So there is an integer k so that $a - b = k \times n$. Thus $b - a = (-k) \times n$ and so n divides $b - a$. Thus $b \equiv a \pmod{n}$. Thus the relation is symmetric.

Suppose that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Thus there are integers h and k so that

$$a - b = h \times n \quad \text{and} \quad b - c = k \times n$$

Adding these equations we have

$$(a - b) + (b - c) = h \times n + k \times n$$

and thus

$$a - c = (h + k) \times n$$

Thus $a \equiv c \pmod{n}$. Thus the relation is transitive and we are done. \square

Solution 10.10.

- If $a \equiv b \pmod{0}$ then $a - b$ is a multiple of zero: that is, $a = b$. So we have $[a]_0 = \{a\}$ for any integer a .
- Suppose that a and b are integers. Thus $a = b + (a - b) \times 1$. Thus $a \equiv b \pmod{1}$, as desired.
- Suppose that $a \equiv b \pmod{n}$. So $a = b + kn$ for some integer k . Thus $a = b + (-k) \times (-n)$. We deduce that $a \equiv b \pmod{-n}$. \square

Solution 10.11.

- Suppose that m is an integer. Note that $m - (m - n) = n = 1 \times n$. Thus $m - (m - n)$ is divisible by n . Thus $m \equiv m - n \pmod{n}$. Similarly, $m - (m + n) = -n = (-1) \times n$. Thus $m \equiv m + n \pmod{n}$, as desired.
- Suppose that r and r' lie in $\llbracket n \rrbracket$. If $r = r'$ then $r - r' = 0$. Since $n|0$ we have that $r \equiv r' \pmod{n}$, as desired. Suppose that $r \equiv r' \pmod{n}$. So n divides $r - r'$. So there is some integer k so that $r - r' = k \times n$. We have two cases: either $r \geq r'$ or $r' \geq r$.

Suppose that $r \geq r'$. Then $r - r'$ is non-negative. Since n is positive, we deduce that k is non-negative. If $k = 0$ then $r = r'$ and we are done. If $k > 0$ then $r - r' = k \times n \geq n$. However, $r - r' \leq n - 1$, a contradiction.

Suppose that $r' \geq r$. Thus $r - r'$ is non-positive. Since n is positive, we deduce that k is non-positive. If $k = 0$ then $r = r'$ and we are done. If $k < 0$ then $r - r' = k \times n \leq -n$. However, $r - r' \geq 1 - n$, a contradiction.

- Let

$$\mathcal{E} = \{[r]_n \mid r \in \mathbb{Z}\}$$

By the above \mathcal{E} has n elements. We claim that $\mathcal{E} = \mathbb{Z}/n\mathbb{Z}$: that is, these are all of the equivalence classes of the relation.

We first deal with the non-negative integers. Suppose that $m < n$. In this case m lies in \mathbb{Z} and we are done. Suppose now that $m \geq n$. Suppose also, for a contradiction, that $[m]_n$ does not lie in \mathcal{E} . We may assume that m is the least such positive integer.¹⁵ Thus $m - n$ is non-negative and less than m . By the above $[m]_n = [m - n]_n$. Thus $[m - n]_n$ does not lie in \mathcal{E} . This contradicts our assumption that m was minimal.

Now suppose that $m < 0$. Suppose for a contradiction that $[m]_n$ does not lie in \mathcal{E} . We may assume that m is the greatest such negative integer. Note that $m + n > m$. By the above we have $[m + n]_n = [m]_n$. If $m + n \geq 0$ then we contradict the previous paragraph. If $m + n < 0$ then we contradict the assumed maximality of m . In either case we are done. \square

Solution 10.17.

