A note about definitions, and a convention

If we are giving a definition $(*)$, then the definition is supposed to say exactly what (*) means $-$ neither more nor less $-$ in terms of concepts we already know. In other words, a definition should say that a new term

(*) is equivalent to $(a\ prescise\ description\ in\ familiar\ terms)$, that is

(*) iff $(....)$

See the following definitions for examples.

Our textbook is careful to write definitions using "iff."

However, there is a convention most mathematicians follow and which some other textbooks use. When something is "announced" as a definition (that is, when there's no confusion that a definition is being made), a mathematician often only write "if" rather than "iff." For example:

Textbook (and, strictly speaking, the correct way):

Definition An integer x is even iff we can write $x = 2k$ for some integer k

A mathematician would usually write:

Definition An integer x is even if we can write $x = 2k$ for some integer k.

Since this is announced to be a definition, the convention is that here "if" really means"iff" (if and only if).

In the definitions that follow, it is assumed that we already know how addition, subtraction, multiplication and division work in the different number systems.

$\mathbb{N} = \{1, 2, 3, ...\}$ = *the set of natural numbers*
$\mathbb{Z} = \{\ ...,\ -2,\ -1, 0, 1, 2, ...\}$ = *the set of integers*
$\mathbb{Q} = \{\frac{p}{q} :\ p, q$ *are integers and* $q \neq 0\}$ = *the set of rational numbers*
$\mathbb{R}$ = *the set of real numbers*
$\mathbb{C}$ = *the set of complex numbers (numbers* $a + bi$ *where* a, b *are real and* $i^2 = -1)$

Some Definitions and Notation for Use in Early Proof Examples
(*most of these are in the Preface to the Student in the text, p. xii*)

1) An integer x is <u>even</u> iff we can write $x = 2k$ for some integer k
(More formally: $(\forall x \in \mathbb{Z})$ (x is even $\Leftrightarrow \exists k \in \mathbb{Z}$ for which $x = 2k$)

2) An integer x is <u>odd</u> iff we can write $x = 2k + 1$ for some integer k
(More formally: $(\forall x \in \mathbb{Z})$ (x is odd $\Leftrightarrow \exists k \in \mathbb{Z}$ for which $x = 2k + 1$)

3) For integers a and b. where $a \neq 0$: <u>a divides b (written $a|b$)</u> iff $b = ak$ for some integer k.
<u>b is divisible by a iff $a|b$</u>
More formally, for integers a and b, with $a \neq 0$:

$$a|b \;\Leftrightarrow\; (\exists k)\,(k \in \mathbb{Z} \;\wedge\; b = ak)$$

If $a|b$, then a is called a <u>divisor</u> or <u>factor</u> of b.

(*The definition of $a|b$ for <u>natural numbers</u> a, b reads in the same way, with $\mathbb{N}$ in place of $\mathbb{Z}$.*
If a, b are nautral numbers, it's no longer necessary to say $a \neq 0$.)

4) A natural number p is <u>prime</u> iff $p > 1$ and the only divisors of p are p and 1.
More formally, for a natural number p :

$$p \text{ is prime} \quad \Leftrightarrow \quad (p > 1) \;\wedge\; (\forall a \in \mathbb{N})\,(a|p \Rightarrow (a = 1 \;\vee a = p))$$

5) A real number x is called <u>rational</u> iff we can write $x = \frac{p}{q}$ where p and q are integers and $q \neq 0$.
More formally,

for a real number x : $\quad x$ is rational $\Leftrightarrow (\exists p \in \mathbb{Z})(\exists q \in \mathbb{Z})$ $(x = \frac{p}{q} \;\wedge x \neq 0)$

6) For a nonnegative integer n, <u>n factorial</u> (denoted by $n!$) is defined as follows:

$$0! = 1, \quad 1! = 1, \quad 2! = 1 \cdot 2, \quad 3! = 1 \cdot 2 \cdot 3, \;\ldots,\; n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1) \cdot n, \;\ldots$$

7) If x is a real number, we define

<u>the floor function</u>, $\lfloor x \rfloor$ = the largest integer that is $\leq x$
For example, $\lfloor 3.1 \rfloor = 3$, $\lfloor -4.1 \rfloor = -5$.
The floor function is also called the "greatest integer function."

