Chapter 1

Fundamentals

The natural numbers[1] are

$$1, 2, 3, 4, 5, 6, \ldots.$$

The integers, or whole numbers, are:

$$\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots.$$

So the natural numbers are the positive integers. We write $\mathbb{N}$ to denote the set of all natural numbers and $\mathbb{Z}$ to denote the set of all integers.

1.1 The Pigeonhole Principle

Theorem 1.1 (Pigeonhole Principle)**.** *Let n be a natural number. If $n + 1$ pigeons are placed in n pigeonholes, then some pigeonhole contains at least two pigeons.*

This statement may seem obvious, especially if you consider a specific value of n (for example, the statement for $n = 2$ says that if 3 pigeons are placed in 2 pigeonholes, then some pigeonhole contains more than one pigeon). However, it is still important to give a proof.

Proof. Suppose for a contradiction that the principle is false. This means that there is some natural number n for which $n + 1$ pigeons can be placed in n pigeonholes so that every pigeonhole contains at most one pigeon. Fix such an n and such a placement of pigeons. Since every pigeonhole contains at most one pigeon, the number of pigeons is at most the number of pigeonholes. So $n + 1 \leq n$, a contradiction. We therefore conclude that the principle must be true.[2] □

[1] Be aware that some books and other sources also consider zero to be a natural number; check to avoid confusion.

[2] This proof is a *proof by contradiction*, where we suppose that the statement in question is in fact false. If we can deduce a contradiction from this assumption, then (since we believe mathematics to be free of contradictions) we conclude that the statement therefore cannot be false, and so must be true. This is a very common method of proof.

The Pigeonhole Principle arises frequently as a useful tool for both mathematical and non-mathematical arguments, as in the following examples.

Example (Socks)**.** In my drawer are 10 black socks and 8 white socks. How many socks must I take from the drawer (without looking) to guarantee that I have a matching pair among the socks I have taken out?

Solution. Three socks. To see this, think of each sock as a pigeon, and as you take them out the drawer, imagine that each white sock is placed in a 'white' pigeonhole and each black sock is placed in a 'black' pigeonhole. So socks in the same pigeonhole are the same colour. After three socks have been taken, there are three pigeons (socks) in two pigeonholes, so by the Pigeonhole Principle (with $n = 2$ pigeonholes) some pigeonhole contains more than one sock, so contains a matching pair. □

Note that the '10' and '8' in the question don't contribute to the final answer.

Example (Summing to 10)**.** Prove that for any six not-necessarily-distinct integers each between 1 and 9, either two of these integers are equal, or two of these integers sum to 10.

Solution. Let $x_1, \ldots, x_6$ be the six integers, and create 'pigeonholes' A, B, C, D and E. For each integer $1 \leq j \leq 6$, place the 'pigeon' x_j into a pigeonhole according to the following rule:

$$\text{Put } x_j \text{ in pigeonhole } \begin{cases} A & \text{if } x_j = 1 \text{ or } x_j = 9, \\ B & \text{if } x_j = 2 \text{ or } x_j = 8, \\ C & \text{if } x_j = 3 \text{ or } x_j = 7, \\ D & \text{if } x_j = 4 \text{ or } x_j = 6, \\ E & \text{if } x_j = 5. \end{cases}$$

Note that this rule places each of the 6 integers into one of the five pigeonholes. The Pigeonhole Principle with $n = 5$ therefore implies that some pigeonhole contains at least two of the integers. Choose two integers which lie in the same pot; then these integers are either equal or sum to 10 by definition of the pots (for example, if D contains two integers, then either they are equal or one is 4 and one is 6, giving a sum of 10). □

Sometimes a problem will require you to take some steps before applying the principle, such as in the following example.

Example. (Numbers of friends) Show that at any party with at least $n \geq 2$ guests, there must be two people with the same number of friends present (assume that if X is a friend of Y then Y is also a friend of X).

It isn't immediately clear that we can use the Pigeonhole Principle here, since any person can have $0, 1, 2, \ldots, n-2$ or $n-1$ friends present, that is, there are n possibilities for the number of friends, the same as the number of people. But by splitting into two cases we can successfully apply the principle.

Solution. We consider two cases:

Case 1: There is a guest with no friends present. Since this guest has no friends, the highest number of friends any other guest can have is $n-2$. That is, every guest has $0, 1, 2, \ldots, n-3$ or $n-2$ friends present. So there are $n-1$ possible numbers of friends for each of n guests, so by the Pigeonhole Principle two of the guests must have the same number of friends.

Case 2: Every guest has at least one friend present. In this case every guest has $1, 2, \ldots, n-2$ or $n-1$ friends present (since in this case 0 is ruled out). So again there are $n-1$ possible numbers of friends for each of n guests, so by the Pigeonhole Principle two of the guests must have the same number of friends.[3] □

As shown in these examples, the 'pigeons' may be any discrete[4] object, mathematical or otherwise, and the pigeonholes can be any collections to which pigeons may be assigned. It isn't necessary to refer to 'pigeons' and 'pigeonholes' when applying the Pigeonhole Principle, but to make sure that your answers are accurate, clear and precise you should always do the following things.[5]

1. Say you are applying the "Pigeonhole Principle", so that the reader knows what you are doing.

2. Make sure it is clear what your 'pigeons' and 'pigeonholes' are.

3. Make sure that your rule for assigning pigeons to pigeonholes is clear and unambiguous. Will *every* pigeon be assigned to *exactly one* pigeonhole?[6] If this is not obvious then explain it.

