§1-1 Propositions and connectives

Def1: A proposition(or statement) is a sentence which we can decide that is true write T, or false write F.

ExampleI

(1) 57 is a prime number(F)

(2) $x>6$ (not a proposition)

Def2: Given two proposition P and Q

(1) Negation of P: not P, write: $\sim P$

(2) Disjunction of P, Q, P or Q, write $P \vee Q$. $P \vee Q$ is exactly T when at least one of P or Q is T.

(3) Conjunction of P, Q, P and Q, write $P \wedge Q$. $P \wedge Q$ is exactly T when both P and Q is T.

P	$\sim P$	Q	$P \vee Q$	$P \wedge Q$
T	F	T	T	T
T	F	F	T	F
F	T	T	T	F
F	T	F	F	F

ExampleII

(1) P: 57 is a prime number / $\sim P$: 57 is not a prime number

(2) P: 7 is prime(T) / Q: 9 is even(F) / R: $11<3$(F)

$P \vee Q$(T), $(P \wedge Q) \vee \sim R$(T)

(3) Given a proposition P, show that $P \vee \sim P$ is always T.

P	$\sim P$	$P \vee \sim P$
T	F	T
F	T	T

Def3: (1) A tautology is a compound proposition that all possible combination of the component yield T

(2) A contradiction is a compound proposition that all possible combination of the component yield F

Rmk4: (1) $P \vee \sim P$ is tautology

(2) $\sim$(tautology) = contradiction

Def5: Two compound propositions R and S are equivalent, write $R \equiv S$, if they have the same truth table

Thm6: (a) $P \equiv \sim(\sim P)$

(b) $P \vee Q \equiv Q \vee P$

(c) $P \wedge Q \equiv Q \wedge P$

(d) $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$

(f) $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$

(g) $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$

(h) $\sim(P \wedge Q) \equiv \sim P \vee \sim Q$

(i) $\sim(P \vee Q) \equiv \sim P \wedge \sim Q$

} Demorgan's Laws

(e) $P\wedge(Q\wedge R)\equiv(P\wedge Q)\wedge R$

§1-2 Condictionals and Biconditionals

Def1: Given two propositions P and Q,

conditional: If P, then Q. (also, P implies Q), write $P\Longrightarrow Q$, in this case, $P\Longrightarrow Q$ is T exactly when P is F or Q is T

P is the hypothesis, and Q is the conclusion.

biconditional: P if and only if Q (as P iff Q), write $P\Longleftrightarrow Q$, in this case, $P\Longleftrightarrow Q$ is T exactly when P and Q have the same truth table.

Def2: (a) $Q\Longrightarrow P$ is called the converse of $P\Longrightarrow Q$

(b) $\sim Q\Longrightarrow\sim P$ is called the contrapositive of $P\Longrightarrow Q$

Thm3: (a) $P\Longrightarrow Q\equiv\sim P\vee Q$ (e) $P\Longleftrightarrow Q\equiv(P\Longrightarrow Q)\wedge(Q\Longrightarrow P)$

(b) $\sim(P\Longrightarrow Q)\equiv P\wedge\sim Q$ (f) $P\Longrightarrow(Q\Longrightarrow R)\equiv(P\wedge Q)\Longrightarrow R$

(c) $\sim(P\wedge Q)\equiv P\Longrightarrow\sim Q$ (g) $P\Longrightarrow(Q\wedge R)\equiv(P\Longrightarrow Q)\wedge(P\Longrightarrow R)$

(d) $\sim(P\wedge Q)\equiv Q\Longrightarrow\sim P$ (h) $(P\vee Q)\Longrightarrow R\equiv(P\Longrightarrow R)\wedge(Q\Longrightarrow R)$

Rmk4: (Some phases in English)

(1) $P\Longrightarrow Q$: If P then Q; P implies Q; Q, if P; Q, when P. P is sufficient for Q, Q is necessary for P.

(2) $P\Longleftrightarrow Q$: P iff Q; P is equivalent to Q; P is necessary and sufficient for Q.

Note: The connective $\sim,\wedge,\vee,\Longrightarrow,\Longleftrightarrow$ are always applied in the order listed.

Example I

(1) $P\Longrightarrow\sim Q\vee R\Longleftrightarrow S$ is $(P\Longrightarrow((\sim Q)\vee R))\Longleftrightarrow R$

(2) $P\Longrightarrow Q\Longrightarrow R$ is $(P\Longrightarrow Q)\Longrightarrow R$

§1-3 Quantified Statements

Two symbols: There exists: $\exists$; for all: $\forall$

Def1: A open sentence (proposition function) is an assertion with one or more variables chosen from a domain S.

e.g. $P(x): x^2<5, x\in\mathbb{N}$ (open sentence with one variable.

