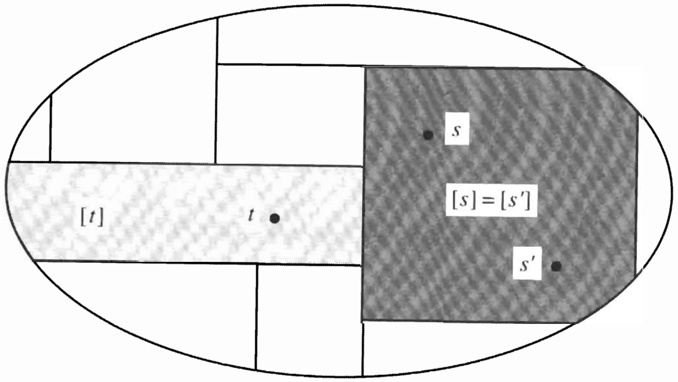

Figure 2 Equivalence classes and representatives.

framework." A picture may be vital in getting you to believe a statement. An analogy with something you know to be true may help you understand it. An authoritative teacher may force you to parrot it. A formal proof, however, is the ultimate and only reason to accept a mathematical statement as true. A recent debate in Berkeley focused the issue for me. According to a math teacher from one of our local private high schools, his students found proofs in mathematics were of little value, especially compared to "convincing arguments." Besides, the mathematical statements were often seen as obviously true and in no need of formal proof anyway. I offer you a paraphrase of Bob Osserman's response.

> But a convincing argument is not a proof. A mathematician generally wants both, and certainly would be less likely to accept a convincing argument by itself than a formal proof by itself. Least of all would a mathematician accept the proposal that we should generally replace proofs with convincing arguments.
>
> There has been a tendency in recent years to take the notion of proof down from its pedestal. Critics point out that standards of rigor change from century to century. New gray areas appear all the time. Is a proof by computer an acceptable proof? Is a proof that is spread over many journals and thousands of pages, that is too long for any one person to master, a proof? And of course, venerable Euclid is full of flaws, some filled in by Hilbert, others possibly still lurking.

> Clearly it is worth examining closely and critically the most basic notion of mathematics, that of proof. On the other hand, it is important to bear in mind that all distinctions and niceties about what precisely constitutes a proof are mere quibbles compared to the enormous gap between any generally accepted version of a proof and the notion of a convincing argument. Compare Euclid, with all his flaws to the most eminent of the ancient exponents of the convincing argument — Aristotle. Much of Aristotle's reasoning was brilliant, and he certainly convinced most thoughtful people for over a thousand years. In some cases his analyses were exactly right, but in others, such as heavy objects falling faster than light ones, they turned out to be totally wrong. In contrast, there is not to my knowledge a single theorem stated in Euclid's *Elements* that in the course of two thousand years turned out to be false. That is quite an astonishing record, and an extraordinary validation of proof over convincing argument.

Here are some guidelines for writing a rigorous mathematical proof. See also Exercise 0.

1. Name each object that appears in your proof. (For instance, you might begin your proof with a phrase, "consider a set X, and elements x, y that belong to X," etc.)
2. Draw a diagram that captures how these objects relate, and extract logical statements from it. Quantifiers precede the objects quantified; see below.
3. Proceed step-by-step, each step depending on the hypotheses, previously proved theorems, or previous steps in your proof.
4. Check for "rigor": all cases have been considered, all details have been tied down, and circular reasoning has been avoided.
5. Before you sign off on the proof, check for counter-examples and any implicit assumptions you made that could invalidate your reasoning.

Logic

Among the most frequently used logical symbols in math are the quantifiers $\forall$ and $\exists$. Read them always as "for each" and "there exists." Avoid reading $\forall$ as "for all," which in English has a more inclusive connotation. Another common symbol is $\Rightarrow$. Read it as "implies."

The rules of correct mathematical grammar are simple: quantifiers appear at the beginning of a sentence, they modify only what follows them in the sentence, and assertions occur at the end of the sentence. Here is an example.