- (1) Using the rules of exponents and modular arithmetic we compute as follows:

$$\begin{array}{ll}
 3^{20} \equiv (3^2)^{10} \pmod{7} & \text{because } 20 = 2 \times 10 \\
 \equiv 9^{10} \pmod{7} & 3^2 = 9 \\
 \equiv 2^{10} \pmod{7} & 9 \equiv 2 \pmod{7} \\
 \equiv (2^5)^2 \pmod{7} & 10 = 5 \times 2 \\
 \equiv (32)^2 \pmod{7} & 2^5 = 32 \\
 \equiv 4^2 \pmod{7} & 32 \equiv 4 \pmod{7} \\
 \equiv 16 \pmod{7} & 4^2 = 16 \\
 \equiv 2 \pmod{7} & 16 \equiv 2 \pmod{7}
 \end{array}$$

¹⁵This requires the *well-ordering principle* proven later as Theorem 16.11.

- (2) Using the rules of exponents and modular arithmetic we compute as follows:

$$\begin{aligned}
 2^{111} &\equiv (2^3)^{37} \pmod{7} && \text{because } 111 = 3 \times 37 \\
 &\equiv 8^{37} \pmod{7} && 2^3 = 8 \\
 &\equiv 1^{37} \pmod{7} && 8 \equiv 1 \pmod{7} \\
 &\equiv 1 \pmod{7} && 1^{37} = 1
 \end{aligned}$$

- (3) We note that

$$[2]_7 \quad [4]_7 \quad [8]_7 = [1]_7$$

are the equivalence classes of 2^1 , 2^2 , and 2^3 , respectively. Thus

$$2^4 \equiv (2^3 \times 2) \equiv 1 \times 2 \equiv 2 \pmod{7}$$

Thus $[2^k]_7$ depends only on the residue of k modulo 3. Said another way, we have

$$[2^k]_7 = \begin{cases} [1]_7, & \text{if } k \equiv 0 \pmod{3} \\ [2]_7, & \text{if } k \equiv 1 \pmod{3} \\ [4]_7, & \text{if } k \equiv 2 \pmod{3} \end{cases}$$

Since $3^{20} \equiv 0 \pmod{3}$ we have $2^{3^{20}} \equiv 1 \pmod{7}$. □

Solution 11.10.

- From the definition of \wedge we deduce that we may replace $(P \wedge P)$ by P . Thus we have the equality of functions

$$((P \wedge P) \wedge (Q \wedge Q)) = (P \wedge Q)$$

The latter is equal to $(\neg((\neg P) \vee (\neg Q)))$.

- From the definition of \rightarrow we deduce that we may replace $(P \rightarrow (\neg P))$ by $(\neg P)$. Thus we have the equality of functions

$$((P \rightarrow (\neg P)) \rightarrow Q) = ((\neg P) \rightarrow Q)$$

The latter is equal to $((\neg(\neg P)) \vee Q)$ which in turn equals $(P \vee Q)$.

- From the definition of \leftrightarrow we deduce that we may replace $(P \leftrightarrow (\neg P))$ by F . Thus we have the equality of functions

$$((P \leftrightarrow (\neg P)) \leftrightarrow (Q \leftrightarrow (\neg Q))) = (F \leftrightarrow F)$$

Thus this is the function (of arity two) that always equals T. □

Solution 11.13.

- The operator $(P \vee Q)$ gives T if either boolean is T. Thus $(P \vee T)$ gives T. On the other hand $(P \vee F)$ gives T if and only if $P = T$.

- If all of P , Q , and R are F then both of the operators $((P \vee Q) \vee R)$ and $(P \vee (Q \vee R))$ give F. On the other hand, if any of P , Q , or R are T then both operators are also T.
- One of P or Q is T if and only if one of Q or P is T.
- We have that $(P \vee Q) = Q$ does *not* hold if and only if $P = T$ and $Q = F$. But this is also the case for $(P \rightarrow Q)$.
- From the definition of \vee we have $(T \vee T) = T$ and $(F \vee F) = F$. \square

Solution 12.2. We take the order on the strings of length three, form two copies, and prefix the strings in the first copy with 0 and those in the second with 1.