<u>the ceiling function</u>, $\lceil x \rceil$ = the smallest integer that is $\geq x$
For example, $\lceil 3.1 \rceil = 4$ and $\lceil -4.1 \rceil = -4$.

<u>the absolute value function</u>, $|\,x\,| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$

A Working Description of "Theorem" and "Proof"

A theorem is a mathematical statement that can be proved. A theorem can be written in various ways in English, but it can always be reworded (if desired) in the form:

Theorem: $P \Rightarrow Q$ ("if P, then Q")

The antecedent, P, in the implication is usually called the hypothesis of the theorem, and the consequent, Q is called the conclusion.

The hypothesis might have several parts: for example, we could have

> Theorem: If n is an even natural number larger than 20, then ...
> *Here, the hypothesis P has the form $R \wedge S$, where R is "n is an even natural number" and S is "$n > 20$"*

or

> Theorem: If every nonnegative real number has a square root, then ...
> *Here, the hypothesis "Every nonnegative real number has a square root" can be written $(\forall x \in \mathbb{R})($ x nonnegative $\Rightarrow$ x has a square root), that is*
> *P has the form $(\forall x)(R(x) \Rightarrow S(x))$*

Similarly, the conclusion may have several parts. For example

> Theorem: If n is a prime number, then $n = 2$ or n is odd
> *This has form :* $P \Rightarrow (R \vee S)$

> Theorem: If (X, d) is a metric space and X is separable, then d is totally bounded
>
> $\uparrow$ P $\quad\quad$ $\uparrow$ Q $\quad\quad$ $\uparrow$ S
>
> if X is compact.
>
> $\uparrow$ R
>
> *This has form:* $(P \wedge Q) \Rightarrow (R \Rightarrow S)$

A proof for a theorem $P \Rightarrow Q$ is a sequence of steps that uses the hypothesis together with any earlier theorems or definitions to argue in logically valid steps to show the conclusion is true.

Sometimes (we will look at examples later) we use logical maneuvers: as an example, instead of proving $P \Rightarrow Q$, we might instead an equivalent statement such as the contrapositive, $\sim Q \Rightarrow \sim P$.

(*For the purpose of the examples, we assume that we already know all about addition, subtraction, mulotiplication, division in the various number systems: natural numbers, integers, reals, etc.*)

Theorem Suppose n is an integer. If n is odd, then $4n + 3$ is odd.

Here is a well-written proof.

Proof Assume n is an odd integer. Then there is an integer k such that $n = 2k + 1$, so

$$\begin{aligned} 4n + 3 &= 4(2k + 1) + 3 = 8k + 7 \\ &= (8k + 6) + 1 \\ &= 2(4k + 3) + 1 \\ &= 2j + 1, \text{ where } j = 4k + 3. \end{aligned}$$

Since j is an integer, $4n + 3$ is odd. •

Exercise Read the proof aloud, exactly as written. How does it "sound?"

Here is a bad proof.

Proof $n = 2k + 1$, $4n + 3 = 4(2k + 1) + 3 = 2j + 1$ so odd. •

Some important pieces for a proof are jotted down here. But

i) what is k? what is n?
ii) why is $n = 2k + 1$?
iii) what is j? after all, if I write $4 = 2(\frac{3}{2}) + 1$, that doesn't show that 4 is odd!
iv) Read it aloud. Does it sound OK? There's nothing like a sentence in it and none of the "thoughts" are tied together.

At the very best, wha'ts given here is bunch of disconnected ideas which could be used in a correct proof – but "some assembly is required" by the reader. When you write a proof, your job is to give the reader a proof, not an "assembly kit" for a proof.

This is the kind of writing where a student might complain "...but I had the main ideas." Maybe; but it's not a well-written proof. And in a more complicated situation, the bad writing may hide any good ideas the writer had.

In your proofs, write sentences and use English words like "then", "so," "because," "therefore," "hence,", "it follows that," "so we see that ..." to connect the pieces of your argument and guide the reader.

Signaling the End of a Proof

Euclid (about 300 B.C.E.) was one of the first writers to systematically treat a subject (geometry) deductively – attempting to show the whole subject could be reduced to just a few initial assumptions ("axioms" or "postulates"), with everything else being logically deduced from them. Euclid concluded his proofs with the Greek words ὅπερ ἔδει δειξαι (“hoper edei deiksai”).