4. Show that the conclusion of the Pigeonhole Principle, that some pigeonhole contains at least two pigeons, implies whatever result you are trying to prove.

The next result is a more general version of the Pigeonhole Principle. The ceiling of a real number x, denoted $\lceil x \rceil$, is the smallest integer greater than or equal to x. So, for example, $\lceil \frac{1}{2} \rceil = 1$, $\lceil \frac{7}{3} \rceil = 3$, and $\lceil -6.7 \rceil = -6$, but $\lceil x \rceil = x$ if x is an integer.

Theorem 1.2 (General Pigeonhole Principle)**.** *Let n and k be natural numbers. If n pigeons are placed in k pigeonholes, then some pigeonhole contains at least $\lceil \frac{n}{k} \rceil$ pigeons.*

Proof. Suppose for a contradiction that every pigeonhole contains fewer than n/k pigeons. Then

$$n = \text{number of pigeons} < \frac{n}{k} \cdot (\text{number of pigeonholes}) = \frac{n}{k} \cdot k = n,$$

so $n < n$, a contradiction! So some pigeonhole must contain at least n/k pigeons. Since the number of pigeons in each hole must be an integer, the number of pigeons in this pigeonhole must be at least $\lceil \frac{n}{k} \rceil$.[7] □

[3] Splitting into cases is a common proof technique. When doing this, the most important thing is to ensure that the cases you consider cover all possibilities, that is, that there is no scenario which you have overlooked (if there is, the proof is not valid).

[4] That is, we can only apply the Pigeonhole Principle to *indivisible* objects (i.e. those which only occur in integer quantities). For example, it is not true that if three pints of milk are poured into two cups, some cup must contain at least two pints, because it is quite reasonable to have 1.5 pints in each.

[5] In fact, it is good practice in mathematical writing to follow these rules when applying any result. That is, you should state clearly what result you are using, how you are applying it (e.g. to what are you applying the result?), how you can be sure that any conditions are justified, and how the result applied gives the conclusion you want.

[6] Formally, this says that the rule for assigning pigeons to pigeonholes is a *well-defined function*, and the Pigeonhole Principle itself says that this function is not *injective*.

[7] If you find this final step confusing, think of this: if there are at least 4.5 people in a room, then there must be at least $5 = \lceil 4.5 \rceil$ people in the room, since you cannot have half a person. This is just the same argument applied to $\frac{n}{k}$ rather than 4.5.

Note that the (mean) average number of pigeons per pigeonhole is n/k. So the General Pigeonhole Principle is equivalent to saying that at least one member of any collection of integers is greater than or equal to the average of the collection, a fact you are probably familiar with.

Example. A hand in Bridge consists of 13 cards from a standard 52-card deck. Prove that any such hand must contain at least four cards of the same suit.

Solution. Divide the 13 cards of the hands into four piles, one for each suit (these piles are the 'pigeonholes', and the cards are the 'pigeons'). Since there are 13 cards and 4 piles, by the General Pigeonhole Principle (applied with $n = 13$ and $k = 4$) some pile must contain at least $\lceil \frac{13}{4} \rceil = \lceil 3.25 \rceil = 4$ cards. □

1.2 Sets

A set A is a collection of objects (e.g. integers, lines in the plane, functions, etc.), which we call elements of A. We can define a set by listing its elements, e.g.

$$A = \{2, 3, 5, 7\},$$

or by giving a property[8] which specifies the elements, e.g.

$$B = \{x : x \text{ is a prime number less than } 10\}.$$

Alternatively we can define the set in words, for example, "let C be the set of prime numbers less than 10". For any set A and any object x, either x is an element of A, which we denote by $x \in A$, or x is not an element of A, which we denote by $x \notin A$. There is no other possibility!

The Axiom of Extension states that two sets are equal if and only if they have the same elements. That is, sets A and B are the same if any only if

(i) every element of A is also an element of B, *and*
(ii) every element of B is also an element of A.

So to prove that two sets are equal you must prove that both (i) and (ii) hold. In particular, the sets A and B defined above are in fact the same, even though at first glance they look different. Some other important consequences of the Axiom of Extension are the following:

(a) It does not matter in which order the elements of a set are written, so, for example $\{2, 3, 5, 7\} = \{2, 5, 3, 7\}$.
(b) Elements cannot appear more than once in a set, so, for example $\{1, 2, 2\} = \{1, 2\}$.[9]

[8] When specifying a set by a property, it is best to limit the potential members of the set by writing, for example, $B = \{x \in \mathbb{N} : x \text{ is a prime number less than } 10\}$. This means that x is the set of members of $\mathbb{N}$ which have this property. This avoids having unintended elements. For example, is the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ a member of the set $\{x : x^2 = x\}$?

[9] You should take careful note of this point, as appearances can deceive: the set $\{1, 2, 2\}$ has *two* elements, whilst the set $\{x_1, \ldots, x_n\}$ has n elements if and only if the elements $x_1, \ldots, x_n$ are all distinct.

