Mathematical reasoning and proofs

February 20, 2017

Steve Mitchell

These are notes for Steve Mitchell's Math 300D class, Winter quarter 2017. Any sections whose title begins "Additional material..." are not required reading. They are intended for students who want to go more deeply into the concepts. Many of these additional sections are highly recommended for those plannning to take advanced pure mathematics courses such as 402, 441, 424.

Preamble

Mathematics is not written in stone and handed down from the mountaintop. It is a beautiful, creative art-form whose practice goes back as far as the historical record, and it is still very much alive today. Mathematics is not something that "they" do; it is something that *we*, *you and I*, do. We are all mathematicians. Enjoy!

Table of Contents:

1 Introduction

One purpose of these notes (and of the course) is to introduce the basics of mathematical logic, set theory, and especially proofs. What makes all this interesting, however, is not the formal mechanics, but rather the intrinsic fascination and beauty of the mathematics itself. So we'll develop these mechanics in the context of interesting questions such as: What is a number? What is a "real" number? What does it mean to say that two sets have "the same number" of elements? What is infinity? Are all infinities the same? How are the prime numbers distributed? How can we count things like the number of k-element subsets of an n-element set? For example, we will explain and prove Cantor's remarkable discovery that some infinities are bigger than others; in particular, there are "more" irrational numbers than there are rational numbers. Although this result is completely standard today, it was quite controversial at the time it was proven (1874), with even philosophers and theologians weighing in on the matter.

In we had more time, we would build the theory systematically from the ground up, starting with the Peano axioms for the natural numbers, defining the real numbers rigorously via Dedekind cuts, and even continuing with the construction of the complex numbers. Alas, that would take much too long. For the time being, we will simply take for granted most of the "usual properties" of the natural numbers, integers, real numbers etc., and sadly will have little if any time for the best number system of them all, the complex numbers. The curious will find some of the aforementioned material at the end of the notes—Peano axioms, Dedekind cuts, and so on.

The mathematical topics considered are also limited by our time constraints. The concept of "proof" applies to any branch of pure mathematics, including of course geometry and calculus. There are a few geometry problems here and there, but almost nothing from calculus. The reason I've avoided calculus is that if we want to do things rigorously—and we do!—we would first have to give a serious, precise treatment of the limits used to define derivatives, Riemann integrals and so on. That would require a course or two or three in itself, such as Math 327 and its sequel courses here at the UW. For these reasons, the topics considered are limited mainly to number theory (prime numbers and so on), combinatorics (finite sets and how to count them), and infinite set theory.

This is a course in pure mathematics and you will see few if any applications. Nevertheless, it is a fact of modern electronic life that number theory and combinatorics are everywhere in the applied, practical world. To mention just one of hundreds of examples, the encryption methods used for secure data transmission, including from your cellphone, depend heavily on number theory. Indeed the trend seems to be that *all* branches of mathematics, no matter how abstract or esoteric they might appear, find applications sooner or later. In this course, however, we are considering mathematics as the beautiful art form that it is, an art form that goes back as far as recorded history.

Finally, mathematics is not something that "they" do. It is something that we, you and I, do. Mathematics is not written in stone and handed down from the mountaintop; it is a living, ever-evolving, creative human enterprise. WE are the mathematicians. YOU are a mathematician!

1.1 Numbers

The following number systems, each contained in the next, are fundamental:

$$\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

Here $\mathbb{N}$ denotes the set of natural numbers, also known as the positive integers: $1, 2, 3, ...$ We take the natural numbers for granted, although later we will come back and characterize them by a set of axioms known as the Peano axioms. The successive expansions of this number system can be viewed in terms of solving equations, as follows:

$\mathbb{N}_0$: In $\mathbb{N}$ there are no solutions to equations such as $1+x = 1$. So we invent a new number called 0 to fill the gap. It is worth noting that mathematics had been around for a long time before anyone thought of introducing the concept "zero" and a symbol for it. Thus it isn't necessarily an obvious concept, although of course we are by now so accustomed to it that we hardly even think about it.

Caution: Some sources call $\mathbb{N}_0$ the natural numbers, and use $\mathbb{N}$ to denote it. It is just a matter of definition (see the section below on "The importance of definitions"); as long as one is consistent it doesn't matter. But for us, 0 is not an element of $\mathbb{N}$.

$\mathbb{Z}$: In $\mathbb{N}_0$ there are no solutions to equations such as $5 + x = 2$. So we invent a new number system, the integers $\mathbb{Z}$, in which such solutions do exist. We do this by introducing the "negative" $-n$ of a natural number n; it serves as a solution to $n + x = 0$. It is a nice consequence that from this we automatically get solutions to every equation of the form $m + x = n$ with $m, n \in \mathbb{N}_0$; namely $x = -m + n$.

$\mathbb{Q}$: In $\mathbb{Z}$ there are no solutions to equations such as $3x = 4$. So we invent a new number system, the rational numbers $\mathbb{Q}$, in which such solutions do exist. Thus $\mathbb{Q}$ consists of "fractions" $\frac{a}{b}$ with $a, b \in \mathbb{Z}$ and $b \neq 0$. Notice however that different choices of a, b can define the same rational number: $\frac{4}{6} = \frac{2}{3}$, for example. Later on we'll want to take a closer look at this, in order to be absolutely precise about what a rational number is.

$\mathbb{R}$: In $\mathbb{Q}$ there are no solutions to equations such as $x^2 = 2$. (It isn't obvious that no rational solution exists—in other words, that $\sqrt{2}$ is not a rational number—but we'll prove it later.) So we invent a new number system, the real numbers $\mathbb{R}$, in which such solutions do exist. It is only fair to point out, however, that giving a precise, rigorous construction of the real number system is difficult. You've been working with the real numbers for years, but what exactly *is* a real number? For the time being, we'll take the real numbers as "given", in some intuitive sense. In the optional reading, we'll sketch a precise definition using the beautiful idea of a *Dedekind cut*.

$\mathbb{C}$: In $\mathbb{R}$ there are no solutions to equations such as $x^2 + 1 = 0$. So we invent a new number system, the complex numbers $\mathbb{C}$, in which such solutions do exist. Then a miracle occurs: By simply introducing $\sqrt{-1}$, it turns out that in this new "complex" number system, *every* polynomial equation has a solution! Equivalently, every polynomial has a root. This fabulous property more than justifies the complex numbers. To mention just one important application that you may have seen (if you haven't, you surely will soon), it follows that

square matrices always have at least one eigenvalue in the complex numbers (whereas such a matrix might have no real eigenvalues).

In all of these number systems except $\mathbb{C}$ (which we won't worry about for now), there is a familiar concept of ordering $x < y$. We take this for granted, for now, and often use the following self-explanatory subscript notation:

$\mathbb{Z}_{<0}$ is the set of all negative integers
$\mathbb{R}_{\geq 0}$ is the set of all non-negative real numbers
$\mathbb{Q}_{>7}$ is the set of all rational numbers > 7

and so on. Note that $\mathbb{Z}_{>0} = \mathbb{N}$, for example.

1.2 The laws of arithmetic

The "laws of arithmetic" will also be taken for granted. But let's at least spell out exactly what these are, for reference purposes. All of the number systems in the previous section have the operations addition $a + b$ and multiplication ab (sometimes we we write $a \cdot b$, if we want a symbol for multiplication), satisfying various familiar rules.

Associative law. Both operations satisfy the associative law: $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$. The significance of the associative law is that there is no ambiguity in the expressions $a + b + c$ and abc; it doesn't matter whether you first add/multiply a and b, then c, or first b and c, then a. For contrast, the vector cross product $v \times w$ of vectors in 3-space is not associative.

Commutative law. Both operations satisfy the commutative law: $a + b = b + a$ and $ab = ba$. For contrast, neither the vector cross product nor matrix multiplication satisfy the commutative law.

Distributive law. Multiplication distributes over addition: $a(b + c) = ab + ac$. Because of the commutative law, we automatically get the distributive law on the other side as well: $(a + b)c = ac + bc$.

Identity elements. All of the above number systems have a *multiplicative identity*, namely the good old number 1. This means $1 \cdot x = x = x \cdot 1$ for all numbers x (whether integers, rationals, etc.). For contrast, the vector cross product doesn't have a multiplicative identity. All of the above number systems except $\mathbb{N}$ have an additive identity, namely 0. This means $x + 0 = x = 0 + x$. We created $\mathbb{N}_0$ from $\mathbb{N}$ precisely to rectify the lack of an additive identity in $\mathbb{N}$.

Additive inverses. An additive inverse of a number x is an number $-x$ such that $x + -x = 0$. Note that $\mathbb{N}_0$ doesn't have additive inverses. When we say this, we mean that there are no additive inverses *in the given number system.* Of course a natural number n has an additive inverse $-n$ *in the integers*, but it does not have one in $\mathbb{N}_0$.

Multiplicative inverses. A multiplicative inverse of a nonzero number x is a number y, sometimes denoted x^{-1} or $1/x$, such that $xy = 1 = yx$. Note that $\mathbb{Q}$ and $\mathbb{R}$ have multiplicative inverses as usual; so does $\mathbb{C}$ (but again, if you're not familiar with the complex number system you can ignore this point). However, $\mathbb{N}$, $\mathbb{N}_0$ and $\mathbb{Z}$ do note have multiplicative inverses. When we say this, we mean that there is no multiplicative inverse *in the given number system.* Any nonzero integer n has a multiplicative inverse $1/n$ *in the rational numbers*, but it does not have one in $\mathbb{Z}$ unless $n = \pm 1$.

All of these laws are familiar from childhood, although probably not stated so formally. Just remember that when you encounter new operations, you can't just assume that such laws hold. A good example to keep in mind is vectors in three space, with the two operations $v + w$ (vector addition) and the cross product $v \times w$. A few of the laws hold, e.g. the distributive law, but the associative, commutative, multiplicative identity and multiplicative inverse laws all fail.

1.3 Finite and infinite sets

One of our goals is a careful study of the concepts "finite" and "infinite". But for now we'll accept the following informal, intuitive definitions and facts. A set A is *finite* if either there is a natural number n such that the elements of A can be listed as $a_1, a_2, ..., a_n$, or A is the empty set $\emptyset$ (the set with no elements). Assuming no element of A has been listed twice, n is the number of elements in the set. The prototypical example of such a set is $[n] = \{1, 2, ..., n\}$, i.e. $[n]$ is the set of all natural numbers from 1 to n. For example $[5] = \{1, 2, 3, 4, 5\}$, and so on. Occasionally we use the notation $[0]$ to denote the empty set, since it has zero elements.

It is clear (intuitively, at least), that any subset of a finite set is finite. Another important fact about finite sets of real numbers is the max/min property. If A is a set of a real numbers, an element $a \in A$ is *maximal* if for all $b \in a$, $b \leq a$. An element $c \in A$ is *minimal* if for all $b \in A$, $c \leq b$. If a maximal element of A exists, then it is clearly unique (because if a' is another maximal element, $a \leq a'$ and $a' \leq a$, so $a = a'$), and similarly for minimal elements.

Max/min property: If A is a nonempty finite set of real numbers, then A has a maximal element and a minimal element.

For example, the maximal element of $[n]$ is n, while its minimal element is $[1]$. The max/min property seems clear enough intuitively from the "number line" visualization of the real numbers. Later we'll give a proof, but for now we just assume this fact. Notice that we have to assume A is nonempty; it can hardly have a maximal or minimal element if it has no elements at all!

A set is *infinite* if it is not finite. The prototypical example of an infinite set is $\mathbb{N}$. Other familiar examples include $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$. Note that none of these examples have a maximal or a minimal element. Another example is to take A to be the set of all rational numbers x with $0 < x < 1$. Then A is clearly infinite, since it contains all fractions m/n with $m, n \in \mathbb{N}$ and $m < n$. Moreover this A has no maximal or minimal element. It's essential to note here that the maximal and minimal elements of a set of real numbers are required to *lie in the set*

itself. So 1 is not a maximal element of A, because it isn't an element of A at all. Similarly 0 is not a minimal element of A.

Exercise: Give an example of an infinite subset $A \subseteq \mathbb{R}$ that *does* have a maximal element and a minimal element.

That's all we need for now. We'll return later to a detailed analysis of finite and infinite sets.

1.4 The role of "silly" examples

When possible I like to illustrate concepts using examples from everyday life. Some of these examples may appear quite silly: cupcakes at a birthday party, baseball teams, and so on. I confess that I enjoy being silly (this is why I get along famously with three-year old children), but these examples in fact have a very serious point. One of the keys to understanding abstract mathematics is to de-abstractify, or "internalize" it. If you have enough examples and the right mental imagery, before long the new concepts won't seem abstract at all. For example, it is my experience that many students have trouble with the concepts *injective, surjective, bijective* that are studied below. Nevertheless I hope to convince you that these concepts are really, really easy (at least when the sets involved are finite). Far from being abstract, they are as concrete as the foundation of Padelford Hall. To see what's going on, all you have to do is conjure up a simple everyday example such as the cupcake function that is considered in detail later. In a nutshell, this is the function whose domain is a set of cupcakes being given out to children at a birthday party, so that each cupcake is assigned to a child. The aforementioned abstract-sounding terms boil down to the following:

- surjective: every child gets at least one cupcake.
- injective: every child gets at most one cupcake.
- bijective: every child gets exactly one cupcake.

That's all there is to it! Of course, if you're happy with purely mathematical examples, maybe you don't need the cupcakes. Or you might want to conjure up similar examples of your own (and indeed you should). The point is that with examples and imagery the most abstract beasts can be tamed, and perhaps even become your favorite pets.

1.5 On the importance of definitions

If we don't define our terms, then we literally don't know what we're talking about. In mathematics precise definitions are critical, since even small ambiguities can lead to misunderstandings, errors, or total nonsense. Now as I've said, *we* are the mathematicians. We are free to define our terms however we like, subject only to the following conditions:

- The definition must be unambiguous and logically consistent.
- The definition should be useful (mathematically speaking).

- The definition shouldn't conflict with established terminology.

For example, consider the definition of a prime number. This means a natural number p such that (i) p is only divisible by itself and 1, and (ii) $p \neq 1$. First of all, why are they called "primes"? The answer is that you could just as well call them "basic numbers", "groovy numbers" or "refried beans", but this would violate the third item above. The terminology "prime" has been established for centuries, and if you start calling them groovy numbers no one will listen to you. A more interesting and very reasonable question that many people ask is this: Why isn't 1 a prime? Well, we could *define it* to be prime if we wanted to, and I believe that centuries ago some people did count it as a prime. There is nothing logically wrong with such a definition. The problem is that if you define the prime numbers to include 1, you'll soon find that many of the most interesting facts about primes have to start with the disclaimer "suppose p is a prime other than 1", which rapidly gets tedious. Experience has shown that it's much more convenient to exclude 1 from the definition. The key point to understand is that when we say 1 is not a prime, we're not asserting any deep, mysterious fact; we are simply excluding it by fiat.

Another example: At some point in early school days, you were told that "you can't divide by zero". If you were curious, sceptical, or just anti-authority, you may have asked "why not?". In fact this is another good question. The real point is not that "you can't divide by zero", but rather "there is no useful way to *define* division by zero". I could for example define $\frac{n}{0} = 17$ for all n, without violating the first item above, but I think you'll agree this would be ridiculous; it would serve no useful purpose whatsoever. A more common suggestion is to define it to be "infinity" and write $\frac{n}{0} = \infty$. But then what do you mean by "infinity"? We could certainly introduce a new symbol ∞, call it a number, and make the definition $\frac{n}{0} = \infty$. But such a definition would be useless because the standard rules of arithmetic would break down. Indeed it would be worse than useless; it would even be dangerous because it leads to all kinds of sloppy, erroneous reasoning. As you know from calculus, there is no useful, consistent way to interpret $\frac{\infty}{\infty}$, $\infty - \infty$, $\frac{0}{0}$ and so on. This is why we choose not to define division by zero at all; there is no good way to do it.

Another example: Recall that $n!$ means the product of all the natural numbers up to n. Symbolically, $n! = 1 \cdot 2 \cdot \ldots \cdot n$ or $n! = \prod_{i=1}^{n} i$. We also *define* $0! = 1$. This might seem perverse; wouldn't it be more logical to define $0! = 0$? The latter suggestion may seem more intuitive, but it turns out that defining $0! = 1$ is much more useful. In fact it is possible to justify this definition on *a priori* logical grounds, but we'll take $0! = 1$ as simply the definition.

Now for the bad news: I've just told you that it's very important to have precise definitions, but, worthy as this goal may be, it won't always be possible to achieve it. For one thing, there always have to be some undefined, or at least not precisely defined, terms to start from. One can give a very precise definition of the rational numbers in terms of the integers. But what are the integers? Well, one can give a very precise definition of the integers in terms of the natural numbers. But what are the natural numbers? You see the problem; we can't go on like this forever; at some point we have to accept a few basic terms without definition. For us, the natural numbers are such a "given"; we won't attempt to define them.

There are also some objects, such as the real numbers, which do have a precise definition in terms of the rational numbers, but the definition is too complicated to include in a one-quarter course such as this one. So we will occasionally resort to the imprecise intuitive idea of "real numbers" that you've used for years. On the other hand, the precise definition in terms of "Dedekind cuts" is given in one of the optional reading sections below.

Another potential problem is that all language is context-based; the definition of a word or symbol may depend on the context. In English, for instance, the bark of a dog and the bark of a tree are very different things, but this never causes ambiguity because the intended meaning is clear from the context. Mathematical language and symbolism works the same way. Certain notations can be confusing because they are used with different meanings in different contexts. For example -1 as an exponent can have several different meanings. Sometimes $f^{-1}(x)$ means the reciprocal $1/f(x)$, assuming $f(x) \neq 0$ for all x being considered; sometimes it means the inverse function, assuming an inverse exists (for this reason I prefer the notation $\arcsin x$ to $sin^{-1}x$). We'll have yet another meaning later. Another familiar example is the notation (a, b), where $a, b \in \mathbb{R}$. It can mean the point (a, b) in the plane, or if $a < b$ it can mean the interval on the real line given by $\{x \in \mathbb{R} : a < x < b\}$. If a, b are integers, it can also mean the greatest common divisor of a, b. If in doubt, consider the context.

Finally, not only can one word or symbol have two different meanings, but also two different words or symbols can have the same meaning. On the surface this flies against the "precise definition" rule; why use two different symbols for the same thing? But consider a familiar example, such as the derivative. If $y = f(x)$, the derivative can be denoted $f'(x)$ or $\frac{dy}{dx}$. In some contexts the first notation is more useful; in other contexts the second notation is very handy.

To sum up, a certain degree of ambiguity and/or redundancy is unavoidable. But let's avoid it as much as we can. Precision, precision, precision!

2 Logic, proofs, and sets

Note: My goal here is to show you how to *use* the basics of mathematical logic, as opposed to developing it as a subject in itself. For a more systematic but still short introduction to logic and proofs, see the nice little book "Introduction to Mathematical Thinking" by Keith Devlin.

As a first approximation, a proof is just a careful explanation of why something is true. As the mathematics involved gets more complicated and subtle, however, more and more careful explanations are required. This is what is meant by "rigorous" proof; everything must be carefully justified in order to be sure no mistakes have been made. Otherwise you may end up "proving" something false! In this section we'll get started with some easy proofs, and at the same time introduce some basic logic and set theory. Many of these proofs require little understanding and no creativity. In such cases the method is often called "unwinding the definitions" or "follow your nose". So they're not too exciting, but have the pleasant feature of being easy. But don't worry; we'll get to harder and more interesting proofs soon enough.

Many of our first proofs will involve divisors and prime numbers, so before getting started we need the precise definitions.

Definition. If $a, b \in \mathbb{Z}$, we say that a *divides* b if there is an integer k such that $b = ka$. In this case we say that a is a *divisor* of b. We use the shorthand notation $a|b$ for "a divides b".

Examples. 1. Any integer divides itself: $a|a$ since $a = 1 \cdot a$.
2. For all $a \in \mathbb{Z}$, $1|a$.
3. For all $a \in \mathbb{Z}$, $a|0$.
4. The positive divisors of 12 are $1, 2, 3, 4, 6, 12$.

Note that for all $a \in \mathbb{Z}$, $-1|a$ and $-a|a$, since $a = (-1)(-a)$. Much of the time, however, when $a \in \mathbb{N}$ we are only interested in the positive divisors of a. For example, the set of *all* divisors of 12 would consist of $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$, but for many purposes the negative divisors are irrelevant.

Definition. A *prime* is a natural number $p > 1$ such that the only positive divisors of p are 1 and p.

The concepts "even and odd" are of course familiar since childhood, but even these need a precise definition.

Definition. An integer a is *even* if $2|a$, i.e. there is a $b \in \mathbb{Z}$ with $a = 2b$. An integer a is *odd* if it is not even.

To say that a is odd is the same as saying that it can be written in the form $a = 2b + 1$ with $b \in \mathbb{Z}$, or equivalently as $a = 2c - 1$ with $c \in \mathbb{Z}$. This is a special case of the "Division Theorem" to be proved later, but we'll take it as known or obvious for now.

2.1 Proving an implication $P \Rightarrow Q$

Consider the assertion: *If p is an even prime, then $p = 2$.* This is a true statement, and indeed may seem obvious, but we insist on proving it. Imagine that you are trying to convince a skeptical friend of this fact. Well, look, if p is even, then p is divisible by 2. But the only divisors (=factors) of a prime number are the number itself and 1. Since 2 is a divisor of p, it follows that $p = 2$. QED.

Note: The letters "QED" are often used to mark the end of a proof. They stand for "quod erat demonstrandum", Latin for "which was to be demonstrated". The symbol □ is often used instead. One can also just say "this completes the proof", or more informally, "done". It's important to mark the end of the proof, because otherwise it might not be clear to the reader whether the proof has really been finished or not.

Mathematical statements such as the one just proved are often labeled as "theorems" or "propositions". I prefer to reserve the term "theorem" for more substantial statements. A typical mathematical statement has the form $P \Rightarrow Q$, to be read as "P implies Q" or "if P, then Q". We think of P as the hypothesis or assumption, and Q as the conclusion. In the preceeding example, the assumption P is "p is an even prime", while Q is the conclusion $p = 2$. Assertions of the form "if P, then Q" will be called *implications*. Here's another easy example (dignifying this simple-minded statement with the label "proposition" may seem excessive, but we have to start somewhere):

Proposition 2.1 *If a and b are odd integers, then $a + b$ is even.*

Note this proposition has the form $P \Rightarrow Q$, where P is the statement "a and b are odd integers", while Q is the statement "$a + b$ is even".
Proof: Here's what I mean by "unwinding the definitions": Clearly one has no hope of proving the proposition without knowing the definition of "odd". Well, to say a is odd means it is not even, and hence can be expressed as $a = 2m+1$ for some integer m .Similarly $b = 2n + 1$ for some integer n. This completes the unwinding of the definitions in the hypothesis. We then make the brilliant calculation

$$a + b = 2m + 1 + 2n + 1 = 2(m + n + 1).$$

This shows that $2|(a + b)$, which is the definition of "even". QED.

This is a proof because it demonstrates the truth of the proposition not merely beyond a reasonable doubt, as would be required in a court of law, but beyond any doubt whatsoever.

Note that Proposition 2.1 could be reworded as follows: For *all* odd integers a and b, $a + b$ is even. This use of the phrase "for all" come up so frequently that we have a special notation for it: the symbol $\forall$ means *for all*. For another example:

$$\forall x \in \mathbb{R},\ x^2 \geq 0$$

means "for all real numbers x, $x \geq 0$, and is equivalent to saying "if $x \in \mathbb{R}$ then $x^2 \geq 0$. This is a true statement; we don't need to prove it because it is part of the basic algebra

that we are assuming. It has the form $P \Rightarrow Q$, where P is the statement "$x \in \mathbb{R}$" and Q is that statement "$x^2 \geq 0$".

The prototype of all "if-then" statements is perhaps $A \subseteq B$, which means "A is a subset of B". We can rephrase this as $x \in A \Rightarrow x \in B$, or in words "if x is an element of A, then x is an element of B", or in yet another way as "$\forall x \in A$, $x \in B$". As an example, consider $A = \{\frac{n}{n+1} : n \in \mathbb{N}\}$. The notation means "the set of all numbers of the form $n/(n+1)$ with $n \in \mathbb{N}$. Let $B = \{x \in \mathbb{Q} : 0 < x < 1\}$ (i.e. the set of rational numbers x that are > 0 and < 1).

Proposition 2.2 *If A, B are defined as above, then $A \subseteq B$.*

Proof: The proposition says that $\forall n \in \mathbb{N}$, $n/(n+1) \in B$. To prove this, we need to check three things: First, $n/(n+1) \in \mathbb{Q}$, i.e. is rational. This is true by definition of the rational numbers. Second, $n/(n+1) > 0$. This is clear. Third, $n/(n+1) < 1$. This too is clear, but just to be complete, we could start from $n < n+1$ (which surely needs no proof!) and then multiply both sides by $1/(n+1)$ to get $n/(n+1) < 1$. Here we are using the fact that multiplication by a *positive* number preserves inequalities.

2.2 Counterexamples: how to "disprove" certain assertions

In the previous section we started with an implication of the form $P \Rightarrow Q$ that was chosen in advance to be true, then proved it. In mathematical real life we are more often faced with a question: Is it true that $P \Rightarrow Q$, or not? The first step is to guess the answer (where by "guess", I mean in some intelligent way!), i.e. to make a conjecture as to whether the implication is true or false, then prove your conjecture. There is no magic formula for the guesswork; it is part of the art of mathematics and takes much practice. For the moment I only want to illustrate how to disprove assertions beginning with $\forall$, so I'll choose assertions where the guess is easy or even obvious.

Examples. 1. Assertion: If p is a prime, then p is odd. Here the symbol $\forall$ occurs in disguise, as we've seen earlier: the assertion is that $\forall$ primes p, p is odd. Now $\forall$ really does mean for *ALL*, no exceptions! So the assertion is FALSE, because 2 is a prime but is not odd. We say that 2 is a *counterexample* to the assertion; that is, it is an example where the hypothesis is true but the conclusion is false. In this case 2 happens to be the only counterexample.

Note: Another frequently used symbol is $\exists$, meaning "there exists". In the preceeding example, we could say using symbols: $\exists$ prime p such that p is even.

2. Assertion: If $x \in \mathbb{R}$ and $x < 1$, then $x^2 < 1$. This is FALSE. Once again it can be rephrased in the form $\forall x \in \mathbb{R}$ such that $x < 1$, $x^2 < 1$. To disprove it we therefore only need to find *one* example of a real number with $x < 1$ and $x^2 \geq 1$. So take $x = -2$; this is a counterexample because it satisfies the hypothesis, i.e. $-2 < 1$, but not the conclusion since $(-2)^2 = 4 \geq 1$. In fact any $x \leq -1$ would serve as a counterexample, but remember that a single counterexample suffices to disprove the assertion.

Once again, we could rebut the false claim by saying NO! $\exists x \in \mathbb{R}$, $x < 1$ but $x^2 \geq 1$...and then give a specific counterexample such as $x = -2$.

3. Assertion: All mammals are cats. This is false (!). Counterexample: pick your favorite mammal that is not a cat; a dog for example. A 3-toed sloth would also be a counterexample. A blue whale would be a counterexample. A ring-tailed lemur would be a counterexample. But you only need *one* counterexample to disprove the assertion. Here's how the assertion looks in "for all" format: $\forall$ mammals x, x is a cat.

4. The previous assertion has the form $A \subseteq B$ where A is the set of mammals and B is the set of cats. To take a random mathematical example, consider the polynomial $f(x) = x^3 + 2x^2 - x - 2$. Take $A = \{x \in \mathbb{R} : f(x) = 0\}$ and $B = \mathbb{R}^+$. Then the assertion $A \subseteq B$ is equivalent to saying "all roots of f are positive". In this case it isn't immediately obvious whether the assertion is true or false. But by factoring f one finds that $A = \{-2, -1, 1\}$. So the assertion is false, as either -2 or -1 gives a counterexample. Here's how it looks in "for all" format: $\forall x$ with $f(x) = 0$, $x > 0$.

A comment on notation: We sometimes describe finite sets by simply listing their elements, as we did for A in example 4. As another example, the set S of primes < 12 is the set $\{2, 3, 5, 7, 11\}$. Simple enough, but there are two possible points of confusion regarding this notation. First, the order in which the elements are listed is irrelevant; the set $\{7, 5, 11, 3, 2\}$ is equal to S. If we want to keep track of orderings, a different notation will be used (to be discussed later, under "Cartesian products"). Second, repetitions are redundant: the sets $\{1, 2, 3, 4\}$ and $\{1, 1, 2, 2, 2, 3, 4, 4\}$ are equal. Once again, we'll have a different notation later if we want to keep track of repetitions.

2.3 Converse and biconditional

The *converse* of an implication $P \Rightarrow Q$ is the implication $Q \Rightarrow P$.

CAUTION: If $P \Rightarrow Q$ is true, it doesn't follow that the converse is true.

This is just common sense. For example, consider the assertion "all cats are mammals". This says "if an animal is a cat, then it is a mammal", which is true. The converse says "if an animal is a mammal, it is a cat", i.e. all mammals are cats—which is false. More abstractly, if $A \subseteq B$, it doesn't follow that $B \subseteq A$. For example, $\mathbb{Z}$ is contained in $\mathbb{Q}$ but $\mathbb{Q}$ is not contained in $\mathbb{Z}$. Maybe this all seems trivial, but experience shows that students who would never say "because all cats are mammals, all mammals are cats" will nevertheless make this mistake in mathematical contexts. Here's a notorious example from first-year calculus:

Example. Consider a differentiable function $f(x)$, where $x \in \mathbb{R}$. A theorem from calculus says that if f has a local minimum or local maximum at x_0, then $f'(x_0) = 0$. A common mistake is to assume that the converse is also true. Now the converse says that if $f'(x_0) = 0$, then f has a local min or a local max at x_0. But this false. To prove that it's false we only need *one* counterexample. The standard counterexample is to take $f(x) = x^3$ and $x_0 = 0$. Then the derivative vanishes at 0 but x^3 does not have a local min or max at 0.

A simple example: If $|x| < 4$ then $x < 4$. This is clearly a true statement. The converse is "if $x < 4$ then $|x| < 4$", which is false: $x = -5$ is one counterexample. In short, it's very common for a true implication to have a false converse.

On the other hand, it may happen that $P \Rightarrow Q$ and the converse $Q \Rightarrow P$ are both true. This is called a *biconditional*, written as $P \Leftrightarrow Q$. Read this as "P is true if and only if Q is true", often contracted to "P if and only if Q". Note that proving a biconditional statement requires *two* proofs: A proof that $P \Rightarrow Q$, and a proof that $Q \Rightarrow P$ (it doesn't matter what order you do these in). An example:

Proposition 2.3 *Suppose $a, b \in \mathbb{Z}$. Then a and b are both odd $\Leftrightarrow$ ab is odd.*

Proof: First we prove $\Rightarrow$. So suppose a, b are both odd. Then there are integers m, n such that $a = 2m+1$ and $b = 2n+1$. Then $ab = (2m+1)(2n+1) = 4mn+2(m+n)+1 = 2k+1$ where $k = 2mn + m + n$, so ab is odd.

Now we prove the converse $\Leftarrow$. We know that $a = 2m+c$ and $b = 2n+d$ where $m, n \in \mathbb{Z}$ c and d are either 0 or 1. We want to show that $c = d = 1$. By assumption $(2m+c)(2n+d)$ is odd. Since $(2m + c)(2n + d) = 4mn + 2md + 2nc + cd$, this forces $cd = 1$ and hence $c = d = 1$.

Remark. The proof is a bit clumsy. A much simpler approach is to use the contrapositive forms, as we will see later.

The most basic example of a biconditional is perhaps the assertion $A = B$ that two sets A, B are equal. To prove this you need to prove two things: $A \subseteq B$, and $B \subseteq A$. This is a biconditional statement because it can be rephrased as: $x \in A \Leftrightarrow x \in B$. We'll see some examples in the next section.

2.4 And/or statements

The use of "and" is very simple and corresponds to everyday useage. For example, a course catalog might list the prerequisites for Math 300 as "Introduction to Quantum Mechanics, and Norwegian Literature 101", meaning that you have to have taken both Quantum Mechanics *and* Norwegian Literature in order to take Math 300. Similarly, the intersection of two sets A, B is by definition the set of elements x such that $x \in A$ *and* $x \in B$. A symbol often used for "and" is $\wedge$. Thus if P is the statement "$x \in A$", and Q is the statement "$x \in B$", then $P \wedge Q$ is the statement "$x \in A$ and $x \in B$". I don't use this symbol very often (except when discussing the logic itself), because the word "and" is short enough for me.

Sometimes the word "and" is hidden in the language or notation used, but in a straightforward way. For example "p is an even prime" means p is even and p is prime. The notation $a < x < b$ means $a < x$ and $x < b$. Similarly, $|x| < c$ means $-c < x < c$, i.e. $-c < x$ and $x < c$.

To illustrate the use of "and" in proofs, consider:

Proposition 2.4 *Suppose $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$, then $a|c$.*

Proof: We want to show there is an integer k such that $c = ka$. Since $a|b$, there is an integer i with $b = ia$. Since $b|c$, there is an integer j with $c = jb$. So $c = jb = jia$, and taking $k = ji$ completes the proof.

The abstract form of the above proposition is $P \wedge Q \Rightarrow R$. In this case P is the statement $a|b$, Q is the statement $b|c$, and R is the statement $a|c$. The point is just that we have two hypotheses P, Q, and we used both of them. The earlier proposition on even primes had the same form, with the "hidden and" as mentioned above.

The case when "and" is in the conclusion instead of the hypothesis is equally easy to interpret. If you want to prove an assertion of the form $P \Rightarrow (Q \wedge R)$, you have to prove two assertions: $P \Rightarrow Q$ and $P \Rightarrow R$.

The use of "or" is also easy, bearing in mind that in mathematics it is always the inclusive "or" (unless otherwise specified). In other words, when we say P is true or Q is true, we always include the possibility that P *and* Q are true. For example, the union $A \cup B$ of two sets is by definition the set of all x such that $x \in A$ or $x \in B$, including those x (if any) that are in A and in B. Note that with this definition, $A \cap B \subseteq A \cup B$. Sometimes the "or" is incorporated into the notation; for example "$x \leq y$" means $x < y$ or $x = y$.

Everyday useage of "or" often agrees with this inclusive form. For instance, you must have taken Math 441 or Math 424 to take Math 442. But we certainly won't turn you away if you've taken both! This is the inclusive "or". On the other hand, if the menu says you can have salad or french fries with your entree, the exclusive "or" is intended. Just remember that in mathematics, "or" is always inclusive unless otherwise specified.[1]

The notation for "P or Q" is $P \vee Q$. Once again, I don't use this notation very often (except when discussing the logic itself), as the word "or" is short enough for me.