For the domain $\mathbb{N}$, the truth set of $P(x)$ is $\{1,2\}$

For the domain $\mathbb{Z}$, the truth set of $P(x)$ is $\{-2,-1,0,1,2\}$

For the domain $\mathbb{R}$, the truth set of $P(x)$ is $(-\sqrt{5}, \sqrt{5})$

Note: Let $P(x)$ be an open sentence over a domain S. Adding the phase "For all $x \in S$" to $P(x)$ propositions (quantified statement)

eg. For all $x \in \mathbb{R}$, $\underbrace{x^2 \geq 0}_{P(x)}$ (T)

Def 2: Given an open sentence $P(x)$,

(1) $\exists$: There exists or For some. $(\exists x)P(x)$: There exists x such that $P(x)$ or For some x, $P(x)$.

$(\exists x)P(x)$ is T if the truth set of $P(x)$ is nonempty.

(2) $\forall$: For all or For every. $(\forall x)P(x)$: For all x, $P(x)$ or For every x, $P(x)$

$(\forall x)P(x)$ is T if the truth set of $P(x)$ is entire domain.

(3) $\exists!$: There is a unique. $(\exists! x)P(x)$: There is a unique x such that $P(x)$.

$(\exists!)P(x)$ is T if the truth set of $P(x)$ has exactly one element

Example I

(1) $(\forall x)(x+2>1)$ ($\mathbb{N}$) (this is, $\forall x \in \mathbb{N}, x+2>1$) (T)

(2) $(\exists! x)$ (x is even and x is prime) ($\mathbb{N}$) (T)

(3) $(\exists x)(x \geq 3 \wedge x^2 = -1)$ ($\mathbb{R}$) (F)

Rmk 3. (1) All $P(x)$ are $Q(x) \equiv (\forall x)(P(x) \Rightarrow Q(x))$

(2) Some $P(x)$ are $Q(x) \equiv (\exists x)(P(x) \wedge Q(x))$

Assume that U: All fruits (Domain), $P(x)$: x is an apple. $Q(x)$: x has a worm.

(hypothesis) (conclusion)
(1) All apples have worms. $\equiv \forall x \in U, P(x) \Rightarrow Q(x)$

(2) Some apples have worms $\equiv \exists x \in U, P(x) \wedge Q(x)$

Example II

(1) For every odd prime x less than 10, x^2+4 is prime.

$\equiv (\forall x)(x \text{ is prime} \wedge x \text{ is odd} \wedge x<10 \Rightarrow x^2+4 \text{ is prime})$

(2) some real numbers have a multiplicative inverse.

$\equiv (\exists x)(x \text{ is a real number} \wedge x \text{ has a real multiplicative inverse})$

$\equiv (\exists x)(x \in \mathbb{R} \wedge (\exists y)(y \in \mathbb{R} \wedge x \cdot y = 1))$

(3) some integers are and some integers are odd.

$\equiv(\exists x)(x \text{ is even}) \wedge (\exists x)(x \text{ is odd})$

$\equiv(\exists x)(x \text{ is even}) \wedge (\exists y)(y \text{ is odd})$

$\not\equiv(\exists x)(x \text{ is even} \wedge x \text{ is odd})$

Def4: The quantified open sentences are equivalent if they are "$\Leftrightarrow$" in every domain.

Example IV

$(\forall x)[(x>3) \Leftrightarrow ([0,\infty)] \Leftrightarrow (\forall x)(x \geq 4) \Leftrightarrow ([0,\infty))$

$(\forall x)(x>3) \Leftrightarrow ((3.1,\infty)) \not\Leftrightarrow (\forall x)(x \geq 4) \Leftrightarrow ((3.1,\infty))$

$\therefore (\forall x)(x>3)$ not equivalent to $(\forall x)(x \geq 4)$

Thm5: Let $A(x)$ be an open sentence with variable x.

Then (a) $\sim(\forall x)A(x)$ is equivalent to $(\exists x)\sim A(x)$

(b) $\sim(\exists x)A(x)$ is equivalent to $(\forall x)\sim A(x)$

Pf: (a) Let $\mathcal{U}$ be any domain.