(c) There is exactly one set with no elements. Indeed, if two sets both have no elements, then they have the same elements as each other, so are the same set! We call this set the empty set, and denote it by $\emptyset$. We say that a set A is non-empty if A is not the empty set (that is, A has at least one element).

We say that a set A is finite if there is a non-negative integer n such that A has n elements, otherwise A is infinite. $\mathbb{N}$ and $\mathbb{Z}$ are two important examples of infinite sets. If A is a finite set, then the size of A, denoted $|A|$, is the number of elements in A. So $|\emptyset| = 0$, $|\{2,3,4\}| = 3$ and so forth.[10] The size of A may also be called the order of A or the cardinality of A.

If A and B are sets such that every element of A is also an element of B, we write $A \subseteq B$ and say that A is a subset of B. So $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. Note that (i) above says that $A \subseteq B$ and (ii) says that $B \subseteq A$. A is a proper, or strict, subset of B if $A \subseteq B$ and $A \neq B$ (so B is not a subset of A); we write $A \subset B$ or $A \subsetneq B$ to denote this.

We say that sets A and B are distinct if they are not equal, that is, if $A \neq B$, and say that A and B are disjoint if $A \cap B = \emptyset$, that is, if A and B have no elements in common. So, for example, the sets $\{2,3\}$ and $\{2,4\}$ are distinct but not disjoint.[11] Confusing these two terms is a common error so please take care to avoid it. If A and B do have an element in common (i.e. are not disjoint, or equivalently $A \cap B \neq \emptyset$) then we say that A intersects B.

Set Operations

We define the following operations on sets, which you will also see in other courses.

- The union of sets A and B is defined by

$$A \cup B = \{x \colon x \in A \text{ or } x \in B\}.$$

  For example, $\{1,2\} \cup \{2,3,4\} = \{1,2,3,4\}$. Similarly, for sets $A_1, \ldots, A_r$, the union is defined by

$$\bigcup_{i=1}^{r} A_i = A_1 \cup \cdots \cup A_r = \{x \colon x \in A_1 \text{ or } x_2 \in A_2 \text{ or } \ldots \text{ or } x \in A_r\}.$$

- The intersection of sets A and B is defined by

$$A \cap B = \{x \colon x \in A \text{ and } x \in B\}.$$

  For example, $\{1,2\} \cap \{2,3,4\} = \{2\}$. Similarly, for sets $A_1, \ldots, A_r$, the intersection is defined by

$$\bigcap_{i=1}^{r} A_i = A_1 \cap \cdots \cap A_r = \{x \colon x \in A_1 \text{ and } x_2 \in A_2 \text{ and } \ldots \text{ and } x \in A_r\}.$$

[10] Note that this definition only applies to finite sets, so our later results on the sizes of sets stipulate that the sets in question are finite.

[11] Exercise: is it true or false that if sets A and B are disjoint then they must be distinct? (Be warned: the answer is not as obvious as it may at first appear)

- The difference of sets A and B is defined by[12]

$$A \setminus B = \{x \colon x \in A \text{ and } x \notin B\}.$$

For example, $\{1,2\} \setminus \{2,3,4\} = \{1\}$, and $\{2,3,4\} \setminus \{1,2\} = \{3,4\}$.[13]

- The Cartesian product of sets A and B is defined by

$$A \times B = \{(a,b) : a \in A \text{ and } b \in B\}.$$

That is, $A \times B$ is the set of *ordered pairs* whose first co-ordinate is a member of A and whose second co-ordinate is a member of B. So, for example, $\{1,2\} \times \{2,3,4\} = \{(1,2),(1,3),(1,4),(2,2),(2,3),(2,4)\}$.

Similarly, the Cartesian product of sets $A_1, \ldots, A_r$ is defined by

$$A_1 \times \cdots \times A_r = \{(x_1, \ldots, x_r) \colon x_1 \in A_1 \text{ and } x_2 \in A_2 \text{ and } \ldots \text{ and } x_r \in A_r\}.$$

So $A_1 \times A_2 \times \cdots \times A_r$ is the set of all ordered r-tuples[14] whose jth co-ordinate is a member of A_j for each j. As with multiplication, given a set A and a non-negative integer n we define

$$A^n = \overbrace{A \times A \times \cdots \times A}^{n \text{ copies of } A}.$$

This should match the definitions of $\mathbb{R}^2$, $\mathbb{R}^3$ etc. with which you are already familiar.

- The power set of a set A is defined by

$$\mathscr{P}(A) = \{X : X \subseteq A\}.$$

So $\mathscr{P}(A)$ is a *set* whose *elements* are the *subsets* of A. For example, if $A = \{1,2,3\}$ then $\mathscr{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$. Note that for any set A, the power set $\mathscr{P}(A)$ contains both $\emptyset$ and A.

Brackets are used to indicate the order in which to perform operations, just as in algebra. So, for example, $(A \setminus B) \setminus C$ means first subtract B from A and then subtract C from the result, whilst $A \setminus (B \setminus C)$ means first subtract C from B, and then subtract the result from A.[15]

A major part of this course will be about counting the sizes of sets. Our first 'counting' result is the following theorem on the size of the power set of a set A.