Now let's consider how "or" statements get processed in proofs. If the assertion to be proved has the form $(P \vee Q) \Rightarrow R$, then you have to prove two assertions: $P \Rightarrow Q$ and $P \Rightarrow R$.

Example. Suppose $x \in \mathbb{R}$. If $x < 0$ or $x > 1$, then $x^2 - x > 0$. *Proof:* Note $x^2 - x = x(x-1)$. We now check the two cases separately: If $x < 0$, then also $x - 1 < 0$, so $x(x-1) > 0$. If $x > 1$, then $x > 0$ and $x - 1 > 0$, so $x(x-1) > 0$. QED.

Proving an assertion of the form $P \Rightarrow (Q \vee R)$ is a bit more interesting. Here we are assuming P, and trying to prove that either Q is true or R is true (or possibly both). If Q is true, we're done, so what we need to show is that if Q is false then R is true (or the other way around).

Example. Suppose $x, y \in \mathbb{R}$. If $xy = 0$, then $x = 0$ or $y = 0$. *Proof:* If $x = 0$, we're done, so suppose $x \neq 0$. Then we can multiply both sides by $1/x$ to get $y = (1/x) \cdot 0 = 0$. QED. (Of course we could just as well have started by supposing $y \neq 0$ and then showing $x = 0$.

We'll analyze the logic here more closely in the next section.

[1] So in a restaurant run by mathematicians, the menu would say "entrees come with a salad or french fries, but not both".

2.5 Negation

The basic idea of negation is simple, and best illustrated by example:

Examples: 1. Assertion: $x = 0$. **Negation:** $x \neq 0$.
2. Assertion: $x \in A$. **Negation:** $x \notin A$.
3. Assertion: p is a prime. **Negation:** p is not a prime.

In general, the negation of "P is true" is "P is false". In practice, however, it's not always so simple, because we often need to unwind "P is false" in more detail. In the first two examples above, there is nothing to "unwind". But in the third example, we need to be able to say exactly what "p is not a prime" means: It means that there exist $a, b \in \mathbb{N}$ with $p = ab$ and $a, b > 1$. The more complicated the assertion, the more difficult it becomes to properly unwind its negation. This is one of the main problems to be addressed in this section. Keep in mind throughout the following basic criterion.

Negation Test. Suppose P and Q are assertions. To say that Q is the negation of P means that P is true or Q is true, but not both. (Or to say it another way: Q is true if and only if P is false.)

So if you have a candidate Q that you think is the negation of P, but aren't sure, ask yourself two questions: (i) Is it always the case that either P or Q is true? (ii) Is it possible for both P and Q to be true? The answers have to be yes to (i) and no to (ii), otherwise you don't have the correct negation. In the simple examples listed above, the test is obviously passed: e.g. in the first example x is either zero or not zero, and can't be both. But as we'll see, things can get more complicated.

In symbols, the negation of P is written $\neg P$. Thus if P is "$x = 0$", $\neg P$ is "$x \neq 0$".

In the context of proofs, understanding negation is important for at least three reasons: (1) Proving an assertion is false amounts to proving its negation is true; (2) one method of proof involves converting an implication to "contrapositive form", in which both the hypothesis and the conclusion are negated; and (3) another very common method is "proof by contradiction" which involves negating the conclusion.

2.5.1 Complements

Complements provide a simple example of negation, but with one possible pitfall. Let X be a set and suppose $A \subseteq X$ is a subset. The *complement* A^c of A in X is

$$A^c = \{x \in X : x \notin A\}.$$

For example, if $X = \mathbb{Z}$ and A is the subset $\mathbb{Z}_{ev}$ of even integers, then A^c is the subset $\mathbb{Z}_{odd}$ of odd integers. Note that $A \cap A^c = \emptyset$, $A \cup A^c = X$, and $(A^c)^c = A$. Finally, note that the negation of $x \in A$ is $x \in A^c$.

The potential pitfall is that the notation A^c is ambiguous without further context. It is the complement of A, but in what? For example, if $A = \mathbb{Z}_{ev}$ is regarded as a subset of $\mathbb{R}$, then A^c is the set of all real numbers that are not even integers. Therefore the notation A^c

should be used only when the context, i.e. the set X in which A is being considered, has been specified.

An alternative and perhaps better notation is

$$X \backslash A = \{x \in X : x \notin A\}.$$

The advantage of this notation is that it displays the set X as well as the subset A, and therefore avoids the above ambiguity. A possible disadvantage is that one can get involved in unsightly combinations such as $X \backslash (X \backslash A) = A$, as opposed to the more attractive $(A^c)^c = A$. We'll usually use the A^c notation, taking care to specify the set X in advance.

2.5.2 Negation of and/or statements

There are two pleasantly simple rules here:

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

and

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

The equal signs are to be interpreted as "is logically equivalent to". Here are some examples of the first rule:

Examples. 1. Assertion: n is even and positive. **Negation:** n is odd or non-positive (i.e. ≤ 0; don't make the mistake of saying "negative" when you mean non-positive).

2. Assertion: $a < x < b$ (remember the hidden "and"). **Negation:** $x \leq a$ or $x \geq b$.

3. Assertion: a divides b and c. **Negation:** a doesn't divide b or a doesn't divide c.

Some examples of the second rule:

Examples. 1. Assertion: $x = 0$ or $x = 1$. **Negation:** $x \neq 0$ and $x \neq 1$ (as a shorthand, we often write this as $x \neq 0, 1$).

2. Assertion: $|x| > 2$. **Negation:** $|x| \leq 2$. To see how this fits Rule 2, note that the assertion can be written as $x < -2$ or $x > 2$. So the negation is $x \geq -2$ and $x \leq 2$, i.e. $|x| \leq 2$.

3. Assertion: n is divisible by 2 or divisible by 3. **Negation:** n is not divisible by 2 and not divisible by 3.

As a final example we consider how these rules are reflected in the very handy "DeMorgan's Laws". These laws are obvious if you draw a picture (a so-called Venn diagram, but you can do this without the venerable Mr. Venn), or just think of an everyday example. We'll prove them anyway to make the connection with the logic.

Proposition 2.5 *Let X be a set and suppose $A, B \subseteq X$. Then*

a) $(A \cap B)^c = A^c \cup B^c$.

b) $(A \cup B)^c = A^c \cap B^c$.

Proof: I'll only do part (a); part (b) is similar and left to you. We need to show that the sets $(A \cap B)^c$ and $A^c \cup B^c$ have the same elements. Well, $x \in (A \cap B)^c$ means $x \notin A \cap B$, which means the negation of the assertion "$x \in A$ and $x \in B$" is true for x. But by our rule, the negation of this latter assertion is "$x \notin A$ or $x \notin B$". This means $x \in A^c$ or $x \in B^c$, which in turn means $x \in A^c \cup B^c$. Thus $x \in (A \cap B)^c \Leftrightarrow x \in A^c \cup B^c$, QED.

2.5.3 Negations involving the quantifiers $\forall$, $\exists$

Recall that $\forall$ means "for all". Another commonly used symbol is $\exists$ for "there exists". The symbols $\forall$ and $\exists$ are known as "quantifiers". Roughly speaking, negation reverses these two symbols. In fact, we've already seen some examples of this when we discussed counterexamples. The first example from that section can be restated as follows:

Assertion: $\forall$ primes p, p is odd.[2] **Negation:** $\exists$ a prime p such that p is even.

Similarly, the negation of "all mammals are cats" is "there is a mammal which is not a cat", which we can restate as:

Assertion: $\forall$ mammals x, x is a cat. **Negation.** $\exists$ a mammal x such that x is not a cat.

Similarly, when we negate a "$\exists$", we get a "$\forall$".

Examples. 1. Assertion: $\exists x \in \mathbb{Q}$ such that $x^2 = 2$. **Negation:** $\forall x \in \mathbb{Q}$, $x^2 \neq 2$.

2. Assertion: $\exists$ a prime p such that p divides n. **Negation.** $\forall$ primes p, p does not divide n.

When there are two or more quantifiers in the same implication, things get more complicated. If you don't let abstract notation bother you, however, it's not so bad. Here's a plain English example:

Example. Assertion: Every student in the class has a relative who is at least six feet tall. **Negation:** There is a student in the class all of whose relatives are less than six feet tall.

Pretty simple, right? Now compare this with:

Example. Assertion: $\forall s \in C$ $\exists r \in R(s)$ such that $h(r) \geq N$. **Negation:** $\exists s \in C$ such that $\forall r \in R(s)$, $h(r) < N$.

This is just the same example in disguise! C is the set of students in the class, $R(s)$ is the set of relatives of student s, $h(r)$ is the height of r (measured in feet), and $N = 6$.

Examples of this type are very common in mathematics. The assertion in the next example is the definition of convergence of a sequence of real numbers (studied in detail in Math 327). If you're trying to show a sequence does *not* converge, you need to know how to negate the definition. This time there are three quantifiers in the original assertion.

Example. Assertion: $\forall \epsilon > 0$ $\exists N \in \mathbb{N}$ such that $\forall n \geq N$ $|x_n - x| < \epsilon$. **Negation:** $\exists \epsilon > 0$ such that $\forall N \in \mathbb{N}$ $\exists n \geq N$ such that $|x_n - x| \geq \epsilon$.

[2]There's an awkward English grammar point here. Many people (including me) often say "for every" instead of "for all". So if $\forall$ is to mean "for every", it should say "prime" instead of "primes". Take your pick!

2.6 The contrapositive and its use in proofs

The *contrapositive* of the implication $P \Rightarrow Q$ is $\neg Q \Rightarrow \neg P$. In contrast to the converse, the contrapositive is logically equivalent to the original implication: one is true if and only if the other is true.

Examples. 1. Assertion: If $x \in \mathbb{Z}$ then $x \in \mathbb{Q}$. **Contrapositive:** If $x \notin \mathbb{Q}$ then $x \notin \mathbb{Z}$.

2. Assertion: All cats are mammals. **Contrapositive:** All non-mammals are non-cats. (This works because "all cats are mammals" can be rephrased as "if an animal is a cat, then it is a mammal".)

3. In this example we suppose A, B are subsets of a given set X. Assertion: $A \subseteq B$. Contrapositive: $B^c \subset A^c$. (This works because $A \subseteq B$ can be rephrased as "$x \in A \Rightarrow x \in B$", while $B^c \subset A^c$ can be rephrased as "$x \notin B \Rightarrow x \notin A$".)

Note that examples 1 and 2 are really just special cases of example 3.

Sometimes we prove an implication by proving its contrapositive instead. Knowing when to do this takes a little practice. Here's a simple example:

Proposition 2.6 *Suppose $n \in \mathbb{Z}$. If n^2 is odd, then n is odd.*

Proof: Recalling that "odd" means "not even", the assertion says that if n^2 is not even, then n is not even. The fact that we have a negation in both the hypothesis and the conclusion strongly suggests that we should simplify life by proving the contrapositive instead: If n is even, then n^2 is even. And indeed the proof of the contrapositive is trivial: If $n = 2m$, then $n^2 = 4m^2$ is divisible by 2, QED.

In fact this is a special case of Proposition 2.3, which showed that if ab is odd then a is odd and b is odd. With the contrapositive we can now give a simpler proof. Using our rule for negating "and", we see that the contrapositive says that if a is even or b is even, then ab is even. In this form the proof is trivial: If a is even, say $a = 2m$, then $ab = 2mb$ is even. The case when b is even is identical. QED.

Remark. When forming the contrapositive of a proposition, don't include "background hypotheses". For example, in the preceeding proposition the assumption $n \in \mathbb{Z}$ is a background hypothesis that just sets the stage (in fact "n is odd" doesn't even make sense unless $n \in \mathbb{Z}$). We are only taking the contrapositive of "n^2 odd $\Rightarrow$ n odd".

2.7 Proof by contradiction

I'll begin with an example, then explain the logic.

Proposition 2.7 *Suppose $m \in \mathbb{Z}$ and for all $n \in \mathbb{N}$, $n|m$. Then $m = 0$.*

Proof: By contradiction, as follows: Suppose $m \neq 0$. By assumption, every natural number n divides m. So if $m > 0$ then $m+1$ divides m and hence $m+1 \leq m$, which is a contradiction. (It's also common to say "which is absurd".) If $m < 0$ then the same reasoning shows $|m|+1$ divides $|m|$, again a contradiction. QED.

In general a proof by contradiction proceeds as follows. We want to prove $P \Rightarrow Q$, i.e. we want to show that if P is true, then Q is true. We suppose (in order to reach a contradiction) that Q is false and deduce a statement R that is known to be false. Since a true statement cannot imply a false conclusion, the assumption "Q false" must itself be false, i.e. Q is true! A more precise analysis of the logic is given below.

A key point: Usually we don't know in advance what the "contradiction" R will be. In some cases it takes a while before we finally arrive at a contradiction. As the next example shows, it's also possible that the "contradiction" method is used only for one step of the proof.

Proposition 2.8 *If $n \in \mathbb{N}$ and $n > 1$, then there is a prime that divides n.*

Proof: Consider the set A consisting of all positive divisors d of n such that $d > 1$. Note that $A \subset \{2, 3, ..., n\}$, so A is a finite and therefore has a minimal element a. In other words, a is the smallest positive divisor of A other than 1. I claim that a is prime. Suppose (in order to reach a contradiction) that a is not prime. Then $\exists b, c \in \mathbb{N}$ such that $b > 1$, $c > 1$ and $bc = a$. But then b, c are also divisors of n, and $b, c < a$, contradicting the minimality of a. So a is a prime dividing n, QED.

Remark. Later we'll show that n can be factored into prime factors, using the method of "proof by induction". In fact you can easily convince yourself that this is true without using induction (try it!). But we'll wait for the induction proof because it is more systematic and

We'll see many more examples of proof by contradiction in the next section and thereafter. It takes some practice to get a feeling for when proof by contradiction is an appropriate strategy.

We conclude this section with a more precise analysis of the logic involved in the method of proof by contradiction. This is not required reading; it isn't necessary to understand the details of the logic in order to *use* the method.

First of all, I claim that $P \Rightarrow Q$ is logically equivalent to $(\neg P) \vee Q$. In fact we know that in general $R \vee S$ is equivalent to $\neg R \Rightarrow S$. Applying this to $R = \neg P$ and $S = Q$ shows that $(\neg P) \vee Q$ is logically equivalent to $\neg(\neg P) \Rightarrow Q$, i.e. to $P \Rightarrow Q$. This proves my claim. If we now apply our rule for negating an "or" statement, we find

$$\neg(P \Rightarrow Q) = \neg(\neg P \vee Q) = P \wedge \neg Q.$$

Once again I am using "=" to mean "is logically equivalent to". In other words, the negation of "P implies Q" is "P and not Q", where in everyday language we might say instead "P but not Q". In a proof by contradiction, what we're actually doing is showing

$$P \wedge \neg Q \Rightarrow R,$$

where R is a false statement. Since a true statement cannot imply a false statement, $P \wedge \neg Q$ must be false, and therefore its negation $P \Rightarrow Q$ is true. Whew!

For still more detail on this logic, see the text by Devlin.

2.8 The empty set, and a peculiarity of logic

The empty set, denoted $\emptyset$, is the set with no elements. It might seem a silly set to consider, but in fact it's very important; I can't imagine doing without it. Indeed the empty set is to sets as zero is to numbers, and who would be willing to do without 0? One way to visualize the situation is to think of a set as a box and its elements as things inside the box; the empty set then corresponds to an empty box.

Example. What is the solution set $S \subset \mathbb{R}$ of $ax^2 + bx + c = 0$? Well, if $b^2 - 4ac < 0$ then $S = \emptyset$, by the quadratic formula (there are still complex solutions, but we're talking about real solutions). If $b^2 - 4ac \geq 0$ then $S \neq \emptyset$; I'll omit writing it out explicitly. The empty set provides a way to denote the case where there are no solutions.

All this is presumably familiar, or in any case transparent. The main point of this section is a peculiarity of the logic of the empty set that is probably not familiar.

First of all, I claim that if X is any set whatsoever, then $\emptyset \subseteq X$; i.e. the empty set is a subset of *every* set. From an intuitive point of view this makes perfect sense: If we want to take a few things out of the box—i.e., choose a subset of X—one option is to take nothing, i.e. choose the empty set. In fact if X is a deck of cards, there are various card games in which (on your turn) you get to take a number of cards from the deck, but with the option of not taking any—i.e. choosing the empty set.

But now let's look at the actual rigorous definition of "subset". To say that $A \subseteq X$ means that $x \in A \Rightarrow x \in X$. Applying this to $A = \emptyset$, we need to show that if $x \in \emptyset$, then $x \in X$. In words, if x is an element of the empty set then it is an element of X. But there aren't any elements in $\emptyset$, so it may seem strange to consider the statement

$$x \in \emptyset \Rightarrow x \in X$$

a true statement. To convince yourself that this makes sense, consider that the only alternative is that the statement is false, which means its negation is true. Now the negation says: $\exists x \in \emptyset$ such that $x \notin X$. This is absolutely, positively, clearly false since there is no $x \in \emptyset$. So the displayed statement really is true.

Pursuing this line of reasoning further leads to the following general fact of life from logic that looks even weirder: Suppose P is a false statement. Then the implication $P \Rightarrow Q$ is automatically true, whether Q is true or not! For a detailed discussion of this issue, see the book by Devlin. We won't need the general fact, however. All we'll need—occasionally—is the discussion above of the empty set.

2.9 Summary of notation

- $\forall$: for all, or for every.
- $\exists$: there exists.
- $P \Rightarrow Q$: P implies Q, or "if P, then Q".
- $P \Leftrightarrow Q$: P if and only if Q; i.e. P and Q are logically equivalent.

- $P \wedge Q$: P and Q.
- $P \vee Q$: P or Q.
- $\neg P$: not P
- $x \in A$: x is an element of A.
- $A \subseteq B$: A is a subset of B.
- $A \cup B$: A union B.
- $A \cap B$: A intersect B
- A^c: the complement of A in X (when X is understood).
- $X \backslash A$: the complement of A in X (when we need to specify X for clarity).
- $\emptyset$: the empty set.
- $a|b$: a divides b (here a, b are integers).

2.10 Exercises

Note: "Show that" means the same thing as "prove". In problems asking for the negation of an assertion, give the negation in expanded form whenever possible. For example, in 6a the answer "A is not bounded above" is unacceptable. The whole point is to give an expanded, precise statement of what it means to be "not bounded above".

1. Suppose $a, b \in \mathbb{N}$. a) Show that $a|b \Rightarrow a \leq b$.

b) State the converse to the assertion in (a). Is the converse true? If true, prove it; if false, give a counterexample.

2. a) Suppose $a, b, c \in \mathbb{Z}$. Show that if $a|b$ and $a|c$, then $a|(b + c)$.

b) State the converse to the assertion in (a). Is the converse true? If true, prove it; if false, give a counterexample.

3. Which natural numbers have an odd number of divisors? Your answer should be a biconditional statement, i.e. n has an odd number of divisors if and only if ...(fill in the blank, and prove your answer!)

Notes: 1. The set of divisors of n is $\{a \in \mathbb{N} : a|n\}$. For example, 15 has four divisors 1,15,3,5, while 25 has 3 divisors 1,5,25.

2. The first step is to guess the answer. For this purpose you should just compute the answer directly for enough small values of n. But you absolutely cannot *prove* anything by just doing examples. Your proof has to work for *all* n.

3. Don't use the unique factorization theorem for integers (if you happen to know it), since we haven't proved it yet.

4. For which natural numbers n is it true that n, $n+2$ and $n+4$ are all prime? Your answer should be stated and proved as a biconditional, as in the previous problem.

5. Find counterexamples to the following statements.
a) All primes are odd.
b) All birds can fly.
c) Every non-constant polynomial with real coefficients has a real root.

6. Suppose A is a set of real numbers. We say that A is *bounded above* if there exists some $B \in \mathbb{R}$ such that $a \leq B$ for all $a \in A$. We say that an element of $x \in A$ is *maximal* if $\forall a \in A$, $a \leq x$.
a) State the negation of "A is bounded above".
b) Is the empty set bounded above?
c) State the negation of "A has a maximal element".
d) Show that if A has a maximal element, then A is bounded above.
e) Is the converse of part (d) true? Prove or disprove.

Remark. There are evident analogous definitions of "bounded below" and "minimal element", and corresponding exercises analogous to abcde above. As an optional exercise, figure out for yourself what the definitions must be. Then formulate and prove the analogous exercises (e.g. part (d) would say "if A has a minimal element, then A is bounded below").

7. State the negations of the following statements:
a) Every child at the party gets a balloon and at least three cookies.
b) $\forall x \in X$, $f(x) = 1$ and $g(x) \geq 3$.
(Note the two parts are logically identical!)

8. The distribution of primes among all the natural numbers is an interesting and much-studied question. As an example of what's meant by the question "how are the primes distributed?", we can ask whether there is any bound to the length of the gap between consecutive primes $p < q$. Up to $p = 7$ the gap is 1 or 2, but four steps are needed to get to the next prime, 11. If $p = 23$, then the next prime is $q = 29$, a gap of 6. Show that in fact arbitrarily large gaps can occur between consecutive primes; i.e. there no upper bound on the size of the gaps.
Hint. For $n \geq 2$, consider the sequence of consecutive numbers $n! + 2, n! + 3, ...n! + n$. Are any of these prime?

9. A real-valued function $f(x)$ on $\mathbb{R}$ is said to be *continuous* at $x_0 \in \mathbb{R}$ if:
$\forall \epsilon > 0$ $\exists \delta > 0$ such that $|x - x_0| < \delta \Rightarrow |f(x) - f(x_0)| < \epsilon$.
Negate this assertion. It contains a "hidden" quantifier after the "such that".

10. In this problem you'll prove the following handy fact:
Proposition: Let $n \in \mathbb{N}$, and $n > 1$. Suppose no prime $p \leq \sqrt{n}$ divides n. Then n is prime.
This greatly speeds up the problem of showing that a given n is prime (or not). For example, is 119 prime? Since $\sqrt{119} < 11$, we only have to check the primes $2, 3, 5, 7$. None of these divide 119, so it is a prime.

Now, for the proof of the proposition: This is a case that calls for the contrapositive. The reason is that the hypothesis and the conclusion are both negative statements, so that taking the contrapositive yields simpler, positive statements. In the case of the conclusion "n is prime" you have to unwind it to see the negativity: n is prime means that it has no divisors other than itself and 1. Your problem then is to:

a) State the contrapositive form of the proposition; and

b) Prove the contrapositive form.

3 Some famous theorems and proofs

3.1 The sum of the first n positive integers

According to a famous story about Gauss, his third-grade teacher once asked the class to add up all the numbers from 1 to a 100 (just to keep them busy, apparently). Gauss wrote down the answer, namely 5050, immediately. How did he do it? Here's where a little creativity comes in. Imagine writing down all the numbers from 1 to 100 in a single horizontal line. You don't need to actually do it; just imagine it. Now write them again in a second row below the first, but in reverse order:

1	2	3	.	.	.	99	100
100	99	98	.	.	.	2	1

Each pair sums to 101. There are 100 pairs. So the total sum of both rows is $(101)\cdot(100) = 10,100$. But this is twice the sum we wanted so we divide by 2 to get 5050.

Since we (you and I) are mathematicians, we aren't satisfied with a single example. We want to know the general formula for the sum of the first n positive integers for *any* positive integer n, not just $n = 100$. But a moment's reflection should convince you that Gauss' method works fine in the general case. Aha! We have our theorem, and its proof, simultaneously:

Theorem 3.1 $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Proof: Write the integers from 1 to n in a horizontal row. Write them again in reverse order, in a second row beneath the first:

1	2	3	.	.	.	n-1	n
n	n-1	n-2	.	.	.	2	1

Each pair sums to $n + 1$. There are n pairs. So the total sum of both rows is $n(n + 1)$. But this is twice the sum we wanted, so we divide by 2 to get $\frac{n(n+1)}{2}$.

I regard this argument as convincing enough to be called a proof. Nevertheless, it will be worth our while to come back later and re-do it via "proof by induction". In the latter form the argument will be rigorous enough for even the strictest Court of Mathematical Law.

3.2 The irrationality of $\sqrt{2}$

Two and a half millenia ago, at the time Pythagoras, Greek mathematicians made the surprising discovery that not all numbers are rational. For example, consider $\sqrt{2}$. Pythagoras knew that a square root of 2 exists, because it is the length of the hypotenuse of a right triangle whose other two sides have length 1. However:

Theorem 3.2 *$\sqrt{2}$ is not a rational number. In other words, there are no integers a, b such that $(\frac{a}{b})^2 = 2$.*

Proof: The method of proof is a common one, known as "proof by contradiction". We suppose that such integers a, b *do* exist, and show that this leads to a contradiction. Since a true assertion cannot imply a false assertion, the assumption we started with must be false. We'll consider proofs by contradiction more systematically soon.

So, suppose (in order to reach a contradiction) that there are integers a, b such that $(\frac{a}{b})^2 = 2$. Of course a, b are nonzero. Moreover, we may assume that a, b have no common factor; for if they did, we could just cancel out the common factor and still have a fraction whose square is 2. Now $a^2 = 2b^2$, so a^2 is an even number. But if a^2 is even, then so is a (why?). By definition, this means that $a = 2c$ for some integer c. Hence $4c^2 = 2b^2$ and $2c^2 = b^2$. Therefore b^2 is even, so b is even. Thus 2 is a common factor of a and b, contrary to assumption. This contradiction proves that our initial assumption $(\frac{a}{b})^2 = 2$ was false, so no such a and b exist. QED!

As it stands, this is a not a very satisfying theorem, for at least two reasons. The first is almost philosophical: If $\sqrt{2}$ isn't a rational number, then what kind of "number" is it? The standard answer is that it is a "real number", but this is no answer at all if we don't first explain what "real number" means. We'll return to this issue later.

The second drawback of the theorem is that it only deals with one little case, namely $\sqrt{2}$. What about $\sqrt{3}$, or $\sqrt{79}$? What about the cube root of 207? We want a theorem that deals with a more general case, so that we can at least answer the question: For which positive integers n is $\sqrt{n}$ rational? We'll return to this later too. In particular, we'll see that there are infinitely many irrational numbers, just as there are infinitely many rational numbers. We'll even prove the amazing fact, due to Cantor, that there are "more" irrational numbers than there are rational numbers. At first this sounds absurd; how can one infinity be bigger than another? Indeed the assertion makes no sense at all without a precise definition of what is meant by "more" or by saying one infinity is "bigger" than another. Cantor's great accomplishment was to recognize that there is a way to make this precise.

3.3 The division theorem

In early school days you learned how to divide one natural number into another, with remainder: 5 goes into 17 three times with a remainder of 2; in other words, $17 = 3 \cdot 5 + 2$. The key point is that the remainder $r = 2$ satisfies $0 \leq r < 5$, and that the numbers 3 and 2 obtained in this way are uniquely determined by 17 and 5. The precise general statement of the result is the division theorem of Euclid, often called the "division algorithm" because the proof in fact yields an algorithm for computing the multiple (i.e. 3 in the above example) and the remainder. It works for all integers and is stated as follows:

Theorem 3.3 *Let n, b be integers with $b > 0$. Then there exist unique integers r, s with $0 \leq r < b$ such that $n = sb + r$.*

Instead of just giving the proof, this time let's think about how you would discover a proof in the first place. Here's one line of thought: First of all, it's a little easier on the brain to start from the special case $n \geq 0$. Also we'll just worry about the existence part first, and consider uniqueness later. Visualize n on the number line. If $n < b$ then obviously we

just take $s = 0$ and $r = n$. So assume $n \geq b$. Start marking off the points $b, 2b, 3b....$ (Use more vivid imagery, if it helps. I picture a little frog hopping along in jumps b units long.) Since $b \geq 1$, eventually we get to a multiple of b, say kb, with $kb > n$. (Hop, hop!) If kb is the smallest such multiple, then taking $s = k - 1$ we see that sb is the largest multiple of b such that $sb \leq n$ (i.e. the last place the frog lands before passing point n). Thus the distance between sb and n is less than the length b of each jump, and this distance is the desired remainder. Now let's make all this precise.

Proof of existence. Assume for the moment that $n \geq 0$; at the end we will easily deduce the result for $n < 0$. Consider all multiples kb of b, $k \geq 0$. Let $s \in \mathbb{N}_0$ be maximal such that $sb \leq n$. Let $r = n - sb$. Then $0 \leq r$, and $n = sb + r$. What remains to be shown is that $r < b$. But if $r \geq b$, then $(s + 1)b \leq n$, contradicting the maximality of s. This completes the proof when $n \geq 0$.

If $n < 0$, we use a little trick to avoid doing the same work over again. By what we already proved $-n = sb + r$, so $n = -sb - r$. If $r = 0$, we're done. If $r \neq 0$, then $0 < b - r < b$, so $n = -(s + 1)b + b - r$ and again we're done (note the remainder in this last case is $b - r$).

Remark. The one possible gap in the above proof is the statement "let s be maximal such that $sb \leq n$". A sceptic might argue that I didn't prove that such an s exists. But as we are taking the natural numbers for granted, we can also take it as "obvious" that s exists (certainly it is obvious to the frog). The skeptic will need to start from the Peano axioms for the natural numbers, and take it from there.

Now let's think about the uniqueness. What does this mean, exactly? The question is whether we could have two expressions of the form $n = s_1 b + r_1$, $n = s_2 b + r_2$ as above. The uniqueness assertion is that we must then have $s_1 = s_2$ and $r_1 = r_2$. The first step in a situation like this is to directly equate the two expressions:

$$s_1 b + r_1 = s_2 b + r_2.$$

Then you have to stare at the equation a while to see how to extract the desired equalities. Don't be afraid to just try something! You don't have to be clairvoyant and see all the way to the end of the proof in advance. Take one step at a time and hope something good happens. In this case you might say to yourself, hey, let's put the b's on one side and the remainder terms on the other, just to see if that leads to inspiration:

$$s_1 b - s_2 b = r_2 - r_1.$$

So, b divides $r_2 - r_1$ (this is synonymous with "$r_2 - r_1$ is a multiple of b"). Aha! We know r_1, r_2 are nonnegative numbers $< b$. So $|r_2 - r_1| < b$, which means there is only one way that $r_2 - r_1$ can be a multiple of b, namely $r_2 - r_1 = 0$. So $r_1 = r_2$. The preceding displayed equation then shows $s_1 = s_2$.

Our official write-up of the proof is shorter:

Proof of uniqueness. Suppose we had two such expressions $n = s_1 b + r_1 = s_2 b + r_2$. We must show $s_1 = s_2$ and $r_1 = r_2$. We can assume $r_1 \geq r_2$ (if not, just switch the subscripts). Then subtracting r_2 from both sides we get $s_1 b + r_1 - r_2 = s_2 b$. Therefore b divides $r_1 - r_2$.

But $0 \leq r_1 - r_2 < b$, so this only possible if $r_1 - r_2 = 0$; hence $r_1 = r_2$. It follows that also $s_1 = s_2$, as we wanted. QED.

3.4 The infinitude of primes

Given that prime numbers are the basic building blocks for all numbers, in the sense described in the previous section, we'd like to know more about them. For starters, is there a finite list of all primes? If so, we certainly want to know what it is. But over two thousand years ago, Euclid showed the answer is "no": there are infinitely many primes.

This assertion could be viewed as flawed, because we haven't even defined the term "infinitely many". After all, "infinity" is a rather subtle concept. Small children often ask "what's the biggest number?". I recently asked a class of kindergarten students (age 5) if they thought there was a "biggest number", and received many enthusiastic replies ranging from "a hundred" to "a million" to my favorite, "two hundred and eight!". Now, how would you explain, or "prove" to a 5-year old that there is no biggest number? You would point out that no matter how big a number we choose, we can always add one to it to get a bigger number. This is a proof by contradiction in disguise: Suppose there is a biggest number N. Then $N + 1$ is bigger, contradiction! For present purposes, rather than talking about the size of the number, I want to rephrase the issue as saying "there are infinitely many positive integers", or "the set of all positive integers is infinite". What do I mean by "infinite"? I mean "not finite". Ah, but what do we mean by "finite"? It's tricky, but for now let's just say, admittedly a bit vaguely, that a set is finite if its elements can be listed in the form $x_1, ..., x_n$ where n is a positive integer.

Theorem 3.4 *There are infinitely many primes.*

Proof: This is another proof by contradiction, parallel to the proof we gave the 5-year old, but requiring a creative step. Suppose (in order to reach a contradiction) that there are only finitely many primes, and label them $p_1, p_2, ..., p_n$. Let

$$m = p_1...p_n + 1.$$

In other words, multiply them together and add one (to think of doing this is the creative step). In the previous section we showed that m can be factored into primes, and in particular there is a prime q that divides m. But none of the p_i's divide m, because by the very definition of m the remainder obtained after dividing m by p_i is 1. So q is not equal to any of the p_i's, contradicting the assumption that the p_i's are the *only* prime numbers. QED.

3.5 Exercises

The goal of these exercises is to prove the following theorems A and B, plus a bit more in Exercise 5. Let $a, b \in \mathbb{R}$ with $a < b$.

Theorem A. There is a rational number x with $a < x < b$.
Theorem B. There is an irrational number y with $a < y < b$.

The significance of these theorems lies in the fact that it doesn't matter how close together a and b are; we can always squeeze a rational number and an irrational number between them.

1. A basic fact about $\mathbb{R}$ that we assume is this: $\forall x \in \mathbb{R}\ \exists n \in \mathbb{N}$ such that $n > x$. (Think of x as positive and large; the point is that it doesn't matter how big x is; we can always find a natural number that's even bigger. With the number line visualization of the real number system, this is intuitively pretty clear.) Using this fact, show that:

a) For all $h > 0$ (no matter how small), there is a rational number r with $0 < r < h$. (Take $r = 1/n$ for suitable $n \in \mathbb{N}$.)

b) For all $h > 0$ (no matter how small) and all $x > 0$, $\exists n \in \mathbb{N}$ such that $nh > x$. ("The journey of a thousand miles begins with a single step.")

2. Assume $a \geq 0$ and prove Theorem A as follows: By 1a we can choose a rational number r with $r < b - a$. By 1b $\exists n \in \mathbb{N}$ such that $nr \geq b$. Choose the minimal such n. Show that $(n-1)r$ is rational and $a < (n-1)r < b$.

3. To complete the proof of Theorem A, we need to consider the case $a < 0$. Deduce this case from the previous case (exercise 2): There exists $n \in \mathbb{N}$ such that $a + n \geq 0$ (why?). Note $a + n < b + n$ and quickly complete the proof.

