Math 214 Foundations of Higher Mathematics C.K. Li

Chapters 3 – 5: Proofs

We practice how to read and write mathematical proofs.

General discussions from Chapters 3 and 5; and examples from Chapter 4.

Terminology Axiom, Theorem, Lemma, Corollary, etc.

In mathematics, we often try to establish "$P(x) \Rightarrow Q(x)$" for $x \in S$.

We also consider "$P(x)$ if and only if $Q(x)$".

§3.1 and §3.2 Trivial proof Assume $x \in S$ and $P(x)$ is true. Then verify Q(x).

We ignore trivial statements/situations: (a) when $P(x)$ is always false, (b) when $Q(x)$ is always true.

In such cases, the proof is **trivial/vacuous**.

Examples If x is real such that $x < 0$, then $x^2 + 1 > 0$.

If $x \in \mathbf{R}$ such that $x^2 - 2x + 3 < 0$, then $20^3 > 100$.

If 3 is even, then $n \in \mathbf{Z}$ is divisible by 5.

Prove or disprove: If $r \in (0, 1)$, then $1/4 \geq r(1 - r)$.

Prove or disprove: If $r \in (0, 1)$, then $1/4 > r(1 - r)$.

§3.2 Direct proof We assume P(x) and verify Q(x) (to get the "theorem").

Examples If $n \in \mathbf{Z}$ and $5n - 7$ is odd, then $9n + 2$ is even. [An integer m is even (odd) if ....]

If a, b, c are integers such that a divides b, and b divides c, then a divides c.

[For integers x and y, we say that x divides y if $y = xz$ for some $z \in \mathbf{N}$.]

If a is not divisible by 3 and b is not divisible by 3, then $a^2 - b^2$ is divisible by 3.

Let A and B be sets. Then $A \cup B = A \cap B$ if and only if $A = B$.

Let A, B, C be sets such that C is non-empty. Then $A \times C \subseteq B \times C$ if and only if $A \subseteq B$.

What if C is empty?

§3.3. Proof by contrapositive To prove "If $P(x)$ then $Q(x)$." we prove "If $\sim Q(x)$, then $\sim P(x)$."
Examples If $n \in \mathbf{Z}$ is such that $15n$ is even, then $9n$ is even.

An integer n is odd (even) if and only if n^2 is odd (even).

§5.2 Proof by contradiction To prove $P \Rightarrow Q$, show that $P \wedge \sim Q$ is impossible.

Also, to prove P, assume $\sim P$ and derive a contradiction.

Examples The sum of a rational number and an irrational number is irrational.

The number $\sqrt{2}$ is irrational. (If $x = \sqrt{2}$, then x is irrational.)

There are infinitely many prime numbers.

(If S is the set of primes, then S has infinitely many elements.)

If $x, y \in \mathbf{R}$ are positive, then $\sqrt{x} + \sqrt{y} \neq \sqrt{x+y}$.

§3.4 Proof by cases

If $n \in \mathbf{Z}$, then $n(n+1)/2$ is an integer.

If $a, b \in \mathbf{Z}$ such that $a + b$ and ab are even, then a and b are even.

§5.4 & 5.5 Proofs of statements involving quantifiers

(1) To prove a statement "P" is true (false) , prove that "$\sim P$" is false (true).

(2.a) To prove "$\exists x, P(x)$" is true, provide and example of $x \in S$ or show that there must be an $x \in S$ such that $P(x)$ holds.

(2.b) To prove that "$\exists x, P(x)$" is false, show that for every $x \in S$ $P(x)$ does not hold.

(3.a) To prove that "$\forall x, P(x)$" is true, show that for every $x \in S$ $P(x)$ holds.

(3.b) To prove that "$\forall x, P(x)$" is false, show that there is $x \in S$ such that $\sim P(x)$ hold. Such an $x \in S$ is call a counter example for the statement "$\forall x, P(x)$".

Examples Prove or disprove the statements:

(a) There are no positive integers m and n such that $m^2 + m + 1 = n^2$.

(b) There are positive irrational numbers a and b such that a^b is rational.

(c) There exist odd integers a and b such that $4|(3a^2 + 7b^2)$.

(d) There is a real number x such that $x^6 + x^4 + 1 = 2x^2$.

§4 & 5. More examples of proofs

Examples Prove or disprove the following.

(a) Let $x, y \in \mathbf{Z}$. If $3 \not| xy$, then $3 \not| x$ and $3 \not| y$.

(b) If $n \in \mathbf{N}$ and $n \geq 7$, then $n = 2a + 3b$.

Congruence of integers

Definition Let $n \in \mathbf{N}$. For $a, b \in \mathbf{Z}$, we say that a is congruent to b modulo n, denoted by $a \equiv b (\mathrm{mod}, n)$, if $a - b$ is divisible by n, i.e., a and b have the same remainder when they are divided by n.

Prove the following for $n \in \mathbf{N}, a, b \in \mathbf{Z}$.

(a) If $a \equiv b (\mathrm{mod}, n)$, then $ka \equiv kb (\mathrm{mod}, n)$ for any $k \in \mathbf{Z}$.

(b) If $a \equiv b (\mathrm{mod}, n)$ and $c \equiv d (\mathrm{mod}, n)$, then $a + c \equiv b + d (\mathrm{mod}, n)$ and $ad \equiv bd (\mathrm{mod}, n)$.

Examples

(a) Suppose $x, y \in \mathbf{R}$. Then $\frac{1}{3}x^2 + \frac{3}{4}y^2 \geq xy$.

(b) Let $S_a = [0, a]$ for $a > 0$. Determine (with explanation/proof) the following:

$$\cup_{a\in[1,2]} S_a, \qquad \cup_{1\in(1,2)} S_a, \qquad \cap_{a\in[1,2]} S_a, \qquad \cap_{a\in(1,2)} S_a.$$