DEFINITIONS

Logic and proof

The language every proof is written in: statements, quantifiers and the standard methods of proof.

54 definitions **5** subtopics By Lucas Potrykus

CONTENTS

1. Statements and connectives 16
2. Quantifiers 5
3. Theorems and the words around them 11
4. Methods of proof 7
5. Integers, primes and divisibility 15

HOW TO USE THIS

Each definition gives the exact meaning of a word or symbol. Where there is a symbol, it is shown next to the name, with how to say it out loud. Most definitions have a short example.

Learn definitions word for word: in proofs and in exams, the precise wording is what earns the marks.

Searchable online, with links to every topic, at lemmamathematics.com/definitions.

STATEMENTS AND CONNECTIVES

More in **Proof I**

Statement (proposition)

A sentence that is either true or false, but not both. Questions, commands and expressions such as $x^2 + 1$ are not statements; "$x^2 + 1 > 0$ for every real x" is.

> EXAMPLE
> "7 is prime" is a true statement; "every odd number is prime" is a false one.

Implies

$\Rightarrow$

SAY *implies; if … then …*

$P \Rightarrow Q$ means that whenever P is true, Q is true as well. It makes no claim about what happens when P is false.

> EXAMPLE
> $x = 2 \Rightarrow x^2 = 4$. The arrow does not reverse: $x^2 = 4$ also allows $x = -2$.

Is implied by

$\Leftarrow$

SAY *is implied by; if*

$P \Leftarrow Q$ means the same as $Q \Rightarrow P$. Useful when you want to keep the conclusion on the left.

> EXAMPLE
> $x^2 = 4 \Leftarrow x = 2$ is true.

If and only if

$\iff$

SAY *if and only if; "iff"*

$P \iff Q$ means $P \Rightarrow Q$ **and** $Q \Rightarrow P$: the two statements are true in exactly the same situations. To prove one, you usually prove both directions separately.

> EXAMPLE
> For real x: $x^3 = 8 \iff x = 2$.

Not

$\neg$

SAY *not*

The negation of a statement: $\neg P$ is true exactly when P is false. Also written $\sim P$ or $\overline{P}$. Negating swaps the quantifiers: $\neg(\forall x,\ P(x))$ is the same as $\exists x,\ \neg P(x)$.

> EXAMPLE
> The negation of "every prime is odd" is "some prime is even", and 2 shows that the negation is true.

And

$\wedge$

SAY *and*

$P \wedge Q$ is true only when both P and Q are true.

> EXAMPLE
> $x > 0 \wedge x < 1$ says the same as $0 < x < 1$.

Or

$\vee$

SAY *or*

$P \vee Q$ is true when at least one of P, Q is true. In mathematics "or" is always **inclusive**: both being true is allowed.

> EXAMPLE
> $x^2 = 1 \iff x = 1 \vee x = -1$.

Converse

The converse of $P \Rightarrow Q$ is $Q \Rightarrow P$. A statement and its converse are logically independent: one can be true while the other is false.

> EXAMPLE
> "If n is divisible by 4 then n is even" is true; its converse, "if n is even then n is divisible by 4", is false ($n = 6$).

Contrapositive

The contrapositive of $P \Rightarrow Q$ is $\neg Q \Rightarrow \neg P$. It is always **equivalent** to the original statement, so proving the contrapositive proves the statement.

> EXAMPLE
> "If n^2 is even then n is even" has contrapositive "if n is odd then n^2 is odd", which is easy to prove directly.

Inverse of a statement

The inverse of $P \Rightarrow Q$ is $\neg P \Rightarrow \neg Q$. It is equivalent to the converse, not to the original statement.

Necessary condition

Q is necessary for P when P cannot happen without Q, that is $P \Rightarrow Q$.

> EXAMPLE
> Being even is necessary for being divisible by 4, but it is not sufficient.

Sufficient condition

P is sufficient for Q when P on its own guarantees Q, that is $P \Rightarrow Q$. "Necessary and sufficient" means $P \iff Q$.

> EXAMPLE
> $x = 3$ is sufficient for $x^2 = 9$ but not necessary, since $x = -3$ also works.

Tautology

A compound statement that is true whatever the truth values of its parts. Its opposite, which is always false, is a contradiction.

> EXAMPLE
> $P \vee \neg P$ is a tautology; $P \wedge \neg P$ is a contradiction.

Truth table

A table listing every combination of truth values of the basic statements, and the resulting truth value of a compound statement. With n basic statements there are 2^n rows.