4. Theorem B now follows easily from Theorem A and the fact that at least one irrational number exists (we know that $\sqrt{2}$ is irrational), in two steps:

a) Show that if z is irrational and c is a nonzero rational, then cz is irrational (proof by contradiction works well here). Hence $c\sqrt{2}$ is irrational for all nonzero $c \in \mathbb{Q}$.

b) Show that there is a nonzero rational c such that $a < c\sqrt{2} < b$. (Use Theorem A for an instant proof!)

5. Theorems A and B are now proved. It's important to note, however, that something much stronger follows automatically: In fact there are infinitely many rational numbers and infinitely many irrational numbers between a and b. Rather than deal with the two cases separately, it's much more efficient and enlightening to formulate a general theorem that includes both:

Theorem C. Let $S \subseteq \mathbb{R}$ be any subset with the property: $\forall a < b \in \mathbb{R}$, $\exists s \in S$ such that $a < s < b$. Then $\forall a < b \in \mathbb{R}$, there are infinitely many $s \in S$ such that $a < s < b$.

Your exercise is to prove this theorem. The form of the theorem strongly suggests using proof by contradiction. Why? Because infinite means "not finite", so when you negate the conclusion "$\forall a < b \in \mathbb{R}$, there are infinitely any $s \in S$ such that $a < s < b$", you'll have an assertion involving only finite sets, which gives you something concrete to start from.

4 Proof by induction

4.1 The induction axiom

In these notes we are taking the natural numbers $\mathbb{N}$ as given. We assume without definition or proof familiar, basic structures such as addition and multiplication, together with the usual rules of arithmetic. We also take for granted the natural ordering $a < b$ and how it fits with the arithmetic. In a later section we'll reconsider these assumptions more carefully. But there is one more crucial assumption we have to make:

Induction Axiom. Suppose A is a subset of $\mathbb{N}$ such that
(i) $1 \in A$; and
(ii) $n \in A \Rightarrow n + 1 \in A$.
Then $A = \mathbb{N}$.

The term "axiom" means that we assume it without proof. It certainly seems a very reasonable assumption. Think of it this way: If $1 \in A$, then taking $n = 1$ in (ii) shows that $2 \in A$. Taking $n = 2$ in (ii) shows that $3 \in A$, and so on ad infinitum; hence every n is in A as we want. We don't consider this a proof because the "so on ad infinitum" is rather vague, and indeed it can't possibly be a proof because we haven't even defined what $\mathbb{N}$ is! Nevertheless it fits very well with our intuitive view of the natural numbers. Later we'll give Peano's more precise set of axioms for $\mathbb{N}$, one of which is the induction axiom.

The reason the induction axiom is so important is that very frequently we want to prove theorems of the form "for all $n \in N$, $P(n)$ is true", where $P(n)$ is some mathematical statement. For example, Gauss's observation about the sum of the numbers from 1 to n is of this form: If we set $s_n = \sum_{i=1}^{n} i$, then the theorem is that for all $n \in \mathbb{N}$, $s_n = \frac{n(n+1)}{2}$. We can prove this using "proof by induction", which in its abstract form is an immediate corollary of the induction axiom:

Corollary 4.1 *P*
Let $P(n)$ be a sequence of mathematical statements, $n \in \mathbb{N}$. Suppose that
(a) $P(1)$ is true, and
(b) if $P(n)$ is true then $P(n + 1)$ is true.
Then $P(n)$ is true for all n.

Proof: Let $A \subset \mathbb{N}$ denote the set of all n such that $P(n)$ is true. By assumption (a) we have $1 \in \mathbb{N}$, and by assumption (b) we know that $n \in A \Rightarrow n + 1 \in A$. Hence $n \in A$ for all n by the Induction Axiom, which is what we wanted to show.

Thus a proof by induction always involves two steps: (a) prove that $P(1)$ is true (this is called the *base case*, and is usually trivial), and (b) show that if $P(n)$ is true then $P(n + 1)$ is true. This second step is called the *inductive step*, and $P(n)$ is the *inductive hypothesis*. It might seem like circular reasoning to assume $P(n)$, but it isn't. At the inductive step we are assuming that $P(n)$ is true for a *particular* n, then showing that the next case $P(n + 1)$ must also be true. Only after the induction proof is complete do we know that $P(n)$ is true for *all* n.

In any case, the best way to get the idea is through examples of proof by induction, to which we now turn.

4.2 Example 1: Gauss' summation formula

As a first illustration, let's give a new proof of Gauss' summation formula.

Proposition 4.2 *Let $s_n = \sum_{i=1}^{n} i$. Then for all $n \in \mathbb{N}$, $s_n = \frac{n(n+1)}{2}$.*

Proof with commentary: We use proof by induction; here $P(n)$ is the statement $s_n = \frac{n(n+1)}{2}$. There are always two things to prove. First we show that $P(1)$ is true, i.e. the result is true for $n = 1$. This is called the *base case*. In the vast majority of cases, the base case is trivial; certainly it is trivial here because it just says that $1 = \frac{1 \cdot 2}{2}$.

The second step, called the *inductive step*, is to show that $P(n) \Rightarrow P(n+1)$. Here $P(n)$ is called the *inductive hypothesis*. Thus we *assume* that $s_n = \frac{n(n+1)}{2}$ for a particular n, and from this assumption *prove* that $s_{n+1} = \frac{(n+1)(n+2)}{2}$ (motto: "one case implies the next").

Now, so far all we've done is set up the inductive step. There's no telling how easy or difficult it will be to carry it out; in some cases considerable ingenuity will be required, just as in proofs in general. In the present case just one simple observation is needed, namely that $s_{n+1} = s_n + n + 1$. We then compute

$$s_{n+1} = s_n + n + 1 = \frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2},$$

where the second equality is by the inductive hypothesis and the third equality is elementary algebra that I'll leave to you to work out. The key point to note is the application of the inductive hypothesis. At any rate, this completes the proof of the proposition.

Note that if all the commentary is removed, the proof is in fact very short and sweet. One might ask, however, why we want a second proof when we already have Gauss' argument. The reason is that Gauss' argument is very special to the particular problem, and moreover requires a clever insight, whereas induction has much broader applicability and in the above case is almost mechanical (once you get used to the induction idea, I mean, and you will!).

4.3 Example 2: the max/min property

Recall the max/min property:

Proposition 4.3 *Let A be a nonempty finite set of real numbers. Then A has a maximal element and a minimal element.*

We've been assuming this statement, but now let's prove it (to be honest, we are still relying on our intuitive definition of "finite"). Along the way we'll make some further comments on proof strategies.

Suppose A has n elements. We'll first show that A has a maximal element, using induction on n. The base case $n = 1$ is dazzlingly clear: If A has a single element a, then a is the maximal element. Now suppose (inductive hypothesis) that the proposition is true for sets with n elements, and let A be a set with $n + 1$ elements $a_1, ...a_{n+1}$. We must show that A has a maximal element. By inductive hypothesis, $\{a_1, ..., a_n\}$ has a maximal element, say a_i. If $a_i \geq a_{n+1}$, then a_i is a maximal element for A as well. If $a_i < a_{n+1}$, then $a_j < a_{n+1}$ for all

$j \leq n$, so a_{n+1} is a maximal element. This completes the inductive step, and we are done! Well, we are done with the maximal case.

We still need to show that A has a minimal element. There are two ways to approach this. One is to simply say something like "the same argument shows that A has a minimal element". This is perfectly legitimate; you should check for yourself that the "same argument" performs as advertised, but there's no reason to write it out in your official proof. Another approach is to notice that the minimal case actually *follows* from the maximal case. Let $-A = \{-a : a \in A\}$ (i.e. just take the negatives of all the elements of a). Then $-A$ is finite, so has a maximal element b by what we already proved. Then $-b$ is the minimal element of A, as you can check.

4.4 Adjusting the base case

Sometimes the sequence $P(n)$ of statements we wish to prove starts with $P(0)$, or perhaps $P(m)$ for some $m > 1$. Induction applies to this situation as well; all we have to do is take the first statement in the sequence as our base case. The justification for this is that we could simply renumber our list of statements so that the first is labeled $P(1)$. For example if the list of statements we have is $P(5), P(6), ...$ we could just relabel these as $P(1), P(2)....$ But instead of relabeling, it's better and less confusing to just start the induction at base case $m = 5$ (or whatever the initial statement may be), then proceed as before. We'll illustrate with two examples. Note that the base case remains easy, and almost all of the work is in the inductive step.

The first example is a basic, important fact from calculus.

Proposition 4.4 *Let $f(x) = a_0 + a_1x + ... + a_nx^n$ be a polynomial of degree n with real coefficients a_i, where $n \geq 0$. Then the $(n+1)$-st derivative of f is identically zero.*

Proof: Write $f^{(n)}$ for the n-th derivative of a function. Let $P(n)$ denote the assertion of the proposition. Since these statements are indexed by $n \geq 0$, not just $n \geq 1$, we take $n = 0$ as our base case. In that case f is a constant function, so its first derivative is zero. At the inductive step we suppose (inductive hypothesis) that $P(n)$ is true, i.e. that a polynomial of degree n has $(n+1)$-st derivative identically zero. We then have to prove that if f has degree $n+1$, then $f^{n+2} = 0$. Well, the derivative $f'(x)$ is again a polynomial, and has degree n. So

$$f^{n+2} = (f')^{n+1} = 0,$$

where the second equality is by inductive hypothesis. QED.

The second example concerns a type of inequality that arises e.g. in the study of infinite sequences and series. We want to prove an inequality of the form $n! > 2^n$. But this isn't always true; for example $2! < 4$ and $3! < 8$. The correct statement is:

Proposition 4.5 *For all $n \geq 4$, $n! > 2^n$.*

Proof: Let $P(n)$ denote the statement $n! > 2^n$. The smallest n for which this statement is true is $n = 4$ ($24 > 16$), so we take $n = 4$ as our base case. At the inductive step, our inductive hypothesis is $n! > 2^n$, and we want to prove $(n+1)! > 2^{n+1}$. Keep in mind that we have already assumed $n \geq 4$. Then

$$(n+1)! = (n+1)n! > (n+1)2^n > 2^{n+1},$$

where the first inequality is by inductive hypothesis and the second is because $n + 1 > 2$. QED.

If k is any natural number (or for that matter, any real number) one can prove a similar equality $n! > k^n$ provided we take n sufficiently large. In other words, the bigger k is, the bigger we'll have to take our base case. Try it with $k = 3$, for example.

4.5 Well-ordering and strong induction

The next result is a variation on the induction theme, even though it looks rather different. It is sometimes called the "well-ordering principle".

Proposition 4.6 *Let A be a nonempty subset of $\mathbb{N}$. Then A has a minimal element (i.e. there is an $a_0 \in A$ such that $a_0 \leq a$ for all $a \in A$).*

Note that the analogous statement for non-negative rational numbers is false, since the subset $\{\frac{1}{n} : n \in \mathbb{N}\}$ of $\mathbb{Q}$ has no minimal element. So this property is something special about $\mathbb{N}$.

Proof with commentary: From an intuitive standpoint this is pretty clear. Since A is nonempty, some number n is in A. If it isn't the minimum, we can choose a smaller number $m < n$ in A. If m isn't the minimum, keep going; eventually the process has to stop because natural numbers can't keep getting smaller indefinitely. At this point we have reached the desired minimum.

The preceeding argument is convincing enough for most of us, but let's give a rigorous proof anyway. Since A is nonempty there is some $n \in A$. So we will show by induction on n that if n is in A then A contains a minimal element. The base case $n = 1$ is immediate, since $1 \leq m$ for *all* $m \in \mathbb{N}$ and in particular for all $m \in A$. At the inductive step we assume that all subsets containing n have a minimal element, and prove that all subsets containing $n + 1$ have a minimal element. So suppose $n + 1 \in A$. Let $B = A \cup \{n\}$. Then by inductive hypothesis B has a minimal element b_0. If $b_0 \in A$, then b_0 is minimal in A too. If $b_0 \notin A$, then we must have $b_0 = n$. In that case it follows that $n + 1$ is the desired minimal element of A. This completes the inductive step, and our proposition is proved.

Remark. In fact the preceding proposition is equivalent to the Induction Axiom. This means that if we wanted to, we could assume the well-ordering principle as an axiom and deduce the Induction Axiom from it, rather than the other way around. See the exercises.

This is essentially what we do to prove the following important variant of induction. It is known as "strong induction", although the term is misleading because it's equivalent to ordinary induction.

Proposition 4.7 *Let A be a subset of $\mathbb{N}$, and suppose the following condition holds for all $n \in \mathbb{N}$:*

(i) $1 \in \mathbb{N}$; and

(ii) If $k \in A$ for all $k < n$, then $n \in A$.

Then $A = \mathbb{N}$.

Proof: We want to show that A^c, the complement of A in $\mathbb{N}$, is empty. Suppose it isn't empty. Then by the well-ordering principle A^c has a minimal element n. Moreover $n > 1$, since by assumption (i). Thus $k \in A$ for all $k < n$. So by hypothesis, $n \in A$. But this is a contradiction, since $n \in A^c$. QED.

Remark. If you examine the logic carefully, you'll see that assumption (i) is implied by assumption (ii) and therefore is superfluous. To see why, note that the set $\{k \in \mathbb{N} : k < 1\}$ is the empty set. Hence the statement "if $k \in \mathbb{N}$ and $k < 1$ then $k \in A$ is true, because no such k exists. Therefore $1 \in A$ by the hypothesis (ii). This is an example of the third row of the truth table for $P \Rightarrow Q$ on p. 27 of Devlin: P is the statement "$k \in \mathbb{N}$ and $k < 1$", which is always false. However, processing this logic can be tricky. In practice the case $n = 1$ of condition (ii) has to be checked separately anyway, because the cases $n = 1$ and $n > 1$ may require different methods of proof. So I think it's easier on the brain to to include (i) in the statement of the theorem. In any event, the base case (i) is usually trivial to check.

As in the case of the induction axiom, we can translate this into a proof technique, called strong induction.

Corollary 4.8 *Let $P(n)$, $n \in \mathbb{N}$ be a sequence of mathematical statements. Suppose that for all $n \in \mathbb{N}$, the following conditions hold:*

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

(ii) if $P(k)$ is true for all $k < n$, then $P(n)$ is true.

Then $P(n)$ is true for all $n \in \mathbb{N}$.

The corollary follows from the proposition in exactly the same way as the analogous corollary for ordinary induction. Prove this yourself! Also, as in the case of ordinary induction it might happen that the statements $P(n)$ are indexed by $n \geq m$ for some $m \geq 0$, instead of $m = 1$. In that case we just take $n = m$ as our base case and get the same result. In other words, if the sequence of statements begins with $P(0)$ or $P(5)$, it still works (after all, we could always renumber the statements to start at $n = 1$).

Remark. As in the proposition, condition (i) is technically superfluous. But it's better to include it, as in practice (i) needs to be checked separately anyway. (As with ordinary induction, the base case might be $n = 0$ or some $n > 1$, depending on the particular problem. In the theorem below the base case is $n = 2$.)

4.6 The fundamental theorem of arithmetic, and an important property of prime numbers

To illustrate strong induction, we will prove the existence and uniqueness of prime factorizations for natural numbers $n \geq 2$. This result is customarily called the "fundamental theorem of arithmetic". Along the way we'll prove another important property of prime numbers, also using induction.

The existence of prime factorizations is comparatively easy, so we begin with that.

4.6.1 Existence of prime factorizations

Theorem 4.9 *Let $n \in \mathbb{N}$, $n \geq 2$. Then there are primes $p_1, ..., p_k$ with $n = p_1...p_k$. (The p_i's need not be distinct.)*

Proof: Let $P(n)$ be the statement "n admits a prime factorization", with $n = 2$ as the base case. The base case is certainly true, since 2 itself is a prime and therefore has a prime factorization with just one factor.

So suppose every $k < n$ has a prime factorization. (This is the strong inductive hypothesis.) We must show that this implies n has one too. If n itself is prime, we are done, for in that case it has a prime factorization with just one factor, namely itself. If n is not prime, then $n = ab$ with $a, b < n$, $a, b \in \mathbb{N}$. By the strong inductive hypothesis applied to a, b, we have factorizations $a = p_1...p_r$ and $b = q_1...q_s$ where the p_i's and q_i's are prime. Then just stick these two factorizations together: $n = p_1...p_r q_1...q_s$ is the desired prime factorization of n. QED.

To see the point of strong (as opposed to ordinary) induction, notice that ordinary induction wouldn't work in the preceding proof. For ordinary induction you need to have some usable relationship between $P(n)$ and $P(n+1)$, in order to show that $P(n) \Rightarrow P(n+1)$. But factorization of n and factorization of $n+1$ aren't related in any reasonable way; having a prime factorization of n tells you nothing at all about having one for $n + 1$. Hence the need for the "strong" inductive hypothesis.

4.6.2 An important property of prime numbers

The goal of this section is to prove:

Theorem 4.10 *Suppose $a, b \in \mathbb{Z}$. If p is a prime and p divides ab, then p divides a or p divides b.*

The proof is one of the least intuitive that we've yet encountered, and is difficult to motivate in advance. Have patience, though, and eventually enlightenment shall be yours.

We begin with a strange-looking lemma.

Lemma 4.11 *Let a, b be nonzero integers. If $a, b \in \mathbb{Z}$ have no common positive divisors other than 1, then there exist $i, j \in \mathbb{Z}$ such that $ia + jb = 1$.*

Before giving the proof, several remarks are in order. First of all, the converse is true and easy to prove. In other words, if such an i, j exist, then it must be the case that a, b have no common positive divisors other than 1. (See the exercises below.) Second, we don't care about actually finding i, j that work; we only care that such numbers exist. For small numbers one can easily find suitable i, j by fiddling around. For example, suppose $a = 10$ and $b = 21$. Then $b - 2a = 1$, so we can take $i = 1$, $j = -2$. Or suppose $a = 6$ and $b = 29$. Then $5a - b = 1$ and we can take $i = 5$, $b = -1$. An interesting project would be to cook up an algorithm for finding such i, j and write a program to implement it. But again, I emphasize that for present purposes we don't need to actually find them. Finally, note that i, j are very far from being unique. If $a = 2$ and $b = 3$, for instance, then $b - a = 1$, $2a - b = 1$, $3b - 4a = 1$,...there are infinitely many solutions, in fact.

Proof of the lemma: We start with a slick application of the Well-Ordering Theorem: Let $C = \{c \in \mathbb{N} : \exists i, j \in \mathbb{Z}\ ia + jb = c\}$. This set is nonempty because it contains, for example, $|a|$ (take $j = 0$ and $i = 1$ or -1 according as a positive or negative). So by the Well-Ordering Theorem C has a minimal element d, and by assumption $d = ia + jb$ for some i, j.

Next we show that $d|a$. Suppose (in order to reach a contradiction) that this is false. Then by the Division Theorem, $a = sd + r$ with $s, d \in \mathbb{Z}$ and $0 < r < d$. Then

$$r = a - sd = a - s(ia + jb) = (1 - si)a - (sj)b.$$

Hence $r \in C$. But $r < d$, contradicting the minimality of d. Hence $d|a$. The same argument shows $d|b$. So d is a common positive divisor of a, b, and therefore $d = 1$ by hypothesis.

This lemma is the key to the theorem, although once again the proof is not intuitive.

Proof of Theorem 4.10: Recall our standard method for proving statements with "or" in the conclusion: We suppose that p does not divide a, and prove that $p|b$. Since the only positive divisors of p are 1 and p, and p does not divide a, it follows that p and a have no common positive divisors other than 1. So by the lemma $\exists i, j \in \mathbb{Z}$ such that $ip + ja = 1$. This probably looks totally unpromising, but a clever algebra trick saves the day:

$$b = 1 \cdot b = (ip + ja)b = ipb + jab.$$

Since $p|ipb$ and $p|jab$, it follows that $p|b$! Cool, eh? I mean, QED!!

As a corollary of the theorem we have the more general statement:

Corollary 4.12 *If p divides $a_1 a_2 ... a_n$ (a product of n integers, $n \in \mathbb{N}$) then p divides at least one of the a_i's.*

Proof: Exercise. Use induction on n and the theorem.

4.6.3 Uniqueness of prime factorization

We've seen that every $n > 1$ can be factored into primes: $n = p_1 p_2 ... p_k$, where the p_i's are primes. It isn't at all obvious, however, that the number k and the primes p_i are uniquely determined by n. For example, is it possible that n has prime factorizations $n = p_1 p_2$ and $n = q_1 q_2 q_3$, where $p_i \neq q_j$ for all i, j? In this section we show this can't happen; the factorization is unique up to re-ordering. ("Up to re-ordering" means that, for example, we regard $30 = 2 \cdot 3 \cdot 5$ and $30 = 5 \cdot 2 \cdot 3$ as the same factorization.) It's a subtle fact, but fortunately we've already done the hard work in Theorem 4.10 and its corollary.

fta

Theorem 4.13 *Suppose $n \in \mathbb{N}$, $n > 1$. If $n = p_1 p_2 ... p_r$ and $n = q_1 q_2 ... q_s$ are prime factorizations, then $r = s$ and after re-ordering if necessary we have $p_i = q_i$ for all i.*

Proof: We use strong induction on n. The base case $n = 2$ is clear: the only possible prime factorization is simply $n = 2$, with one factor. At the inductive step we suppose (strong inductive hypothesis) that the theorem is true for all $m < n$, and consider two factorizations as in the statement of the theorem. Thus by assumption

$$p_1 p_2 ... p_r = n = q_1 q_2 ... q_s.$$

Then $p_r | (q_1 q_2 ... q_s)$, so by Corollary 4.12 $p_r | q_i$ for some i; after re-ordering if necessary, we can assume $i = s$. But p_r, q_s are primes, so $p_r | q_s \Rightarrow p_r = q_s$. Hence we can cancel this common factor from both sides of the above equation, obtaining

$$p_1 p_2 ... p_{r-1} = m = q_1 q_2 ... q_{s-1},$$

where $m = n/p_r = n/q_s$. Since $m < n$, by inductive hypothesis $r - 1 = s - 1$, and after re-ordering if necessary we can assume $p_i = q_i$ for $1 \leq i \leq r - 1$. Hence $r = s$, and since we already have $p_r = q_r$, this completes the proof.

In the above theorems we're writing the factorization with repetitions, e.g. $72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$. Usually it's more convenient to rewrite this as $72 = 2^3 \cdot 3^2$. Carrying out this simplification in general, we get the following equivalent form of the fundamental theorem of arithmetic:

Theorem 4.14 *If $n > 1$, then n can be factored as*

$$n = q_1^{k_1} q_2^{k_2} ... q_m^{k_m}$$

where the q_i's are distinct primes and $k_i \in \mathbb{N}$. Moreover the set of primes q_i and the exponents k_i are uniquely determined by n.

4.6.4 Another application of Theorem 4.10: More irrational numbers

With Theorem 4.10 in hand, let's return to the study of irrational numbers. We proved earlier that $\sqrt{2}$ is irrational, but it's highly unsatisfying to leave it at that. What can one say more generally? Is $\sqrt{3}$ irrational? What about the cube root of 2? We want a more general theorem. The nice surprise is that we can now very easily prove a vastly more general theorem.

Theorem 4.15 *Let $n, k \in \mathbb{N}$ and there is a rational number x such that $x^k = n$. Then $x \in \mathbb{N}$. Hence $\sqrt[k]{n}$ is irrational unless it is a natural number.*

Proof: Let $x = \frac{a}{b}$, where $a, b \in \mathbb{N}$ have no common divisors (other than 1). We want to show that $b = 1$. Suppose (in order to reach a contradiction) that $b > 1$. Then some prime p divides b. Now $a^k = nb^k$, and since $p|b$ we have $p|a^k$. But then $p|a$ by Theorem 4.10, contradicting the assumption that a and b have no common divisors. QED!

Let's look at some examples to get a better idea of what the theorem says. Often one says that n is a "perfect square" if it is the square of a natural number. So only the perfect squares have a rational square root. So we get an infinite list of irrational numbers $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}...$ But we get much more. For example, consider "perfect cubes". For n up to a hundred only $1, 8, 27, 64$ are perfect cubes, and so have a rational cube root. Or if someone on the street happens to ask you "hey, is the fifth root of 129 rational?", you can immediately answer "no", because 129 is not the fifth power of any natural number. (Well, maybe not immediately. But all you have to compute is that $2^5 < 129$ and $3^5 > 129$, which even a slow brain like mine can do without resort to electronic devices.) In any case, the main conceptual point revealed by the theorem is that irrational numbers are very common.

4.7 Another example of strong induction: expansion in a base

As another example of proof by strong induction we consider "expansion in a base". In this case, one could make ordinary induction work too, but I think it's simpler to use strong induction.

For everyday use, the standard choice of base in our world is base 10. We write a number n as a string of "digits" such as $n = 3956$, to be interpreted as $3 \cdot (10)^3 + 9 \cdot (10)^2 + 5 \cdot (10) + 6$. However, the choice of base 10 is just an artifact of our anatomy: ten fingers, ten toes. Any natural number $b > 1$ could be used in place of 10. The most natural choice is the smallest possible base, namely $b = 2$. Then the digits are all 0 or 1, which makes base 2 especially suitable for computer calculation. For example, in base 2

$$101101 = 2^5 + 0 \cdot 2^4 + 2^3 + 2^2 + 0 \cdot 2 + 1$$

which in base 10 is 43. Or if we start with 74 in base 10 and rewrite it in base 2, we get $1001010 = 2^6 + 2^3 + 2^1$ (check this!).

Note that in base b you need b different symbols to represent the digits. In base 10 we have the usual $0, 1, 2, ..., 9$. In any base $b < 10$ we can use the same symbols up to $b - 1$; e.g. in base 3 we would use $0, 1, 2$ as our digits. But if $b > 10$ then we need some new symbols to denote the higher digits. In computer science, for example, base 16 is common, and the symbols a, b, c, d, e, f are used for the new "digits". See the exercises for more on this point. The ancient Babylonians used base 60, an odd choice that has survived in vestigial form to the present day: 60 seconds in a minute, 60 minutes in an hour, $360 = (60)^2$ degrees in a circle. So the Babylonians needed 60 different symbols just for the digits!

A modern example comes from computer science, where base 16 is commonly used in place of base 2 (the problem with base 2 being that so many digits are required even for relatively small numbers). In that case the numbers 10 through 15 have to represented by

special symbols, with the usual choice being the letters $abcdef$. For example, the number 270 in base 10 is written $2e$ in base 16, since $270 = (16)^2 + 14$ and 14 is represented by the "digit" e.

Now, for "expansion in a base" to be useful, we need to know that (a) such expansions are always possible, and (b) the expansion is unique (we wouldn't want two different sequences of digits to represent the same number). Our next theorem assures us that it works.

Theorem 4.16 *Suppose $b \in \mathbb{N}$ with $b > 1$, and $n \in \mathbb{N}$.. Then n can be written uniquely in the form*

$$n = \sum_{i=0}^{t} a_i b^i$$

with $0 \leq a_i < b$ and $a_r \neq 0$.

Proof: We first prove that such an expansion exists, by strong induction on n. The base case is (as usually happens) trivial: If $n = 1$, then the single digit 1 is the base b expansion no matter what b is. At the inductive step we suppose (inductive hypothesis) that such an expansion exists for all $m < n$, and prove that there exists one for n. First write $n = sb+r$ as in the division theorem. Then $s < n$, so by inductive hypothesis we have a base b expansion

$$s = \sum_{i=0}^{k} c_i b^i.$$

Then

$$n = sb + r = \sum_{i=0}^{k} c_i b^{i+1} + r.$$

This is the expansion we want; all we have to do is relabel things:

$$n = \sum_{i=0}^{k+1} a_i b^i$$

where $a_0 = r$ and $a_i = c_{i-1}$ for $i > 0$.

For the uniqueness one again uses strong induction, as you'll show in the exercises.

4.8 Recursive definition

Sequences, say of real numbers, are customarily denoted with subscripts, e.g. $x_n = 1/n$ defines the sequence $1, 1/2, 1/3, ...$ This is the same thing, however, as a function from $\mathbb{N}$ to $\mathbb{R}$; we could equally well use function notation and write $x(n)$ instead of x_n. In some ways this is a better notation, since it emphasizes the function aspect, but we'll use both notations. We also allow the sequence to start at some $n > 1$, or perhaps at $n = 0$. In other words, we allow our functions to be defined on $\mathbb{N}_{\geq m}$ for some $m > 1$, or on $\mathbb{N}_0$.

Often sequences are defined by an explicit formula, such as $x_n = 1/n$ or $f(n) = \frac{n(n+1)}{2}$. It is also common to find sequences defined *recursively*, meaning that $f(n)$ is given in terms of $f(n-1)$ or perhaps in terms of several or all of the previous values $f(1), f(2), ..., f(n-1)$, together with an initial condition to get the ball rolling.

Example 1. Let $f(1) = 1$ (the initial condition), and for $n > 1$ define $f(n)$ by the *recursion formula* $f(n) = nf(n-1)$. Then $f(2) = 2 \cdot f(1) = 2$, $f(3) = 3 \cdot f(2) = 6$, $f(4) = 4 \cdot f(3) = 24$, and so on. Then $f(n)$ is the product of the first n natural numbers, otherwise known as $n!$.

Example 2. In this example our sequence has domain $\mathbb{N}_0$. Let $f(0) = 1$ and for $n > 1$ define $f(n)$ by the recursion formula $f(n) = f(n-1) + \frac{1}{2^n}$. Thus $f(1) = 1 + \frac{1}{2}$, $f(2) = 1 + \frac{1}{2} + \frac{1}{4}$, and so on; $f(n)$ is just the n-th partial sum of a familiar geometric series. As you may recall, there is a simple explicit formula for $f(n)$, namely

$$f(n) = \frac{1 - (\frac{1}{2})^{n+1}}{1 - \frac{1}{2}} = 2 - 2^{-(n+1)}.$$

It's a good exercise to prove this by induction on n.

Example 3. Take $A = \mathbb{R}$ and define a sequence $f(n)$ by $f(1) = \sqrt{2}$, plus the *recursion formula* $f(n+1) = \sqrt{2 + f(n)}$. So for example, $f(2) = \sqrt{2 + \sqrt{2}}$, $f(3) = \sqrt{2 + \sqrt{2 + \sqrt{2}}}$, and so on. In this case there is no apparent formula for $f(n)$, of the sort we found in example 2. Nevertheless one can analyze the sequence in terms of the recursion formula alone. For instance, if you know about limits of sequences of real numbers, it is an interesting problem (a standard exercise in Math 327) to show that $lim_{n \to \infty} f(n)$ exists and to find it explicitly.

Example 4 (The Collatz conjecture). Take $A = \mathbb{N}$ and choose some $a \in \mathbb{N}$. Define a sequence of natural numbers by $f(1) = a$ and the recursion formula

$$f(n+1) = \begin{cases} n/2 & \text{if } n \text{ even} \\ 3n+1 & \text{if } n \text{ odd} \\ 1 & \text{if } n = 1 \end{cases}$$

For example, if $a = 3$ the sequence is $3, 10, 5, 16, 8, 4, 2, 1, 1, 1, ...$ Note that by the recursion formula, if the sequence ever reaches 1 it remains there for the rest of its life. With initial condition $a = 7$ we get $7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, 1, ...$ It seems that no matter what initial condition you plug in, the sequence always returns to 1. Try it! For $a \leq 26$ it's not hard to do by hand. For $a = 27$ it still works but takes 111 steps and a high of 9,232 is reached before eventually descending back to 1. The Collatz conjecture, also known as the "3n+1 problem" is that no matter what a is, the sequence eventually returns to 1. But this remains an open problem; no one knows whether it's true or not. If you can solve it, you will be famous!

Example 5: Fibonacci numbers. In the general form of recursion, $f(n+1)$ can depend on more than one of the previous values, perhaps even on all of them. The most famous example is no doubt the sequence of Fibonacci numbers. In this case the recursion formula is

$$f(n+1) = f(n) + f(n-1),$$

in other words, to get the next number in the sequence you sum the previous two. To get started, therefore, we need two initial conditions instead of just one: We set $f(1) = 1 = f(2)$. Then the sequence begins $1, 1, 2, 3, 5, 8, 13, 21, ...$ These are the Fibonacci numbers. They have many amazing properties and applications; a good research project would be to learn more about them (and about their inventor, Leonardo of Pisa a.k.a. Fibonacci). They satisfy the surprising formula:

$$f(n) = \frac{(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n}{\sqrt{5}}.$$

It's possible to prove this formula by induction on n, with some tricky algebra at the inductive step. But that would be pointless, as it gives no insight whatsoever into how you would guess the formula in the first place. Why does $\sqrt{5}$ enter the picture? It's all very mysterious. In fact there is a beautiful, surprising proof of the formula, based on linear algebra. The matrices involved are just 2×2 matrices, but you need a good understanding of eigenvalues, eigenvectors, and the relationship between matrices and linear transformations. Then the formula will appear by magic! For those who have an understanding of the relevant linear algebra, I highly recommend looking into this.

Finally, we note that the recursion formula could even involve *all* of the previous elements. For example, one could define a sequence a_n recursively by $a_1 = 1$ and $a_{n+1} = a_1 + a_2 + ...a_n$. See the exercises.

Remark. The above discussion and the examples give a reasonably clear idea of what it means to define a sequence recursively. But what is "recursion" exactly? And how do we know that a recursion formula really does define a sequence? Recursion is closely related to induction, and indeed in many sources you'll find authors writing things like "define a sequence inductively by $f(1) = a$, $f(n+1) = f(n)^2 + 1$ or whatever the recursion formula happens to be. Although such language is common it is technically not correct; induction as we have described it applies to *proving* things, not *defining* things. We won't worry about this, and will somewhat carelessly think of recursion as being like induction. If you're curious about how it's done rigorously, one good but challenging reference for this and other matters is the chapter "Set theory and logic" in the textbook *Topology* by J.R. Munkres (often used as the text for Math 441); see the section entitled "The principle of recursive definition".

4.9 A summary of induction strategy

1. The first thing to decide is whether or not to use induction at all. Induction is only appropriate when the statement to be proved is a sequence of statements indexed by the natural numbers. For example, if the problem is "prove that the angles of a triangle sum to π radians", induction would be useless and indeed completely irrelevant, as there is no sequence of statements involved.

2. The next decision is between ordinary and strong induction. To carry out ordinary induction, you need to have or be able to figure out some relationship between $P(n)$ and

$P(n+1)$. If this doesn't seem to work, try strong induction. (In rare cases it might be easier to use the well-ordering principle, but in general you should stick with induction.)

3. Determine which case is the base case (usually it is $n = 1$, but it might be $n = 0$ or some $n > 1$, as illustrated above), and prove it. This step is usually trivial, but it still needs to be stated and checked.