Later, medieval geometers translated this concluding phrase into Latin as "quod erat demonstrandum" ("that which was to be proven"). According to one historian, the earliest known use in print of this phrase appears in a translation of Euclid's work by Bartholemew Zamberti, published in Venice in 1505. A tradition began of ending a matehmatical prrof with "Q.E.D."

"Q.E.D." became such a symbol of irrefutable logic that other scholars, in a pretense (?) of great rigor, began to use it in nonmathematical settings. For example, in 1665 Spinoza wrote a treatise *Ethica More Geometrico Demonstrata*, in which he "proved" various ethical propositions in a geometric manner – giving each one his seal of approval "Q.E.D." It is still used this way, sometimes, especially in conversation, but usually with a "tongue-in-cheek" spirit.

The abbreviation "Q.E.D." is no longer used much in mathematics (at least in the United States), and when it does occur it seems quaint and a bit pretentious. If a mathematician wants to signal the end of a proof nowadays, a symbol such as "•" or "□" or "■" is often used.

Examples

(*Italicized statements are just commentary for students; they are not actually part of the proof.)*

Theorem Let x and y be integers. If x and y are even, then xy is even.

$$\begin{array}{ccc} P & \Rightarrow & Q \\ || & & \\ R \wedge S & & \end{array}$$

Proof Assume x and y are even. Then there are integers m and n such that $x = 2m$ and $y = 2n$. Therefore $xy = (2m)(2n) = 4mn = 2(2mn)$. Since $2mn$ is an integer, xy is even. •

Theorem Assume that n is an integer. If n is odd, then $4n + 3$ is odd.

Proof Assume n is an integer and that n is odd. Then there is an integer k so that $n = 2k + 1$. Therefore $4n + 3 = 4(2k + 1) + 3 = 8k + 7 = (8k + 6) + 1 = 2(4k + 3) + 1$. Since $4k + 3$ is an integer, $4n + 3$ is odd. •

Theorem If x is an integer, then x is either even or odd.

$$\begin{array}{ccc} P & \Rightarrow & Q \vee R \end{array}$$

Use that $P \Rightarrow Q \vee R$ is equivalent to $P \wedge \sim Q \Rightarrow R$

Proof Assume x is an integer and that x is not even. If we divide x by 2 we get an integer k and a remainder. The remainder cannot be 0, so the remainder is 1. Therefore $x = 2k + 1$ so x is odd. •

Theorem If x is an integer, then $x^2 + x$ is even.

Proof Assume x is an integer. By the preceding Theorem, x is either even or odd
(*Now we argue that* $(x$ *is even* $\vee\ x$ *is odd*$) \Rightarrow x^2 + x$ *is even. This implication has a compound hypothesis:* $(R \vee S) \Rightarrow Q$. *We prove this in two cases: if* $R \vee S$ *is true, then either i)* R *is true, or ii)* S *is true.*)

> Case i) Assume x is even, so that there is an integer m for which $x = 2m$. Then $x^2 + x = (2m)^2 + (2m) = 4m^2 + 2m = 2(2m^2 + m)$. Since $2m^2 + m$ is an integer, $x^2 + x$ is even.
>
> Case ii) Assume x is odd, so that there is an integer m for which $x = 2m + 1$. Then $x^2 + x = (2m + 1)^2 + (2m + 1) = 4m^2 + 4m + 1 + 2m + 1 = 4m^2 + 6m + 2 = 2(2m^2 + 3m + 1)$. Since $2m^2 + 3m + 1$ is an integer, $x^2 + x$ is even.

Since $x^2 + x$ is even both cases, $x^2 + x$ must be even. •

Theorem Suppose p, q, r, a, b are integers, where $p \neq 0$. If $p|q$ and $p|r$, then $p|(aq + br)$

(*Use the definition of "divides."* To prove that $p|(aq + br)$, w*e need to show that there is an integer k such that $aq + br = pk$. This equation would be true if we could factor a p out of $aq + br$. Can we?*)

Proof Assume that $p|q$ and $p|r$. Then there are integers m and n such that $q = mp$ and $r = np$, so $aq + br = a(mp) + r(np) = (am + rn)p$. Since $am + rn$ is an integer, $p|(aq + br)$. •

(*Assume you know the definitions of the trig functions and that* $\sin^2 x + \cos^2 x = 1$ *for all* x.)