Theorem 1.3. *If A is a set with $|A| = n$, then $|\mathscr{P}(A)| = 2^n$. Equivalently, a set with n elements has 2^n subsets.*

[12] Some sources write $A - B$ instead of $A \setminus B$, but we will use $\setminus$ throughout this course to avoid confusion with ordinary subtraction.

[13] Note from these examples that difference is not symmetric, unlike union and intersection.

[14] An ordered r-tuple is a sequence of r objects, so an ordered 2-tuple is an ordered pair, and ordered 3-tuple is an ordered triple, and so forth. Make sure that you don't confuse ordered pairs or r-tuples with sets; unlike for sets, the order of an ordered pair or r-tuple matters, so e.g. $(1,2) \neq (2,1)$. Also, elements may be repeated in a pair or r-tuple, so e.g. $(3,3)$ is a valid pair.

[15] Exercise: prove that these two expressions, $(A \setminus B) \setminus C$ and $A \setminus (B \setminus C)$, are not the same in general.

Proof. Let $A = \{x_1, \ldots, x_n\}$. We can form a subset $B \subseteq A$ by proceeding through the elements of A and deciding whether each element should be in B or not. There are two choices for each element (in B or not in B), so $2 \times 2 \times 2 \times \cdots \times 2 = 2^n$ possible ways to choose B. This gives 2^n subsets of B, which are all distinct as if we make a different choice at element x_j then the resulting subsets differ in element x_j.[16] □

Sets containing sets

Sets may contain any object as a member, including other sets (for example, we have just seen that the power set $\mathscr{P}(A)$ of a set A is a set). The crucial thing to remember in such scenarios is that membership (i.e. being an element of a set) is not transitive (that is, it is *not* true that just because $A \in B$ and $B \in C$ we must have $A \in C$). So, for example 9 is *not* a member of the set $\{4, \{5, 9\}\}$: this set has *two* elements, namely the integer 4 and the set $\{5, 9\}$. Similarly, the set $\{\mathbb{N}\}$ has *one* element, namely the set $\mathbb{N}$, even though $\mathbb{N}$ itself is a set with infinitely many elements. Set operations must also be treated carefully, for example, we have

$$\{1, 2, \{3, 4\}\} \cap \{\{1, 2\}, 3, 4\} = \emptyset.$$

Sometimes you will see a set referred to as a class or collection, especially when the members of the set are themselves sets. You should treat the words ‘class’, ‘set’, and ‘collection’ as meaning the same thing.

1.3 The Sum Rule, Product Rule, and Inclusion-Exclusion Formulae

The Sum Rule

The sum rule for sets specifies the size of the union $C \cup D$ of sets C and D which are *disjoint* (remember this means C and D have no elements in common). Note that the theorem does *not* hold for sets which are not disjoint.

Theorem 1.4 (Sum rule for sets)**.** *If C, D are disjoint finite sets then $|C \cup D| = |C| + |D|$.*

Proof. Let $m = |C|$ and $n = |D|$, and write $C = \{x_1, \ldots, x_m\}$ and $D = \{y_1, \ldots, y_n\}$. Then the elements $x_1, \ldots, x_m, y_1, \ldots, y_n$ are all distinct because C and D are disjoint. So

$$C \cup D = \{x_1, \ldots, x_m, y_1, \ldots, y_n\}$$

has $m + n = |C| + |D|$ elements. □

[16] We will see more proofs of a similar nature later. Alternatively, you can prove this by induction (*try this as an exercise*).

The Inclusion-Exclusion Formula

If sets A and B are not disjoint then we cannot apply the sum rule to find $|A \cup B|$. Instead we can calculate this by the inclusion-exclusion formula, *provided* that we know the size of $|A \cap B|$. The form for two sets is the following.

Theorem 1.5 (Inclusion-exclusion for two sets)**.** *Suppose that A and B are finite sets. Then*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

We give two proofs of this result. The first proof uses two applications of the sum rule.

Proof 1. Note that A and $B \setminus A$ are disjoint sets whose union is $A \cup (B \setminus A) = A \cup B$.[17] So by Theorem 1.4 applied with $C = A$ and $D = B \setminus A$ we have

$$|A \cup B| = |A \cup (B \setminus A)| = |A| + |B \setminus A|. \tag{1.1}$$

Next note that $B \cap A$ and $B \setminus A$ are disjoint sets whose union is $(B \cap A) \cup (B \setminus A) = B$. So by Theorem 1.4 applied with $C = B \cap A$ and $D = B \setminus A$ we have

$$|B| = |(B \cap A) \cup (B \setminus A)| = |B \cap A| + |B \setminus A|. \tag{1.2}$$

Combining (1.1) and (1.2) completes the proof. □

The second proof, perhaps simpler, is by a "counting argument".

Proof 2. Each term of the equation counts members of a set, so we consider the contribution any x makes to each side. For this note that for any x we have the following truth table, where 1 denotes True and 0 denotes False.