4. Prove the inductive step. In ordinary induction this means you *assume* as inductive hypothesis that $P(n)$ is true, and then *deduce* that $P(n + 1)$ is true. In strong induction it means you *assume* as inductive hypothesis that $P(k)$ is true for all $k < n$, and then *deduce* that $P(n)$ is true.

In either case there is no magic formula for carrying out the inductive step; it depends on the particular problem. It might be an easy calculation, a difficult calculation, or a subtle argument requiring creative thinking.

Further refinements of the induction idea will be considered as they arise.

4.10 Exercises

1. In this problem you will prove that $\sum_{i=1}^{n} 2i - 1 = n^2$, in three different ways. Each of the three ways is instructive, and it's worth doing them all. When faced with the above sum, the first thing you notice is that it's similar to Gauss's sum $\sum_{i=1}^{n} i = n(n + 1)/2$. This suggests two possible strategies: (i) Use the same method of proof on the new formula, namely induction; or (ii) instead of imitating the proof of the old result, try to deduce the new result directly from the old (after all, why do the same work twice?).

a) First proof (option (i)): Use induction on n.

b) Second proof (option (ii)): Let $s_n = \sum_{i=1}^{n} i$ and let $t_n = \sum_{i=1}^{n} 2i - 1$. Express t_n in terms of s_n and use the formula we already have for s_n to get the formula for t_n.

c) A third, geometric method: Picture an $n \times n$ chessboard, which has n^2 squares in all. Find a way to partition (i.e. divide up into disjoint subsets) the squares into subsets of size $1, 3, 5, ..., 2n - 1$ in such a way that the above formula becomes "obvious".

(This geometric argument might not qualify as a rigorous proof, but if done right it certainly fits the requirements for an informal but very convincing demonstration.)

2. If $a, b \in \mathbb{R}$, the triangle inequality says that $|a + b| \leq |a| + |b|$. Use this fact and induction to prove that for all $n \in \mathbb{N}$, if $a_1, ..., a_n$ are real numbers then $|\sum_{i=1}^{n} a_i| \leq \sum_{i=1}^{n} |a_i|$.

3. Use strong induction to prove the uniqueness statement for expansion in a base. First let's write down the uniqueness statement explicitly. Suppose $n = \sum_{i=0}^{r} a_i b^i$ with $0 \leq a_i < b$ and $a_r \neq 0$, and also $n = \sum_{i=0}^{s} c_i b^i$ with $0 \leq c_i < b$ and $c_s \neq 0$. You need to show that $r = s$ and $a_i = c_i$ for all i.

4. Use induction to prove that $\frac{(2n)!}{2^n n!}$ is an odd integer.

5.a) Use induction on n to show that $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.

b) Part (a) is standard textbook problem. In my view, however, the problem by itself is a bit silly, since it ignores the key question of how you would ever guess such a formula in the first place. Without the guess, you're nowhere. Just to illustrate, here's one way that one could arrive at the formula above. We already know that the sum of the first n natural numbers is $n(n+1)/2 = \frac{n^2}{2} + \frac{n}{2}$. Note this is a quadratic polynomial with zero constant term. So if we're feeling lucky, we might say hey, maybe the sum of the first n squares is given by a cubic polynomial with zero constant term (the sum of the first powers leads to a quadratic polynomial, so why not be wildly optimistic and hope the sum of the second powers leads to a cubic?). If we assume such a formula exists, we can determine what the coefficients have to be, as follows: Let $s_n = \sum_{i=1}^{n} i^2$, and *assume* $s_n = an + bn^2 + cn^3$ for certain constants a, b, c. Plugging in the values $n = 1, 2, 3$ and computing s_n directly leads to three equations in a, b, c. For example, plugging in $n = 2$ yields $2a + 4b + 9c = 5$. Solve these equations (you'll find there is a unique solution). This leads to a conjectural (i.e. a guess!) formula of the form $s_n = an + bn^2 + cn^3$. (Caution: it only *proves* the formula for the special cases $n = 1, 2, 3$.) Then check that your cubic agrees with the one in part (a).

6. Use induction on n to show that for all $n \geq 0$, a set with n elements has 2^n different subsets. (Remember that for any set X, $\emptyset$ and X are subsets of X.)

7. Define a sequence a_n recursively by $a_1 = 1$ and $a_{n+1} = \sum_{k=1}^{n} a_k$. In other words, each new term is the sum of the previous terms. By checking some small values of n, guess an explicit formula for a_n. Then prove your formula by induction.

8. Use induction and Theorem 4.10 to prove Corollary 4.12.

5 Products of sets

5.1 The product of two sets

Let X and Y be sets. Their product (or "Cartesian product", in honor of Rene Descartes), denoted $X \times Y$, is the set of ordered pairs (x, y) with $x \in X$ and $y \in Y$. The most familiar example is probably the case $X = Y = \mathbb{R}$, in which case $\mathbb{R} \times \mathbb{R}$ is the usual xy-plane. But the idea makes perfectly good sense for any two sets X and Y. For example, X could be the set of famous mathematicians and Y could be the set of species of lizard; then (Gauss, blue-tailed skink) would be an element of $X \times Y$.

If $A \subseteq X$ and $B \subseteq Y$, then $A \times B \subseteq X \times Y$. Many examples of products arise in this way.

Examples. 1. $\mathbb{Z} \times \mathbb{Z} \subseteq \mathbb{R} \times \mathbb{R}$ is the set of all points in the plane having integer coordinates.

2. $\mathbb{R} \times \mathbb{N} \subseteq \mathbb{R} \times \mathbb{R}$ is the union of the horizontal lines $y = n$ with $n \in \mathbb{N}$.

3. For $a < b \in \mathbb{R}$, let $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$ (as usual). If $a < b$ and $c < d$, then $[a, b] \times [c, d]$ is the rectangle in $\mathbb{R} \times \mathbb{R}$ with corners $(a, c), (a, d), (b, c), (b, c)$.

Caution. The notation (a, b) is used for at least three completely different things in mathematics: (i) ordered pairs as described above; (ii) in the case of real numbers a and b with $a < b$, it is used to mean $\{x \in \mathbb{R} : a < x < b\}$; and (iii) in the case of integers a and b it is sometimes used for the greatest common divisor of a and b. If in doubt, consider the context to determine which meaning is intended.

Caution. Do not confuse an ordered pair (a, b) with the *set* $\{a, b\}$. In the latter case the order doesn't matter: $\{a, b\} = \{b, a\}$, where is $(a, b) \neq (b, a)$ unless $a = b$. And besides, they are different animals altogether: (a, b) is an element of $A \times B$, whereas $\{a, b\}$ is a subset of $A \cup B$. Similarly the ordered pair (a, a) is not the same thing as the set $\{a, a\}$, since $\{a, a\} = \{a\}$; they are two different animals.

Finally, note that if either X or Y is the empty set, then $X \times Y$ is also empty. Suppose, for example, that $X = \emptyset$. Then $\emptyset \times Y$ is the set of pairs (x, y) such that $x \in \emptyset$ and $y \in Y$. But there are no $x \in \emptyset$, so $\emptyset \times Y = \emptyset$. Similarly $X \times \emptyset = \emptyset$.

5.2 Multiple products

We can define 3-fold products, 4-fold products and even n-fold products in a similar way. Suppose $X_1, ..., X_n$ are sets. Then the product

$$\prod_{i=1}^{n} X_i = X_1 \times X_2 \times ... \times X_n$$

is the set of ordered n-tuples $(x_1, ..., x_n)$ with $x_i \in X_i$. The most familiar case of this construction is $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$. More generally we write X^n for the product of n copies of the set X. For example $\mathbb{Z}^4$ means ordered $4-tuples$ of integers (n_1, n_2, n_3, n_4).

Note that if $A_i \subset X_i$ for each i, then $\prod_{i=1}^{n} A_i \subset \prod_{i=1}^{n} X_i$.

6 Functions

A function consists of three pieces of data: a set A called the *domain*, a set B called the *codomain*, and a "rule" f assigning to each element $a \in A$ an element $f(a) \in B$. We summarize this data with the symbol $f : A \longrightarrow B$. In the optional reading we'll be more precise about what we mean by a "rule", but the idea should be clear enough as it stands. Keep in mind that

(i) $f(a)$ must be defined for *all* $a \in A$.
(ii) the definition of $f(a)$ must be unambiguous; it can't yield more than one element of the codomain. This condition is usually expressed by saying f is *well-defined*.

Here's an example in which both conditions fail, or at least could fail: Suppose A is the set of students in the class, and B is the set of all women in the world. Suppose I said "define a function $f : A \longrightarrow B$ by $f(a) =$ the sister of student a". This violates condition (i) because not every student in the class has a sister. It also violates condition (ii), i.e. is not well-defined, because some students have more than one sister and hence the "definition" of f is ambiguous; how do we know which sister to pick? Of course, if it happened to be the case that every student in the class has a unique sister (which seems very unlikely!), then f *would* be a function.

In the most familiar case where $A = B = \mathbb{R}$, our definition of function is just the usual definition that you're accustomed to. We input an element of A, and out pops an element of B. In fact another more suggestive terminology is to call the domain the *source* of the function and the codomain the *target*.

A critical point to note, however, is that **THE DOMAIN AND THE CODOMAIN MUST BE SPECIFIED**; otherwise you don't have a function, by this definition. For example, if you say "f is the function given by $f(x) = x^2$, you have not specified a function because you didn't specify the domain and codomain. The following are all different functions ($\mathbb{R}_{\geq 0}$ denotes the nonnegative real numbers):

Note: We do *not* require that every element of the codomain gets "hit" by some element of the domain. In other words, for $b \in B$ there might not be any element of a such that $f(a) = b$. For example, with $A = B = \mathbb{R}$ and $f(x) = e^x$, $f(x)$ is always positive. But this is still a function $\mathbb{R} \longrightarrow \mathbb{R}$. Similarly, again with $A = B = \mathbb{R}$, the function $g(x) = \sin x$ takes values between -1 and 1. But it is still a function $\mathbb{R} \longrightarrow \mathbb{R}$. The values of f that actually occur constitute the *image* of f, to be defined and discussed later.

$f_1 : \mathbb{R} \longrightarrow \mathbb{R}$ given by $f_1(x) = x^2$.
$f_2 : \mathbb{R}_{\geq 0} \longrightarrow \mathbb{R}$ given by $f_2(x) = x^2$.
$f_3 : \mathbb{R}_{\geq 0} \longrightarrow \mathbb{R}_{\geq 0}$ given by $f_3(x) = x^2$.
$f_4 : \mathbb{N} \longrightarrow \mathbb{N}$ given by $f_4(x) = x^2$.

In each case the rule is the same, but the domain and codomain are different. It is essential to pay attention to this point (especially in the context of injections, surjections and bijections in the next chapter).

Often the domain and codomain are numbers of some kind (integers, rational numbers, real numbers, complex numbers) and the rule consists of an explicit formula, as in the above examples. Other familiar examples include $f : \mathbb{R} \longrightarrow \mathbb{R}$ given by $f(x) = \sin x$, $g : \mathbb{R} \longrightarrow \mathbb{R}$ given by $g(x) = e^x$, etc. Or one can consider multi-variable functions such as $h : \mathbb{R}^3 \longrightarrow \mathbb{R}^2$ given by $h(x, y, z) = (x^2 + y^2 + z^2, x - y + z)$. But there are many other types of functions:

- Let $gcd(m, n)$ denote the greatest common divisor of the nonzero integers m, n. This defines a function $(\mathbb{Z} - 0) \times (\mathbb{Z} - 0) \longrightarrow \mathbb{N}$. For example, $gcd(6, 15) = 3$, $gcd(-4, 18) = 2$, etc.

- Let X denote the set of all finite subsets of the set of prime numbers. Define a function $S : \mathbb{N}_{\geq 2} \longrightarrow X$ by defining $S(n)$ to be the set of primes that divide n. For example $S(6) = \{2, 3\}$, $S(700) = \{2, 5, 7\}$.

- Let X be the set of all circles C in $\mathbb{R}^2$, and define $\phi : X \longrightarrow \mathbb{R}^2 \times \mathbb{R}_{>0}$ by $\phi(C) = (a, b, r)$ where (a, b) is the center of C and r is the radius of C.

- Let X be the set of all differentiable real-valued functions on $\mathbb{R}$, and let Y be the set of all real-valued functions on $\mathbb{R}$. Define $D : X \longrightarrow Y$ by $D(f) = f'$ (the derivative of f).

The possibilities are endless. In order to emphasize the simplicity of the basic concept, however, let's mention a "silly" example. I'll use this one frequently, to help de-abstractify various concepts that arise later.

The cupcake function. The domain C is a set of cupcakes (sitting on a tray at a birthday party). The codomain K is the set of children (kids) at the party. The function f assigns to each cupcake c a child $f(c)$. Note that every cupcake *must* be given to a child, as otherwise the domain is not the entire set C. Note also that every cupcake goes to exactly one child; you can't cut it in half and split it between two children, as otherwise the function is not well-defined.

Finally, here are some basic functions that can be defined on sets in general:

- If X is any set, the *identity function* Id_X is defined by $Id_X(x) = x$.

- More generally, if $A \subseteq X$ is any subset, the *inclusion function* $i : A \longrightarrow X$ is defined by $i(a) = a$. (Unless $A = X$ this is not the identity function of A, because the codomain is X, not A.)

- If X, Y are sets, a *constant function* $f : X \longrightarrow Y$ is a function of the form $f(x) = y_0$, where $y_0 \in Y$ is a fixed element (independent of x).

- If $X_1, ..., X_n$ are sets, the *projection functions* $\pi_j : X_1 \times X_2 ... \times X_n \longrightarrow X_j$ are defined by $\pi_j(x_1, ..., x_n) = x_j$. We often call this "projection on the j-th coordinate".

The most familiar case of the last item (projections) is $\mathbb{R} \times \mathbb{R}$ or $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$; this is where the term "coordinate" comes from. One can use coordinates in a simple way to describe functions from a set A into a product set $X_1 \times X_2 \times ... \times X_n$. For example, suppose we want to define a curve in 2-space $\mathbb{R}^2$. Then it suffices to say what the x and y coordinates of the curve are. To be specific, take the curve $\phi : [0, 2\pi] \longrightarrow \mathbb{R}^2$ given by $\phi(t) = (\cos t, \sin t)$. The functions $x = \cos t$, $y = \sin t$ are the coordinate functions of the curve, and they completely describe it.

This works just as easily in our abstract setting. Suppose we are given a function $f : A \longrightarrow X_1 \times ... \times X_n$. The coordinate functions $f_i : A \longrightarrow X_i$ are defined by $f_i = \pi_i \circ f$. This is just saying that $f(a) = (f_1(a), ..., f_n(a))$. Conversely if we want to *define* a function $f : A \longrightarrow X_1 \times ... \times X_n$, all we have to do is define functions $f_i : A \longrightarrow X_i$ for each i.

6.1 Composition

Suppose we are given functions $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$. Then we can "compose" them to get a new function $g \circ f$ given by $(g \circ f)(x) = g(f(x))$. Note that this is only possible when the codomain of f is the same as the domain of g. Note also that the notation is peculiar (at least in a language that reads from left to right, like English), since the notation $g(f(x))$ has to be interpreted from right to left: put x into f, then put the output $f(x)$ into g. It would be more logical to write it in the other order, but since the notation has been established for centuries, there is no point in trying to change it.

In any case, this is no doubt a familiar concept, especially in the case $X = Y = Z = \mathbb{R}$. Thus if $f(x) = \sin x$ and $g(x) = x^2$, $(g \circ f) = (\sin x)^2$. There's not much to it, but as the example just given illustrates, even when $X = Y = Z$—so that both $f \circ g$ and $g \circ f$ are defined—composition is *not* commutative. In the example $(f \circ g)(x) = \sin(x^2)$, which is certainly not the same as $(\sin x)^2$.

On the other hand composition *is* associative, meaning the following: Suppose we are given functions

$$W \xrightarrow{f} X \xrightarrow{g} Y \xrightarrow{h} Z.$$

Then $(h \circ g) \circ f = h \circ (g \circ f)$. The proof of this fact is trivial, since for any $x \in X$ the two sides of the equation each yield $h(g(f(x)))$. Even trivial facts are worth noting, however!

6.2 Images

Suppose $f : X \longrightarrow Y$ is a function. The *image* of f is

$$Im\, f = \{y \in Y : \exists x \in X\, f(x) = y\}.$$

In other words, the image consists of all the points in the codomain that are "hit" by an element of the domain; i.e. all y such that $y = f(x)$ for some $x \in X$. (Note: Some people call the image the "range", but let's avoid this term as others use "range" to mean the codomain.)

Examples. 1. Suppose $X = Y = \mathbb{R}$. If $f(x) = e^x$, $Im\, f = \mathbb{R}_{>0}$. If $f(x) = \sin x$, $Im\, f = [-1, 1]$. If $f(x) = x^3$, $Im\, f = \mathbb{R}$.

2. Let $X = \mathbb{R}$, $Y = \mathbb{R}^2$, $f(t) = (\cos t, \sin t)$. Then the image of f is the unit circle centered at the origin.

3. Let $X = \mathbb{N} \times \mathbb{N}$, $Y = \mathbb{N}$, $f(a, b) = a^2 + b^2$. What is the image of f? By definition it is the set of all natural numbers that can be written as a sum of two squares. For example $2 = 1^2 + 1^2$, $13 = 2^2 + 3^2$ so 2 and 13 are both in the image of f. On the other hand $3, 6, 7$ are not in the image of f, as you can easily check directly. There is a very interesting and not at all obvious theorem that describes the answer; as an interesting project you could investigate this in a number theory source.

6.3 Inverse images and fibers

Returning to our general function $f : X \longrightarrow Y$, let $B \subseteq Y$ be a subset of Y. The *inverse image* of B is

$$f^{-1}B = \{x \in X : f(x) \in B\};$$

in other words, all the elements of X that f maps into B.

Caution. The notation f^{-1} has, unfortunately, a number of different uses. In the present case the notation in no way implies the existence of an "inverse function", and it certainly cannot mean the reciprocal since B is not number!

Examples. 1. Let $f : \mathbb{R} \longrightarrow \mathbb{R}$ be given by $f(x) = x^2$. Then $f^{-1}([0, 4]) = [-2, 2]$. On the other hand $f^{-1}\mathbb{R}_{<0} = \emptyset$.

2. If X, Y are any sets and $f : X \longrightarrow Y$ is any function whatsoever, then $f^{-1}\emptyset = \emptyset$ and $f^{-1}Y = X$. (I recommend looking at extreme cases of any new definition.)

3. Let $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ be given by $f(m, n) = m + n$. Then $f^{-1}\mathbb{Z}_{ev}$ is the subset $A \subset \mathbb{Z} \times \mathbb{Z}$ consisting of those (m, n) such that m and n are both even or both odd.

Let's consider example 3 above in more detail, to illustrate what has to be done to prove such an assertion. We are trying to show that $f^{-1}\mathbb{Z}_{ev} = A$. As usual, we break this into two steps. First we show $A \subseteq f^{-1}\mathbb{Z}_{ev}$. In other words, if m, n are both even or both odd, then $m + n$ is even. Second, we show $f^{-1}\mathbb{Z}_{ev} \subseteq A$. In other words, if $m + n$ is even then either m, n are both even, or both are odd. Both of these proofs are easy, and already done in an earlier exercise.

The *fibers* of f are the inverse images of singleton subsets of Y. More precisely, if $y \in Y$ then the *fiber over* y is

$$f^{-1}\{y\} = \{x \in X : f(x) = y\}.$$

Once again this notation in no way implies the existence of an "inverse function", and should not be confused with a reciprocal (which wouldn't even make sense since Y isn't necessarily a set of numbers). Note the use of the brackets $\{y\}$; this is because we are taking the inverse image of the *set* consisting of the single element y. It is only fair to point out, however, that many of us get tired of writing the brackets and simply write $f^{-1}y$ for the fiber over y. This abbreviated notation is legitimate as long as it is used with due caution.

Why is it called the "fiber"? The best answer is that it doesn't matter; one shouldn't lose sleep over why things are named the way they are. In this case, however, there is simple visual image that motivates the terminology. Take $X = [0,1] \times [0,1]$ (the unit square in the first quadrant of $\mathbb{R}^2$) and $Y = [0,1]$. Define $f : X \longrightarrow Y$ by $f(a,b) = a$. Then the fiber over a given $a \in [0,1]$ is the vertical line segment defined by $x = a$, $0 \leq y \leq 1$. We can think of these vertical segments as threads, or fibers. Moreover X consists of all the fibers bundled together.

Examples. 1. Let $f : \mathbb{R} \longrightarrow \mathbb{R}$ be given by $f(x) = \sin x$. Then $f^{-1}0$ is the set of all integer multiples of 2π.

2. Let $f : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ be given by $f(x,y) = x^2 + y^2$. Then $f^{-1}a$ is the circle of radius $\sqrt{a}$ centered at the origin if $a > 0$, while $f^{-1}0 = (0,0)$. If $a < 0$ then $f^{-1}a$ is the empty set.

Examples. 1. Consider the cupcake function. Its domain is the set C of cupcakes provided for the birthday party, and its codomain is the set K of children at the party. The function f assigns to each cupcake c a child $f(c)$. The fiber over child c is the set of cupcakes received by that child. Therefore we had better be sure that all the fibers are nonempty; if $f^{-1}c = \emptyset$ then child c will be very unhappy.

2. The bridge (as in the card game) function: Let S be a normal deck of 52 cards, $P = \{a, b, c, d\}$ a set of four people playing bridge. Thirteen cards are dealt to each player, thereby defining a function $f : S \longrightarrow P$. The fiber over player a is just the hand (=set of cards) dealt to a, and similarly for b, c, d.

So you see, the concept "fiber" is easy!

6.4 The graph of a function

The concept "graph of a function" is familiar for functions $f : \mathbb{R} \longrightarrow \mathbb{R}$ or $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$. In fact this concept makes perfectly good sense for *any* function $f : X \longrightarrow Y$. We define

$$graph\, f = \{(x,y) \in X \times Y : y = f(x)\}.$$

In the aforementioned familiar cases, this is exactly the familiar definition. In everyday life, one frequently uses graphs of functions from one finite set to another—although probably without calling them "graphs". For example, I have a class list with student names and student numbers. If S is the set of students, then there is a function $f : S \longrightarrow \mathbb{N}$ assigning to each student his or her student number. My class list gives the graph of this function, namely the set of pairs $(x, n(x))$ where $n(x)$ is the student number of student x. Another example is implicit in dictionaries: Let X denote the set of words in the English language, and let Y denote the set of 26 letters of the Roman alphabet. Define $f : X \longrightarrow Y$ by assigning a word to its first letter. Then the graph of f consists of all pairs (word w, first letter of word w), e.g. (chair, c), (f,fish), (r, run) and so on. Think up more examples of such graphs!

6.5 Restricting the domain and codomain

Suppose $f : X \longrightarrow Y$ is a function, and $A \subseteq X$. The *restriction of f to A*, denoted $f|_A$, is given by

$$f|_A(a) = f(a).$$

.
The "rule" is the same, but we've made the domain smaller and therefore have a different function. Notice that we have *not* changed the codomain, but it's possible that the image has gotten smaller:

Example: Let $f(x) = \sin x : \mathbb{R} \longrightarrow \mathbb{R}$. Then $Im\, f = [-1, 1]$. Now let $A = [0, \pi]$. Then $Im\,(f|_A) = [0, 1]$.

Example: Consider the cupcake function $f : C \longrightarrow K$, where we now suppose there are chocolate cupcakes and strawberry cupcakes. Let's assume every child gets a cupcake, so that $Im\, f = K$. Let $S \subset C$ denote the set of strawberry cupcakes. Then $Im(f|_S)$ is the set of children who get a strawberry cupcake. Simple!

Restriction of the domain is defined for any subset of the domain. Restriction of the codomain is slightly different, because we can only consider subsets $B \subseteq Y$ that contain the image of f. For this reason, and because it fits with the domain/codomain terminology, we'll call it *corestriction*. Here's the definition: Suppose $Im\, f \subseteq B \subseteq Y$. Then the corestriction of f to B, denoted $f|^B$, is defined by

$$f|^B(x) = f(x).$$

Again the "rule" is the same, but we've made the codomain smaller and therefore have a different function.

STOP! Did you allow yourself to be intimidated by the fancy terminology or the notation? Cease and desist immediately!

Sure, "corestriction" is a fancy word, but don't let this obscure the simplicity of the concept. Just look at some examples:

Example. Take $f(x) = \sin x : \mathbb{R} \longrightarrow \mathbb{R}$ and $B = [-1, 1]$. Then $f|^B : \mathbb{R} \longrightarrow [-1, 1]$ is just the sin function with its codomain shrunk all the way down to its image (the minimal possible choice of codomain).

Example. Take $g(n) = 6n : \mathbb{Z} \longrightarrow \mathbb{Z}$ and let $B = \mathbb{Z}_{ev}$, the even integers. Then $Im\, g \subset B$ so we can corestrict to get $g|^B : \mathbb{Z} \longrightarrow \mathbb{Z}_{ev}$. As in the previous example, however, a much more common corestriction would be to take B to be the image of g, i.e. the integers divisible by 6.

We can even restrict and corestrict at the same time, although the notation above starts to get a bit unwieldy. I'll just mention that we can restrict the domain to A, and corestrict the codomain to B simultaneously, provided $f(A) \subseteq B$. This new function could be denoted $f|^B_A : A \longrightarrow B$. This is getting too convoluted, however, and nobody really wants to use such notation. It's easier to just use a new letter. For example, take $f(x) = \sin x : \mathbb{R} \longrightarrow \mathbb{R}$ again.

We can define a new function $g : [0, \pi] \longrightarrow [0, 1]$ by the rule $g(x) = \sin x$. The rule is the same, but both the domain and codomain have been made smaller. That's all there is to it. In practice, most mathematicians wouldn't even bother to introduce a separate notation; we'd just say something like "consider the sin function $[0, \pi] \longrightarrow [0, 1]$". This is legitimate *only* if you are super-precise and make clear what is the domain and what is the codomain.

6.6 Exercises

No proofs are required on these problems, just a good answer. Feel free to use what you know from previous courses.

1. In each case, determine the image of the given function (i.e. describe it explicitly).
a) $f = e^{-x^2} : \mathbb{R} \longrightarrow \mathbb{R}$
b) $g : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ given by $g(a, b) = a + b$.
c) $h : \mathbb{Z} \times (\mathbb{Z} - \{0\}) \longrightarrow \mathbb{R}$ given by $h(a, b) = \frac{a}{b}$.

2. In each case determine the inverse image of the given subset B (i.e. describe it explicitly).
a) $f : \mathbb{N} \times \mathbb{N}$ given by $f(a, b) = ab$, $B = \{6\}$.
b) $g : \mathbb{R} \longrightarrow \mathbb{R}$ given by $g(x) = e^x$, $B = (-\infty, 1]$.
(Remember, the symbols $\pm\infty$ have no meaning on their own; they acquire meaning only in certain contexts. For instance, $(-\infty, 1]$ is just a traditional notation for $\{x \in \mathbb{R} : x \leq 1\}$.
c) Let $h : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ be given by $h(x, y) = xy$, and let $c \in \mathbb{R}$ be a constant. Describe $h^{-1}\{c\}$, considering the cases $c > 0$, $c < 0$ and $c = 0$ separately.

3. Define $f : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R} \times \mathbb{R}$ by $f(x, y) = (e^x \cos y, e^x \sin y)$. This is one of the most important functions in mathematics, known as the "complex exponential function".
a) For a constant c, let L_c denote the vertical line defined by $x = c$. Describe $f(L_c)$.
b) What is the image of f?
c) Let $\mathbb{R}_+$ denote the positive part of the x-axis. Describe the inverse image $f^{-1}\mathbb{R}_+$.

7 Additional material on products and functions

This is optional reading.

7.1 The definition of a function, revisited

The problem with the definition we gave of a function lies in the words "a rule...assigning to"; after all, we never defined what a "rule" is. The definition works well and we'll continue to use it, but it's worth pointing out that there is a more precise definition based on the product of two sets. In a nutshell, the idea is that a function is determined by its graph, so why not use the graph to *define* functions? Here's what I'll call the "abstract" definition of a function, to distinguish from the "ordinary" definition that you know and love.

Definition. A function with domain X and codomain Y is a subset $W \subseteq X \times Y$ with the property that for all $x \in X$ there is a unique $y \in Y$ such that $(x, y) \in W$.

If we have a function $f : X \longrightarrow Y$ in the ordinary sense, we get such a W by taking $W = \mathit{graph}\, f$. Conversely if we start with a W as in the abstract definition, we get $f : X \longrightarrow Y$ in the ordinary sense by defining $f(x)$ to be the unique $y \in Y$ such that $(x, y) \in X \times Y$. The moral of the story is that not only does a function determine the graph; the graph determines the function.

Although the abstract definition is simple, and in a sense more precise and rigorous than the ordinary definition, it lacks intuition and is cumbersome to work with. For example, defining and thinking about composition of functions using the abstract definition is awkward to say the least. Furthermore, the domain and codomain might themselves be products of sets, further confusing the picture. This is why I avoid the abstract definition in these notes. The abstract definition does, however, help clarify certain questions regarding the empty set, as discussed in the next section.

7.2 Functions whose domain or codomain is the empty set

It probably seems bizarre to consider functions with domain or codomain equal to the empty set, and for most readers of these notes this is not an important issue. Nevertheless, the empty set *is* a set, and if we want a complete theory we can't ignore it. Using the abstract definition of function from the previous section clarifies the issue:

1. I claim that for any set Y, there is a unique function $f : \emptyset \longrightarrow Y$, namely the "empty function". *Proof:* Since $\emptyset \times Y = \emptyset$, the only possible W (as in the abstract definition of function) is $W = \emptyset$. But does it in fact satisfy the definition? For this we must show that if $x \in \emptyset$, there is a unique $y \in Y$ such that $(x, y) \in \emptyset$. According to the rules logic, since the hypothesis is never satisfied, this is a true statement!

2. I claim that if X is any *nonempty* set, then there are no functions $f : X \longrightarrow \emptyset$. *Proof:* According to the abstract definition, such a function would be a subset $W \subseteq X \times \emptyset = \emptyset$ such that if $x \in X$ then there is a unique $y \in \emptyset$ such that $(x, y) \in W$. Since we are assuming there exists at least one $x \in X$, this is impossible because no such y exists.

Note: If X and Y are both empty, then as in item 1 there is a unique function $\emptyset \longrightarrow \emptyset$, namely the empty function.

These arguments may make matters seem more bizarre rather than less (the logic takes some getting used to). But at least the outcome is simple and easy to remember:

- For any set Y, there is a unique function $\emptyset \longrightarrow Y$, called the empty function.
- For any nonempty set X, there are no functions $f : X \longrightarrow \emptyset$.

7.3 Orderings

In the real number system, there is the familiar concept of *order*, expressed either in terms of strict inequality $x < y$ or non-strict inequality $x \leq y$. The strict and non-strict versions determine each other, so we can focus on either one; my choice is $x \leq y$. This ordering satisfies four standard properties:

1. *Transitive law:* $x \leq y$ and $y \leq z \Rightarrow x \leq z$

2. *Reflexive law:* $x \leq x$

3. *Non-symmetry:* $x \leq y$ and $y \leq x \Rightarrow x = y$

4. *Comparability:* For all x, y, either $x \leq y$ or $y \leq x$.

This is all simple enough, but the question arises: What exactly is an "ordering"? Can we express the concept in more basic set-theoretic terms? Indeed we can, and in a very nice way. The ordering concept for real numbers involves certain pairs of real numbers $x \leq y$. So a sensible thing to do is to *define* an ordering on a set X as a subset of $X \times X$ having certain properties. This is what we'll do, but let's call it a *total ordering* so as to distinguish it from a variant called a *partial ordering* that we'll define later.

Here's the definition: A *total order* on a set X is a subset $R \subset X \times X$ satisfying the following four axioms (note these are modelled directly on the four properties listed above):

1. *Transitive law:* $(x, y) \in R$ and $(y, z) \in R \Rightarrow (x, z) \in R$

2. *Reflexive law:* $\forall x \in X$, $(x, x) \in R$

3. *Non-symmetry:* $(x, y) \in R$ and $(y, x) \in R \Rightarrow x = y$

4. *Comparability:* For all $x, y \in X$, either $(x, y) \in R$ or $(y, x) \in R$

In the case of the usual ordering on $\mathbb{R}$, we take $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x \leq y$. In this case the four standard properties are equivalent to the four abstract axioms just listed (an easy check), so the usual ordering on $\mathbb{R}$ is a total ordering in the abstract sense. Even in the abstract case, we write $x \leq y$ to mean $(x, y) \in R$, in which case the four axioms can be re-written in this notation and become identical to the four standard properties listed originally!

So it's a fair question to ask: What's the advantage of introducing the abstract flim-flam of a subset $R \times X \times X$? Why don't we just write $x \leq y$, use the four standard properties and be done with it? The answer is that for many practical purposes there is no particular advantage—where by "practical" I mean even for applications within mathematics itself. Nevertheless (as in the case of functions) it gives an elegant, precise definition of "ordering" in terms of more basic concepts: sets, subsets, and products. In more advanced mathematics, this abstract definition can be essential.

A *partial order* on a set X is a subset $R \subset X \times X$ satisfying the first three axioms but not necessarily the fourth. In other words, we don't assume that any two elements are comparable. As with total orders, in practice we don't really think in terms of the subset R; we say more informally that a partial order is a relation $x \leq y$ on pairs of elements of X satisfying:

1. *Transitive law:* $x \leq y$ and $y \leq z \Rightarrow x \leq z$

2. *Reflexive law:* $x \leq x$

3. *Non-symmetry:* $x \leq y$ and $y \leq x \Rightarrow x = y$

Note: In order to avoid conflicts of notation, we may want to use a symbol other than $\leq$ in some cases. We might use xRy for example. See also the examples below.

There are many interesting examples of partial orders. Here I'll just mention two of the most basic:

Example. Ordering $\mathbb{N}$ by divisibility. For $a, b \in \mathbb{N}$ we defined $a|b$ to mean a divides b. This is a partial order. In fact we've already checked the three axioms: $a|b$ and $b|c$ implies $a|c$; $a|a$, and if $a|b$ and $b|a$ then $a = b$. Note, however, that this is not a total ordering; in other words, we can have neither $a|b$ nor $b|a$. In this case we say a, b are not comparable. For example, any two distinct primes, such as $a = 2$, $b = 3$, are not comparable.

Of course $\mathbb{N}$ also has its usual total order $a \leq b$, which is quite different: if $a|b$ then $a \leq b$, but the converse is false. For number-theoretic questions involving divisibility, the divisibility ordering is often the more relevant of the two.