Theorem If x is a real number for which $\cos x \neq 0$, then $1 + \tan^2 x = \sec^2 x$
"Proof" Assume that x is a real number for which $\cos x \neq 0$. Then $\sec x = \frac{1}{\cos x}$ and $\tan x = \frac{\sin x}{\cos x}$ are defined and

$$\begin{aligned} & 1 + \tan^2 x = \sec^2 x \\ = \ & 1 + \tfrac{\sin^2 x}{\cos^2 x} = \tfrac{1}{\cos^2 x} \\ = \ & \cos^2 x + \sin^2 x = 1. \quad \bullet \end{aligned}$$

What is wrong with the preceding "proof"?

i) Everything is connected by " = " signs, and that creates nonsense. Although things are written on separate lines, what is written says that

$1 + \tan^2 x = \sec^2 x = 1 + \frac{\sin^2 x}{\cos^2 x} = \frac{1}{\cos^2 x} = \cos^2 x + \sin^2 x = 1$
(so $1 + \tan^2 x = 1$!!!???)

We never say that two equations are equal to each other. However, we could write

$$\begin{aligned} & 1 + \tan^2 x = \sec^2 x \\ \Rightarrow \ & 1 + \tfrac{\sin^2 x}{\cos^2 x} = \tfrac{1}{\cos^2 x} \\ \Rightarrow \ & \cos^2 x + \sin^2 x = 1 \end{aligned}$$

because each equation here does imply the next equation: if the first equation is true, so is the second, etc. Or we could use English words like "so" or "hence" or "therefore" to connect equations.

Some students sprinkle " = " signs throughout their writing in meaningless ways, in the same way some students spinkle phrases such as "like, you know..." throughout a conversation – just as filler rather than adding anything to the meaning. Never write " = " unless you mean to say that what's on the left is literally equal to what's on the right.

ii) But there's a more serious problem:

> Assume that x is a real number for which $\cos x \neq 0$. Then $\sec x = \frac{1}{\cos x}$ and $\tan x = \frac{\sin x}{\cos x}$ are defined and
>
> $1 + \tan^2 x = \sec^2 x$ ← **WHY? You don't know this is true; it's what you're trying to prove!**

The steps are backwards: the argument should "move" in a direction from what you know toward the conclusion.

Here is a correct proof:

Proof We know that $\cos^2 x + \sin^2 x = 1$. We are assuming that x is a real number for which $\cos x \neq 0$, so we can divide both sides of the equation by $\cos^2 x$

$$1 + \frac{\sin^2 x}{\cos^2 x} = \frac{1}{\cos^2} x$$

Since $\sec x = \frac{1}{\cos x}$ and $\tan x = \frac{\sin x}{\cos x}$, this equations saysare defined and

$$1 + \tan^2 x = \sec^2 x. \quad \bullet$$

Theorem If n is an odd integer, then n^2 is odd.

What is wrong with these proofs?

> **Proof 1** $1^2 = 1,\ 3^2 = 9,\ 5^2 = 25,\ 7^2 = 49,\ 9^2 = 81$. Whenever an odd integer is squared the result always ends in a $1, 5,\ 9$. So the square of an odd integer is odd. $\bullet$

> **Proof 2** Suppose that n^2 is odd. By an earlier theorem, if n were even, then n^2 would be even. Therefore n must be odd. $\bullet$

A correct proof:

Proof Suppose that n is an odd integer, so that there is an integer k such that $n = 2k + 1$. Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Since $2k^2 + 2k$ is an integer, this proves that n^2 is odd. $\bullet$

Theorem Assume x is a complex number and that a, b, c are real. Prove that if $a \neq 0$ and $ax^2 + bx + c = 0$, then $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

Proof Assume that $ax^2 + bx + c = 0$ and that $a \neq 0$. Since $a \neq 0$, we can write

$x^2 + \frac{b}{a}x + \frac{c}{a} = 0.$ Adding $\frac{b^2}{4a^2}$ and $-\frac{c}{a}$ to both sides gives

$x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} = \frac{b^2}{4a^2} - \frac{c}{a}.$ Factoring the left side and combining fractions on the right gives

$(x + \frac{b}{2a})^2 = \frac{b^2 - 4ac}{4a^2}.$ Therefore

$x + \frac{b}{2a} = \pm\sqrt{\frac{b^2 - 4ac}{4a^2}} = \pm\frac{\sqrt{b^2 - 4ac}}{2a}$, so

$x = -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$ •