	(i) $x \in A \cup B$	(ii) $x \in A$	(iii) $x \in B$	(iv) $x \in A \cap B$	(ii) + (iii) - (iv)
$x \notin A, x \notin B$	0	0	0	0	0
$x \notin A, x \in B$	1	0	1	0	1
$x \in A, x \notin B$	1	1	0	0	1
$x \in A, x \in B$	1	1	1	1	1

Now, the contribution of any x to the left hand side of the equation is the entry for x in column (i). Similarly, the contribution of x to the right hand side of the equation is the entry for x in column (ii), plus the entry in the column (iii), minus the entry in column (iv); these values are given in the rightmost column. Since this column is identical to column (i), we conclude that *any* x makes equal contribution to both sides of the equation, and so both sides must be equal. □

[17] Make sure you understand why these sets are disjoint and have the claimed union, and also the similar remark following (1.1).

The use of the inclusion-exclusion formula is that it allows us to calculate information we don't know from information that we have available, as in the following example. Most commonly, as in the following example, we will know the sizes of the sets and their intersections and wish to calculate the size of the union, but other scenarios are possible, such as calculating $|B|$ from $|A|$, $|A \cap B|$ and $|A \cup B|$.

Example. If Facebook tells us that I have 155 friends, you have 274 friends, and we have 25 mutual friends, how many friends do we have between us?

Solution. We can describe this scenario in set terms: let A be the set of my friends and B be the set of your friends. Then we are told that $|A| = 155$ and $|B| = 274$. Also, $A \cap B$ is the set of people who are my friend and your friend, that is, a mutual friend, so $|A \cap B| = 25$. The set of people who are my friend or your friend is $A \cup B$, so applying the inclusion-exclusion formula we find that the number of such people is

$$|A \cup B| = |A| + |B| - |A \cap B| = 155 + 274 - 25 = 304.$$

So we have 304 friends between us. □

To find the size of the union of three sets we sum the set sizes, then subtract the sizes of the pairwise intersections, then add the three-way intersection, as follows.

Theorem 1.6 (Inclusion-exclusion for three sets)**.** *Suppose that A, B and C are finite sets. Then*

$$\begin{aligned}|A \cup B \cup C| =& |A| + |B| + |C| \\ &- |A \cap B| - |A \cap C| - |B \cap C| \\ &+ |A \cap B \cap C|.\end{aligned}$$

This theorem can be proved by a counting argument similar to the second proof of Theorem 1.5, but the truth table is inconveniently large. We could also use the sum rule repeatedly as in the first proof of Theorem 1.5, but many applications are required for this. Instead we will proceed by applying Theorem 1.5 (the inclusion-exclusion formula for two sets) three times, and also making use of a distributivity law which you should be familiar with from VGLA (Theorem 1.12 from that course), which states that for any sets A, B and C we have $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof. Let $Y = B \cup C$. Then Theorem 1.5 implies that

$$|A \cup B \cup C| = |A \cup Y| = |A| + |Y| - |A \cap Y| \tag{1.3}$$

But the distributivity law above and then Theorem 1.5 imply that

$$\begin{aligned}|A \cap Y| &= |A \cap (B \cup C)| = |(A \cap B) \cup (A \cap C)| \\ &= |A \cap B| + |A \cap C| - |(A \cap B) \cap (A \cap C)| \\ &= |A \cap B| + |A \cap C| - |A \cap B \cap C|\end{aligned} \tag{1.4}$$

Also, Theorem 1.5 implies that

$$|Y| = |B \cup C| = |B| + |C| - |B \cap C| \tag{1.5}$$

Now the result follows by substituting (1.4) and (1.5) into (1.3). □

One significant application of this formula is in counting integers which are divisible by one of several specified integers, as in the following example.

Example. How many integers between 1 and 1000 are divisible by at least one of the integers 2, 3 and 5?

Solution. Define sets A, B and C as follows.

$$\begin{aligned} A &= \{n \in \mathbb{Z} : 1 \leq n \leq 1,000 \text{ and } n \text{ is divisible by } 2\},\\ B &= \{n \in \mathbb{Z} : 1 \leq n \leq 1,000 \text{ and } n \text{ is divisible by } 3\},\\ C &= \{n \in \mathbb{Z} : 1 \leq n \leq 1,000 \text{ and } n \text{ is divisible by } 5\}. \end{aligned}$$

Then

$$\begin{aligned} A \cap B &= \{n \in \mathbb{Z} : 1 \leq n \leq 1,000 \text{ and } n \text{ is divisible by } 6\},\\ A \cap C &= \{n \in \mathbb{Z} : 1 \leq n \leq 1,000 \text{ and } n \text{ is divisible by } 10\},\\ B \cap C &= \{n \in \mathbb{Z} : 1 \leq n \leq 1,000 \text{ and } n \text{ is divisible by } 15\},\\ A \cap B \cap C &= \{n \in \mathbb{Z} : 1 \leq n \leq 1,000 \text{ and } n \text{ is divisible by } 30\}. \end{aligned}$$

For any integer r, the number of integers between 1 and 1,000 which are divisible by r is equal to $\lfloor \frac{1000}{r} \rfloor$. So $|A| = 500$, $|B| = 333$, $|C| = 200$, $|A \cap B| = 166$, $|A \cap C| = 100$, $|B \cap C| = 66$, $|A \cap B \cap C| = 33$.