Therefore ∴

SAY *therefore; so*

Introduces a conclusion that follows from what came before. In a written proof, words such as "so" or "hence" are usually clearer.

> EXAMPLE
> $2x + 1 = 7$, $\therefore x = 3$.

Because ∵

SAY *because; since*

Introduces a reason. Rarely used in modern writing, where "since" reads better.

> EXAMPLE
> $\sqrt{x^2} = x \because x \geq 0$.

QUANTIFIERS

More in **Proof I**

For all ∀

SAY *for all; for every*

The universal quantifier. $\forall x \in S,\ P(x)$ says that $P(x)$ is true for every element x of S. One counterexample is enough to make it false.

> EXAMPLE
> $\forall x \in \mathbb{R},\ x^2 \geq 0$: every real number has a non-negative square.

There exists ∃

SAY *there exists; there is at least one*

The existential quantifier. $\exists x \in S$ such that $P(x)$ says that at least one element of S makes $P(x)$ true. One example is enough to prove it.

> EXAMPLE
> $\exists x \in \mathbb{R}$ such that $x^2 = 2$ (namely $x = \sqrt{2}$). But there is no such $x \in \mathbb{Q}$.

There exists a unique

$\exists!$

SAY *there exists exactly one*

There is one, and only one, element with the property. Proving it takes two parts: existence (find one) and uniqueness (show any two must be equal).

> EXAMPLE
> $\exists!\, x \in \mathbb{R}$ such that $x^3 = 8$. But not $\exists!\, x$ with $x^2 = 4$, since there are two.

Counterexample

A single example showing that a "for all" statement is false. One counterexample is a complete disproof; no number of examples is a proof.

> EXAMPLE
> $n = 41$ is a counterexample to "$n^2 + n + 41$ is prime for every natural number n", since $41^2 + 41 + 41 = 41 \times 43$.

Arbitrary

"Let x be arbitrary" means x stands for any element at all, with no special properties assumed. Whatever is then proved about x holds for every element, which is how "for all" statements are proved.

THEOREMS AND THE WORDS AROUND THEM

More in **Proof I**

Axiom

A statement accepted as true without proof, used as a starting point. Every proof ultimately rests on axioms and definitions.

> EXAMPLE
> Euclid's axiom that a straight line can be drawn between any two points.

Definition

A precise statement of what a word or symbol means. Definitions are not proved; they are agreed.

Theorem

An important statement that has been proved.

> EXAMPLE
> Pythagoras' theorem; the fundamental theorem of calculus.

Lemma

A smaller result proved mainly as a step towards a theorem. (This site is named after it.)

Corollary

A result that follows quickly from a theorem just proved.

> EXAMPLE
> From "the angles of a triangle add to $180°$" follows the corollary "each angle of an equilateral triangle is $60°$".

Conjecture

A statement believed to be true but not yet proved.

> EXAMPLE
> Goldbach's conjecture: every even number greater than 2 is the sum of two primes.

Proof

A logical argument that establishes, beyond any doubt, that a statement is true, starting from definitions, axioms and results already proved.

Without loss of generality

"WLOG" announces that I am about to assume something special (such as $a \leq b$) because the other cases work in exactly the same way.

> EXAMPLE
> For two integers, WLOG $a \leq b$: otherwise swap their names.

Hence and hence or otherwise

In an exam, "hence" means you must use the previous result; "hence or otherwise" means using it is the quickest route, but any correct method earns the marks.

Show that

An instruction to reach a given answer, with every step written out. Because the answer is printed, the marks are all for the working.

End of proof

■

SAY *QED; "which was to be shown"*

Marks the end of a proof. Also written □ or QED, from the Latin *quod erat demonstrandum*, "which was to be shown".

METHODS OF PROOF

More in **Proof I**

Proof by deduction (direct proof)

Start from known facts or the hypothesis and reach the conclusion by a chain of logical steps.

> EXAMPLE
> If $m = 2a$ and $n = 2b$ are even then $m + n = 2(a + b)$ is even.

Proof by exhaustion

Split the statement into a finite number of cases and check every one.

> EXAMPLE
> Every square number leaves remainder 0 or 1 on division by 3: check $n = 3k$, $3k + 1$ and $3k + 2$.

Proof by contradiction

Assume the statement is false, and deduce something impossible. The assumption must therefore be wrong, so the statement is true.

> EXAMPLE
> The classic proofs that $\sqrt{2}$ is irrational and that there are infinitely many primes.