$$\begin{aligned} 0000 &\leq 0001 \leq 0010 \leq 0011 \leq 0100 \leq 0101 \leq 0110 \leq 0111 \leq \\ 1000 &\leq 1001 \leq 1010 \leq 1011 \leq 1100 \leq 1101 \leq 1110 \leq 1111 \end{aligned} \quad \square$$

Solution 12.6. We give the completed truth table.

$$\begin{array}{c} ((P \wedge (P \rightarrow Q)) \rightarrow Q) \\ \hline \begin{array}{ccccccc} T & T & T & T & T & \mathbf{T} & T \\ T & F & T & F & F & \mathbf{T} & F \\ F & F & F & T & T & \mathbf{T} & T \\ F & F & F & T & F & \mathbf{T} & F \end{array} \end{array}$$

The final entries (in bold) are all T, thus the operator is a tautology. \square

Solution 13.4.

- The given sentence is

$$(\forall p (\exists n ((p > n) \wedge \text{PRIME}(p))))$$

which directly translates to

for all p there exists an n so that $p > n$ and p is prime

This does not hold. For consider $p = 4$. Then the sentence after the universal quantifier becomes

there exists an n so that $4 > n$ and 4 is prime

This does not hold, regardless of the n we consider, because 4 is not prime.

- The given sentence is

$$(\exists n (\forall p ((p > n) \wedge \text{PRIME}(p))))$$

which directly translates to

there exists an n such that for any p we have $p > n$ and p is prime

This does not hold. Suppose for a contradiction that such an n exists. Then inner clause holds for all p . So we may take $p = n$. We deduce that $n > n$; this is the desired contradiction.

- The given sentence is

$$(\exists p (\forall n ((p > n) \wedge \text{PRIME}(p))))$$

which directly translates to

there exists a p so that, for any n , we have $p > n$ and p is prime

This does not hold. Again, for a contradiction we suppose that such a p existed. Since the inner clause holds for all n , we may take $n = p$. We deduce that $p > p$; this is the desired contradiction. \square

Solution 13.8.

- Suppose that

$$(\forall x (R(x) \rightarrow S(x)))$$

holds. Suppose further that $(\forall x R(x))$ holds. We must show that $(\forall x S(x))$ holds. So fix any x' in X . Thus $R(x')$ and $(R(x') \rightarrow S(x'))$ both hold. From modus ponens we deduce that $S(x')$ holds. As x' was arbitrary, we deduce that $(\forall x S(x))$ holds, as desired.

- We now show, by means of an example, that

$$((\forall x R(x)) \rightarrow (\forall x S(x)))$$

need not imply

$$(\forall x (R(x) \rightarrow S(x)))$$

Suppose that X is the set $\{0, 1\}$. Suppose that $R(x)$ is the property $(x = 0)$. Suppose that $S(x)$ is the property $(x = 1)$. Then the sentence

$$((\forall x R(x)) \rightarrow (\forall x S(x)))$$

translates to

If every number in X equals zero, then every number in X equals one.

The hypothesis does not hold and neither does the conclusion. Therefore the implication holds (Definition 11.6). On the other hand, the sentence

$$(\forall x (R(x) \rightarrow S(x)))$$

translates to

For any x in X , if $x = 0$ then $x = 1$.

Since $0 \neq 1$, this does not hold. \square

Solution 14.4. Suppose that n is a positive integer. Let \mathcal{P} be the set of primes less than or equal to n which are congruent to 3 modulo four. By Lemma 17.12 the set \mathcal{P} is finite. Let $(p_i)_{i=0}^k$ be list of elements of \mathcal{P} , in order of size. We define M to be the product of these primes. We now define N to be

$$N = \begin{cases} M + 2, & \text{if } M \equiv 1 \pmod{4} \\ M + 4, & \text{if } M \equiv 3 \pmod{4} \end{cases}$$

Thus N is congruent to 3 modulo four. Thus N is odd and so not divisible by two. Also, N is not divisible by any prime p in \mathcal{P} .