The set of integers divisible by at least one of 2, 3 and 5 is $A \cup B \cup C$, so by the inclusion-exclusion formula the number of such integers is

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|\\ &= 500 + 333 + 200 - 166 - 100 - 66 + 33 = 734. \end{aligned}$$

□

The versions of this formula for two and three sets give a hint of the general formula which applies for any number of sets: we add the sizes of the given sets, then subtract the sizes of their pairwise intersections. Then we add back the sizes of the three-way intersections, before subtracting the sizes of the four-way intersections, and so forth until all intersections have been included in the calculation.

Theorem 1.7 (General inclusion-exclusion formula[18])**.** *Suppose that $A_1, A_2, \ldots, A_r$ are finite sets. Then*

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots \cup A_r| = &|A_1| + |A_2| + \cdots + |A_r|\\ &- (|A_1 \cap A_2| + |A_1 \cap A_3| + \cdots + |A_{r-1} \cap A_r|)\\ &+ (|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \ldots)\\ &- (|A_1 \cap A_2 \cap A_3 \cap A_4| + \ldots)\\ &\cdots\\ &\pm |A_1 \cap A_2 \cap \cdots \cap A_r|, \end{aligned}$$

where the sum in the jth line of the right hand side consists of the sizes of all intersections of j sets. The sign in the final line is '$+$' if n is odd and '$-$' if n is even.

The Product Rule

Recall that the Cartesian product (or set product) of sets $A_1, A_2, \ldots, A_r$ is

$$A_1 \times A_2 \times \cdots \times A_r = \{(a_1, a_2, \ldots, a_r) : a_1 \in A_1, a_2 \in A_2, \ldots, a_r \in A_r\},$$

so the elements of $A_1 \times A_2 \times \cdots \times A_r$ are ordered r-tuples whose jth co-ordinate is a member of A_j for each j. One subtle consequence of this definition is that, given sets A, B and C, the products $A \times B \times C$ and $(A \times B) \times C$ are not quite the same thing: the first is a set of ordered triples (a, b, c), whilst the second is a set of ordered pairs whose first co-ordinate is an ordered pair $((a, b), c)$. However, there is a natural one-to-one correspondence between the two sets given by

$$(a, b, c) \longleftrightarrow ((a, b), c).$$

Using this natural correspondence, the sets $A \times B \times C$ and $(A \times B) \times C$ are essentially equivalent for most purposes (in particular, they have the same size); a similar correspondence shows that the is true of $A_1 \times A_2 \times \cdots \times A_{r-1} \times A_r$ and $(A_1 \times A_2 \times \cdots \times A_{r-1}) \times A_r$.

The product rule tells us the size of the Cartesian product of a collection of sets. Note that unlike for the sum rule, we do not require that the sets are disjoint.

Theorem 1.8 (Product rule for two sets)**.** *If A, B are finite sets, then $|A \times B| = |A| \cdot |B|$.*

Proof. Let $A = \{a_1, \ldots, a_m\}$ and $B = \{b_1, \ldots, b_n\}$. So $|A| = m$ and $|B| = n$. We can list the elements of $A \times B$ as

$$\begin{Bmatrix} (a_1, b_1), & (a_1, b_2), & \ldots & (a_1, b_n), \\ (a_2, b_1), & (a_2, b_2), & \ldots & (a_2, b_n), \\ \ldots & \ldots & \ldots & \ldots \\ (a_m, b_1), & (a_m, b_2), & \ldots & (a_m, b_n) \end{Bmatrix}$$

So altogether there are m rows and n columns in the table, so it has $m \cdot n = |A||B|$ entries; since these are all distinct, we have $|A \times B| = |A||B|$. □

An inductive argument based on the product rule for two sets yields a product rule for any number of finite sets.

Theorem 1.9 (Product rule for r sets)**.** *For any natural number r and any finite sets $A_1, A_2, \ldots, A_r$ we have*

$$|A_1 \times A_2 \times \cdots \times A_r| = |A_1||A_2| \ldots |A_r|.$$

[18] Try to prove this as an exercise. Proceed by induction on r, and in the inductive step mimic the proof of Theorem 1.6, using the distributive law

$$(A_1 \cup \cdots \cup A_k) \cap A_{k+1} = (A_1 \cap A_{k+1}) \cup \cdots \cup (A_k \cap A_{k+1}).$$

Proof. We proceed by induction on r.[19] For any $r \in \mathbb{N}$ let $P(r)$ denote the statement that for any sets $A_1, A_2, \ldots, A_r$ we have $|A_1 \times A_2 \times \cdots \times A_r| = |A_1||A_2| \ldots |A_r|$.

We first verify that $P(1)$ is true.[20] This is immediate since $P(1)$ is the statement that $|A_1| = |A_1|$.

Now suppose that $P(k)$ is true for some $k \in \mathbb{N}$, and let $A_1, \ldots, A_{k+1}$ be finite sets. Then

$$\begin{aligned} |A_1 \times A_2 \times \cdots \times A_{k+1}| &= |(A_1 \times A_2 \times \cdots \times A_k) \times A_{k+1}| \\ &= |A_1 \times A_2 \times \cdots \times A_k||A_{k+1}| \\ &= |A_1||A_2| \ldots |A_{k+1}|, \end{aligned}$$

where the first equality holds by the one-to-one correspondence discussed earlier, the second equality holds by the product rule for two sets applied to the sets A_{k+1} and $A_1 \times \cdots \times A_k$, and the final equality holds by the inductive hypothesis (that is, our assumption that $P(k)$ is true). We deduce that $P(k+1)$ is true also.