Example. Ordering subsets of a set by inclusion. Let S be a set, and let X be the set of subsets of X. Then the usual inclusion relation $A \subseteq B$ on subsets of X is a partial ordering (check this!). However, it is not a total ordering; clearly one can have subsets A, B such that neither one is contained in the other; I leave it to you to give specific examples.

8 Injections, surjections and bijections

The concepts in this section are fundamental in all of mathematics. Fortunately, they are also very easy concepts—provided you refuse to be intimidated by mere terminology, and make use of simple everyday examples to see through the abstraction. Before even giving the abstract definition, I'll illustrate using the cupcake function f. This function has as its domain X a set of cupcakes on a tray at a birthday party, and as codomain Y the set of children at the party; f assigns each cupcake x to a child $f(x)$. Recall that (i) every cupcake goes to some child (otherwise the domain would be a proper subset of X, not X), and (ii) we aren't allowed to split a cupcake between two or more children (since then we wouldn't have a well-defined function). In this case our terminology works as follows:

- f is surjective: every child gets at least one cupcake
- f is injective: every child gets at most one cupcake
- f is bijective: every child gets exactly one cupcake

That's all there is to it. Notice that "bijective" is equivalent to "injective and surjective", so really there are only two concepts to understand.

In fact you're already familiar with these concepts in the context of equations, even though you probably didn't use the terminology. Suppose now $g : X \longrightarrow Y$ is a function (think of the familiar case $X = Y = \mathbb{R}$), and consider the equation $y = f(x)$. A standard problem that arises is to solve the equation for x. In this case our three terms have the following meaning:

- f is surjective: For every y, $y = f(x)$ has at least one solution.
- f is injective: For every y, $y = f(x)$ has at most one solution.
- f is bijective: For every y, $y = f(x)$ has exactly one solution.

Keep these models in mind as we proceed through the details.

8.1 Surjections

Suppose X and Y are sets, and $f : X \longrightarrow Y$ is a function. We say that f is *surjective* if for every $y \in Y$ there exists an $x \in X$ with $y = f(x)$. (There might be more than one such x.) Note that the following statements are logically equivalent:

- f is surjective
- $Im\, f = Y$
- For all $y \in Y$, the fiber $f^{-1}\{y\}$ is nonempty
- For all $y \in Y$, the equation $y = f(x)$ has a solution $x \in X$.

Be sure you understand why these are equivalent. In particular, if you understand the concept of "image of a function", then there is nothing new at all in the concept "surjective"; it just means the image is the entire codomain.

Another common term for surjective is "onto". But let's stick with "surjective".

Examples. 1. $f : \mathbb{R} \longrightarrow \mathbb{R}$ given by $f(x) = 2x + 1$ is surjective. To prove this, we must show that given any $y \in \mathbb{R}$, there exists at least one x such that $y = 2x + 1$. In this case there is exactly one such x, namely $x = (y - 1)/2$.

2. $g : \mathbb{R} \longrightarrow \mathbb{R}$ given by $g(x) = e^x$ is not surjective. Since the surjective condition is a "for every" type of assertion, to prove that a function is not surjective we need only produce one counterexample; in other words, we need only exhibit a single $y \in \mathbb{R}$ such that $y = e^x$ has no solution. We could take $y = 0$ for example. Another, perhaps more enlightening way of proving that g is not surjective is to note that the image of g is $\{y \in \mathbb{R} : y > 0\}$. So the image is not all of $\mathbb{R}$ and hence g is not surjective.

3. The function $h : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ given by $h(m, n) = mn$ is surjective: Given $a \in \mathbb{N}$, $a = h(1, a)$.

4. The function $\phi : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ given by $\phi(x, y) = (e^x \cos y, e^x \sin y)$ is not surjective because $(0, 0) \notin Im\, \phi$. To prove this, we note that if $(a, b) = \phi(x, y)$, then $a^2 + b^2 = e^{2x} > 0$. Since $0^2 + 0^2 = 0$, it follows that $(0, 0) \notin Im\, \phi$.

5. The cupcake function is surjective if and only if each child gets at least one cupcake (leaving open the possibility that some lucky children get more than one).

Caution. When discussing surjectivity it is critical to specify the domain and codomain of the function in question. For example, the function $f : \mathbb{R} \longrightarrow \mathbb{R}$ given by $f(x) = x^2$ is not surjective, since its image is $\mathbb{R}_{\geq 0}$ which is not equal to all of $\mathbb{R}$. On the other hand, if we restrict the codomain and define $g : \mathbb{R} \longrightarrow \mathbb{R}_{\geq 0}$ by $g(x) = x^2$, then g *is* surjective.

Summary of proof strategy: To show a function $f : X \longrightarrow Y$ is surjective, you have to show that $\forall y \in Y$, $\exists x \in X$ such that $f(x) = y$.

To show that f is not surjective, you must find a specific $y \in Y$ such that $y \notin Im\, f$ (and of course you have to *prove* that it is not in the image!).

8.2 Injections

A function $f : X \longrightarrow Y$ is *injective* if it satisfies either of the following two logically equivalent statements:

- For all $x_1 \neq x_2$ in X, $f(x_1) \neq f(x_2)$ in Y. In other words, distinct inputs yield distinct outputs.
- For all $x_1, x_2 \in X$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

These two statements are logically equivalent because the second is the contrapositive of the first.

IMPORTANT NOTE: It is almost invariably easier to use the second version in proofs. In other words, to show f is injective, you suppose $f(x_1) = f(x_2)$ and show this implies $x_1 = x_2$. We'll do some examples shortly. But first note that the following statements are logically equivalent:

- f is injective
- For all $y \in Y$, the fiber $f^{-1}y$ has at most one element.
- For all $y \in Y$, the equation $y = f(x)$ has at most one solution in X.

Be sure you understand why these three statements are logically equivalent. Note that there could be elements y such that the fiber $f^{-1}y$ is empty, i.e. $y = f(x)$ has no solutions.

Another common term for injective is "one-to-one". But this is very dangerous because in some contexts "one-to-one" is also taken to imply surjectivity. Let's stick with "injective".

Examples. 1. $f : \mathbb{R} \longrightarrow \mathbb{R}$ given by $f(x) = 2x + 3$ is injective. To prove this, we suppose that $2x_1 + 3 = 2x_2 + 3$. Then $2x_1 = 2x_2$ and $x_1 = x_2$, done.

2. $g : \mathbb{R} \longrightarrow \mathbb{R}$ given by $f(x) = \sin x$ is not injective, because $\sin 0 = 0 = \sin \pi$. (In fact the fiber over $y = 0$ is infinite, consisting of all integer multiples of π. So injectivity fails very badly here.)

3. The function $h : \mathbb{N} \longrightarrow \mathbb{N}$ given by $h(n) = n + 1$ is injective. To prove this, all we have to do is show that if $n_1 + 1 = n_2 + 1$, then $n_1 = n_2$—which is obvious.

4. Let X be the set of all differentiable functions $\mathbb{R} \longrightarrow \mathbb{R}$, and let Y be the set of all functions $\mathbb{R} \longrightarrow \mathbb{R}$. Define $\phi : X \longrightarrow Y$ by $\phi(g) = g'$, where g' is the derivative. This function is not injective because for any function g and constant c, $(g + c)' = g'$. This is a case where it's much more enlightening, although not logically necessary, to describe the general way in which injectivity fails rather than just give one counterexample.

5. The cupcake function is injective if and only if each child receives at most one cupcake (leaving open the possibility that some children get none).

Caution. A common mistake is to say something like "this function is injective because every input goes to a unique output". This is not at all what the definition says. In fact, the statement in quotes is satisfied by *every* function, and has nothing to do with injectivity. Injectivity means that every element in the codomain comes from at most one input, which is another kettle of fish entirely. Consider the cupcake function, for instance. Each cupcake is given to a unique child (we don't cut the cupcakes up in pieces); otherwise it wouldn't be a function. This is true no matter how the cupcakes are distributed. To say the function is injective means that no child gets *more than one* cupcake.

Summary of proof strategy: To show that a function $f : X \longrightarrow Y$ is injective, suppose that $f(x_1) = f(x_2)$ and prove that $x_1 = x_2$.

To show that f is not injective, you must produce explicit distinct elements $x_1 \neq x_2$ such that $f(x_1) = f(x_2)$ (and prove it, of course).

8.3 Bijections

A function $f : X \longrightarrow Y$ is called a *bijection* if it is both injective and surjective. Another term is "one-to-one correspondence", but this term can be misleading. Let's use "bijection" (or "bijective correspondence", a term to be explained later). Note the following are logically equivalent:

- f is bijective
- For all $y \in Y$, the fiber $f^{-1}y$ consists of a single element.
- For all $y \in Y$, the equation $y = f(x)$ has a unique solution $x \in X$. (Existence is the surjective property, uniqueness the injective property.)

Examples. 1. Let $\mathbb{N}_{ev}$ denote the even natural numbers, and define $f : \mathbb{N} \longrightarrow \mathbb{N}_{ev}$ by $f(n) = 2n$. Then f is a bijection. The proof is completely trivial: f is surjective because by definition if m is even then $m = 2n$ for some n. And clearly f is injective, since $f(n_1) = f(n_2) \Rightarrow 2n_1 = 2n_2 \Rightarrow n_1 = n_2$.

2. *Maps and polar coordinates.* A map of a region of the earth's surface establishes a bijection between points on the map (or gps coordinates, if you prefer) and points on the earth's surface. The bijection property is obviously important here, since we want each point on the map to correspond to a unique point of the region, and vice-versa. Similarly, in pure and applied mathematics we often use various kinds of coordinates—Cartesian (xyz), cylindrical, spherical, polar and so on to "map" regions of the plane, 3-space, and even higher-dimensional spaces.

For example, consider polar coordinates (r, θ) in the xy-plane. The point is that $F(r, \theta) = (r\cos\theta, r\sin\theta)$ defines a bijection from $[0, 2\pi) \times \mathbb{R}_{>0}$ to $\mathbb{R}^2 - \{0, 0\}$. (The minus sign means "remove the origin".) Note that 2π isn't included in the domain, because then F would fail to be injective. The origin is not included in the codomain because then F would fail to be surjective. The proof that F is a bijection is left to the exercises.

3. Here's an especially interesting example of a bijection: Let S be any set, and let $\mathcal{P}(S)$ denote the set of all subsets of S. To keep things more concrete, let's consider only the special case where $S = [n]$. Let B_n denote the set of all binary strings of length n, that is to say, ordered n-tuples $(x_1, x_2, ..., x_n)$ where each a_i is 0 or 1. For example, B_2 consists of the four elements $(0, 0), (1, 0), (0, 1), (1, 1)$. Then there is a bijection $\phi : \mathcal{P}([n]) \longrightarrow B_n$ defined as follows: Given a subset $A \subseteq [n]$, we define $\phi(A)$ to be the n-tuple given by $x_i = 0$ if $i \in A$ and $x_i = 1$ if $i \notin A$. For example, if $n = 4$ and $A = \{1, 3\}$, then $\phi(A) = (0, 1, 0, 1)$. Note also that $\phi(\emptyset) = (1, 1, ..., 1)$ and $\phi([n]) = (0, 0, ..., 0)$.

I claim that ϕ is a bijection. The proof will be inserted here later. Meanwhile, we'll prove it in class (or better, prove it yourself!).

There is another way to think about bijections, using *inverse functions.* Suppose $f : X \longrightarrow Y$ is a function. Suppose there is a function $g : Y \longrightarrow X$ such that $g \circ f = Id_X$ and $f \circ g = Id_Y$. In general there is no reason such a function should exist, but if does we call it

the *inverse* of f. Note the concept is symmetric: If g is the inverse of f, then f is the inverse of g. When it exists, the inverse g is the function that "undoes" or "reverses" whatever f did. You already know many examples of inverse functions, but be sure to be careful about specifying the domain and codomain. For instance:

Examples. 1. Define $f : \mathbb{R}_{\geq 0} \longrightarrow \mathbb{R}_{\geq 0}$ by $f(x) = x^2$. Then f has an inverse, namely $g(x) = \sqrt{x}$. To prove this you simply check the equations $\sqrt{x^2} = x$ and $(\sqrt{x})^2 = x$, which are valid for $x \geq 0$ and which we take for granted in this class. Note however that if we used all of $\mathbb{R}$ as our domain, this doesn't work: $\sqrt{x^2} = x$ is false for $x < 0$.

By the way, we really are taking something for granted when we assert that the above squaring function has an inverse given by the square root. How do you know that every non-negative real number has a square root? We can't possibly answer this question at the moment because we haven't even defined the real numbers! We'll return to this point later.

2. Define $f : \mathbb{R} \longrightarrow \mathbb{R}_{>0}$ by $f(x) = e^x$. Then f has an inverse called $\log x$. Again this isn't obvious, but we're taking it for granted. See the remark at the end of the section.

3. Suppose $f : \mathbb{R} \longrightarrow \mathbb{R}$ is given by $f(x) = ax + b$, where a and b are real constants and $a \neq 0$. Then f has an inverse g given by $g(x) = (1/a)(x - b)$. You could prove this by just directly computing $f(g(x)) = x$ and $g(f(x)) = x$, but see below for a better way to think of it.

4. When the domain and codomain are the same, it can happen that f is its own inverse. For example $f : \mathbb{R} - 0 \longrightarrow \mathbb{R} - 0$ given by $1/x$. To "undo" the reciprocal you just take the reciprocal again: $1/(1/x) = x$. Or let X be any set and define $f : \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$ by $f(A) = A^c$, the complement of A. Taking the complement of the complement just gives you the original set back again.

Here is the key fact about inverse functions:

Proposition 8.1 *Let $f : X \longrightarrow Y$ be a function. Then f has an inverse g if and only if f is a bijection. Moreover in that case g is unique and is also a bijection.*

Proof: This is a good example of a "follow your nose" proof. I remind you that you don't need to be clairvoyant in these proofs; just proceed one little step at a time and with luck it will all work out.

Suppose f has an inverse g. We want to show f is surjective and injective. First let's show it's surjective. Let $y \in Y$. We want to find an $x \in X$ with $f(x) = y$. Do we have some way to get from elements of Y to elements of X staring us in the face? Indeed we do: the function g. So we try taking $x = g(y)$. Then $f(x) = f(g(y)) = Id_Y(y) = y$, so it works.

Now let's show f is injective. We suppose $f(x_1) = f(x_2)$, and must show $x_1 = x_2$. What to do? Well, the only obvious thing to try is to apply g to both sides of the equation and see what happens: $g(f(x_1)) = g(f(x_2))$. But $g(f(x_1)) = Id_X(x_1) = x_1$, and similarly for x_2. So $x_1 = x_2$ as desired.

Conversely, suppose f is a bijection. Then for every $y \in Y$ there is a unique $x \in X$ such that $f(x) = y$. We then *define* $g(y)$ to be this x. To show that g is inverse to f, first note

that $f(g(y)) = y$ for all y by the definition of g. It remains to show that $g(f(x)) = x$ for all $x \in X$. Note that $f(g(f(x))) = f(x)$ by what we already proved (i.e. $f(g(y)) = y$). Since f is injective, it follows from the definition of "injective" that $g(f(x)) = f(x)$.

For the second part, note that g has an inverse, namely f. So by what we've already proved (reversing the roles of f and g), g is a bijection. It only remains to prove the uniqueness. In other words, we must show that if g, h are both inverse functions for f, then $g = h$. Well, $g(f(x)) = x$ and $h(f(x)) = x$ by definition of inverse function. This shows that $g(y) = h(y)$ for all y in the image of f. But f is surjective, so $Im\, f = Y$. So $g(y) = h(y)$ for all $y \in Y$, QED.

Caution: Once again, it is absolutely critical to specify the domain and codomain when discussing inverse functions. For example, you probably know the arcsin function as the "inverse function" of the sin function. But as a function from $\mathbb{R}$ to $\mathbb{R}$, $\sin x$ has no inverse, as it is neither injective nor surjective. First of all we have to restrict the codomain to be the interval $[-1, 1]$, i.e. the image of sin. We have to restrict the domain to some interval on which sin is injective. The customary choice is to take the interval $[-\pi/2, \pi/2]$, but this is not the only possible choice. At any rate, if we define a function $f : [-\pi/2, \pi/2] \longrightarrow [-1, 1]$ by $f(x) = \sin x$, then *this* function does have an inverse $g(y) = \arcsin y$. To prove this, we have to show that f is bijective. This isn't easy to do rigorously, but thinking about the sin function makes it intuitively clear, more or less.

Remark: On a related note, the "conversely" part of the previous proof is exactly what is used in basic calculus or pre-calculus to obtain various inverse functions. For example, there is the familiar fact that $f(x) = e^x : \mathbb{R} \longrightarrow \mathbb{R}_{>0}$ has an inverse function $\ln x$. But how do we know such a function exists? Well, if you go back to your calculus text, you'll see that the crux of the matter is to show that f is bijective. Then we *define* $\ln y$ to be the unique x such that $e^x = y$, exactly as in the proof of the "conversely" above. (Or maybe your calculus text defines ln first by some other method, and then *defines* e^x to be the inverse to ln! This works too, and still requires showing that $\ln : \mathbb{R}_{>0} \longrightarrow \mathbb{R}$ is bijective.)

Summary of proof strategy: To show that a function $f : X \longrightarrow Y$ is bijective, there are two different (although closely related) approaches:

1. Show that f is surjective and injective.
2. Show that there is an inverse function $g : Y \longrightarrow X$.

We'll discuss this further in class.

8.4 Balls and boxes

In this section I'll give another simple example to illustrate injections and surjections (and hence, automatically, bijections). It involves composition of functions as well. Once again, I hope to convince you that these concepts are very simple.

A toy factory manufactures colored rubber balls as children's toys. On any given day you start with a set of balls labeled $1, 2, 3...$, a set of colors (red, blue, green, etc.) and a set of boxes labeled $A, B, C...$ The number of balls, colors and boxes varies from day to day. Let X denote the set of balls, Y the set of colors and Z the set of boxes on a particular

day. Each ball in X is assigned a color and painted with that color. This defines a function $f : X \longrightarrow Y$. Each color is assigned a box; this defines a function $g : Y \longrightarrow Z$. The composition $h = g \circ f : X \longrightarrow Z$ assigns to each ball the appropriate box. For example:

Suppose there are four balls $1, 2, 3, 4$, three colors $red, blue, green$, and five boxes A, B, C, D, E. One possible function f is defined by painting balls 1 and 2 red, ball 3 blue, and ball 4 green. One possible function g assigns red and blue to box C, and green to box E. Then the composite function h takes balls 1,2,3 to box C and ball 4 to box E.

Note that we even allow extreme cases such as painting all the balls the same color, and putting all the colors in the same box. Now, let's consider the meaning of injective and surjective for functions of this type (in general, not just the example above).

- f is injective if no two balls are painted the same color.
- g is injective if no two colors go to the same box.
- $h = g \circ f$ is injective if no two balls go the same box.

For surjectivity we have:

- f is surjective if for each color, at least one ball is painted that color.
- g is surjective if for each box, at least one color goes to that box.
- $h = g \circ f$ is surjective if for each box, at least one ball goes to that box.

Draw some pictures of the situation, with specific functions, and convince yourself that these really are simple concepts!

8.5 Exercises

1. Determine whether or not the following functions are surjective. If the function is surjective, prove it; if not, give an explicit counterexample.

a) $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ given by $f(m, n) = mn$.

b) $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ given by $f(m, n) = m + n$.

c) $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ given by $f(m, n) = (m + n, m - n)$.

2. For the three functions given in the previous problem, determine whether not the function is injective. If it is, prove it; if it isn't, give a counterexample (i.e. exhibit two distinct elements $a \neq b$ of the domain such that $f(a) = f(b)$).

3. Suppose given sets X, Y, Z and functions $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$.

3.1a) Show that if g and f are surjective, then the composition $g \circ f$ is surjective.

3.1 b) Show that if $g \circ f$ is surjective, then g is surjective.

3.1 c) If $g \circ f$ is surjective, does it follow that f is surjective? (As always, proof or counterexample required.)

3.2a) Show that if g and f are injective, then the composition $g \circ f$ is injective.

3.2 b) Show that if $g \circ f$ is injective, then f is injective.

3.2 c) If $g \circ f$ is injective, does it follow that g is injective? (As always, proof or counterexample required.)

Suggestion for all 6 parts: The "balls and boxes" example might help your intuition on this problem. However, 3.1ab and 3.2ab have extremely short proofs that can be found even with no intuition whatsoever; just follow your nose!

4. Let $\mathbb{N}_{odd}$ denote the set of odd natural numbers. Define $\phi : \mathbb{N}_{odd} \times \mathbb{N}_0 \longrightarrow \mathbb{N}$ by $\phi(s, n) = s2^n$. Show that ϕ is bijective.

5. Show that the function $F : \mathbb{R}_{>0} \times [0, 2\pi) \longrightarrow \mathbb{R}^2 - \{(0, 0\}$ defined by $F(r, \theta) = (r\cos\theta, r\sin\theta)$ is a bijection. You may assume without proof that the function $g : [0, 2\pi) \longrightarrow S^1$ given by $g(\theta) = (\cos\theta, \sin\theta)$ is a bijection, where S^1 denotes the circle of radius 1 centered at the origin.

6. This problem (or at least half of it) will be used frequently later. Let A, B be nonempty sets. Show that there exists a surjection $A \longrightarrow B$ if and only if there exists an injection $B \longrightarrow A$.

Suggestion for $\Rightarrow$: If $f : A \longrightarrow B$ is a surjection, then for all $b \in B$ the fiber $f^{-1}b$ is nonempty. Define a function $g : B \longrightarrow A$ as follows. For each b choose an element of $f^{-1}b$ and $g(b)$ to be this element. Then g is injective; why? (I won't give a hint for $\Leftarrow$, so as not to spoil the fun.)

Just to have a convenient name for this fact, let's call it the "surjection/injection trick".

7. Let $\mathcal{P}(A)$ denote the set of all subsets of a set A. If $f : A \longrightarrow B$ is a function, it "induces" a function $\phi_f : \mathcal{P}(A) \longrightarrow \mathcal{P}(B)$ by the rule $\phi_f(X) = f(X)$. Here X is a subset of A, and $f(X)$ is just the image of X in B. (The word "induces" is an informal term meaning that ϕ_f is associated in some natural way to f, which is certainly the case here.) Show that f is a bijection if and only if ϕ_f is a bijection.

8. Let c be an integer, and define a function $f_c : \mathbb{Z} \longrightarrow \mathbb{Z}$ by $f_c(n) = cn$.

a) For which values of c is f_c injective?

b) For which values of c is f_c surjective?

9. Let $\mathcal{P}_{ev}[n]$ denote the set of all subsets of $[n]$ having an even number of elements. Let $\mathcal{P}_{odd}[n]$ denote the set of all subsets of $[n]$ having an odd number of elements. Show that there is a bijection $f : \mathcal{P}_{ev} \longrightarrow \mathcal{P}_{odd}$ by explicitly defining such an f, and of course proving that it is indeed a bijection. (This is a cool problem. Be creative!)

9 Finite sets and counting

Even in its most basic form, the concept "number" is very abstract. You probably don't think of it as abstract, but that's because you thoroughly internalized it in childhood. Take the number 5, for instance. What is it? It's the thing that five fingers, five oranges and five armadillos have in common. What it really means is that the number of oranges is said to be "five" if and only if they are in bijective correspondence with the fingers on my left hand, except that you would probably prefer to use your own hand. In particular it is independent of the word "five" and the symbol "5" used in English to represent it. In fact, it is possible to count things without even having words to represent the numbers in question. Some "primitive" societies didn't have words for numbers bigger than three. Nevertheless one could determine whether or not two large herds of goats were equal in number by grouping them in pairs, one from each herd. If this can be done with no goat from either herd being left unpaired, then the number of goats in each herd is the same—by definition!

Of course this "pairing" is the same thing as a bijective correspondence, so the concept "number of elements in a set" really boils down to the concept of bijection. We'll see later that the concept can even be extended to infinite sets, but for now let's stick to the more familiar, intuitive world of finite sets. This raises an even more basic question: What do we mean by "finite"?

9.1 Definition of finite sets and cardinality

Since we are taking the natural numbers as given, we can make the following definition:

Definition. A set A is *finite* if there is a bijection $[m] \longrightarrow A$ (or equivalently, $A \longrightarrow [m]$) for some $m \geq 0$. (The case $m = 0$ corresponds to the empty set.)

This suggests making the standard, seemingly obvious definition that the number of elements in a finite set A is the number m occurring in the previous definition. Unfortunately, there is a subtle problem with this: How do we know that it is well-defined? If there is a bijection $f : [m] \longrightarrow A$ and also a bijection $g : [n] \longrightarrow A$ for some $n \neq m$, then the definition is ambiguous. If such a situation occurred then $h := g^{-1} \circ f$ would be a bijection from $[m]$ to $[n]$, so what we need to show is: If $h : [m] \longrightarrow [n]$ is a bijection, then $m = n$. This is done in the optional reading below; here we take it as "intuitively obvious". We use the notation $|A|$ for the number of elements in the finite set A. A fancy name for it is the *cardinality* of the set A. For example $\{2, 5, 8, 17\}$ has cardinality 4.

Another obvious fact we take for granted:

Proposition 9.1 *If A is finite and $B \subset A$, then B is finite and $|B| \leq |A|$. Moreover $|B| = |A|$ if and only if $B = A$.*

Closely related to this is the equally obvious:

Proposition 9.2 *Let X, Y be finite sets, and let $h : [m] \longrightarrow [n]$ be a function. Then:*
a) If h is injective, $|X| \leq |Y|$.
b) If h is surjective, $|X| \geq |Y|$;
c) If h is bijective, $|X| = |Y|$.

Note. The contrapositive forms if (a) and (b) go by the name of "the pigeonhole principle" (a name that must have been invented in a country with lots of pigeons and holes to put them in, presumably England). The idea is that set A is the pigeons and set B is the set of pigeonholes to put them in. Let's write out these contrapositive forms explicitly, taking as given that A and B are both finite.

a) If $|A| > |B|$, then there must be two elements $a_1 \neq a_2$ of A such that $f(a_1) = f(a_2)$ (i.e. two pigeons have to share the same hole).

b) If $|A| < |B|$, then there must be some element $b \in B$ that is not in the image of f (i.e. there must be at least one unoccupied pigeonhole).

This kind of imagery can be very helpful; you should invent your own! In terms of my cupcake function, part (a) says that at least one child gets two or more cupcakes, while part (b) says at least one child gets no cupcake.

Part (c) has a converse version:

Proposition 9.3 *Suppose A, B are finite sets and $|A| = |B|$. Then there is a bijection $f : A \longrightarrow B$.*

Proof: Let $|A| = n = |B|$. Then there is a bijection $g : A \longrightarrow [n]$ and a bijection $h : [n] \longrightarrow B$. Let $f = h \circ g$; then f is a composition of bijections and so is a bijection (by a problem from the previous chapter).

I'll leave it to you to work out analogous "converse" versions of (a) and (b).

Finally, here's a handy fact that can cut your work in half:

Proposition 9.4 *Suppose A, B are finite sets, $|A| = |B|$, and $f : A \longrightarrow B$ is a function.*
a) If f is injective, then f is bijective.
b) If f is surjective, then f is bijective.

Proof: a) Let $n = |A| = |B|$. Since f is injective, it defines a bijection onto its image $Im\, f$. Hence $|Im\, f| = n$. Since $n = |B|$ this forces $Im\, f = B$. In other words, f is also surjective, hence bijective.

b) Since f is surjective, for each $b \in B$ we can choose an element $a \in A$ with $f(a) = B$. Call this subset of chosen elements C. Then by construction the restriction of f to C is still surjective but also injective (because we cooked it up so there is a unique element of C in each fiber $f^{-1}b$), hence we have a bijection from C to B. So $|C| = n$. Since also $|A| = n$, this forces $C = A$. Therefore f is bijective, QED.

Caution: The point of this last proposition is that it allows you to prove f is a bijection by proving only one of the two conditions injective/surjective. But it only applies in a very special situation: both sets are finite, and have the same cardinality (you would have to know the cardinalities are the same in advance, by some other means). It doesn't work for infinite sets or for finite sets of different cardinalities.

9.2 Finite unions of finite sets

It's clear how cardinality works for the union of two finite sets:

Proposition 9.5 *Suppose A, B are finite sets. Then $A \cup B$ is finite, and*

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

In particular, if A, B are disjoint, then

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

A formal proof is hardly necessary (if you want one, see the optional reading). The disjoint case is completely obvious (if you have two dogs and three cats, you have five pets in all!). In the case when $A \cap B \neq \emptyset$, to begin we just count the elements of A, then count the elements of B, then add. However, the elements of $|A \cap B|$ have been counted twice, so we have to subtract $|A \cap B|$ to get the correct final answer.

Now let's consider a finite collection of pairwise disjoint finite sets $A_1, ..., A_n$. By "pairwise disjoint" we mean that for all $i \neq j$, $A_i \cap A_j = \emptyset$; i.e. there is no "overlap" between any two of the sets.

Proposition 9.6 *Let $A_1, ..., A_n$ be a finite collection of finite sets.*
a) The union $\cup_{i=1}^n A_i$ is finite.
b) If the A_i's are pairwise disjoint, then $|\cup_{i=1}^n A_i| = \sum_{i=1}^n |A_i|$.

Proof: We prove (a) and(b) simultaneously by induction on n, in a particular way that gets recycled later in similar proofs. Note that the base case $n = 1$ is completely trivial, almost silly, since there is only one set in the collection. But instead of proceding immediately to the inductive step, we first do the case $n = 2$. Luckily, we already did this in the preceding proposition; the case $n = 2$ is proved.

Now suppose the result is true for a collection of n sets; we need to show it is true for a collection of $n + 1$ sets. So suppose given finite sets $A_1, ..., A_{n+1}$. Let $A = \cup_{i=1}^n A_i$ and let $B = A_{n+1}$. Then by inductive hypothesis A is finite, so $A \cup B$ is finite by the case of two sets already done. Similarly if the A_i's are pairwise disjoint, then $|A| = \sum_{i=1}^n |A_i|$ by inductive hypothesis. Note that $A \cap B = \emptyset$, since A_{n+1} doesn't intersect any of the other A_i's, by assumption. So again by the case of two sets that we already did,

$$|\cup_{i=1}^{n+1} A_i| = |A \cup B| = |A| + |B| = \sum_{i=1}^{n+1} |A_i|.$$

Comparing the second proposition with the first, we see that something is missing: the second proposition doesn't give a formula for $|\cup_{i=1}^n A_i|$ in the case where the A_i's aren't pairwise disjoint. The formula for this is called the "inclusion-exclusion formula", and is considerably more complicated. See the optional reading. Meanwhile, try to discover and prove a formula for three sets: $|A \cup B \cup C| =?$. The formula should be in the spirit of the two-set case.

9.3 Finite products of finite sets

Suppose A and B are finite sets. Then surely the product set $A \times B$ is finite, with cardinality $|A \times B| = |A| \cdot |B|$ (where the dot as usual indicates multiplication; it's good to put the dot in, as the notation $|A||B|$ is rather cramped). I say "surely" because, intuitively at least, this is the essence of multiplication. For example, the standard notation used for squares on a chessboard is to label the rows (as viewed by the player with the white pieces) using the numbers 1 through 8, and the columns by the first 8 letters of the alphabet $abcdefgh$. If we call this set of letters B, then altogether the squares are labeled by the product set $[8] \times B$, i.e. pairs (k, x) where $1 \leq k \leq 8$ and x is one of the eight letters. The total number of squares is then $8 \cdot |B| = 8 \cdot 8$. Or a room 6 feet by 9 feet tiled with 1 by 1 squares requires $6 \cdot 9$ tiles. So this is just the everyday notion you've known for years.

Let's consider the matter more carefully, however. What exactly is "multiplication" of natural numbers? The answer is that it is iterated addition: $m \cdot n$ is n added to itself m times: $n + n + ... + n$ where there are m terms. Incidentally, when you define it this way it isn't obvious that $m \cdot n = n \cdot m$, in other words that adding m to itself n times gives the same result. We think of it as obvious by just picturing an $m \times n$ array of dots (or walnuts, or zebras, or whatever strikes your fancy). Then we can count the total by thinking of it as m rows of n dots each or n columns of m dots each. So we're implicitly using the concept "product of sets".

Once again, therefore, we'll take the trouble to prove the desired formula rigorously. While we're at it, we may as well consider finite products $A_1 \times ... \times A_n$ of a collection of finite sets.

Proposition 9.7 *Let $A_1, ..., A_n$ be a finite collection of finite sets. Then $\prod_{i=1}^n A_i$ is finite, and $|\prod_{i=1}^n A_i| = \prod_{i=1}^n |A_i|$. (Note we are using the same symbol for products of sets and products of numbers.)*

Proof: We use induction on n, following the model above for disjoint unions. Again the case $n = 1$ is silly but true, since there is only one set. Instead of proceeding to the inductive step, we first consider the case of two finite sets A, B. Our proof for this case is exactly in the spirit of the intuitive discussion above: $A \times B$ is the disjoint union of the slices $A \times \{b\}$, $b \in B$. There are $|B|$ slices, each of which has $|A|$ elements. So by what we already proved for disjoint unions,

$$|A \times B| = |A| + |A| + ... + |A| = |A| \cdot |B|,$$

where there are $|B|$ terms $|A|$ in the sum.

The general case is now proved by induction on n, making use of the two-set case at the inductive step just as we did in the disjoint union proof. The details are left as an exercise.

10 Combinatorics, or how to count things

The branch of mathematics known as "combinatorics" is about counting finite sets. This is an oversimplification, of course, but not so far from the truth. But don't let this simple-minded description fool you! Combinatorics is a vast subject, filled with many deep and

beautiful theorems, and moreover having many practical applications. As basic examples of what we might want to count, consider the following questions.

- How many subsets does a set with n elements have?
- How many k-element subsets does a set with n elements have?
- How many ways are there to order a set with n elements?

This is what I mean by "counting finite sets": You're given a finite set A, and wish to compute $|A|$. In these examples the answer will be a sequence of formulas depending on n, so it's natural to expect that induction will enter in. For that you first you have to guess what the answer is, then prove it by induction. Another method: Suppose you can find another set B whose cardinality you already know, and can show by hook or by crook that A and B are in bijective correspondence. Then $|A| = |B|$ and you have your answer. Or maybe you can partition A in some relevant way as $A = \coprod_{i=1}^{n} A_i$; then $|A| = \sum |A_i|$, which might prove to be a useful formula.

Now, let's get on to the examples!