By Proposition 16.12, the integer N is divisible by some prime. Thus there is some prime q dividing N . So q does not lie in the set \mathcal{P} . Also, since q is not equal to two, we deduce that q is odd.

Let (q_i) be the list of primes dividing N , ordered by size.¹⁶ Note that none of the q_i lie in \mathcal{P} .

Suppose, for a contradiction, that all of the q_i are congruent to 1 modulo four. Then the same holds of their product, N . This contradicts the definition of N . Thus there is at least one prime q in the list (q_i) which is congruent to 3 modulo four. This completes the proof. \square

Solution 15.4. Suppose that n is an odd integer. Thus there is an integer k so that $n = 2k + 1$. We find that $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Thus n^2 is odd, as desired. \square

Solution 15.7. Suppose that $X \subset Y$. Thus, by Definition 1.10 we have that, every x in X also lies in Y . Recall from Definition 5.10 that we have

$$X \cap Y = \{z \mid z \in X \text{ and } z \in Y\}$$

Note that $X \cap Y \subset X$, by Lemma 5.13.

We now prove that $X \subset X \cap Y$. Suppose that x is any element of X . Since $X \subset Y$ we have that x lies in Y . Thus x lies in X and x lies in Y . So x lies in $X \cap Y$. Thus $X \subset X \cap Y$.

Since $X \cap Y \subset X$ and $X \subset X \cap Y$ Lemma 1.16 tells us that $X \cap Y = X$, as desired. \square

Solution 15.8. Since f and g are bijections, they are both injections. By Lemma 6.7 we have that $g \circ f$ is an injection. Similarly, since f and g are bijections, they are both surjections. By Lemma 6.7 we have that $g \circ f$ is a surjection. Since $g \circ f$ is both an injection and a surjection, it is a bijection, as desired. \square

Solution 15.12. Suppose that p is a sum of three squares: say $p = x^2 + y^2 + z^2$. We now break into cases depending on the residues of

¹⁶This step requires the *fundamental theorem of arithmetic* – see Theorem 17.3.

x , y , and z modulo four. For example, suppose that $x = 4w + b$ where b lies in $\llbracket 4 \rrbracket$. Thus $x^2 = 16w^2 + 8wb + b^2$. Taking this modulo eight we get either 0, 1, or 4. The same holds for y^2 and z^2 . The sum of all three modulo eight is one of the following:

$$\begin{array}{llll} 0 \equiv 0 + 0 + 0 & 1 \equiv 1 + 0 + 0 & 2 \equiv 1 + 1 + 0 & 3 \equiv 1 + 1 + 1 \\ 4 \equiv 4 + 0 + 0 & 5 \equiv 4 + 1 + 0 & 6 \equiv 4 + 1 + 1 & \end{array}$$

In no case do we obtain a residue of seven modulo eight. \square

Solution 15.15. Suppose that, for a contradiction, there is a rational number $r = p/q$ with $r^2 = 3$. Changing the signs of *both* p and q (if needed) we may assume that q is positive. Since $r^2 = (-r)^2$ we may further assume that p is positive.

We now descend. By hypothesis, $p^2 = 3q^2$. So p^2 is a multiple of three. So the same holds of p . Thus we may write $p = 3u$. Thus $q^2 = 3u^2$. We deduce that q is a multiple of three. Thus we may write $q = 3v$. Thus $r = u/v$ where $u < p$ and $v < q$. This completes the descent.

We have shown that if $r = p/q$ then there is a smaller pair of positive numbers u and v having the same ratio. Repeating this indefinitely contradicts the well-ordering principle (Theorem 16.11). \square

Solution 15.16. Suppose that, for a contradiction, there is a rational number $r = p/q$ with $r^3 = 2$. Changing the signs of *both* p and q (if needed) we may assume that q is positive. Note that r^3 has the same sign as r itself. Thus $p > 0$.