Having proved that

(i) $P(1)$ is true, and

(ii) for any $k \in \mathbb{N}$, if $P(k)$ is true then $P(k+1)$ is true also,

we conclude by the Principle of Mathematical Induction that $P(r)$ is true for every $r \in \mathbb{N}$.

□

One significant application of the product rule is in counting the number of factors of an integer, as in the following example.

Example. How many positive integers are factors of 1200?

Solution. The prime factorisation of 1200 is $2^4 \cdot 3 \cdot 5^2$, so the factors of 1200 are the integers of the form $2^a \cdot 3^b \cdot 5^c$ for $0 \leq a \leq 4$, $0, \leq b \leq 1$ and $0 \leq c \leq 2$ (this is a consequence of uniqueness of prime factorisation, which likewise implies that the integers of this form are all distinct). That is, the factors are $2^a \cdot 3^b \cdot 5^c$ for $(a, b, c) \in A \times B \times C$, where $A = \{0, 1, 2, 3, 4\}$, $B = \{0, 1\}$ and $C = \{0, 1, 2\}$. So by the product rule, the number of factors is

$$|A \times B \times C| = |A| \cdot |B| \cdot |C| = 5 \cdot 2 \cdot 3 = 30.$$

□

1.4 Relations

Definition. A binary relation on a set A is a subset $\sim \subseteq A \times A$. We often just say relation instead of 'binary relation', but be aware that there are other types of relation.

However, we usually think of $\sim$ as being a collection of statements: we say that "a is related to b by $\sim$", written $a \sim b$, to mean that $(a, b) \in \sim$, and we say that "a is not related to b", written $a \not\sim b$, to mean that $(a, b) \notin \sim$. So for any $a, b \in A$ we have either $a \sim b$ or $a \not\sim b$. For example, $=$ and $\leq$ are relations on $\mathbb{R}$ with which you are familiar: for any real numbers x and y, either $x = y$ or $x \neq y$, and either $x \leq y$ or $x \not\leq y$. We often define a relation in this way, that is, by saying that "$\sim$ is the relation on <some set> given by $x \sim y$ if <some property>".

[19] Exercise: prove Theorem 1.9 by counting choices as in the proof of Theorem 1.3.

[20] Alternatively, we could take $P(2)$ as the base case, which is Theorem 1.8.

Example. The following are all valid relations.

(i) $<$ on $\mathbb{Z}$ given by the standard definition of $<$.
(ii) $\leq$ on $\mathbb{Z}$ given by the standard definition of $\leq$.
(iii) $\sim$ on $\mathbb{N}$ given by $x \sim y$ if $|x - y| \leq 2$.
(iv) The relation $\sim$ on the set of all people, where $a \sim b$ if a and b share a biological parent, or a is a biological parent of b, or b is a biological parent of a.
(v) $\overset{3}{\equiv}$ on $\{1, 2, \ldots, 13\}$ given by $x \overset{3}{\equiv} y$ if x and y have the same remainder when divided by 3.

There are three commonly-useful properties that relations can have; these are the following.

Definition. Suppose that $\sim$ is a relation on a set A. We say that

(i) $\sim$ is reflexive if for any $a \in A$ we have $a \sim a$.
(ii) $\sim$ is symmetric if for any $a, b \in A$ with $a \sim b$ we have $b \sim a$.
(iii) $\sim$ is transitive if for any $a, b, c \in A$ with $a \sim b$ and $b \sim c$ we have $a \sim c$.

So, for example, to prove that a given relation $\sim$ on A is transitive, one should suppose that a, b, c are elements of A such that $a \sim b$ and $b \sim c$, and (using the given definition of $\sim$) deduce from this that $a \sim c$. On the other hand, to prove that a given relation on A is not transitive one merely has to exhibit some $a, b, c \in A$ such that $a \sim b$ and $b \sim c$ but $a \not\sim c$.

Example.
(i) $<$ on $\mathbb{Z}$ is not reflexive since, for example, $3 \not< 3$. It is not symmetric since, for example, $2 < 3$ but $3 \not< 2$. It is transitive since for any $a, b, c \in \mathbb{Z}$ with $a < b$ and $b < c$ we have $a < c$.
(ii) $\leq$ on $\mathbb{Z}$ is reflexive since $n \leq n$ for any $n \in \mathbb{Z}$. Similarly as for $<$ it is not symmetric but is transitive.
(iii) The relation $\sim$ on $\mathbb{N}$ given by $x \sim y$ if $|x - y| \leq 2$ is reflexive, since for any $n \in \mathbb{N}$ we have $|n - n| = |0| = 0 \leq 2$, so $n \sim n$. It is symmetric as for any $n, m \in \mathbb{N}$ with $n \sim m$ we have $|n - m| \leq 2$, so $|m - n| \leq 2$, so $m \sim n$. It is not transitive since, for example $3 \sim 4$ and $4 \sim 6$ but $3 \not\sim 6$.
(iv) The relation $\sim$ on the set of all people defined in (iv) of the last example is reflexive and symmetric, but not transitive, since, for example, my aunt is related to my mother, and my mother is related to me, but my aunt is not related to me (by this definition!).
(v) The relation $\overset{3}{\equiv}$ on $\{1, 2, 3, \ldots, 13\}$ given by $x \overset{3}{\equiv} y$ if x and y have the same remainder when divided by 3 is reflexive, symmetric and transitive.