10.1 The set of subsets of a finite set

If S is any set, not necessarily finite, we let $\mathcal{P}(S)$ denote the set of all subsets of S. (The choice of the letter P comes from the fact that $\mathcal{P}(S)$ is often called the "power set" of S. Eventually, we'll explain where this name comes from.) For the time being, though, we are concerned only with the case $\mathcal{P}(A)$ for a finite set A. Our goal is to determine $|\mathcal{P}(A)|$.

The first thing to observe is that if $|A| = |B|$, then $|\mathcal{P}(A)| = |\mathcal{P}(B)|$. This is left to you to prove, in the exercises. So if $|A| = n$, we may as well just consider the case $A = [n]$. Let's see if we can guess the answer by looking at small values of n. Recall that the empty set and A itself are always subsets of A.

If $n = 0$ then A is the empty set, so A has just one subset, namely itself.

If $n = 1$, then $[1]$ has two subsets, $\emptyset$ and $[1]$.

If $n = 2$, there are four subsets: $\emptyset$, $[2]$, $\{1\}$ and $\{2\}$.

If $n = 3$ there are eight subsets. Rather than list them, I'll describe them: The empty set and the whole set give you 2. The singletons give you 3. Finally there are three subsets with 2 elements, giving 8 in all.

Okay, $1, 2, 4, 8...$ I think we see a pattern. But experimental evidence does not constitute a proof, even if you checked the first billion cases on a computer. All we have a conjecture. Since the conjecture turns out to be true, I'll state it as a theorem.

Theorem 10.1 $|\mathcal{P}([n])| = 2^n$.

We've already proved the theorem, in fact, in previous exercises. One proof was by induction on n. Another is to show there is a bijection $\mathcal{P}([n]) \longrightarrow \{0,1\}^n$. The set $\{0,1\}^n$ has 2^n elements by Proposition 9.7, so once again we conclude the theorem.

We can refine the theorem a bit. Let $\mathcal{P}_{ev}[n]$ denote the set of subsets of $[n]$ with even cardinality, and similarly let $\mathcal{P}_{odd}[n]$ denote those of odd cardinality.

Theorem 10.2 $|\mathcal{P}_{ev}[n]| = |\mathcal{P}_{odd}[n]| = 2^{n-1}$.

Again the proof is an interesting exercise.

10.2 Permutations and orderings of a finite set

How many ways are there to order a set A with n elements, i.e. as $a_1, a_2, ..., a_n$? I claim the answer is $n!$, and that we can prove this as follows: There are n possible choices for the first element a_1. That leaves $n-1$ choices for the second element a_2, then $n-3$ choices for a_3, and so on. So all in all we have $n \cdot (n-1) \cdot (n-2)... \cdot 2 \cdot 1 = n!$ possibilities. (The only reason I did it in reverse order, starting with the last element instead of the first, is to make the notation more consistent with the induction proof to be given shortly.)

If a proof is "a convincing explanation of why something is true", then I regard the informal argument above as a proof. It is completely convincing, so much so that asking for a "rigorous" proof seems redundant. Nevertheless, the fact remains that it does not meet the standard of rigorous proof established thus far in these notes. For one thing, we never even defined "ordering". For another, all this talk about "choices" makes no use at all of the theory we've so carefully developed, so what exactly are we really doing? See the optional reading for a pedantically rigorous proof; here we'll stick with the more enlightening informal argument. However, we do know how to make precise the concept of "ordering" of a finite set A with $|A| = n$. It is the same thing as a bijection $[n] \longrightarrow A$. To sum up, we have proved the following:

Proposition 10.3 *Suppose A is a finite set with $|A| = n$. Then the number of distinct orderings of A, i.e. the number of bijections $[n] \longrightarrow A$, is $n!$.*

A *permutation* of a set A (which for now we assume finite) is a bijection $f : A \longrightarrow A$. Let $Perm\, A$ denote the set of all permutations of A. If $A = [n]$, it is customary to write S_n for $Perm\,[n]$ (S is for "symmetric".) If $A = [n]$, then a permutation of $[n]$ is the same thing as an ordering of $[n]$, and the last proposition shows that $|S_n| = n!$.

Since S_n consists of bijections from $[n]$ to itself (permutations), we can compose any two permutations f, g to get a third permutation $f \circ g$. Since composition of functions is associative, this operation on permutations is associative: $f \circ (g \circ h) = (f \circ g) \circ h$. Moreover any permutation f has an inverse (since it is a bijection) f^{-1}, i.e. $f \circ f^{-1} = f^{-1} \circ f = Id_{[n]}$. This combination of properties makes S_n a "group", a type of structure that arises almost everywhere in mathematics. We won't pursue this concept any further, except to note that the composition operation is *not* commutative. The simplest counterexample to commutativity occurs for S_3, which has a grand total of $3! = 6$ elements. The following two elements are typical:

$f(1) = 2$, $f(2) = 1$, $f(3) = 3$ (switch 1 and 2, leave 3 alone)
$g(1) = 2$, $g(2) = 3$, $g(3) = 1$ (shift everything to the right, except the last element 3 wraps back around to the start)

I leave it to you to check that $f \circ g \neq g \circ f$. By the way, there's no reason to limit oneself to numbers. Check this in some more vivid physical way, perhaps using an ace, king and

queen from a deck of cards; or get three friends to act it out for a YouTube video. For larger n you could find many more interesting examples of non-commuting permutations; make it a dance video set to music. The moral of the story is that there is nothing strange about failure of the commutative law; it fails frequently in simple down-to-earth settings.

Two last notes about the "group" concept: (1) Don't lose any sleep over why it's called a group. Whoever invented the term back in the 1800's thought it was good at the time, and it stuck. (2) At the UW you can learn more about groups in Math 402.

10.2.1 Counting injections and surjections

The method used to count bijections carries through almost verbatim to count injections. Recall that we define 0! to be 1.

Proposition 10.4 *Let A be a set with n elements. Then for $1 \leq k \leq n$, the number of injections $[k] \longrightarrow A$ is*

$$n(n-1)...(n-k+1) = \frac{n!}{(n-k)!}.$$

Proof: Consider the possible injections $f : [k] \longrightarrow A$. There are n choices for $f(1)$, $n-1$ choices for $f(2)$, and so on, until finally there are $n-k+1$ choices for $f(k)$. Hence there are $n(n-1)...(n-k+1)$ injections, and this number is equal to $n!/(n-k)!$ by simple algebra. QED.

It's good to check extreme cases of any new definition or proposition, and make sure they make sense (otherwise something is wrong with your proposition!). In the preceding proposition, one extreme is $k = 1$. Then it says that the number of injections from a one-element set to an n-element set is n. This makes sense; any function whose domain is a one-element set is injective, so we just get the set of all functions $[1] \longrightarrow A$, which has cardinality n. At the opposite extreme with $k = n$, we know that then any injection is a bijection, so this agrees with the previous answer $n!$ for bijections.

The natural question still staring us in the face is: Can we "count", i.e. find a formula for, the number of surjections $[k] \longrightarrow A$ (where $k \geq 2$)? This turns out to be harder than the count for injections; we'll do it later using the "inclusion/exclusion principle". Meanwhile, a good exercise is to find the answer directly when $|A| = 2$.

10.3 The k-element subsets of a set with n elements

How many distinct 5-card poker hands are there? It's the number of five-element subsets of a set with 52 elements (the deck of cards). The number of distinct bridge hands is the number of 13-element subsets of a set with 52 elements.

More generally, let $\mathcal{P}_k[n]$ denote the set of k-element subsets of $[n]$. How many are there? The number $|\mathcal{P}_k[n]|$ is denoted $\binom{n}{k}$ and pronounced "n choose k". It's also called a "binomial coefficient", for reasons that will be explained later. Our problem, then, is to compute $\binom{n}{k}$. Let's start with some easy facts:

$\binom{n}{0} = 1$. There is only one subset with zero elements, namely the empty set.

$\binom{n}{n} = 1$. There's only one subset with n elements, namely the whole set.

$\binom{n}{1} = n$. There are n different singletons, i.e. subsets with one element.

$\binom{n}{k} = \binom{n}{n-k}$. Why? Prove it! We call this property *symmetry*.

The first case requiring a little thought is $\binom{n}{2}$. We'll study it as a warm-up for the general case. As usual, you should have some mental image in mind. I'll think of a deck of cards, so $n = 52$. I want to pick a pair of elements (pick a card, any card...). There are n choices for the first element. That leaves $n - 1$ choices for the second element. So the answer is $n(n-1)$? No! We're only counting subsets, not orderings of subsets. If I pick the ace of hearts first and then the jack of clubs, I get the same pair by picking the jack first and then the ace. This observation tells us how to correct our formula. The count given by $n(n-1)$ is counting every pair twice, so to get the right formula we have to divide by 2:

$$\binom{n}{2} = \frac{n(n-1)}{2}.$$

Indeed, you will recall that $n(n-1)$ is the number of injections $[2] \longrightarrow [n]$. For every 2-element subset A of $[n]$, there are two different injections with image A. The particular injection puts an ordering on A, but we don't want to count orderings, hence the division by 2. Incidentally, $\frac{n(n-1)}{2} = 1 + 2 + 3 + ... + n - 1$, by the Gauss formula. A good exercise is to show combinatorially that $\binom{n}{2} = 1 + 2 + ... + n - 1$; see the exercises.

The general case follows an identical pattern. Suppose I want to choose a k-element subset of an n-element set. There are n choices for the first element, $n - 1$ for the second, and so on down to $n - (k-1) = n - k + 1$ for the k-th element. This leads to the number $n(n-1)...(n-k+1)$. But here again we don't want to count the ordering. As we already proved earlier, this number counts the number of injections $[k] \longrightarrow [n]$, whereas now we only care about the *image* of the injection. For each k-element subset A, there are $k!$ bijections $[k] \longrightarrow A$. Hence our preliminary count of $n(n-1)...(n-k+1)$ is counting very subset $k!$ times. To get the right formula we divide by $k!$:

$$\binom{n}{k} = \frac{n(n-1)...(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}.$$

Here the second equality is easy algebra (check it!). Note that the fraction on the right is symmetric in k and $n - k$, so this fits with the symmetry $\binom{n}{k} = \binom{n}{n-k}$ we noticed earlier. One striking feature of the equality is that it is not at all obvious that the fraction is an integer. Yet it must be an integer, since $\binom{n}{k}$ is an integer by definition!

For small values of n, the numbers $\binom{n}{k}$ are easily computed by hand from this formula. You could, of course, just look them up or compute them electronically, but I highly recommend doing a few by hand to get a feel for it. For example, even my slow brain can compute $\binom{7}{k}$ for all k with no artificial aids at all: $\binom{7}{0} = 1$ and $\binom{7}{1} = 7$ are the trivial cases, while

$\binom{7}{2} = 7 \cdot 6/2 = 21$ and $\binom{7}{3} = (7 \cdot 6 \cdot 5)/(3 \cdot 2) = 35$. The remaining cases follow immediately by symmetry, e.g. $\binom{7}{4} = \binom{7}{3} = 35$, and so on.

A larger example that you probably don't want to compute by hand is the number of 5-card poker hands:

$$\binom{52}{5} = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5!} = 2,598,960.$$

The number of bridge hands is much larger, and I'll leave that computation to those who really want to know.

Before going further, let's take the preceding informal argument and turn it into a more precise proof.

Proposition 10.5 $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Proof: Let S denote the set of all injections $[k] \longrightarrow [n]$, and for each $A \in \mathcal{P}_k[n]$ let $S_A = \{f \in S : Im\, f = A\}$. Then the S_A's form a partition of S, and for all A we have $|S_A| = k!$ by Proposition 11.12. So

$$|S| = \sum_{A \in \mathcal{P}_k[n]} |S_A| = \sum_{A \in \mathcal{P}_k[n]} k! = k! |\mathcal{P}_k[n]|.$$

Since $|S| = \frac{n!}{(n-k)!}$, we conclude

$$|\mathcal{P}_k[n]| = \frac{|S|}{k!} = \frac{n!}{k!(n-k)!}.$$

QED.

For future reference, we record the following surprising formula:

Proposition 10.6

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

Proof: You certainly wouldn't want to use the algebraic formula $\frac{n!}{k!(n-k)!}$ to prove this; that would create a big mess. Instead, we begin by noting that $(-1)^k$ is $+1$ for k even and -1 for k odd. So if we move the negative terms to the other side of the equation, what we want to prove is

$$\sum_{k\,\text{even}} \binom{n}{k} \stackrel{?}{=} \sum_{k\,\text{odd}} \binom{n}{k}.$$

But the left-hand side above is $|\mathcal{P}_{ev}[n]|$, while the right-hand side is $|\mathcal{P}_{odd}[n]|$. So the proposition follows from Theorem 11.11.

Note. I put a question mark over the equality to emphasize that it is something we want to prove, as opposed to something we have already proved. I recommend this practice to avoid circular reasoning.

10.3.1 Pascal's identity and Pascal's triangle

Pascal's identity is the following simple formula:

Proposition 10.7 $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$.

Proof: One could easily prove this using the algebraic formula for $\binom{n}{k}$ (just add the fractions on the left and see what you get). But even easier (at least after you get used to doing a little combinatorics), and certainly more enlightening and fun, is to do it combinatorially. In this case I mean find a partition of $\mathcal{P}_k[n+1]$ into two sets whose cardinalities are the two terms on the left of the formula; then you're done. Here we define $X \subset \mathcal{P}_k[n+1]$ to be those subsets that contain $n+1$, and Y to be those that don't. Thus we have a partition

$$\mathcal{P}_k[n+1] = X \coprod Y.$$

Now, a subset A containing $n+1$ is uniquely determined by the $k-1$ remaining elements, which lie in $[n]$. Hence $|X| = \binom{n}{k-1}$. A subset A that doesn't contain $n+1$ is the same thing as a subset of $[n]$, so $|Y| = \binom{n}{k}$. QED.

Pascal's formula is the basis for the famous Pascal's triangle. A picture of Pascal's triangle will eventually go here. Meanwhile, one can find many such pictures on the internet. You'll find many in pretty colors, but don't neglect the basic model that just has the numbers. In any case, Pascal's identity gives an easy way to compute binomial coefficients recursively. In a very short time you can compute by hand $\binom{n}{k}$ for, let's say, $n \leq 10$ and all k. The point is that if you know $\binom{n-1}{k}$ for all k, then Pascal's identity easily yields $\binom{n}{k}$ for all k. Pascal's triangle is just a convenient way of displaying this information. You can, of course, just look up the values of $\binom{n}{k}$, have a computer do it or whatever. But I highly recommend working out Pascal's triangle by hand up to at least $n = 8$, because it's easy (up to 8 you can do in a minute) and the process helps you to internalize the concept.

10.4 The binomial theorem

One of the most important ways in which the numbers $\binom{n}{k}$ arise is in the binomial theorem; this is where the term "binomial coefficients" comes from. In early school days you learn the formula

$$(x+y)^2 = x^2 + 2xy + y^2.$$

At some point you also learn

$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3,$$

or even

$$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4.$$

But let's get serious and find the general formula for $(x+y)^n$, n any natural number. Here we'll take for granted the concept "polynomial", of which $(x+y)^n$ is an example. Looking at the sequence of coefficients in the above examples, we find $1, 2, 1$ (for $n = 2$), $1, 3, 3, 1$ (for $n = 3$), and $1, 4, 6, 4, 1$ (for $n = 4$). Comparing with Pascal's triangle, we notice that these are exactly the numbers $\binom{n}{k}$ for $n = 2, 3, 4$ respectively. This suggests a conjecture as to the general answer, and it turns out to be true:

Theorem 10.8

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

By symmetry we could just as well write $x^k y^{n-k}$ in place of $x^{n-k}y^k$. I chose the latter option because then the sum begins with $x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + ...$, which to me looks better than the other way. It's a personal aesthetic choice; there are more of these in mathematics than you might think.
First proof: The n-power on the left is

$$(x+y)^n = (x+y)(x+y)...(x+y),$$

where there are n factors $x+y$. If we expand this out by the distributive law, without collecting "like terms", we'll have a sum with 2^n terms in it: Run through the n factors and pick either x or y from each one. Each term is of the form $x^{n-k}y^k$ for some k. For fixed k, we obtain this term by choosing y from k factors and x from the others. In other words, we choose k factors from n factors, and the total number is $\binom{n}{k}$. QED.

Second proof: Use induction on n. The base case $n = 1$ says that $x + y = x + y$, and a truer statement you'll never find. Now suppose (inductive hypothesis) that the result is true for n. We must prove it for $n+1$. To see this, we have

$$(x+y)^{n+1} = (x+y)^n(x+y) = (\sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k)(x+y) = \sum_{k=0}^{n} \binom{n}{k} x^{n-k+1}y^k + \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^{k+1}.$$

Here the first equality is by inductive hypothesis, and the second is just the distributive law. Each of the two sums contains one term of the form $x^{n-k+1}y^k$ (for a fixed k). In the left-hand sum the coefficient of this term is $\binom{n}{k}$, while in the right-hand sum (look closely!) it is $\binom{n}{k-1}$. So if we collect these two like terms, the coefficient we get is $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ by Pascal's identity. QED.

We can use the binomial theorem to prove results about $\binom{n}{k}$. For example, we now have a stunningly simple proof of the complicated looking identity

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

Just substitute $x = 1$, $y = -1$ in the binomial theorem, and the above formula pops out by magic!

10.5 Exercises

1. Consider the theorem: $|\mathcal{P}([n])| = 2^n$.

a) Prove it by induction on n.

b) Prove it by constructing a bijection between $\mathcal{P}([n])$ and $\{0,1\}^n$ (the n-fold product of the set consisting of 0 and 1, also known as "binary strings of length n").

2. Prove the theorem: $|\mathcal{P}_{ev}[n]| = |\mathcal{P}_{odd}[n]| = 2^{n-1}$. Do not use induction; instead use two previous homework problems to give a short and simple proof.

3. Let $f(x) = a_0 + a_1x + ... + a_nx^n$ be a polynomial with real coefficients a_i and $a_n \neq 0$. Then f has at most n real roots (and so in particular, the set of real roots of f is finite).

Prove this by induction on n, using calculus (review Rolle's theorem, if necessary).

Note: In fact f has at most n roots, period, i.e. even if we count complex roots. But a different proof (and of course a solid knowledge of the complex number system) would be needed for this.

4. These are "short answer" problems, requiring only a very brief explanation.

a) Is there an injection $[5] \times [7] \longrightarrow [24]$?

b) Is there a surjection $[4] \times [8] \longrightarrow [3] \times [11]$?

c) Is there a bijection $\mathcal{P}([5]) \longrightarrow [8] \times [2] \times [2]$?

5. Decide whether or not the following two sets are finite, and prove your answer.

a) The set of all $(a_1, a_2, a_3, a_4, a_5) \in \mathbb{N}^5$ such that $a_1 + a_2 + a_3 + a_4 + a_5 = 100$.

b) The set of all $(a_1, a_2, a_3, a_4, a_5) \in \mathbb{Z}^5$ such that $a_1 + a_2 + a_3 + a_4 + a_5 = 100$.

6. Suppose $r > 0$ is a real number, and let $A_r = \{(x, y) \in \mathbb{R}^2\}$ satisfying the following two conditions: (i) $x^2 + y^2 \leq r^2$ and (ii) $x, y \in \mathbb{Z}$. Show that A_r is a finite set.

7. Give a combinatorial proof of the identity $\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$. More specifically, consider $\mathcal{P}_n[2n]$, the set of all n-element subsets of a $2n$-element set. Think of a way to partition it into subsets of cardinality $\binom{n}{k}^2$ to get the result.

Remark. This is a really cool problem. Be creative, and persistent.

8. Let m, n be natural numbers. In the first quadrant of $\mathbb{R}^2$, consider the points with integer coordinates (a, b) such that $0 \leq a \leq m$ and $0 \leq b \leq n$. Each pair of horizontally or vertically adjacent points is connected by a line segment; think of this as a street map in which the 1×1 squares are city blocks and points (a, b) are street intersections. You start at the origin $(0, 0)$ and walk to (m, n) along the streets, without going through any buildings. In other words, you follow the vertical and horizontal line segments. Of course there are many different ways you could do this. Show that the total number of distinct routes you can take is $\binom{m+n}{m} = \binom{m+n}{n}$.

9. *Binomial coefficients mod 2.* There's a ton of stuff on the internet about this, but do yourself a favor and avoid the internet. Figure it out yourself first, and only after that peek

online. It's a fun and instructive problem, but not if you let someone else do it for you. (Of course, the same comment applies to many of these problems.)

In a nutshell, the problem to be considered here is the *parity* of the binomial coefficients, i.e. whether a given $\binom{n}{k}$ is even or odd. It turns out that there are some beautiful patterns. The first thing to notice is that Pascal's identity/triangle is perfectly adapted to this situation, because of the rules: even + even=even, odd + odd =even, even + odd =odd. On the other hand, it seems silly to keep writing out the words "even" and "odd". Instead we represent "even" by the number 0 and "odd" by the number 1, which incidentally puts us back into the binary world of computerland. Then the above rules can be written $0+0=0$, $1+1=0$, $0+1=1$ (and also $1+0=1$, by the commutative law). This is called "mod 2 arithmetic", which is the easiest kind of arithmetic there is.

a) This part doesn't require any proofs. Write out Pascal's triangle "mod 2" in the above sense, using only 0's and 1's and making use of mod 2 arithmetic. Now the computations are so easy that you can literally do it as fast as you can write or type, so go out to at least $n = 16$. If you go out far enough, you start to see some interesting patterns, including "fractal" patterns, which are especially pretty if you use different colors for the 0's and 1's. What patterns do you see?

b) One pattern you'll notice is that when n is a power of 2, you get all 0's between the outer 1's. In fact the following proposition is true: $\binom{n}{k}$ is even for all $0 < k < n$ if and only if n is a power of 2. Prove this.

Suggestions: First show that if n is a power of two, say $n = 2^m$, then $\binom{n}{k}$ is even for all $0 < k < n$. The best way I know to do this is via the binomial theorem and induction on m. Note that $(x+y)^{2^{m+1}} = ((x+y)^{2^m})^2$.

Prove the other direction in contrapositive form, i.e. show that if n is not a power of 2 then there exists a k with $0 < k < n$ such that $\binom{n}{k}$ is odd. Again the binomial theorem gives a slick way: We can write $n = s2^m$ with s odd and $s > 1$. Look at $(x+y)^{s2^m} = ((x+y)^{2^m})^s$ to find an odd coefficient.

10. Poker problem. To be done in class.

11. This problem requires knowledge of the rules of chess. In addition to the standard rules, tournament chess has (or at least used to have; I don't know if this is still the case) a rule stating that if fifty consecutive moves are made without a pawn being moved or a piece being taken, then the game is declared a draw. Prove that under this rule, the total number of possible chess games (meaning the entire sequence of moves from beginning to end) is finite.

(Needless to say, the cardinality of this finite set is enormous. On move one each player has twenty possible moves (16 pawn moves, 4 knight moves), so even after just one move we are up to 400 theoretically possible games. In practice only a handful of the twenty possible opening moves are actually used. But remember we are talking about all possible moves, not just intelligent moves! It is then easy to see that without the fifty move rule, the number of possible games is infinite. For example, each player could just move a knight back and forth from its original square, and after n moves one player resigns. Or, somewhat more

realistically, the players could kill off all each other's pieces except the kings, and then move the kings around in random ways.)

12. Let $\sigma \in S_n$ be a permutation of $[n]$. Let σ^k denote σ iterated k times. In other words, $\sigma^2 = \sigma \circ \sigma$, $\sigma^3 = \sigma \circ \sigma \circ \sigma$, and so on.

a) For each n, give an example of a $\sigma \in S_n$ for which σ^n is the identity but σ^k is not the identity for any $k < n$.

b) Since σ is a bijection $[n] \longrightarrow [n]$ by definition, it has an inverse $\sigma^{-1} : [n] \longrightarrow [n]$; i.e. $\sigma(\sigma^{-1}(i)) = i = \sigma^{-1}(\sigma(i))$ for all $i \in [n]$. Use induction on k to show that $(\sigma^k)^{-1} = (\sigma^{-1})^k$.

c) Show that for all $\sigma \in S_n$ there exists $k \in \mathbb{N}$ such that σ^k is the identity permutation (k will depend on σ); in other words, for this k we have $\sigma^k(i) = i$ for all $i \in [n]$.

Examples: Suppose $n = 3$ and σ switches 1 and 2, leaving 3 alone. Then σ^2 is the identity. Or take σ to be the "right shift" given by $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$.

13. Let p be a prime number. Show that for all k such that $0 < k < p$, $\binom{p}{k}$ is divisible by p.

11 Finite sets and counting, revisited

This section is optional reading. It is a longer version of the previous section entitled "Finite sets and counting", with more rigorous proofs. There is also a section on the "inclusion-exclusion formula".

Even in its most basic form, the concept "number" is very abstract. You probably don't think of it as abstract, but that's because you thoroughly internalized it in childhood. Take the number 5, for instance. What is it? It's the thing that five fingers, five oranges and five armadillos have in common. What it really means is that the number of oranges is said to be "five" if and only if they are in bijective correspondence with the fingers on my left hand, except that you would probably prefer to use your own hand. In particular it is independent of the word "five" and the symbol "5" used in English to represent it. In fact, it is possible to count things without even having words to represent the numbers in question. Some "primitive" societies didn't have words for numbers bigger than three. Nevertheless one could determine whether or not two large herds of goats were equal in number by grouping them in pairs, one from each herd. If this can be done with no goat from either herd being left unpaired, then the number of goats in each herd is the same—by definition!

Of course this "pairing" is the same thing as a bijective correspondence, so the concept "number of elements in a set" really boils down to the concept of bijection. We'll see later that the concept can even be extended to infinite sets, but for now let's stick to the more familiar, intuitive world of finite sets. This raises an even more basic question: What do we mean by "finite"?

11.1 Definition of finite sets and cardinality

Since we are taking the natural numbers as given, we can make the following definition:

Definition. A set A is *finite* if there is a bijection $[m] \longrightarrow A$ (or equivalently, $A \longrightarrow [m]$) for some $m \geq 0$. (The case $m = 0$ corresponds to the empty set.)

This suggests making the standard, seemingly obvious definition that the number of elements in a finite set A is the number m occurring in the previous definition. Unfortunately, there is a subtle problem with this: How do we know that it is well-defined? If there is a bijection $f : [m] \longrightarrow A$ and also a bijection $g : [n] \longrightarrow A$ for some $n \neq m$, then the definition is ambiguous. If such a situation occurred then $h := g^{-1} \circ f$ would be a bijection from $[m]$ to $[n]$, so what we need to show is: If $h : [m] \longrightarrow [n]$ is a bijection, then $m = n$. While we're at it, we'll prove a more precise result. It might seem that we're going to a lot of trouble to prove something that is "intuitively obvious", but it's worth giving some thought to the matter.

Proposition 11.1 *Let $h : [m] \longrightarrow [n]$ be a function. Then:*
a) If h is injective, $m \leq n$;
b) If h is surjective, $m \geq n$;
c) If h is bijective, $m = n$.

Proof: a) We use induction on n. The base case $n = 1$ is clear, since then h injective $\Rightarrow$ $m = 1$. So suppose (inductive hypothesis) that (a) is true for n (and for all m); we must show it is true for $n + 1$. Consider first the case that $h(m) = n + 1$. Since h is injective, m is the unique element of $[m]$ that hits $n + 1$. Therefore the restriction of h to $[m - 1]$ has image contained in $[n]$. This restricted function is still injective, so by inductive hypothesis $m - 1 \leq n$ and hence $m \leq n + 1$ as desired.

It remains to consider the case $h(m) \neq n + 1$. We'll use a nice little trick to reduce this case to the previous case. Suppose $h(m) = j$, where by assumption $j < n + 1$. Let $g : [n + 1] \longrightarrow [n + 1]$ be the functioned defined by $g(j) = n + 1$, $g(n + 1) = j$, and for all $i \neq j, n+1$, $g(i) = i$. In other words, g switches j and $n+1$ and leaves all the other elements alone. Then g is a bijection (in fact g is its own inverse). So $g \circ h : [m] \longrightarrow [n+1]$ is injective, since the composition of two injections is an injection. But $(g \circ h)(m) = g(h(m)) = g(j) = n + 1$. Therefore by the previous case, applied to $g \circ h$, $m \leq n + 1$. QED.

b) By the surjection/injection trick (see the exercises to the previous section), there is an injection $g : [n] \longrightarrow [m]$. Hence $n \leq m$ by part (a). So $m \geq n$.

c) By parts (a) and (b) we have $m \leq n$ and $m \geq n$, so $m = n$.

In view of part (c), we may now unambiguously define the *cardinality* of a finite set A to be n if there is a bijection $[n] \longrightarrow A$ (or equivalently $A \longrightarrow [n]$). We also define the cardinality of the empty set to be 0. We use the notation $|A| = n$. Thus "cardinality" is just a fancy word for "number of elements". It's worth having a fancy word, partly as a reminder that we now have a very precise definition of "number of elements in a finite set", and also because the concept of cardinality will later be extended to infinite sets.

11.2 Basic properties of finite sets and cardinality

11.2.1 Behavior with respect to surjections, injections and bijections

The most basic property of all (without which these definitions would be useless) is that the finiteness of a set, and its cardinality, are "invariant under bijection". The precise meaning of the statement in quotes is given in the following proposition.

Proposition 11.2 *Suppose there exists a bijection $f : A \longrightarrow B$. Then A is finite if and only if B is finite, in which case $|A| = |B|$.*

Proof: Suppose A is finite. Then there is a bijection $g : [n] \longrightarrow A$, where $n = |A|$. Hence $f \circ g$ is a bijection $[n] \longrightarrow B$, so B is finite and $|B| = n$. The converse, where we assume B is finite, is proved the same way. (In fact, usually one would just say that the converse follows "by symmetry", because the existence of a bijection between A and B is symmetric in A and B.)

The previous proposition says in particular that if A, B are finite sets and there is a bijection $f : A \longrightarrow B$, then $|A| = |B|$. The following converse also holds (and once again, if this wasn't true then there would be something wrong with our definitions!):

Proposition 11.3 *Suppose A, B are finite sets and $|A| = |B|$. Then there is a bijection $f : A \longrightarrow B$.*

Proof: Let $|A| = n = |B|$. Then there is a bijection $g : A \longrightarrow [n]$ and a bijection $h : [n] \longrightarrow B$. Let $f = h \circ g$; then f is a composition of bijections and so is a bijection (by a problem from the previous chapter).

The next proposition seems so obvious that it's hard to imagine why we'd bother proving it. But we will, just to be careful.

Proposition 11.4 *If B is finite and $A \subseteq B$, then A is finite and $|A| \leq |B|$. Moreover, strict inequality $|A| < |B|$ holds if and only if A is a proper subset of B (i.e. $A \neq B$).*

Proof: Choose a bijection $f : B \longrightarrow [n]$, where $n = |B|$. Next observe that we can at least find injections $g : [m] \longrightarrow A$ for certain values of m (for example, we can certainly do it for $m = 1$). For such a g, consider the composition of functions

$$[m] \xrightarrow{g} A \xrightarrow{i} B \xrightarrow{f} [n],$$

where i is the inclusion function of A into B. Since each of the three maps is injective, so is the composite $f \circ i \circ g$, and hence by Proposition 11.1a we have $m \leq n$. In other words, for such a g we must have $m \in [n]$. Therefore we can choose g so that m is maximal. I claim this g is surjective. For if it wasn't, then $k \notin Im\, g$ for some $k \in A$, and hence we could define an injective function $h : [m+1] \longrightarrow A$ by by setting $h(i) = g(i)$ for $i \leq m$ and $h(m+1) = k$. This would contradict the maximality of m. So g is surjective, hence bijective, proving that A is finite with $|A| = m \leq n = |B|$.

The proof of the "moreover" statement is left as an exercise.

As in Proposition 11.1, we can refine Proposition 11.2 to a statement about injections and surjections. If you've absorbed the concepts "injective" and "surjective", you might object that the next proposition is also "obvious", in which case I couldn't really argue with you. But just to be careful, we'll prove it.

Proposition 11.5 *Let A, B be sets and suppose $f : A \longrightarrow B$ is a function.*
a) If B is finite and f is injective, then A is finite and $|A| \leq |B|$.
b) If A is finite and f is surjective, then B is finite and $|A| \geq |B|$.

Proof: a) Any injective function defines a bijection onto its image. Since $Im\, f$ is finite and $|Im\, f| \leq |B|$ by the previous proposition, this proves part (a).

b) Use the surjection/injection trick to deduce this from (a).

Note. In most applications, we already know that both sets are finite; thus the main content of the proposition is the inequality on cardinalities. In their contrapositive forms, these two statements then go by the name of "the pigeonhole principle" (a name that must have been invented in a country with lots of pigeons and holes to put them in, presumably England). The idea is that set A is the pigeons and set B is the set of pigeonholes to put

them in. Let's write out these contrapositive forms explicitly, taking as given that A and B are both finite.

a) If $|A| > |B|$, then there must be two elements $a_1 \neq a_2$ of A such that $f(a_1) = f(a_2)$ (i.e. two pigeons have to share the same hole).

b) If $|A| < |B|$, then there must be some element $b \in B$ that is not in the image of f (i.e. there must be at least one unoccupied pigeonhole).

This kind of imagery can be very helpful; you should invent your own! In terms of my cupcake function, part (a) says that at least one child gets two or more cupcakes, while part (b) says at least one child gets no cupcake.

Finally, here's a handy fact that can cut your work in half:

Proposition 11.6 *Suppose A, B are finite sets, $|A| = |B|$, and $f : A \longrightarrow B$ is a function.*

a) If f is injective, then f is bijective.

b) If f is surjective, then f is bijective.

Proof: a) Let $n = |A| = |B|$. Since f is injective, it defines a bijection onto its image $Im\, f$. Hence $|Im\, f| = n$. Since $n = |B|$ this forces $Im\, f = B$. In other words, f is also surjective, hence bijective.

b) Since f is surjective, for each $b \in B$ we can choose an element $a \in A$ with $f(a) = B$. Call this subset of chosen elements C. Then by construction the restriction of f to C is still surjective but also injective (because we cooked it up so there is a unique element of C in each fiber $f^{-1}b$), hence we have a bijection from C to B. So $|C| = n$. Since also $|A| = n$, this forces $C = A$. Therefore f is bijective, QED.

Caution: The point of this last proposition is that it allows you to prove f is a bijection by proving only one of the two conditions injective/surjective. But it only applies in a very special situation: both sets are finite, and have the same cardinality (you would have to know the cardinalities are the same in advance, by some other means). It doesn't work for infinite sets or for finite sets of different cardinalities.