(1) *For each integer n there is a prime number p which is greater than n.*

In symbols the sentence reads

$$\forall n \in \mathbb{Z} \quad \exists p \in P \quad \text{such that} \quad p > n,$$

where P denotes the set of prime numbers. (A **prime number** is a whole number greater than 1 whose only divisors in $\mathbb{N}$ are itself and 1.) In English, the same idea can be re-expressed as

(2) *Every integer is less than some prime number*

or

(3) *A prime number can always be found which is greater than any given integer.*

These sentences are correct in English grammar, but disastrously WRONG when transcribed directly into mathematical grammar. They translate into disgusting mathematical gibberish:

(WRONG 2) $\forall n \in \mathbb{Z} \quad n < p \quad \exists p \in P$

(WRONG 3) $\exists p \in P \quad p > n \quad \forall n \in \mathbb{Z}.$

Moral Quantifiers first and assertions last. In stating a theorem, try to apply the same principle. Write the hypothesis first and the conclusion second. See Exercise 0.

The order in which quantifiers appear is also important. Contrast the next two sentences in which we switch the position of two quantified phrases.

(4) $(\forall n \in \mathbb{N}) \quad (\forall m \in \mathbb{N}) \quad (\exists p \in P) \quad \text{such that} \quad (nm < p).$

(5) $(\forall n \in \mathbb{N}) \quad (\exists p \in P) \quad \text{such that} \quad (\forall m \in \mathbb{N}) \quad (nm < p).$

(4) is a true statement but (5) is false. A quantifier modifies the part of a sentence that follows it but not the part that precedes it. This is another reason never to end with a quantifier.

Moral Quantifier order is crucial.

There is a point at which English and mathematical meaning diverge. It concerns the word "or." In mathematics "a or b" always means "a or b or both a and b," while in English it can mean "a or b but not both a and b." For example, Patrick Henry certainly would not have accepted both liberty and death in response to his cry of "Give me liberty or give me death." In mathematics, however, the sentence "17 is a prime or 23 is a prime" is correct even though both 17 and 23 are prime. Similarly, in mathematics $a \Rightarrow b$ means that if a is true then b is true but that b might also be true for reasons entirely unrelated to the truth of a. In English, $a \Rightarrow b$ is often confused with $b \Rightarrow a$.

Moral In mathematics, "or" is inclusive. It means *and/or*. In mathematics, $a \Rightarrow b$ is not the same as $b \Rightarrow a$.

It is often useful to form the negation or logical opposite of a mathematical sentence. The symbol $\sim$ is usually used for negation, despite the fact that the same symbol also indicates an equivalence relation. Mathematicians refer to this as an **abuse of notation**. Fighting a losing battle against abuse of notation, we write $\neg$ for negation. For example, if $m, n \in \mathbb{N}$ then $\neg(m < n)$ means it is not true that m is less than n. In other words

$$\neg(m < n) \quad \equiv \quad m \geq n.$$

(We use the symbol $\equiv$ to indicate that the two statements are equivalent.) Similarly, $\neg(x \in A)$ means it is not true that x belongs to A. In other words,

$$\neg(x \in A) \quad \equiv \quad x \notin A.$$

Double negation returns a statement to its original meaning. Slightly more interesting is the negation of "and" and "or." Just for now, let us use the symbols & for "and" and $\vee$ for "or." We claim

(6) $$\neg(a \,\&\, b) \quad \equiv \quad \neg a \vee \neg b.$$

(7) $$\neg(a \vee b) \quad \equiv \quad \neg a \,\&\, \neg b.$$

For if it is not the case that both a and b are true then at least one must be false. This proves (6), and (7) is similar. Implication also has such interpretations:

(8) $$a \Rightarrow b \quad \equiv \quad \neg a \Leftarrow \neg b \quad \equiv \quad \neg a \vee b.$$

$$(9) \qquad \neg(a \Rightarrow b) \quad \equiv \quad a \,\&\, \neg b.$$

What about the negation of a quantified sentence such as

$$\neg(\forall n \in \mathbb{N}, \exists p \in P \text{ such that } n < p).$$

The rule is: change each $\forall$ to $\exists$ and vice versa, leaving the order the same, and negate the assertion. In this case the negation is

$$\exists n \in \mathbb{N}, \quad \forall p \in P, \quad n \geq p.$$

In English it reads "There exists a natural number n, and for all primes p, $n \geq p$." The sentence has correct mathematical grammar but of course is false. To help translate from mathematics to readable English, a comma can be read as "and" or "such that."