Those relations which have all three properties are particularly useful.

Definition. Suppose that $\sim$ is a relation on a set A. We say that $\sim$ is an equivalence relation if it is reflexive, symmetric and transitive.

Example. $=$ is an equivalence relation on any set. Of the other relations we have mentioned, only $\overset{3}{\equiv}$ on $\{1, 2, \ldots, 13\}$ is an equivalence relation.

The principal reason that equivalence relations are useful is that they divide the set on which they are defined into sets called *equivalence classes* which form a *partition* of A, meaning that every element of A lies in precisely one equivalence class. We now define these terms formally.

Definition. A partition P of a set A is a set of nonempty subsets $X \subseteq A$ such that for any $a \in A$ there is precisely one $X \in P$ with $a \in X$.[21]

Informally, you can think of a partition as splitting up a set into one or more non-overlapping pieces.

Example. There are five possible partitions of $\{1, 2, 3\}$. These are

$$P_1 = \{\{1, 2, 3\}\},$$

$$P_2 = \{\{1, 2\}, \{3\}\},$$
$$P_3 = \{\{1, 3\}, \{2\}\},$$
$$P_4 = \{\{2, 3\}, \{1\}\},$$
$$P_5 = \{\{1\}, \{2\}, \{3\}\}.$$

For any set A, $\{A\}$ is a partition of A, and $\{\{a\} : a \in A\}$ is a partition of A.

Definition. Suppose that $\sim$ is an equivalence relation on a set A. For any $a \in A$, the equivalence class of a is the set $[a]_\sim = \{b \in A : a \sim b\}$, that is, the set of all elements of A to which a is related (note that we must have $a \in [a]_\sim$ since $\sim$ is reflexive).

Example. For the relation $\overset{3}{\equiv}$ on $\{1, 2, \ldots, 13\}$ we have

$$[1]_{\overset{3}{\equiv}} = \{1, 4, 7, 10, 13\}$$
$$[2]_{\overset{3}{\equiv}} = \{2, 5, 8, 11\}$$
$$[3]_{\overset{3}{\equiv}} = \{3, 6, 9, 12\}$$
$$[4]_{\overset{3}{\equiv}} = \{1, 4, 7, 10, 13\}$$
$$[5]_{\overset{3}{\equiv}} = \{2, 5, 8, 11\}$$
$$[6]_{\overset{3}{\equiv}} = \{3, 6, 9, 12\}$$
$$[7]_{\overset{3}{\equiv}} = \{1, 4, 7, 10, 13\}$$

and so forth; these are the equivalence classes of $\overset{3}{\equiv}$. So the set of equivalence classes of $\overset{3}{\equiv}$ is $\{\{1, 4, 7, 10, 13\}, \{2, 5, 8, 11\}, \{3, 6, 9, 12\}\}$.[22]

Theorem 1.10. *Suppose that $\sim$ is an equivalence relation on a set A. Then the set of equivalence classes of $\sim$ is a partition of A.*

Proof. We need to show that every element of A lies in precisely one element of the set of equivalence classes of $\sim$. So fix an arbitrary $a \in A$. As we noted in the definition, since $\sim$ is reflexive we have $a \in [a]_\sim$, that is, a lies in its own equivalence class. So we need to prove that a does not lie in any equivalence class which is *distinct* from $[a]_\sim$. To put it another way, we want to show that for any $b \in A$, if $a \in [b]_\sim$ then $[a]_\sim = [b]_\sim$.

So suppose that $b \in A$ is such that $a \in [b]_\sim$, which means that $b \sim a$; since $\sim$ is symmetric we also have $a \sim b$. Then:

[22] Remember that a set cannot have repeated elements!

i) For any $c \in [a]_\sim$ we have $a \sim c$, which together with $b \sim a$ implies that $b \sim c$ (since $\sim$ is transitive). This means that $c \in [b]_\sim$.

ii) For any $c \in [b]_\sim$ we have $b \sim c$, which together with $a \sim b$ implies that $a \sim c$. This means that $c \in [a]_\sim$.

So $[a]_\sim = [b]_\sim$, completing the proof.[23] □

Theorem 1.10 shows that an equivalence relation on a set A generates a partition of A; the next proposition shows that the reverse is also true.

Proposition 1.11. *Let A be a set and let P be a partition of A. Define a relation $\sim$ on A by*

$$a \sim b \text{ if there is some } X \in P \text{ with } a, b \in X.$$

Then $\sim$ is an equivalence relation on A whose equivalence classes are the elements of P.

Proof. See problem sheets. □

So for any set A, partitions of A and equivalence relations on A are essentially the same thing: each equivalence relation on A corresponds to a partition of A and vice versa.

[23] Note that we used all three parts of the definition of an equivalence relation in this proof. As an exercise, give examples to show that no two parts of the definition suffice to ensure that the set of 'equivalence classes' of $\sim$ is a partition of A.