We now descend. By hypothesis, $p^3 = 2q^3$. So p^3 , and thus p , is even. Thus we may write $p = 2u$. So $p^3 = 8u^3 = 2q^3$. Thus $q^3 = 4u^3$. We deduce that q is even. Thus we may write $q = 2v$. Thus $q^3 = 8v^3 = 4u^3$. So, finally, $u^3 = 2v^3$. Thus $r = u/v$ where $u < p$ and $v < q$. This completes the descent.

We have shown that if $r = p/q$ then there is a smaller pair of positive numbers u and v having the same ratio. Repeating this indefinitely contradicts the well-ordering principle (Theorem 16.11). \square

Solution 15.19. The smallest number with four distinct prime factors is $2 \times 3 \times 5 \times 7$ which equals 210. As this is less than 1000 we are done. \square

Solution 15.20. Suppose that $r = \epsilon p/q$ where $\epsilon = \pm 1$, where $p \geq 0$, where $q > 0$, where p and q share no common factors, and where $\epsilon = 1$ if $p = 0$. We define $f: \mathbb{Q} \rightarrow \mathbb{N}$ by $f(r) = 2^{\epsilon+1} 3^p 5^q$.

We now show that f is an injection. Suppose that $r = \epsilon p/q$ and $s = \delta u/v$ is a pair of rational numbers. Suppose that $n = f(r) = f(s)$. Since $q > 0$ the number n is greater than or equal to five. By Theorem 17.3

the number n has a unique prime factorisation. Thus we may recover ϵ , p , and q from n . Thus $\epsilon = \delta$, $p = u$, and $q = v$. Thus $r = s$, as desired. \square

Solution 16.4. Suppose that n is a natural number. Let $P(n)$ be the sentence “ n is congruent to zero, one, or two, modulo three”.

We now deal with the base case, where $n = 0$. Since $0 = 3 \times 0$, the number zero congruent to zero modulo three. Thus $P(0)$ holds.

We now deal with the induction step. Suppose that k is a natural number. Suppose that $P(k)$ holds. Thus there are natural numbers ℓ and i so that $k = 3\ell + i$ and $i \leq 2$. Adding one we find that $k + 1 = 3\ell + i + 1$. If $i = 0$ or 1 we are done. If $i = 2$ then $k + 1 = 3\ell + 3 = 3(\ell + 1)$ and again we are done. Thus $P(k)$ implies $P(k + 1)$, establishing the induction step.

Thus we are done by induction. \square

Solution 16.9. With notation as in Theorem 16.6, we take $F(k, \ell) = k + \ell$ and $a = 0$. This gives a function $f: \mathbb{N} \rightarrow \mathbb{N}$ where

- $f(0) = 0$ and
- $f(n + 1) = n + 1 + f(n)$.

We compute the first few values of f .

$$\begin{aligned} f(0) &= 0 \\ f(1) &= 0 + 1 + f(0) = 1 \\ f(2) &= 1 + 1 + f(1) = 2 + 1 = 3 \\ f(3) &= 2 + 1 + f(2) = 3 + 2 + 1 = 6 \\ f(4) &= 3 + 1 + f(3) = 4 + 3 + 2 + 1 = 10 \\ f(5) &= 4 + 1 + f(4) = 5 + 4 + 3 + 2 + 1 = 15 \end{aligned}$$

This leads us to the following.

Lemma A.2. *The sum of the first n natural numbers equals $\frac{(n+1)n}{2}$.*

Since $f(n)$ is defined by recursion, we give a proof by induction.