All mathematical assertions take an implication form $a \Rightarrow b$. The hypothesis is a and the conclusion is b. If you are asked to prove $a \Rightarrow b$, there are several ways to proceed. First you may just see right away why a does imply b. Fine, if you are so lucky. Or you may be puzzled. Does a really imply b? Two routes are open to you. You may view the implication in its equivalent contrapositive form $\neg a \Leftarrow \neg b$ as in (8). Sometimes this will make things clearer. Or you may explore the possibility that a fails to imply b. If you can somehow deduce from the failure of a implying b a contradiction to a known fact (for instance if you can deduce the existence of a planar right triangle with legs x, y but $x^2 + y^2 \neq h^2$ where h is the hypotenuse) then you have succeeded in making an **argument by contradiction**. Clearly (9) is pertinent here. It tells you what it means that a fails to imply b, namely that a is true and, simultaneously, b is false.

Euclid's proof that $\mathbb{N}$ contains infinitely many prime numbers, is a classic example of this method. The hypothesis is that $\mathbb{N}$ is the set of natural numbers and that P is the set of prime numbers. The conclusion is that P is an infinite set. The proof of this fact begins with the phrase "Suppose not." It means: suppose, after all, that the set of prime numbers P is merely a finite set, and see where this leads you. It does not mean that we think P really is a finite set, and it is not a hypothesis of a theorem. Rather it just means that we will try to find out what awful consequences would follow from P being finite. In fact if P were[†] finite then it would consist of m numbers $p_1, \dots, p_m$. Their product $N = 2 \cdot 3 \cdot 5 \cdot \dots \cdot p_m$ would be evenly divisible (i.e., remainder 0 after division) by each p_i and therefore $N + 1$ would be evenly divisible by no prime (the remainder of p_i divided into $N + 1$ would always be 1), which would contradict the fact that every integer ≥ 2 can be factored as a product of primes. (The latter fact has nothing to do with P being finite or not.) Since the supposition that P is finite led to a contradiction of a known fact, prime factorization, the supposition was incorrect, and P is, after all, infinite.

Afficionados of logic will note our heavy use here of the "law of the excluded middle," to wit, that a mathematically meaningful statement is either true or false. The possibilities that it is neither true nor false, or that it is both true and false, are excluded.

Metaphor and Analogy

In high school English, you are taught that a metaphor is a figure of speech in which one idea or word is substituted for another to suggest a likeness or similarity. This can occur very simply as in "The ship plows the sea." Or it can be less direct, as in "his lawyers dropped the ball." What give a metaphor its power and pleasure are the secondary suggestions of similarity. Not only did the lawyers make a mistake, but it was their own fault, and, like an athlete who has dropped a ball, they could not follow through with their next legal action. A secondary implication is that their enterprise was just a game.

Often a metaphor associates something abstract to something concrete, as "Life is a journey." The preservation of inference from the concrete to the abstract in this metaphor suggests that like a journey, life has a beginning and an end, it progresses in one direction, it may have stops and detours, ups and downs, etc. The beauty of a metaphor is that hidden in a simple sentence like "Life is a journey" lurk a great many parallels, waiting to be uncovered by the thoughtful mind.

Metaphorical thinking pervades mathematics to a remarkable degree. It is often reflected in the language mathematicians choose to define new concepts. In his construction of the system of real numbers, Dedekind could have referred to $A|B$ as a "type-two, order preserving equivalence class," or worse, whereas "cut" is the right metaphor. It corresponds closely to one's physical intuition about the real line. See Figure 3. In his book, *Where Mathematics Comes From*, George Lakoff gives a comprehensive view of metaphor in mathematics.

[†] In English grammar, the subjunctive mode indicates doubt, and I have written Euclid's proof in that form – "if P *were* finite" instead of "if P *is* finite," "each prime *would* divide N evenly," instead of "each prime *divides* N evenly," etc. At first it seems like a fine idea to write all arguments by contradiction in the subjunctive mode, exhibiting clearly their impermanence. Soon, however, the subjunctive and conditional language becomes ridiculously stilted and archaic. For consistency then, as much as possible, *use the present tense.*

An analogy is a shallow form of metaphor. It just asserts that two things are similar. Although simple, analogies can be a great help in accepting abstract concepts. When you travel from home to school, at first you are closer to home, and then you are closer to school. Somewhere there is a halfway stage in your journey. You *know* this, long before you study mathematics. So when a curve connects two points in a metric space (Chapter 2), you should expect that as a point "travels along the curve," somewhere it will be equidistant between the curve's endpoints. Reasoning by analogy is also referred to as "intuitive reasoning."

Moral Try to translate what you know of the real world to guess what is true in mathematics.