Contradiction

$\Rightarrow\!\!\!\!\!\!\not\Leftarrow$

SAY *contradiction*

Marks the moment in a proof by contradiction where two statements clash, so the original assumption must be false. Also written $\bot$, # or simply the word "contradiction".

> EXAMPLE
> Assume $\sqrt{2} = \frac{p}{q}$ in lowest terms … so p and q are both even $\Rightarrow\!\!\!\!\!\!\not\Leftarrow$.

Proof by contrapositive

To prove $P \Rightarrow Q$, prove the equivalent statement $\neg Q \Rightarrow \neg P$ instead.

Disproof by counterexample

Showing a "for all" statement is false by giving one case where it fails.

Proof by induction

Prove a statement for a first value (the base case), then prove that if it holds for $n = k$ it holds for $n = k + 1$. Together these prove it for every integer from the first value onwards.

More in **Mathematical induction**

INTEGERS, PRIMES AND DIVISIBILITY

More in **Proof I**

Integer

A whole number: positive, negative or zero. The set of integers is $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

Even and odd

An integer is even if it can be written $2k$ for an integer k, and odd if it can be written $2k + 1$. Every integer is exactly one of the two; this is its **parity**.

Factor (divisor)

a is a factor of b if $b = ak$ for some integer k.

> EXAMPLE
> The factors of 12 are 1, 2, 3, 4, 6 and 12.

Multiple

b is a multiple of a if $b = ak$ for some integer k.

> EXAMPLE
> The multiples of 7 are $\ldots, -7, 0, 7, 14, \ldots$

Divides

$a \mid b$

SAY *a divides b*

a divides b exactly: $b = ka$ for some integer k. Not to be confused with $\frac{a}{b}$, which is a number; $a \mid b$ is a statement that is true or false.

> EXAMPLE
> $3 \mid 12$ but $5 \nmid 12$.

Prime number

A natural number greater than 1 whose only positive factors are 1 and itself. 1 is **not** prime.

> EXAMPLE
> 2, 3, 5, 7, 11, 13, … 2 is the only even prime.

Composite number

A natural number greater than 1 that is not prime, so it has a factor other than 1 and itself.

> EXAMPLE
> $91 = 7 \times 13$ is composite.

Fundamental theorem of arithmetic

Every integer greater than 1 can be written as a product of primes, and this **prime factorisation** is unique apart from the order of the factors.

> EXAMPLE
> $360 = 2^3 \times 3^2 \times 5$.

Greatest common divisor

$\gcd(a, b)$

SAY *g c d of a and b; highest common factor*

The largest integer dividing both a and b, also written $\operatorname{hcf}(a, b)$ or just (a, b). The partner is $\operatorname{lcm}(a, b)$, the lowest common multiple, and $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$ for positive integers.

> EXAMPLE
> $\gcd(12, 18) = 6$ and $\operatorname{lcm}(4, 6) = 12$.

Coprime

Two integers are coprime when their only common positive factor is 1, that is $\gcd(a, b) = 1$.

> EXAMPLE
> 8 and 15 are coprime, although neither is prime.

Quotient and remainder

For integers a and $b > 0$ there are unique integers q and r with $a = bq + r$ and $0 \le r < b$. q is the quotient and r the remainder.

> EXAMPLE
> $47 = 6 \times 7 + 5$: quotient 7, remainder 5.

Congruent modulo n

$a \equiv b \pmod{n}$

SAY *a is congruent to b mod n*

a and b leave the same remainder when divided by n; equivalently $n \mid a - b$. It is the arithmetic of a clock with n hours.

> EXAMPLE
> $17 \equiv 2 \pmod{5}$, and $10^k \equiv 1 \pmod{9}$, which is why the digit-sum test for 9 works.

Rational number

A number that can be written $\frac{p}{q}$ with p, q integers and $q \neq 0$. Their decimals either stop or repeat.

> EXAMPLE
> $0.\overline{3} = \frac{1}{3}$ and $-2.5 = -\frac{5}{2}$ are rational.

Irrational number

A real number that is not rational. Its decimal expansion never ends and never repeats.

> EXAMPLE
> $\sqrt{2}$, π and e are irrational.

Perfect square

An integer that is the square of an integer. Similarly a perfect cube is the cube of an integer.

> EXAMPLE
> $0, 1, 4, 9, 16, \ldots$

Spotted a mistake, or a definition that should be here? Email lpotry31@gmail.com. More at lemmamathematics.com.