In the base case we have $f(0) = 0 = \frac{(0+1)0}{2}$

For the induction step, we suppose that $f(k) = \frac{(k+1)k}{2}$. We now compute as follows.

$$\begin{aligned}
 f(k+1) &= k+1 + f(k) && \text{definition of } f \\
 &= k+1 + \frac{(k+1)k}{2} && \text{induction hypothesis} \\
 &= \frac{2(k+1)}{2} + \frac{k(k+1)}{2} && \text{common denominator} \\
 &= \frac{(k+2)(k+1)}{2} && \text{add and factor}
 \end{aligned}$$

Since the base case and the induction step hold we are done by induction. \square

Solution 17.6.

- (1) Suppose that $S = b_0b_1b_2b_3 \dots b_{n-1}$ is a binary string of length n . Suppose also that, for all $i > 0$ we have that b_{i+1} is different from b_i . Then b_0 determines b_1 , which determines b_2 , and so on. Thus b_0 determines S . Thus there are exactly two possibilities for S : either S begins 01010... or begins 10101....
- (2) Suppose that F_n is the set of binary strings of length n where no adjacent bits are both zero. Suppose that f_n is the number of such strings. We now gather a bit of data.

n	f_n	F_n
0	1	ϵ_B
1	2	0, 1
2	3	01, 10, 11
3	5	010, 011, 101, 110, 111
4	8	0101, 0110, 0111, 1010, 1011, 1101, 1110, 1111
5	13	01010, 01011, 01101, 01110, 01111, 10101, 10110, 10111, 11010, 11011, 11101, 11110, 11111

Equipped with this, we now claim that $f_{n+2} = f_{n+1} + f_n$ for all $n \geq 0$. [That is, the numbers f_n are the Fibonacci numbers (with indexing off by one).]

We prove this as follows. Suppose that F_n^0 is the set of those strings in F_n ending with a zero. Suppose that F_n^1 is the set of those strings in F_n ending with a one. For example, $F_4^0 = \{0110, 1010, 1110\}$ and $F_4^1 = \{0101, 0111, 1011, 1101, 1111\}$ contain three and five strings, respectively. Let $f_n^0 = |F_n^0|$ and $f_n^1 = |F_n^1|$. Note that $f_n = f_n^0 + f_n^1$.

Thus, to prove that $f_{n+2} = f_{n+1} + f_n$ it suffices to prove that $f_{n+2}^0 = f_n$ and $f_{n+2}^1 = f_{n+1}$. And to prove that it suffices to find bijections $F_{n+2}^0 \rightarrow F_n$ and $F_{n+2}^1 \rightarrow F_{n+1}$.

Suppose that w is a binary string in F_{n+2}^1 . Thus the final bit of w is a 1. We delete this last bit to obtain the string w' . Note that w' lies in F_{n+1} . Furthermore, every element of F_{n+1} is obtained, exactly once, in this way.

Suppose that w is a binary string in F_{n+2}^0 . So the last bit of w is a 0. Since adjacent zeros are not allowed, the second to last bit of w is a 1. We delete these two final bits to obtain w'' . Note that w'' lies in F_n . Furthermore, every element of F_n is obtained, exactly once, in this way. \square

Solution 17.10.

- (1) Suppose that n is a natural number. Suppose that $g: \llbracket n+1 \rrbracket \rightarrow \llbracket n \rrbracket$ is an injection. By Lemma 6.5 we have a left inverse $f: \llbracket n \rrbracket \rightarrow \llbracket n+1 \rrbracket$ which is a surjection. This contradicts Theorem 17.8.
- (2) Suppose that m and n are natural numbers, with $m > n$. Suppose that $g: \llbracket m \rrbracket \rightarrow \llbracket n \rrbracket$ is an injection. Note that $\llbracket n+1 \rrbracket$ is a subset of $\llbracket m \rrbracket$. Thus the restriction $h = g|_{\llbracket n+1 \rrbracket}$ is an injection of $\llbracket n+1 \rrbracket$ to $\llbracket n \rrbracket$. This contradicts (1).
- (3) Suppose that n is a natural number. Suppose that $g: \mathbb{N} \rightarrow \llbracket n \rrbracket$ is a bijection. Thus g is an injection. Thus $h = g|_{\llbracket n+1 \rrbracket}$ is also an injection. This contradicts (1).
- (4) Suppose that we are given bijections from X to $\llbracket m \rrbracket$ and to $\llbracket n \rrbracket$. By inverting and composing we obtain a bijection from $\llbracket m \rrbracket$ to $\llbracket n \rrbracket$. In particular we have injections from $\llbracket m \rrbracket$ to $\llbracket n \rrbracket$ and from $\llbracket n \rrbracket$ to $\llbracket m \rrbracket$. Thus, by (2) we have $m \leq n$ and $n \leq m$. Thus $m = n$.
- (5) Suppose that X is a finite set. Since cardinality is unique, we may assume that $X = \llbracket n \rrbracket$ for some $n \in \mathbb{N}$. Suppose that $f: \llbracket n \rrbracket \rightarrow \llbracket n \rrbracket$ is a function.