Two pieces of advice

A colleague of mine regularly gives his students an excellent piece of advice. When you confront a general problem and do not see how to solve it, make some extra hypotheses, and try to solve it then. If the problem is posed in n dimensions, try it first in two dimensions. If the problem assumes that some function is continuous, does it get easier for a differentiable function? The idea is to reduce an abstract problem to its simplest concrete manifestation, rather like a metaphor in reverse. At the minimum, look for at least one instance in which you can solve the problem, and build from there.

Moral If you do not see how to solve a problem in complete generality, first solve it in some special cases.

Here is the second piece of advice. Buy a notebook. In it keep a diary of your own opinions about the mathematics you are learning. Draw a picture to illustrate every definition, concept, and theorem.

2 Cuts

We begin at the beginning and discuss $\mathbb{R}$ = the system of all real numbers from a somewhat theological point of view. The current mathematics teaching trend treats the real number system $\mathbb{R}$ as a given — it is defined axiomatically. Ten or so of its properties are listed, called axioms of a complete ordered field, and the game becomes: deduce its other properties from the axioms. This is something of a fraud, considering that the entire structure of analysis is built on the real number system. For what if a system satisfying the axioms failed to exist? Then one would be studying the empty set! However, you need not take the existence of the real numbers on faith alone — we will give a concise mathematical proof of it.

It is reasonable to accept all grammar school arithmetic facts about

The set $\mathbb{N}$ of natural numbers, $1, 2, 3, 4, \ldots$.

The set $\mathbb{Z}$ of integers, $0, 1, -1, -2, 2, \ldots$.

The set $\mathbb{Q}$ of rational numbers p/q where p, q are integers, $q \neq 0$.

For example, we will admit without question facts like $2 + 2 = 4$, and laws like $a + b = b + a$ for rational numbers a, b. All facts you know about arithmetic involving integers or rational numbers are fair to use in homework exercises too.[†] It is clear that $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$. Now $\mathbb{Z}$ improves $\mathbb{N}$ because it contains negatives and $\mathbb{Q}$ improves $\mathbb{Z}$ because it contains reciprocals. $\mathbb{Z}$ legalizes subtraction and $\mathbb{Q}$ legalizes division. Still, $\mathbb{Q}$ needs further improvement. It doesn't admit irrational roots such as $\sqrt{2}$ or transcendental numbers such as π. We aim to go a step beyond $\mathbb{Q}$, completing it to form $\mathbb{R}$ so that

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

As an example of the fact that $\mathbb{Q}$ is incomplete we have

1 Theorem *No number r in $\mathbb{Q}$ has square equal to 2; i.e., $\sqrt{2} \notin \mathbb{Q}$.*

Proof To prove that every $r = p/q$ has $r^2 \neq 2$ we show that $p^2 \neq 2q^2$. It is fair to assume that p and q have no common factors since we would have canceled them out beforehand. Two integers without common factors can not both be even, so at least one of p, q is odd.

Case 1. p is odd. Then p^2 is odd while $2q^2$ is not. Therefore $p^2 \neq 2q^2$.

Case 2. p is even and q is odd. Then p^2 is divisible by 4 while $2q^2$ is not. Therefore $p^2 \neq 2q^2$. □

The set $\mathbb{Q}$ of rational numbers is incomplete. It has "gaps," one of which occurs at $\sqrt{2}$. These gaps are really more like pinholes; they have zero width. Incompleteness is what is *wrong* with $\mathbb{Q}$. Our goal is to complete $\mathbb{Q}$ by filling in its gaps. An elegant method to arrive at this goal is **Dedekind cuts** in which one visualizes real numbers as places at which a line may be cut with scissors. See Figure 3.

Definition A **cut** in $\mathbb{Q}$ is a pair of subsets A, B of $\mathbb{Q}$ such that

(a) $A \cup B = \mathbb{Q}$, $A \neq \emptyset$, $B \neq \emptyset$, $A \cap B = \emptyset$.

(b) If $a \in A$ and $b \in B$ then $a < b$.

(c) A contains no largest element.

[†] A subtler fact that you may find useful is the prime factorization theorem mentioned above. Any integer ≥ 2 can be factored into a product of prime numbers. For example, 120 is the product of primes $2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$. Prime factorization is unique except for the order in which the factors appear. An easy consequence is that if a prime number p divides an integer k and if k is the product mn of integers then p divides m or it divides n. After all, by uniqueness, the prime factorization of k is just the product of the prime factorizations of m and n.