11.2.2 Finite unions of finite sets

Suppose A, B are disjoint finite sets. Then surely $A \cup B$ is finite and $|A \cup B| = |A| + |B|$. Indeed this is the very essence of what it means to "add" two numbers, so it has to be true if we've made the right definitions. Well then, let's prove it carefully. While we're at it, let's consider the more general case where A, B are not necessarily disjoint. In that case it's clear that the answer isn't $|A| + |B|$, because that would mean you counted the elements of $A \cap B$ twice (draw a picture or use your personal mental imagery!). With a little thought we find:

Proposition 11.7 *Suppose A, B are finite sets. Then $A \cup B$ is finite, and*

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

In particular, if A, B are disjoint, then

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

Proof: Choose bijections $f : [m] \longrightarrow A$ and $g : [n] \longrightarrow B$. Let's first do the case when A, B are disjoint. We need to find a bijection $h : [m+n] \longrightarrow A \cup B$. Define $h(i) = f(i)$ if $i \leq m$, and $h(i) = g(i-m)$ if $m+1 \leq i \leq m+n$. In other words, map the first m elements to A using f, then map the last n elements to B using g. You can (and should!) easily check that h is bijective. This proves that $A \cup B$ is finite with cardinality $|A| + |B|$, as desired.

For the general case, with A, B not necessarily disjoint, let $C = B - A \cap B$ denote the complement of $A \cap B$ in B. (Draw a Venn diagram or other picture to make all this transparent.) Then B is the disjoint union of $A \cap B$ and C, so by the part we already proved, $|B| = |A \cap B| + |C|$. Also $A \cup B = A \coprod C$ (recall $\coprod$ indicates *disjoint* union), so $A \cup B$ is finite and

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

QED.

Reminder. Don't let all the verbiage and notation get in the way of your intuition. You can draw a picture such as a Venn diagram that makes the proposition intuitively obvious. The verbiage and notation might seem superfluous now, but it's important to get in the habit of rigorous proof. As the mathematics gets more and more complicated, naive intuition becomes increasingly unreliable.

Now let's consider a finite collection of pairwise disjoint finite sets $A_1, ..., A_n$. By "pairwise disjoint" we mean that for all $i \neq j$, $A_i \cap A_j = \emptyset$; i.e. there is no "overlap" between any two of the sets.

Proposition 11.8 *Let $A_1, ..., A_n$ be a finite collection of finite sets.*
a) The union $\cup_{i=1}^n A_i$ is finite.
b) If the A_i's are pairwise disjoint, then $|\cup_{i=1}^n A_i| = \sum_{i=1}^n |A_i|$.

Proof: We prove (a) and(b) simultaneously by induction on n, in a particular way that gets recycled later in similar proofs. Note that the base case $n = 1$ is completely trivial, almost silly, since there is only one set in the collection. But instead of proceding immediately to the inductive step, we first do the case $n = 2$. Luckily, we already did this in the preceding proposition; the case $n = 2$ is proved.

Now suppose the result is true for a collection of n sets; we need to show it is true for a collection of $n+1$ sets. So suppose given finite sets $A_1, ..., A_{n+1}$. Let $A = \cup_{i=1}^n A_i$ and let $B = A_{n+1}$. Then by inductive hypothesis A is finite, so $A \cup B$ is finite by the case of two sets already done. Similarly if the A_i's are pairwise disjoint, then $|A| = \sum_{i=1}^n |A_i|$ by inductive hypothesis. Note that $A \cap B = \emptyset$, since A_{n+1} doesn't intersect any of the other A_i's, by assumption. So again by the case of two sets that we already did,

$$|\cup_{i=1}^{n+1} A_i| = |A \cup B| = |A| + |B| = \sum_{i=1}^{n+1} |A_i|.$$

Comparing the second proposition with the first, we see that something is missing: the second proposition doesn't give a formula for $|\cup_{i=1}^n A_i|$ in the case where the A_i's aren't

pairwise disjoint. We'll do this in a later section; meanwhile, try to discover and prove a formula for three sets: $|A \cup B \cup C| = ?$. The formula should be in the spirit of the two-set case.

11.2.3 Finite products of finite sets

Suppose A and B are finite sets. Then surely the product set $A \times B$ is finite, with cardinality $|A \times B| = |A| \cdot |B|$ (where the dot as usual indicates multiplication; it's good to put the dot in, as the notation $|A||B|$ is rather cramped). I say "surely" because, intuitively at least, this is the essence of multiplication. For example, the standard notation used for squares on a chessboard is to label the rows (as viewed by the player with the white pieces) using the numbers 1 through 8, and the columns by the first 8 letters of the alphabet $abcdefgh$. If we call this set of letters B, then altogether the squares are labeled by the product set $[8] \times B$, i.e. pairs (k, x) where $1 \leq k \leq 8$ and x is one of the eight letters. The total number of squares is then $8 \cdot |B| = 8 \cdot 8$. Or a room 6 feet by 9 feet tiled with 1 by 1 squares requires $6 \cdot 9$ tiles. So this is just the everyday notion you've known for years.

Let's consider the matter more carefully, however. What exactly is "multiplication" of natural numbers? The answer is that it is iterated addition: $m \cdot n$ is n added to itself m times: $n + n + ... + n$ where there are m terms. Incidentally, when you define it this way it isn't obvious that $m \cdot n = n \cdot m$, in other words that adding m to itself n times gives the same result. We think of it as obvious by just picturing an $m \times n$ array of dots (or walnuts, or zebras, or whatever strikes your fancy). Then we can count the total by thinking of it as m rows of n dots each or n columns of m dots each. So we're implicitly using the concept "product of sets".

Once again, therefore, we'll take the trouble to prove the desired formula rigorously. While we're at it, we may as well consider finite products $A_1 \times ... \times A_n$ of a collection of finite sets.

Proposition 11.9 *Let $A_1, ..., A_n$ be a finite collection of finite sets. Then $\prod_{i=1}^n A_i$ is finite, and $|\prod_{i=1}^n A_i| = \prod_{i=1}^n |A_i|$. (Note we are using the same symbol for products of sets and products of numbers.)*

Proof: We use induction on n, following the model above for disjoint unions. Again the case $n = 1$ is silly but true, since there is only one set. Instead of proceeding to the inductive step, we first consider the case of two finite sets A, B. Our proof for this case is exactly in the spirit of the intuitive discussion above: $A \times B$ is the disjoint union of the slices $A \times \{b\}$, $b \in B$. There are $|B|$ slices, each of which has $|A|$ elements. So by what we already proved for disjoint unions,

$$|A \times B| = |A| + |A| + ... + |A| = |A| \cdot |B|,$$

where there are $|B|$ terms $|A|$ in the sum.

The general case is now proved by induction on n, making use of the two-set case at the inductive step just as we did in the disjoint union proof. The details are left as an exercise.

11.3 Combinatorics, or how to count things

The branch of mathematics known as "combinatorics" is about counting finite sets. This is an oversimplification, of course, but not so far from the truth. But don't let this simple-minded description fool you! Combinatorics is a vast subject, filled with many deep and beautiful theorems, and moreover having many practical applications. As basic examples of what we might want to count, consider the following questions.

- How many subsets does a set with n elements have?
- How many k-element subsets does a set with n elements have?
- How many ways are there to order a set with n elements?

This is what I mean by "counting finite sets": You're given a finite set A, and wish to compute $|A|$. In these examples the answer will be a sequence of formulas depending on n, so it's natural to expect that induction will enter in. For that you first you have to guess what the answer is, then prove it by induction. Another method: Suppose you can find another set B whose cardinality you already know, and can show by hook or by crook that A and B are in bijective correspondence. Then $|A| = |B|$ and you have your answer. Or maybe you can partition A in some relevant way as $A = \coprod_{i=1}^{n} A_i$; then $|A| = \sum |A_i|$, which might prove to be a useful formula.

Now, let's get on to the examples!

11.3.1 The set of subsets of a finite set

If S is any set, not necessarily finite, we let $\mathcal{P}(S)$ denote the set of all subsets of S. (The choice of the letter P comes from the fact that $\mathcal{P}(S)$ is often called the "power set" of S. Eventually, we'll explain where this name comes from.) For the time being, though, we are concerned only with the case $\mathcal{P}(A)$ for a finite set A. Our goal is to determine $|\mathcal{P}(A)|$.

The first thing to observe is that if $|A| = |B|$, then $|\mathcal{P}(A)| = |\mathcal{P}(B)|$. This is left to you to prove, in the exercises. So if $|A| = n$, we may as well just consider the case $A = [n]$. Let's see if we can guess the answer by looking at small values of n. Recall that the empty set and A itself are always subsets of A.

If $n = 0$ then A is the empty set, so A has just one subset, namely itself.

If $n = 1$, then $[1]$ has two subsets, $\emptyset$ and $[1]$.

If $n = 2$, there are four subsets: $\emptyset$, $[2]$, $\{1\}$ and $\{2\}$.

If $n = 3$ there are eight subsets. Rather than list them, I'll describe them: The empty set and the whole set give you 2. The singletons give you 3. Finally there are three subsets with 2 elements, giving 8 in all.

Okay, $1, 2, 4, 8...$ I think we see a pattern. But experimental evidence does not constitute a proof, even if you checked the first billion cases on a computer. All we have a conjecture. Since the conjecture turns out to be true, I'll state it as a theorem.

Theorem 11.10 *$|\mathcal{P}([n])| = 2^n$.*

There are several interesting, enlightening ways to prove the theorem, and as I don't want to deprive you of the fun, I'll leave it as an exercise with minimal hints (see the exercises below).

We can refine the theorem a bit. Let $\mathcal{P}_{ev}[n]$ denote the set of subsets of $[n]$ with even cardinality, and similarly let $\mathcal{P}_{odd}[n]$ denote those of odd cardinality.

Theorem 11.11 $|\mathcal{P}_{ev}[n]| = |\mathcal{P}_{odd}[n]| = 2^{n-1}$.

Again the proof is an interesting exercise.

11.3.2 Permutations and orderings of a finite set

How many ways are there to order a set A with n elements, i.e. as $a_1, a_2, ..., a_n$? I claim the answer is $n!$, and that we can prove this as follows: There are n possible choices for the last element a_n. That leaves $n-1$ choices for the second to last element a_{n-1}, then $n-3$ choices for a_{n-3}, and so on. So all in all we have $n \cdot (n-1) \cdot (n-2)... \cdot 2 \cdot 1 = n!$ possibilities. (The only reason I did it in reverse order, starting with the last element instead of the first, is to make the notation more consistent with the induction proof to be given shortly.)

If a proof is "a convincing explanation of why something is true", then I regard the informal argument above as a proof. It is completely convincing, so much so that asking for a "rigorous" proof seems redundant. Nevertheless, the fact remains that it does not meet the standard of rigorous proof established thus far in these notes. For one thing, we never even defined "ordering". For another, all this talk about "choices" makes no use at all of the theory we've so carefully developed, so what exactly are we really doing?

Let's make it all more precise. First, we define an *ordering* of A to be a bijection $f : [n] \longrightarrow A$. In the informal argument, $f(i) = a_i$. So this is a sensible, intuitive definition; the function f tells you exactly in what "order" to arrange the elements of A. Thus what we're saying is:

Proposition 11.12 *Let A be a set with n elements, where $n \geq 1$, and let $B([n], A)$ denote the set of bijections $[n] \longrightarrow A$. Then $|B([n], A)| = n!$.*

Proof: We use induction on n. The base case $n = 1$ is trivial as usual; given two sets with one element each, there is only one map between them!

Now suppose (inductive hypothesis) that the result is true for n. We need to show that it is true for $n+1$. So let $|A| = n+1$. We can partition $B([n+1], A)$ into $n+1$ disjoint subsets $B_i = \{f : f(n+1) = i\}$. If $f \in B_i$ then f is completely determined by its restriction to $[n]$. Moreover, $f|_{[n]}$ is a bijection $[n] \longrightarrow [n+1] - \{i\}$. Since $[n+1] - \{i\}$ has n elements, by inductive hypothesis we have $|B_i| = n!$ for all i. So

$$|B([n], A)| = \sum_{i=1}^{n+1} |B_i| = \sum_{i=1}^{n+1} n! = (n+1)n! = (n+1)!.$$

QED.

This proof is really just a formal version of the one we already gave. On the other hand, the informal argument we started with is more enlightening, and easier to follow. From here

on we will often stick with the informal argument, keeping in mind that we could make it more rigorous if we had to.

A *permutation* of a set A (which for now we assume finite) is a bijection $f : A \longrightarrow A$. Let $Perm\, A$ denote the set of all permutations of A. If $A = [n]$, it is customary to write S_n for $Perm\,[n]$ (S is for "symmetric".) If $A = [n]$, then a permutation of $[n]$ is the same thing as an ordering of $[n]$, and the last proposition shows that $|S_n| = n!$. It follows that for any set A with n elements, $|Perm\, A| = n!$. (Why? Prove this!)

Since S_n consists of bijections from $[n]$ to itself (permutations), we can compose any two permutations f, g to get a third permutation $f \circ g$. Since composition of functions is associative, this operation on permutations is associative: $f \circ (g \circ h) = (f \circ g) \circ h$. Moreover any permutation f has an inverse (since it is a bijection) f^{-1}, i.e. $f \circ f^{-1} = f^{-1} \circ f = Id_{[n]}$. This combination of properties makes S_n a "group", a type of structure that arises almost everywhere in mathematics. We won't pursue this concept any further, except to note that the composition operation is *not* commutative. The simplest counterexample to commutativity occurs for S_3, which has a grand total of $3! = 6$ elements. The following two elements are typical:

$f(1) = 2$, $f(2) = 1$, $f(3) = 3$ (switch 1 and 2, leave 3 alone)
$g(1) = 2$, $g(2) = 3$, $g(3) = 1$ (shift everything to the right, except the last element 3 wraps back around to the start)

I leave it to you to check that $f \circ g \neq g \circ f$. By the way, there's no reason to limit oneself to numbers. Check this in some more vivid physical way, perhaps using an ace, king and queen from a deck of cards; or get three friends to act it out for a YouTube video. For larger n you could find many more interesting examples of non-commuting permutations; make it a dance video set to music. The moral of the story is that there is nothing strange about failure of the commutative law; it fails frequently in simple down-to-earth settings.

Two last notes about the "group" concept: (1) Don't lose any sleep over why it's called a group. Whoever invented the term back in the 1800's thought it was good at the time, and it stuck. (2) At the UW you can learn more about groups in Math 402.

11.3.3 Counting injections and surjections

The method used to count bijections carries through almost verbatim to count injections. Recall that we define 0! to be 1.

Proposition 11.13 *Let A be a set with n elements. Then for $1 \leq k \leq n$, the number of injections $[k] \longrightarrow A$ is*

$$n(n-1)...(n-k+1) = \frac{n!}{(n-k)!}.$$

Proof: Consider the possible injections $f : [k] \longrightarrow A$. There are n choices for $f(1)$, $n-1$ choices for $f(2)$, and so on, until finally there are $n-k+1$ choices for $f(k)$. Hence there are $n(n-1)...(n-k+1)$ injections, and this number is equal to $n!/(n-k)!$ by simple algebra. QED.

Note. This is what I call the "informal" proof. It could be converted into a more pedantic, rigorous proof by induction, exactly as we did for bijections.

It's good to check extreme cases of any new definition or proposition, and make sure they make sense (otherwise something is wrong with your proposition!). In the preceding proposition, one extreme is $k = 1$. Then it says that the number of injections from a one-element set to an n-element set is n. This makes sense; any function whose domain is a one-element set is injective, so we just get the set of all functions $[1] \longrightarrow A$, which has cardinality n. At the opposite extreme with $k = n$, we know that then any injection is a bijection, so this agrees with the previous answer $n!$ for bijections.

The natural question still staring us in the face is: Can we "count", i.e. find a formula for, the number of surjections $[k] \longrightarrow A$ (where $k \geq 2$)? This turns out to be harder than the count for injections; we'll do it later using the "inclusion/exclusion principle". Meanwhile, a good exercise is to find the answer directly when $|A| = 2$.

11.3.4 The k-element subsets of a set with n elements

How many distinct 5-card poker hands are there? It's the number of five-element subsets of a set with 52 elements (the deck of cards). The number of distinct bridge hands is the number of 13-element subsets of a set with 52 elements.

More generally, let $\mathcal{P}_k[n]$ denote the set of k-element subsets of $[n]$. How many are there? The number $|\mathcal{P}_k[n]|$ is denoted $\binom{n}{k}$ and pronounced "n choose k". It's also called a "binomial coefficient", for reasons that will be explained later. Our problem, then, is to compute $\binom{n}{k}$. Let's start with some easy facts:

$\binom{n}{0} = 1$. There is only one subset with zero elements, namely the empty set.

$\binom{n}{n} = 1$. There's only one subset with n elements, namely the whole set.

$\binom{n}{1} = n$. There are n different singletons, i.e. subsets with one element.

$\binom{n}{k} = \binom{n}{n-k}$. Why? Prove it! We call this property *symmetry*.

The first case requiring a little thought is $\binom{n}{2}$. We'll study it as a warm-up for the general case. As usual, you should have some mental image in mind. I'll think of a deck of cards, so $n = 52$. I want to pick a pair of elements (pick a card, any card...). There are n choices for the first element. That leaves $n - 1$ choices for the second element. So the answer is $n(n-1)$? No! We're only counting subsets, not orderings of subsets. If I pick the ace of hearts first and then the jack of clubs, I get the same pair by picking the jack first and then the ace. This observation tells us how to correct our formula. The count given by $n(n-1)$ is counting every pair twice, so to get the right formula we have to divide by 2:

$$\binom{n}{2} = \frac{n(n-1)}{2}.$$

Indeed, you will recall that $n(n-1)$ is the number of injections $[2] \longrightarrow [n]$. For every 2-element subset A of $[n]$, there are two different injections with image A. The particular injection puts an ordering on A, but we don't want to count orderings, hence the division by 2. Incidentally, $\frac{n(n-1)}{2} = 1 + 2 + 3 + ... + n - 1$, by the Gauss formula. A good exercise is to show combinatorially that $\binom{n}{2} = 1 + 2 + ... + n - 1$; see the exercises.

The general case follows an identical pattern. Suppose I want to choose a k-element subset of an n-element set. There are n choices for the first element, $n-1$ for the second, and so on down to $n - (k-1) = n - k + 1$ for the k-th element. This leads to the number $n(n-1)...(n-k+1)$. But here again we don't want to count the ordering. As we already proved earlier, this number counts the number of injections $[k] \longrightarrow [n]$, whereas now we only care about the *image* of the injection. For each k-element subset A, there are $k!$ bijections $[k] \longrightarrow A$. Hence our preliminary count of $n(n-1)...(n-k+1)$ is counting very subset $k!$ times. To get the right formula we divide by $k!$:

$$\binom{n}{k} = \frac{n(n-1)...(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}.$$

Here the second equality is easy algebra (check it!). Note that the fraction on the right is symmetric in k and $n-k$, so this fits with the symmetry $\binom{n}{k} = \binom{n}{n-k}$ we noticed earlier. One striking feature of the equality is that it is not at all obvious that the fraction is an integer. Yet it must be an integer, since $\binom{n}{k}$ is an integer by definition!

For small values of n, the numbers $\binom{n}{k}$ are easily computed by hand from this formula. You could, of course, just look them up or compute them electronically, but I highly recommend doing a few by hand to get a feel for it. For example, even my slow brain can compute $\binom{7}{k}$ for all k with no artificial aids at all: $\binom{7}{0} = 1$ and $\binom{7}{1} = 7$ are the trivial cases, while $\binom{7}{2} = 7 \cdot 6/2 = 21$ and $\binom{7}{3} = (7 \cdot 6 \cdot 5)/(3 \cdot 2) = 35$. The remaining cases follow immediately by symmetry, e.g. $\binom{7}{4} = \binom{7}{3} = 35$, and so on.

A larger example that you probably don't want to compute by hand is the number of 5-card poker hands:

$$\binom{52}{5} = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5!} = 2,598,960.$$

The number of bridge hands is much larger, and I'll leave that computation to those who really want to know.

Before going further, let's take the preceding informal argument and turn it into a more precise proof.

Proposition 11.14 $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Proof: Let S denote the set of all injections $[k] \longrightarrow [n]$, and for each $A \in \mathcal{P}_k[n]$ let $S_A = \{f \in S : Im\, f = A\}$. Then the S_A's form a partition of S, and for all A we have $|S_A| = k!$ by Proposition 11.12. So

$$|S| = \sum_{A \in \mathcal{P}_k[n]} |S_A| = \sum_{A \in \mathcal{P}_k[n]} k! = k! |\mathcal{P}_k[n]|.$$

Since $|S| = \frac{n!}{(n-k)!}$, we conclude

$$|\mathcal{P}_k[n]| = \frac{|S|}{k!} = \frac{n!}{k!(n-k)!}.$$

QED.

For future reference, we record the following surprising formula:

Proposition 11.15

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

Proof: You certainly wouldn't want to use the algebraic formula $\frac{n!}{k!(n-k)!}$ to prove this; that would create a big mess. Instead, we begin by noting that $(-1)^k$ is $+1$ for k even and -1 for k odd. So if we move the negative terms to the other side of the equation, what we want to prove is

$$\sum_{k \, \text{even}} \binom{n}{k} \stackrel{?}{=} \sum_{k \, \text{odd}} \binom{n}{k}.$$

But the left-hand side above is $|\mathcal{P}_{ev}[n]|$, while the right-hand side is $|\mathcal{P}_{odd}[n]|$. So the proposition follows from Theorem 11.11.

Note. I put a question mark over the equality to emphasize that it is something we want to prove, as opposed to something we have already proved. I recommend this practice to avoid circular reasoning.

11.3.5 Pascal's identity and Pascal's triangle

Pascal's identity is the following simple formula:

Proposition 11.16 $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$.

Proof: One could easily prove this using the algebraic formula for $\binom{n}{k}$ (just add the fractions on the left and see what you get). But even easier (at least after you get used to doing a little combinatorics), and certainly more enlightening and fun, is to do it combinatorially. In this case I mean find a partition of $\mathcal{P}_k[n+1]$ into two sets whose cardinalities are the two terms on the left of the formula; then you're done. Here we define $X \subset \mathcal{P}_k[n+1]$ to be those subsets that contain $n+1$, and Y to be those that don't. Thus we have a partition

$$\mathcal{P}_k[n+1] = X \coprod Y.$$

Now, a subset A containing $n+1$ is uniquely determined by the $k-1$ remaining elements, which lie in $[n]$. Hence $|X| = \binom{n}{k-1}$. A subset A that doesn't contain $n+1$ is the same thing as a subset of $[n]$, so $|Y| = \binom{n}{k}$. QED.

Pascal's formula is the basis for the famous Pascal's triangle. A picture of Pascal's triangle will eventually go here. Meanwhile, one can find many such pictures on the internet. You'll find many in pretty colors, but don't neglect the basic model that just has the numbers. In any case, Pascal's identity gives an easy way to compute binomial coefficients recursively. In a very short time you can compute by hand $\binom{n}{k}$ for, let's say, $n \leq 10$ and all k. The point is that if you know $\binom{n-1}{k}$ for all k, then Pascal's identity easily yields $\binom{n}{k}$ for all k. Pascal's triangle is just a convenient way of displaying this information. You can, of course, just look up the values of $\binom{n}{k}$, have a computer do it or whatever. But I highly recommend working out Pascal's triangle by hand up to at least $n = 8$, because it's easy (up to 8 you can do in a minute) and the process helps you to internalize the concept.

11.3.6 The binomial theorem

One of the most important ways in which the numbers $\binom{n}{k}$ arise is in the binomial theorem; this is where the term "binomial coefficients" comes from. In early school days you learn the formula

$$(x+y)^2 = x^2 + 2xy + y^2.$$

At some point you also learn

$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3,$$

or even

$$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4.$$

But let's get serious and find the general formula for $(x+y)^n$, n any natural number. Here we'll take for granted the concept "polynomial", of which $(x+y)^n$ is an example. Looking at the sequence of coefficients in the above examples, we find $1, 2, 1$ (for $n = 2$), $1, 3, 3, 1$ (for $n = 3$), and $1, 4, 6, 4, 1$ (for $n = 4$). Comparing with Pascal's triangle, we notice that these are exactly the numbers $\binom{n}{k}$ for $n = 2, 3, 4$ respectively. This suggests a conjecture as to the general answer, and it turns out to be true:

Theorem 11.17

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

By symmetry we could just as well write $x^k y^{n-k}$ in place of $x^{n-k}y^k$. I chose the latter option because then the sum begins with $x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + ...$, which to me looks better than the other way. It's a personal aesthetic choice; there are more of these in mathematics than you might think.

First proof: The n-power on the left is

$$(x+y)^n = (x+y)(x+y)...(x+y),$$

where there are n factors $x+y$. If we expand this out by the distributive law, without collecting "like terms", we'll have a sum with 2^n terms in it: Run through the n factors and pick either x or y from each one. Each term is of the form $x^{n-k}y^k$ for some k. For fixed k, we obtain this term by choosing y from k factors and x from the others. In other words, we choose k factors from n factors, and the total number is $\binom{n}{k}$. QED.

Second proof: Use induction on n. The base case $n = 1$ says that $x + y = x + y$, and a truer statement you'll never find. Now suppose (inductive hypothesis) that the result is true for n. We must prove it for $n + 1$. To see this, we have

$$(x+y)^{n+1} = (x+y)^n(x+y) = (\sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k)(x+y) = \sum_{k=0}^{n} \binom{n}{k} x^{n-k+1}y^k + \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^{k+1}.$$

Here the first equality is by inductive hypothesis, and the second is just the distributive law. Each of the two sums contains one term of the form $x^{n-k+1}y^k$ (for a fixed k). In the left-hand sum the coefficient of this term is $\binom{n}{k}$, while in the right-hand sum (look closely!) it is $\binom{n}{k-1}$. So if we collect these two like terms, the coefficient we get is $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ by Pascal's identity. QED.

We can use the binomial theorem to prove results about $\binom{n}{k}$. For example, we now have a stunningly simple proof of the complicated looking identity

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

Just substitute $x = 1$, $y = -1$ in the binomial theorem, and the above formula pops out by magic!

11.4 The inclusion-exclusion formula

The formula of Proposition ? can be used in a surprising way to answer the earlier question about the cardinality of a finite union of finite sets. The general formula is called the "inclusion-exclusion" formula.

Recall that the question is whether there is a formula for $|A_1 \cup A_2 \cup ... \cup A_n|$, where the A_i's are finite sets. When $n = 2$ we had the relatively easy formula $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$.

In order to guess what form the general formula might take, let's consider the case $n = 3$. We start with the count $|A_1| + |A_2| + |A_3|$. As in the $n = 2$ case, this number is too big; we've counted the elements of $A_1 \cap A_2$ twice, and similarly for $A_1 \cap A_3$ and $A_2 \cap A_3$. So our next attempt is

$$|A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3|.$$

Ah, but what about the elements of $A_1 \cap A_2 \cap A_3$? These poor fellows now haven't been counted at all! Or more precisely, they've been counted three times in the first three positive terms of the above formula, but then counted negatively three times in the last three terms, with the net result that they've been counted zero times and so feel sadly neglected. Thus it appears that the formula we want is

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

In fact this is correct, and we've essentially proved it. But what we're looking for at the moment is a conjecture as to what the general formula might be. Staring at the $n = 3$ case, we notice that each A_i gets a plus sign, each $A_i \cap A_j$ gets a minus sign, and $A_1 \cap A_2 \cap A_3$ gets a plus sign. Taking the optimist's approach to mathematics, we conjecture that this pattern continues in general. In other words, if $n = 4$ we would have a fourth term $|A_1 \cap A_2 \cap A_3 \cap A_4|$ that would get a minus sign. So in general, a k-fold intersection should get a plus sign if k is odd and a minus sign if k is even.

In order to have any hope of proving such a formula, we first have to state it clearly. This is where well-chosen notation, and a little patience, comes in. We return to the general case where there are n sets $A_1, ..., A_n$. We select k elements of $[n]$ and label them $i_1, ..., i_k$ To be specific, we put them in increasing order: $i_1 < i_2 < ... < i_k$. Then we form the intersection $A_{i_1} \cap A_{i_2} ... \cap A_{i_k}$ of these k sets. The notation takes a little getting used to, because we have double subscripts; read A_{i_1} as "A sub i sub 1", A_{i_2} as "A sub i sub 2", and so on. For example, suppose $n = 6$, $k = 3$ and we choose the three elements $2, 4, 5$. Then $i_1 = 2$, $i_2 = 3$, and $i_3 = 5$. The intersection is just $A_2 \cap A_4 \cap A_5$. We will need to consider all such intersections, for all k with $1 \leq k \leq n$.

Theorem 11.18 *Let $A_1, ..., A_n$ be finite sets. Then*

$$|A_1 \cup A_2 \cup ... \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} |A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_k}|,$$

where the indices $i_1, ..., i_k$ range over all increasing sequences $i_1 < ... < i_k$ with $1 \leq i_1$ and $i_k \leq n$.

Before proving the theorem, let's examine the sum that occurs on the right (and refuse to be intimidated by it!). It has one term for every nonempty subset $\{i_1, ..., i_k\}$ of $[n]$. So it has $2^n - 1$ terms in all. Ignoring the sign for the moment, the terms are just the cardinalities of all possible intersections of sets chosen from the A_i's, as illustrated in the examples above. As to the signs, our guess (which turns out to be correct) was that intersections of an odd number of A_i's should get a sign $+1$, while intersections of an even number of A_i's should get a -1. That's why we have the exponent $k + 1$ instead of k in $(-1)^{k+1}$; it makes it $+1$ for odd k and -1 for even k.

Proof: It is possible to prove the result by induction on n, but there is a really cool, slick proof that is surprisingly short. The trick required is already illustrated in the $n = 3$ example above: We focus our attention on a single element $x \in A_1 \cup ... \cup A_n$, and ask how many times it gets counted (with sign) in the sum. For every subset $\{i_1, ..., i_k\}$ such that $x \in A_{i_1} \cap ... \cap A_{i_k}$,

x will get counted once positively if k is odd and once negatively if k is even. We need to add up all these ± 1's and show that the answer is $+1$; i.e., after the smoke has cleared and the dust has settled, x has been counted exactly once. That will prove the formula.

First of all, clearly we need only consider the set of indices $J = \{j \in [n] : x \in A_j\}$; the A_j's that don't contain x won't contribute anything. Let $|J| = m$. Each k-element subset of J will contribute $(-1)^{k+1}$ to our count. There are $\binom{m}{k}$ such subsets, so the number we wish to compute is

$$\sum_{k=1}^{m}(-1)^{k+1}\binom{m}{k}.$$

Hmm....looks familiar, doesn't it? We proved earlier that $\sum_{k=0}^{m}(-1)^k\binom{m}{k} = 0$. This is very close to the sum we want. In fact if we write out the latter sum term by term, the equation reads

$$1 - \binom{m}{1} + \binom{m}{2} - ... + (-1)^m\binom{m}{k} = 0.$$

Aha! just move everything except the leading 1 to the other side of the equation! Since $-(-1)^k = (-1)^{k+1}$, we get

$$1 = \sum_{k=1}^{m}(-1)^{k+1}\binom{m}{k},$$

which is exactly what we wanted! QED!!! Isn't that awesome?

As an application let's return to the surjection problem: If A has n elements, how many surjections are there $[k] \longrightarrow A$? We may as well assume $A = [n]$. Rather than state the theorem and then prove it, let's see how one might be led to the rather surprising formula in the first place. First of all, we saw earlier that the total number of functions $[k] \longrightarrow [n]$ is n^k. So if we can compute the number of *non*-surjective functions $[k] \longrightarrow [n]$, subtracting this number from n^k will give us the formula we want.

Just to simplify the writing, let's use X to denote the set of all non-surjective functions $[k] \longrightarrow [n]$. If $f : [k] \longrightarrow [n]$ is non-surjective, then some $i \in [n]$ is not in the image of f. Letting $X_i = \{f : [k] \longrightarrow [n] : i \notin Im\, f\}$, we therefore have $X = X_1 \cup X_2 ... \cup X_n$. Note these subsets are not disjoint, however. For instance, $X_1 \cap X_2$ consists of those functions f such that neither 1 nor 2 is in the image of f. Aha! This is exactly the setup for inclusion/exclusion. So as a first formula for $|X|$, we have (by the inclusion/exclusion principle)

$$|X| = \sum_{r=1}^{n}(-1)^{r+1}|X_{i_1} \cap X_{i_2} \cap ... \cap X_{i_r}|,$$

where the sum is over all indices $1 \leq i_1 < i_2 < ... < i_r \leq n$. When $r = n$ there is only one term $|X_1 \cap X_2 ... \cap X_n|$ and it is zero because the intersection of *all* the X_i's is empty: A function f has to have at least one value in its image. So we could just omit that term, but let's leave it in for now.

The real problem confronting us is that the formula needs to be made more explicit; as it stands, it isn't very helpful. Let's take a closer look at a typical intersection $X_{i_1} \cap ... \cap X_{i_r}$.

What is it, exactly? It consists of all functions f such that none of $i_1, ..., i_r$ is in the image of f. In other words, it consists of all functions $f : [k] \longrightarrow [n]$ whose image is contained in the complement of $\{i_1, ..., i_r\}$. So the total number of such functions is the same as the number of functions from a k-element set to a $(n-r)$-element set, i.e. $(n-r)^k$. Summarizing:

$$|X_{i_1} \cap ... \cap X_{i_r}| = (n-r)^k.$$

Staring at this formula for a while, we notice a quite wonderful fact about it: *It doesn't depend on the particular choice of $i_1, ..., i_r$; it only depends on r* (and of course on n, k but these numbers were fixed from the beginning). Hence if we group all the terms for fixed r together, we get

$$|X| = \sum_{r=1}^{n} (-1)^{r+1} \binom{n}{r} (n-r)^k.$$

This is an explicit formula indeed. We now have our theorem:

Theorem 11.19 *For $k \geq n$, the number of surjections $[k] \longrightarrow [n]$ is*

$$\sum_{r=0}^{n-1} (-1)^r \binom{n}{r} (n-r)^k.$$

Proof: All the hard work has already been done. The number we want is $n^k - |X|$. Because of the minus sign, all the $(-1)^{r+1}$'s get replaced by $(-1)^r$'s. The number n^k can be put into to the sum as an $r = 0$ term, and we're done! QED. (The $r = n$ term is still zero, so we just omitted it.)

Let's compute some special cases, starting with the extreme case $n = 1$. In that case there is only one function $[k] \longrightarrow [n]$, and it is surjective, but it's worth plugging it in anyway as a reality check on our formula. There's only one term in the sum, namely $r = 0$, so we get $(-1)^0 \binom{1}{0} (1-0)^k$ which is indeed 1. Whew! It would be embarassing if it failed in this trivial case!