Suppose that f is not a surjection. Thus $\llbracket n \rrbracket$ is non-empty (and so $n > 0$). Post-composing with a permutation we may assume that $n-1$ does not lie in the image of f . Restricting the codomain to $\llbracket n-1 \rrbracket$, we obtain a function $f': \llbracket n \rrbracket \rightarrow \llbracket n-1 \rrbracket$. By (1) we have f' is not an injection, and thus neither is f .

For the opposite direction, suppose that f is not an injection. Thus $\llbracket n \rrbracket$ is non-empty (and so $n > 0$). Pre-composing with a permutation we may assume that $f(\ell) = f(n-1)$ for some $\ell < n-1$. Restricting the domain to $\llbracket n-1 \rrbracket$, we obtain a function $f': \llbracket n-1 \rrbracket \rightarrow \llbracket n \rrbracket$. By Theorem 17.8 we have that f' is not a surjection, and thus neither is f . \square

APPENDIX B. GLOSSARY

We give very short and informal explanations of some of the more common bits of mathematical jargon.

axiom – A mathematical statement assumed to hold, without further justification.

conjecture – A mathematical statement which is thought to hold.

corollary – A mathematical statement, following directly from a previously proved statement.

definition – A name for a mathematical object that already exists.

implication – A mathematical statement of the form “if P then Q ”. Here P and Q are themselves mathematical statements called the *hypothesis* and *conclusion* of the implication.

lemma – A mathematical statement, usually part of a larger result, followed by a proof.

proposition – A mathematical statement, usually not as substantial as a theorem, followed by a proof.

theorem – A mathematical statement followed by a proof.

INDEX

- \diamond , end of definition, remark, or similar, 1
- \square , end of proof, axiom, or similar, 2
- \mathbb{N} , natural numbers, Notation 1.3, 1
- \mathbb{Z} , integers, Notation 8.15, 25
- \mathbb{Q} , rational numbers, 28
- \mathbb{R} , real numbers, Example 2.11, 5
- \mathbb{C} , complex numbers, 30
- $\llbracket n \rrbracket$, the natural numbers less than n , Notation 1.13, 3
- \emptyset , empty set, Axiom 1.8, 2
- $\{\dots\}$, set, Notation 1.2, 1
- $x \in X$, x is an element of X , Notation 1.4, 2
- $x \notin X$, x is not an element of X , Notation 1.4, 2
- $\{x \in X \mid S(x)\}$, the set of $x \in X$ so that $S(x)$ holds, Notation 2.5, 4
- $f(Z) = \{f(z) \mid z \in Z\}$, the image of Z under f , Definition 6.12, 19
- $f^{-1}(W) = \{x \in X \mid f(x) \in W\}$, the preimage of W under f ,
Definition 6.13, 19
- $X \subset Y$, X is a subset of Y , Definition 1.10, 3
- $X \cup Y$, union of X and Y , Notation 5.4, 14
- $X \cap Y$, intersection of X and Y , Definition 5.10, 15
- $X - Y$, set-theoretic difference, Definition 5.16, 16
- $\{x, y\}$, unordered pair, Axiom 4.2, 10
- (x, y) , ordered pair, Definition 4.3, 10
- $X \times Y$, cartesian product of X and Y , Definition 4.6, 10
- X^2 , cartesian product of X with itself, 11
- $\mathcal{P}(X)$, power set of X , Axiom 2.2, 4
- $f: X \rightarrow Y$, function from X to Y
informal, Definition 2.8, 5
formal, Definition 4.16, 12
- $f(x)$, image of x under f , Definition 2.10, 5
- Id_X , identity function on X , Definition 2.9, 5
- $g \circ f$, g composed with f , Definition 6.2, 17
- (\dots) , list, Notation 4.19, 12
- $\epsilon_{\mathcal{A}}$, empty string over \mathcal{A} , Definition 4.21, 13
- xRy , relation between x and y , Definition 4.12, 11
- $[x]_E$, equivalence class of x under E , Definition 8.5, 23
- X/E , quotient of X by the equivalence relation E , Notation 8.8, 23
- q_E , quotient map given by E , Notation 8.8, 23
- T, F, booleans, Definition 11.2, 31
- $\neg P$, negation of P , Definition 11.5, 32
- $P \vee Q$, P or Q , Definition 11.6, 32

$P \wedge Q$, P and Q , Definition 11.6, 32
 $P \rightarrow Q$, P implies Q , Definition 11.6, 32
 $P \leftrightarrow Q$, P is equivalent to Q , Definition 11.6, 32
 $\forall x \in X$, for all x in X , Notation 13.2, 38
 $\exists x \in X$, there exists x in X , Notation 13.2, 38

REFERENCES

- [1] Rittaud Benoît and Albrecht Heeffer. The pigeonhole principle, two centuries before Dirichlet. *Mathematical Intelligencer*, 36(2):27–29, 2014. doi:10.1007/s00283-013-9389-1. [51]
- [2] Yale Babylonian Collection, 2022. Images of YBC 07289. <https://collections.peabody.yale.edu/search/Record/YPM-BC-021354>. [44]
- [3] Herbert B. Enderton. *Elements of set theory*. Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1977. [47]
- [4] Euclid. *The thirteen books of Euclid's Elements translated from the text of Heiberg. Vol. I: Introduction and Books I, II. Vol. II: Books III–IX. Vol. III: Books X–XIII and Appendix*. Dover Publications, Inc., New York, 1956. Translated with introduction and commentary by Thomas L. Heath, 2nd ed. [38, 40, 49]
- [5] Euclid. *Elementa (MS. D'Orville 301)*. Stephanos the clerk, Byzantine Empire, 888. https://medieval.bodleian.ox.ac.uk/catalog/manuscript_4146. [40]
- [6] Paul R. Halmos. *Naive set theory*. The University Series in Undergraduate Mathematics. D. Van Nostrand Co., Princeton, N.J.-Toronto-London-New York, 1960. [1, 2, 47]
- [7] Lars-Daniel Öhman. Are induction and well-ordering equivalent? *Math. Intelligencer*, 41(3):33–40, 2019. <https://0-doi-org.pugwash.lib.warwick.ac.uk/10.1007/s00283-019-09898-4>, doi:10.1007/s00283-019-09898-4. [49, 50]
- [8] Tilman Piesk. The 52 partitions of a 5-element set represented by matrices of equivalence relations, 2012. https://en.wikipedia.org/wiki/Equivalence_relation. [61]
- [9] N. J. A. Sloane. Bell numbers, 2022. Entry A000110 in the Online Encyclopedia of Integer Sequences. <http://oeis.org/A000110>. [21]
- [10] Kurt Von Fritz. The discovery of incommensurability by Hippasus of Metapontum. *Annals of Mathematics*, 46(2):242–264, 1945. doi:10.2307/1969021. [44]