For $n = 2$ we get

$$\binom{2}{0}(2-0)^k - \binom{2}{1}(2-1)^k = 2^k - 2.$$

This should be what you got in the earlier exercise. For $n = 3$ we get

$$\binom{3}{0}(3-0)^k - \binom{3}{1}(3-1)^k + \binom{3}{2}(3-2)^k = 3^k - 3 \cdot 2^k + 3.$$

12 Infinite sets

Note: This chapter is not in final form. In particular, it should be supplemented by the handout "Strange happenings at the Cantor hotel". As it stands, there is a barrage of abstraction and a shortage of intuitive discussion. Try to think through the theorems and their proofs informally in "strange happenings" style!

A set X is *infinite* if it is not finite. The first and most basic example of an infinite set is $\mathbb{N}$. This is another one of those cases where a proof seems superfluous; surely it is in the very nature of the natural numbers that they never end! Nevertheless, it's worth pondering this for a moment. Recall the child's question "what's the biggest number?", and the standard reply "there isn't a biggest number, because no matter how big n is, we can always find a bigger number $n+1$". Implicit in this reply is the following fact, which we take for granted (it is one of the Peano axioms for the natural numbers):

Fact: The function $S : \mathbb{N} \longrightarrow \mathbb{N}$ given by $S(n) = n + 1$ is injective, and $1 \notin Im\, S$.

The letter S is for "successor", the idea being—as we explained to the child—that every number n has a successor $n+1$. I think you'll agree that this fact is obvious: If $n+1 = m+1$, then $n = m$ (so S is injective), and if $n \geq 1$ then $n + 1 \geq 2$ (so $1 \notin Im\, S$). But we have no way to prove it; we simply take it for granted and use it to prove:

Proposition 12.1 *$\mathbb{N}$ is infinite.*

Proof: Recall that if A is a finite set, then every injective function $f : A \longrightarrow A$ is also surjective. By the fact above, there is an injective function $\mathbb{N} \longrightarrow \mathbb{N}$ that is not surjective. So $\mathbb{N}$ is not finite, i.e. is infinite.

Proposition 12.2 *If $A \subseteq B$ and A is infinite, then B is infinite.*

Proof: This is just the contrapositive of "if B is finite then A is finite"; the latter statement was proved in the previous chapter. QED.

So for example, we conclude that any set containing $\mathbb{N}$ is infinite; e.g. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are all infinite.

Proposition 12.3 *Suppose X and Y are sets, and there exists a bijection $X \longrightarrow Y$ (or equivalently, a bijection $Y \longrightarrow X$). Then X is infinite if and only if Y is infinite.*

Proof: The assertion is logically equivalent to "X is finite if and only if Y is finite" (check this!), which we already proved. QED.

Proposition 12.4 *A set X is infinite $\Leftrightarrow$ there is an injective function $f : \mathbb{N} \longrightarrow X \Leftrightarrow$ there is a surjective function $X \longrightarrow \mathbb{N}$.*

Proof: Suppose there is an injective function $f : \mathbb{N} \longrightarrow X$. By the previous proposition, $Im\, f$ is infinite (since any injective function defines a bijection onto its image). So X has an infinite subset and therefore is infinite.

Conversely, suppose X is infinite. We will define injective functions $f_n : [n] \longrightarrow X$ recursively. Choose any element $x_1 \in X$ and define $f(1) = x_1$. Now, having defined an injective function $f_n : [n] \longrightarrow X$, choose any element $x_{n+1} \notin Im\, f_n$. Such an element exists because otherwise f_n would be surjective, hence bijective, contradicting X infinite. Then set $f_{n+1}(n+1) = x_{n+1}$, and for $i \in [n]$ set $f_{n+1}(i) = f_n(i)$. Then f_{n+1} is injective by construction. Finally define $f : \mathbb{N} \longrightarrow X$ by $f(n) = f_n(n)$. To see that f is injective, suppose $f(m) = f(n)$, i.e. $f_m(m) = f_n(n)$. We can assume $m < n$. Then $f_n(m) = f_m(m)$ by definition, so $f_n(m) = f_n(n)$. Since f_n is injective, it follows that $m = n$. This completes the proof of the first biconditional.

The second biconditional follows from the injection/surjection trick.

Theorem 12.5 *A set X is infinite if and only if there is a function $g : X \longrightarrow X$ that is injective but not surjective.*

Proof: Suppose X is infinite. By the preceding proposition there is an injective function $f : \mathbb{N} \longrightarrow X$. Define g on the image of f by $g(f(n)) = f(n+1)$. For $x \notin Im\, f$, define $g(x) = x$. Then g is injective, but is not surjective because $f(1) \notin Im\, g$.

(It's easier to visualize this argument in informal terms. The function f sticks a copy of $\mathbb{N}$ inside X. On this copy of $\mathbb{N}$ we just "shift to the right", i.e. send n to $n+1$, while all other elements of X just sit there like bumps on a log, going nowhere.)

For the converse, we prove the contrapositive. This says that if X is finite, then every injective function $X \longrightarrow X$ is also surjective. Hey, we already proved this! Done.

The property "there exists a function $g : X \longrightarrow X$ that is injective but not surjective" is often taken as the *definition* of an infinite set. Whether we take it as a definition or a theorem, the nice thing about this property is that it depends only on X itself; it does not involve comparing X to other sets such as $\mathbb{N}$, $[n]$.

12.1 Countable sets

A set X is *countable* if either there is a bijection $\mathbb{N} \longrightarrow X$ (or equivalently, $X \longrightarrow \mathbb{N}$, or X is finite.

Caution. Some sources define "countable" to mean there is a bijection $\mathbb{N} \longrightarrow X$, and exclude finite sets from the definition.

Examples. 1. $\mathbb{N}$ is countable (use the identity function).

2. $\mathbb{N}_{ev}$ is countable, since $n \mapsto 2n$ defines a bijection $\mathbb{N} \longrightarrow \mathbb{N}_{ev}$. Similarly, $\mathbb{N}_{odd}$ is countable.

3. $\mathbb{N}_0$ is countable: Define $f : \mathbb{N} \longrightarrow \mathbb{N}_0$ by $f(n) = n - 1$. Then f is bijective (with inverse $g(n) = n + 1$).

4. $\mathbb{Z}$ is countable: Define a bijection $f : \mathbb{Z} \longrightarrow \mathbb{N}$ as follows. If $n > 0$, $f(n) = 2n$. If $n < 0$, $f(n) = -2n + 1$. And finally $f(0) = 1$. I leave it to you to check this is a bijection. (Positive

integers go bijectively to the even natural numbers and negative integers go bijectively to odd natural numbers ≥ 3, leaving room for poor little zero to go to 1!)

Note. If every set was countable, this would be a silly definition. In the next section, however, we'll see that the real numbers are uncountable.

Proposition 12.6 *Suppose there exists a bijection $f : X \longrightarrow Y$. Then X is countable if and only if Y is countable.*

Proof: Exercise.

Proposition 12.7 *Every subset of a countable set is countable.*

Proof: Let X be a countable set. If X is finite, then every subset of X is finite and hence countable. If X is infinite, choose a bijection $f : X \longrightarrow \mathbb{N}$. If $A \subseteq X$ then f maps A bijectively onto a subset of $\mathbb{N}$, so in view of the preceding proposition, we may as well assume $X = \mathbb{N}$. If A is finite then A is countable.

This brings us to the key case: A is an infinite subset of $\mathbb{N}$. Define a bijection $h : \mathbb{N} \longrightarrow A$ recursively as follows: By the well-ordering theorem, A has a minimal element a_1, and we set $h(1) = a_1$. Now let a_2 be the minimal element of $A - \{a_1\}$ and set $h(2) = a_2$. In general, having defined $h(n)$ we then define $h(n+1)$ to be the minimal element of $A - \{h(i) : i \leq n\}$. Note that since A is infinite, this latter set is nonempty and so has a minimal element by the well-ordering theorem.

Thus we obtain a function $h : \mathbb{N} \longrightarrow A$ with the properties (i) $\forall n \in \mathbb{N}$, $h(n) < h(n+1)$, and (ii) $\forall n \in \mathbb{N}$, there are no elements of A with $h(n) < a < h(n+1)$. Property (i) implies h is injective. Property (ii) implies h is surjective, for the following reason: Given $a \in A$, let n be maximal such that $h(n) \leq a$. If $h(n) < a$ then $h(n+1) > a$, contradicting (ii). So $h(n) = a$, QED.

Corollary 12.8 *If X is countable and there is an injection $f : A \longrightarrow X$, then A is countable.*

Proof: The image of f is countable by the proposition. Since f defines a bijection of A onto its image, A is countable.

The next result is useful because it avoids having to consider the infinite and finite cases of countability separately.

Proposition 12.9 *Suppose X is nonempty. Then X is countable if and only if there is a surjection $\mathbb{N} \longrightarrow X$.*

Proof: Suppose X is countable. If X is infinite, then by definition there is a bijection $\mathbb{N} \longrightarrow X$, whichis in particular a surjection. If X is finite, then there is an injection $X \longrightarrow \mathbb{N}$, and since X is nonempty the injection/surjection trick shows that there is a surjection $\mathbb{N} \longrightarrow X$.

Conversely, suppose there is a surjection $f : \mathbb{N} \longrightarrow X$. By the injection/surjection trick, there is an injection $g : X \longrightarrow \mathbb{N}$. Hence X is countable by Corollary 12.8.

We now come to a key theorem. It has several different, interesting proofs.

Theorem 12.10 $\mathbb{N} \times \mathbb{N}$ *is countable.*

Proof: I leave it as a very important and enlightening exercise to prove this in two different ways, as follows:

First proof: In an earlier exercise, we showed that every $n \in \mathbb{N}$ can be written uniquely in the form $n = s2^m$ with s odd and $m \geq 0$. Use this fact to construct an explicit bijection $\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$.

Second proof: Partition $\mathbb{N} \times \mathbb{N}$ into the finite sets $A_c = \{(m, n) \in \mathbb{N} \times \mathbb{N} : m + n = c\}$. Here $c \geq 2$; note also that $|A_c| = c - 1$. (Draw the picture in the first quadrant; these are the positive integer points intersected with the various lines of slope -1.) Make use of this partition to define a bijection $\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$. (One way involves working out an explicit formula. An easier way leaves the formula implicit but still rigorously yields a bijection.)

Other proofs are possible too, including no doubt some I haven't even thought of!

Corollary 12.11 *Every countable union of countable sets is countable.*

Proof: Suppose we are given a countable collection of sets $A_1, A_2, ...$, each of which is itself countable, and let $A = \cup_{i=1}^{\infty} A_i$. Choose surjections $f_k : \mathbb{N} \longrightarrow A_k$. Then define $f : \mathbb{N} \times \mathbb{N} \longrightarrow A$ by $f(n, k) = f_k(n)$. In other words, on the k-th horizontal slice of $\mathbb{N} \times \mathbb{N}$ (draw/visualize the picture!) we define $f = f_k$. Then f is surjective. Since $\mathbb{N} \times \mathbb{N}$ is countable, it follows that A is countable too, as desired. QED.

Since finite sets are countable, we immediately get as special cases of the corollary:

Corollary 12.12 *a) Every finite union of countable sets is countable.*
b) Every countable union of finite sets is countable.

Proposition 12.13 *Suppose $A_1, ..., A_n$ are countable sets. Then the product $A_1 \times A_2 \times ... \times A_n$ is countable.*

Proof: We use induction on n, using a particular strategy we've seen before: The base case $n = 1$ is trivial. But before proceding to the inductive step, we first digress to prove the case $n = 2$. So suppose A, B are countable sets; we want to show $A \times B$ is countable. It's worth explaining two different ways to do this:

First way: Since A and B are countable, there are surjections $f : \mathbb{N} \longrightarrow A$ and $g : \mathbb{N} \longrightarrow B$. Then $f \times g : \mathbb{N} \times \mathbb{N} \longrightarrow A \times B$ is surjective, and since $\mathbb{N} \times \mathbb{N}$ is countable, so is $A \times B$. ($f \times g$ is the function $(f \times g)(m, n) = (f(m), g(n))$.)

Second way: For each $b \in B$, let S_b denote the "horizontal" slice $A \times \{b\} \subset A \times B$. Each slice is countable since it is in bijective correspondence with A, and since B is countable there are countably many slices. Hence $A \times B$ is a countable union of countable sets, and so is countable.

Now we come back to the inductive step of the proof. We assume (inductive hypothesis) that a product of n countable sets is countable, and wish to show that a product of $n+1$ countable sets A_i is countable. Let $A = A_1 \times ... \times A_n$ and let $B = A_{n+1}$. Then $A_1 \times ... \times A_{n+1} = A \times B$. Since A is countable by inductive hypothesis, and B is countable by assumption, we're done by the $n = 2$ case already proved.

Theorem 12.14 *The set of rational numbers $\mathbb{Q}$ is countable.*

If one encountered this theorem without any preliminaries, it would probably seem rather surprising. But we already know that $\mathbb{N} \times \mathbb{N}$ is countable, which makes the above theorem very plausible: After all, the positive rational numbers are represented by pairs of natural numbers (m, n), so this ought to be enough to prove the theorem. And indeed it is, but let's do it carefully.
Proof: The function $h : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{Q}_{>0}$ given by $h(m, n) = \frac{m}{n}$ is surjective, by the definition of rational numbers. Since $\mathbb{N} \times \mathbb{N}$ is countable, so is $\mathbb{Q}_{>0}$. The function $\mathbb{Q}_{>0} \longrightarrow \mathbb{Q}_{<0}$ given by $f(x) = -x$ is bijective, so $\mathbb{Q}_{<0}$ is countable. Then

$$\mathbb{Q} = \mathbb{Q}_{>0} \cup \mathbb{Q}_{<0} \cup \{0\}$$

is a finite union of countable sets and so is countable.

12.2 Exercises

1. Show that the set of all finite subsets of a countable set is countable. (Apply suitable results from above to keep this short; don't try to do it directly.)

2. Let $f : X \longrightarrow Y$ be a surjective function. We showed that if X is countable, then so is Y. Later we'll show that the converse is false. But at least the following holds: Suppose Y is countable, and in addition assume that all the fibers $f^{-1}y$ are countable. Show that X is countable. (Look for a short and simple proof based on applying suitable theorems.)

3. Give two proofs of Theorem 12.10, as suggested there.

4. In this problem you'll prove a surprising characterization of finite sets. It is in the spirit of Theorem 12.5, in the sense that it only involves the set itself and not comparisons with other sets. Suppose X is a set and $f : X \longrightarrow X$ a function. A subset $A \subset X$ is said to be *f-invariant* if $f(A) \subseteq A$; in other words, $a \in A \Rightarrow f(a) \in A$. Note that the empty set and the entire set X are automatically f -invariant. So the interesting case is when A is a proper nonempty subset of X.

For example, suppose $X = \mathbb{N}$ and $f : \mathbb{N} \longrightarrow \mathbb{N}$ is given by $f(n) = 2n$. Then the subset of even numbers is f-invariant but the subset of odd numbers is not. Or consider the subsets $A = \{n \in \mathbb{N} : n \leq 100\}$ and $B = \{n \in \mathbb{N} : n \geq 100\}$. Then B is f-invariant, but A is not.

Now, here's the theorem you're going to prove:

Theorem 12.15 *Let X be a set. Then X is finite if and only if there exists a function $f : X \longrightarrow X$ with no proper nonempty f-invariant subsets.*

Use the following outline:

(I). Suppose X is finite. We must produce an f with no proper nonempty f-invariant subsets.

Case 1 (a silly case, but it must be considered): $|X| \leq 1$. If X has one element then there is a trivial reason f exists; do you see why? The case of the empty set is peculiar and can be omitted if it doesn't make sense to you; you have to go back to the rigorous definition of a function to see that there is a unique function from the empty set to itself, namely the empty function. (Weird, I know...)

Case 2 (the interesting part): $|X| \geq 2$. If $|X| = n$, we can list the elements of X as $x_1, ..., x_n$. Now construct a suitable f explicitly, and prove it has the desired property. (Imagine n people seated at a circular table. What are some easy ways to permute them? Play a bit of "musical chairs"!)

(II). Now suppose there is a function $f : X \longrightarrow X$ with no proper nonempty invariant subsets. We must show X is finite. At first glance this is very mysterious. Try the following steps:

1. X can't be the empty set, so we can choose an element $x_0 \in X$. Define a sequence of elements of X recursively by $x_1 = f(x_0)$, $x_2 = f(x_1)$, and in general $x_{n+1} = f(x_n)$. In other words, x_n is obtained from x_0 by iterating f n times. Let A denote the subset consisting of all the x_n's. Then in fact $A = X$; why? Prove this.

2. By step 1 we know that $X = \{x_0, x_1, x_2, ...\}$. I claim that there exists $n \in \mathbb{N}$ such that $x_n = x_0$. In other words, if we iterate f enough times we eventually get back to x_0. Why? Prove this.

3. Choose n as in Step 2. Then $X = \{x_0, x_1, x_2, ..., x_{n-1}\}$ and therefore is finite, QED!! Prove this.

12.3 Uncountable sets

The German mathematician Georg Cantor (1845-1918) made a remarkable discovery: some infinities are bigger than others. At the time, his theory was controversial not only among mathematicians but even philosophers and theologians (see the Wikipedia article on Cantor, for example). Nowadays, however, Cantor's set theory is completely standard. However, the statement "some infinities are bigger than others" is hopelessly vague, indeed meaningless, as it stands. We'll come back to this point later; for now, our goal is to show that there exist sets that are uncountable, where "uncountable" means "not countable". In other words, there exist infinite sets X such that there is no surjection $\mathbb{N} \longrightarrow X$ (or equivalently, no injection $X \longrightarrow \mathbb{N}$). Notice that since X is infinite, we can always find a surjection $X \longrightarrow \mathbb{N}$ (and in injection $\mathbb{N} \longrightarrow X$) by Proposition 12.4. This gives a precise meaning to the statement that X is a "bigger infinity" than $\mathbb{N}$.

We are going to show the following sets are all uncountable:

- the set of all subsets of $\mathbb{N}$
- the set of all functions from $\mathbb{N}$ to $\{0, 1\}$ (in other words, infinite sequences of 0's and 1's)
- the set of real numbers

The set of real numbers is by far the most familiar of the three, but we'll consider the other two first, for several reasons. First of all, the proofs in the other two cases are much simpler than the proof for the real numbers. Second, the proof for infinite sequences of 0's and 1's is via Cantor's famous "diagonal argument", which is also used for the real numbers but is more complicated in the latter case. Doing it with sequences of 0's and 1's provides a good warmup. And third, we haven't even given a rigorous definition of the real number system yet. We'll be on shaky ground when we claim to give a rigorous proof concerning a set we haven't even rigorously defined! The first two sets have completely unambiguous, rigorous definitions already. If you want to see how it works for the real numbers first—at least to get the general idea—see the handout "Strange happenings at the Cantor hotel".

So let's start with the set $\mathcal{P}(\mathbb{N})$ of all subsets of $\mathbb{N}$. Although extremely large, it's a perfectly reasonable, concrete sort of set that we work with all the time. Among its vast variety of subsets I will list the following: the even numbers, the odd numbers, the primes, the perfect squares, $\{n \in \mathbb{N} : n > 7\}$, the finite sets $[n]$, the singletons $\{n\}$, the empty set, the entire set. Earlier we showed that the set of all *finite* subsets of $\mathbb{N}$ is countable. But:

Theorem 12.16 *$\mathcal{P}(\mathbb{N})$ is uncountable.*

Proof: The proof is stunningly simple, yet hard to get your head around at first. We'll do it by contradiction. Suppose $\mathcal{P}(\mathbb{N})$ is countable. Then there is a surjective function $f : \mathbb{N} \longrightarrow \mathcal{P}(\mathbb{N})$. Define a subset $A \subseteq \mathbb{N}$ by

$$A = \{n \in \mathbb{N} : n \notin f(n)\}.$$

In plain English, A is the set of those n such that n is not an element of the n-th subset of the list. Therefore $A \neq f(n)$, since n is in A but not in $f(n)$. Since this is true for all n, A is not in the image of f. This contradicts the assumption that f was surjective. QED!!

We now turn to our second example of an uncountable set. Let $F(\mathbb{N}, \{0,1\})$ denote the set of all functions $\mathbb{N} \longrightarrow \{0,1\}$. In other words, it's the set of all sequences whose entries are all 0 or 1, e.g. 11000101000000001110011..... and so on.

Theorem 12.17 *$F(\mathbb{N}, \{0,1\})$ is uncountable.*

Proof: Again we suppose given a surjection $f : \mathbb{N} \longrightarrow F(\mathbb{N}, \{0,1\})$, and derive a contradiction. Each $f(n)$ is a sequence of 0's and 1's, so let's write it as

$$f(n) = a_{n1}a_{n2}a_{n3}...$$

where each a_{ni} is 0 or 1. It may help to visualize this as a "matrix" of infinite size:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & ... \\ a_{21} & a_{22} & a_{23} & a_{24} & ... \\ a_{31} & a_{32} & a_{33} & a_{34} & ... \\ a_{41} & a_{42} & a_{43} & a_{44} & ... \\ ... & ... & ... & ... & ... \end{pmatrix}$$

The dots ... indicate that the matrix continues infinitely down and to the right. I now call your attention to the "diagonal" entries a_{nn}, so named for the evident visual reason; a_{nn} is the n-th entry of the n-th sequence on the list. Define a new sequence $b_1, b_2, ...$ by

$$b_n = \begin{cases} 0 & \text{if } a_{nn} = 1 \\ 1 & \text{if } a_{nn} = 0 \end{cases}$$

This sequence is not on the list, i.e. is not in the image of f, because it differs from f_n in the n-th place. This contradicts the assumption that f was surjective, QED again!

Cantor's most shocking (to some people) revelation was that the set of real numbers is uncountable. Given the subtlety of the concept "uncountable", it would be absurd to attempt a proof of this fact without a precise definition of $\mathbb{R}$, or at least a precise axiomatic description of it. The usual proof proceeds via decimal expansions. But this just brings us back to the same problem: We can hardly talk about the decimal expansion of a real number if we haven't defined "real number". A definition will be given later, but I don't want to make it a prerequisite for understanding Cantor's beautiful idea. We'll assume the decimal expansion concept, but if we're going to do so we should at least be precise about what we're assuming. Moreover it seems silly to use decimal expansions, since these are based on the arbitrary choice of base 10 and involve needlessly many digits. We are in the Computer Age, after all; why not use base 2? We will use binary expansions instead, so that all digits are either 0 or 1. A digression is in order to make precise what this means. (If you want to see how the argument goes with base 10 expansions, see "Strange happenings at the Cantor hotel".)

12.3.1 Digression on binary expansion of real numbers

Earlier we defined the binary expansion of a natural number. At the opposite extreme we now define "binary expansion" of a real number between 0 and 1, assuming for the moment that we know what a real number is. We first consider finite binary expansion. Suppose given a finite sequence $a_1, ..., a_n$ of 0's and 1's. We then define

$$.a_1a_2 \cdots a_n = \frac{a_1}{2} + \frac{a_2}{4} + ...\frac{a_n}{2^n}.$$

or in summation notation

$$\sum_{i=1}^{n} a_i 2^{-i}.$$

Note this is exactly analogous to decimal expansion. In a decimal expansion we put non-negative powers of 10 to the left of the decimal point, and negative powers to the right. Here we're just doing the same thing, but with 2 in place of 10. For example in binary

$$.11 = \frac{1}{2} + \frac{1}{4} = \frac{3}{4}$$

$$.01011 = \frac{1}{4} + \frac{1}{16} + \frac{1}{32} = \frac{11}{32}$$

and so on. Note that a number given by such a finite binary expansion is a sum of rational numbers, and therefore is rational.

As with decimal expansions (even though you've probably never done this rigorously), one can go further and make sense of *infinite* binary expansions. Symbolically we write

$$.a_1a_2a_3 \cdot \cdot \cdot = \sum_{i=1}^{\infty} a_i 2^{-i},$$

bearing in mind that we haven't yet defined the infinite sum on the right; for the moment we just assume that it "converges" in some suitable sense to a real number. Once this is made precise, one can show that every such binary expansion defines a real number x with $0 \leq x \leq 1$, and conversely every real number x with $0 \leq x \leq 1$ has a binary expansion. There is one minor complication, however, namely that the binary expansion isn't necessarily unique. If you are familiar with convergent geometric series, this is easy to see. For example the number 1 can be written either as 1.0 or as

$$0.1111111 \cdot \cdot \cdot \cdot = \sum_{i=1}^{\infty} \frac{1}{2^i} = 1.$$

Indeed this example goes back more than 2000 years, to Zeno's Paradox: Achilles is trying to run a mile, but he never gets there. The trouble is that first he has to run to the half-way point, or .1 in binary. From there he again has to run half the distance to the mile marker, at which point he's gone .11 miles in binary. Continuing in this way, he has to run to the .111 marker, the .1111 and so on. It never ends! The mathematical resolution of this "paradox" lies in the theory of convergent series. At any rate, it makes it reasonable to say

that the infinite sum above is equal to 1. In decimal notation, the analogous statement is $.99999 \cdot \cdot \cdot = 1$, where every digit on the left is a 9.

This brings us to a final technical point: neither binary expansions nor decimal expansions are unique. For example in binary .1111.... = 1.0, and similarly in decimal .9999... = 1.0. This phenomenon propagates in the following way: Observe that inserting a 0 after the binary point is the same thing as multiplying by 1/2: .11 = 3/4, .011 = 3/8 and so on. It follows that .011111... (all 1's at the end) is equal to .10000... (all zeros). Similarly .001111.... = .01000... and so on. From this it follows for example that in binary .101011111... (all 1's) is equal to .10110000... (all zeros). For a decimal example, .4999999... (all 9's) is equal to .50000... (all zeros).

To get a unique binary (or decimal) expansion, we make the following definition: A sequences of binary digits $.a_1a_2...$ *ends in all 1's* if $\exists n \in bn$ such that $\forall k \geq n$, $a_k = 1$. (The analogous concept in decimal would be "ends in all 9's"). We let $F_0(\mathbb{N}, \{0,1\})$ denote the subset of $F(\mathbb{N}, \{0,1\})$ consisting of all sequences that *do not* end in all 1's.

Lemma 12.18 $F_0(\mathbb{N}, \{0,1\})$ *is uncountable.*

Proof: To make the notation easier on the brain, in the proof we'll use the abbreviations $A = F(\mathbb{N}, \{0,1\})$, $B = F_0(\mathbb{N}, \{0,1\})$ and $C =$ the complement of B. Thus $A = B \cup C$, and C is the set of sequences ending in all 1's. We'll show that C is countable. This implies B is uncountable, since otherwise A would be the union of two countable sets, hence countable, contradicting Theorem 12.17.

To see that C is countable, let $C_n = \{(a_1, a_2, ...) : a_k = 1 \, \forall k \geq n\}$ (the sequences that are all 1's from the n-th place on). Then C_n is a finite set, and indeed has cardinality 2^{n-1} (there are 2^{n-1} possibilities for the first $n-1$ entries). By definition, C is the union of the C_n's. Thus C is the union of a countable number of finite sets, and so is countable. QED.

Finally, here is what we need to assume about the real numbers, where the notation $[0,1)$ means $\{x \in \mathbb{R} : 0 \leq x < 1\}$.

Theorem 12.19 *There is a bijection* $F_0(\mathbb{N}, \{0,1\}) \longrightarrow [0,1)$*, given by sending a sequence* $a_1a_2...$ *to* $.a_1a_2....$

This ends our digression on binary expansion.

12.4 The real numbers are uncountable!

We now have all the ingredients for a proof of Cantor's remarkable result:

Theorem 12.20 $\mathbb{R}$ *is uncountable.*

Proof: Any subset of a countable set is countable, so by taking the contrapositive we conclude that if a set X has an uncountable subset A, then X is uncountable. In the present case we take $X = \mathbb{R}$ and $A = [0,1)$; it then suffices to show that $[0,1)$ is uncountable. But $F_0(\mathbb{N}, \{0,1\})$ is uncountable by Lemma , so $[0,1)$ is uncountable by Theorem 12.19!

Now we can finally make precise the claim that "there are more irrational numbers than rational numbers".

Corollary 12.21 *The set of irrational numbers is uncountable.*

Proof: By contradiction. Suppose the set of irrational numbers is countable. We know that the rationals are countable, so then $\mathbb{R}$ would be the union of two countable sets and hence countable, contradicting the theorem.

12.5 Bigger and bigger infinities

Let X be any set. I claim that $\mathcal{P}(X)$, the set of all subsets of X, is always "bigger" than X, in the following precise sense:

Theorem 12.22 *There is an injection $X \longrightarrow \mathcal{P}(X)$, but there is no injection $\mathcal{P}(X) \longrightarrow X$.*

Proof: I leave it as an exercise to prove that there is an injection $X \longrightarrow \mathcal{P}(X)$. To show that there is no injection $\mathcal{P}(X) \longrightarrow X$, by the injection/surjection trick it is equivalent to show that there is no surjection $X \longrightarrow \mathcal{P}(X)$. In Theorem 12.16, we proved this for $X = \mathbb{N}$. But if you look closely at the proof there, you'll see that we never used anything about $\mathbb{N}$; the same proof goes through verbatim for *any* set X! QED.

12.6 Transcendental numbers

What kinds of irrational numbers are out there? We've shown, for example, that if $n \in \mathbb{N}$ is not a perfect k-th power, then $\sqrt[k]{n}$ is irrational. We also showed that certain cubic polynomials have an irrational real root. The method we used extends to higher degree polynomials as well.

Theorem 12.23 *a) Let $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ be a polynomial of degree n with integer coefficients a_i (note we are assuming the coefficient a_n of x^n is 1). If c is a rational root of f, then c is an integer that divides the constant term a_0.*

b) If f as above has odd degree, and for all divisors d (including negative divisors) of a_0 we have $f(d) \neq 0$, then f has an irrational root.

Proof: a) In an exercise we showed that rational roots of such an f have to be integers. So let c be an integer root. Then $f(c) = 0$ so $c^n + a_{n-1}c^{n-1} + ... + a_1c = -a_0$, and it follows that $c|a_0$ as claimed.

b) In an exercise we showed that any odd degree polynomial with real coefficients has a real root. (Well, we didn't really prove it from scratch. We had to assume without proof the Intermediate Value Theorem and facts from calculus.) So the f considered here has a real root α, and I claim α is irrational: If α is rational then it has to be an integer d dividing a_0, hence is not a root by assumption.

Using this theorem, we can find many examples of polynomials with irrational roots. For example, for f as in part (b), suppose $a_0 = 1$. Then the only possible rational roots of f are ± 1, and we can check whether 1 or -1 is a root by plugging it in. For example—just to

show that we can even find polynomials of arbitrarily high degree with this property—let n be any odd number ≥ 3 and consider $f(x) = x^n + x^{n-1} + 1$. Neither 1 nor -1 is a root, so by the above method we conclude that f has an irrational root.

The point of this discussion was to show that there we can produce lots of irrational numbers as roots of polynomials with integer coefficients. This raises the question: Are *all* irrational numbers of this type? To make the question precise, we'll make the following definitions:

Definition. 1. A real number α is *algebraic* if there is a polynomial $f(x)$ with rational coefficients such that α is a root of f.

2. A real number α is *transcendental* if it is not algebraic.

Notice that it wouldn't change the definition if we replaced "rational coefficients" by "integer coefficients". For suppose $f(x)$ has rational coefficients and $f(\alpha) = 0$. Let $a_i = m_i/n_i$ be the coefficients of f, where $m_i, n_i \in \mathbb{Z}$. Let n denote the product of all the denominators n_i. Then $g(x) = nf(x)$ is a polynomial with integer coefficients, and $g(\alpha) = 0$.

With this definition, the question is: Do transcendental numbers exist?

We will show the answer is yes, by a very surprising method of proof. We will show that transcendental numbers exist by showing that in fact the set of all transcendental numbers is uncountable. Moreover we will do this without constructing a single specific example of a transcendental number!

Here is the key result:

Theorem 12.24 *The set $\mathbb{A}$ of algebraic numbers is countable.*

Proof: Step 1. Let P_n denote the set of polynomials with rational coefficients and of degree $\leq n$. Then P_n is countable.

Consider a typical element of P_n, namely a polynomial $f(x) = a_0 + a_1x + ... + a_nx^n$, where the a_i's are rational numbers. Such a polynomial is uniquely determined by its coefficients, and there are no restrictions on which rational numbers can occur. In other words, there is a bijection $\phi : P_n \longrightarrow \mathbb{Q}^{n+1}$ given by $\phi(f) = (a_0, a_1, ..., a_n)$. Since $\mathbb{Q}$ is countable, and any product of countable sets is countable, it follows that P_n is countable. This completes the proof of Step 1.

Step 2. Let P denote the set of all polynomials with rational coefficients. Then P is countable.

P is the union of all the P_n's. So by step 1 it is a countable union of countable sets, hence is countable.

Step 3. $\mathbb{A}$ is countable.

We know that each $f \in P$ has finitely many roots, and $\mathbb{A}$ is by definition the union of all such roots for all such f. Hence $\mathbb{A}$ is a countable union of finite sets, and so is countable.

Corollary 12.25 *The set of transcendental numbers is uncountable. In particular, transcendental numbers exist.*

Proof: By definition, the set $\mathbb{R}$ is the union of the algebraic and transcendental numbers. If the transcendental numbers were countable, then since a union of two countable sets is countable, we would conclude from the theorem that $\mathbb{R}$ is countable—contradiction!

Thus not only do transcendental numbers exist, but in a sense, "most" numbers are transcendental. Paradoxically, it is very difficult to produce explicit examples of transcendentals. For example, e and π are known to be transcendental, but the proof is extremely difficult and well beyond the scope of these notes.

12.7 Exercises

1. Show that for any set X, there is a bijection $\phi : F(X, \{0,1\}) \longrightarrow \mathcal{P}(X)$. Here $F(X, \{0,1\})$ denotes the set of all functions from X to $\{0,1\}$.

Hint. Define $\phi(f) = f^{-1}0$. In other words, we map the function f to its fiber over 0.

By taking $X = \mathbb{N}$, we see that $F(\mathbb{N}, \{0,1\}$ is uncountable if and only if $\mathcal{P}(\mathbb{N})$ is uncountable. Hence Theorem 12.16 and Theorem 12.17 are equivalent.

2. Let X be any set. Show that there is an injection $X \longrightarrow \mathcal{P}(X)$.

3. a) We showed that $[0,1)$ is uncountable. It follows immediately that $(0,1)$ is uncountable; why?

b) Let $a, b \in \mathbb{R}$ with $a < b$. Show that (a,b) is uncountable by constructing an explicit bijection $(0,1) \longrightarrow (a,b)$ and applying part (a).