$\sim(\forall x)A(x)$ is T in $\mathcal{U}$

$\Leftrightarrow (\forall x)A(x)$ is F in $\mathcal{U}$

$\Leftrightarrow$ the truth set of $A(x)$ is not the domain $\mathcal{U}$

$\Leftrightarrow$ the truth set of $\sim A(x)$ is nonempty

$\Leftrightarrow (\exists x)\sim A(x)$ is T in $\mathcal{U}$.

Example V

(1) ~Every positive number has a multiplicative inverse

$\Leftrightarrow \sim(\forall x)(x>0 \Rightarrow (\exists y)(xy=1))(\mathbb{R})$

$\Leftrightarrow \sim \forall x \in \mathbb{R}(x>0 \Rightarrow (\exists y \in \mathbb{R})(xy=1))$

$\Leftrightarrow \exists x \in \mathbb{R} \sim (x>0 \Rightarrow (\exists y \in \mathbb{R})(xy=1))$

$\Leftrightarrow \exists x \in \mathbb{R}(x>0 \wedge (\forall y \in \mathbb{R})(xy \neq 1))$

(2) $\sim \lim_{x \to 2} \frac{1}{x} = \frac{1}{2}$

$\Leftrightarrow$ ~ For every number $\varepsilon>0$

$\Leftrightarrow$ ~ For every number $\varepsilon>0$, there is a number $\delta>0$, s.t. for every $x\in\mathbb{R}$, if $0<|x-2|<\delta$, then $|\frac{1}{x}-\frac{1}{2}|<\varepsilon$

$\Leftrightarrow \sim(\forall\varepsilon>0, \exists\delta>0, \forall x\in\mathbb{R}, 0<|x-2|<\delta \Rightarrow |\frac{1}{x}-\frac{1}{2}|<\varepsilon)$

$\Leftrightarrow(\exists\varepsilon>0, \forall\delta>0, \exists x\in\mathbb{R}, 0<|x-2|<\delta \wedge |\frac{1}{x}-\frac{1}{2}|\geq\varepsilon)$

Thm 6: Let $P(x)$ be an open sentence with variable x.

Then (1) $(\exists!x)P(x)\Rightarrow(\exists x)P(x)$

(2) $(\exists!x)P(x)$ is equivalent to $\underbrace{(\exists x)P(x)}_{\text{existence}}\wedge\underbrace{(\forall y)(\forall z)(Py=Pz\Rightarrow y=z)}_{\text{uniqueness}}$

§1-4, 1-5 Basic Proof Methods.

Give two proposition (or opensentence) P, Q, show that "$P\Rightarrow Q$" (or "$P\Leftrightarrow Q$")

(I) Direct Proof of $P\Rightarrow Q$:

Assume P,

⋮

Therefore, Q

Thus, $P\Rightarrow Q$

Example I

Let $x\in\mathbb{R}$. Prove that if $x^2<1$ (P), $\Rightarrow$ then $x^2-7x>-10$ (Q)

Pf: Assume $x^2\leq 1$ (P), then $-1\leq x\leq 1$, then $x<5$ and $x<2$ Idea: $x^2-7x>-10 \Leftrightarrow x^2-7x+10>0 \Leftrightarrow (x-2)(x-5)>0$

Hence, $x-5<0$ and $x-2<0$, thus $(x-5)(x-2)>0$ $\Leftrightarrow (x-2)<0\wedge(x-5)<0$ or $(x-2)>0\wedge(x-5)>0$

Hence, $x^2-7x+10>0$, and this is $x^2-7x>-10$ (Q)

Example II

Let $a,b,c\in\mathbb{Z}$. Prove that if $a|b$ and $b|c$, then $a|c$.

Pf: Let $a,b,c\in\mathbb{Z}$

Assume $a|b$ and $b|c$

Then $b=ak$ and $c=bm$ for some $k,m\in\mathbb{Z}$

Then, $c=bm=(ak)m=a(km)$ for some $k, m\in\mathbb{Z}$

Since k and m are integers, we have $km\in\mathbb{Z}$

Thus, a|c

Rmk 1: (1) $P \Rightarrow (Q \wedge R) \equiv (P \Rightarrow Q) \wedge (P \Rightarrow R)$

(2) $(P \vee Q) \Rightarrow R \equiv (P \Rightarrow R) \wedge (Q \Rightarrow R)$

(3) $P \Rightarrow (Q \vee R) \equiv (P \Rightarrow Q) \vee (P \Rightarrow R) \equiv (P \wedge \sim R) \Rightarrow Q \equiv (P \wedge \sim R) \Rightarrow Q$

(4) $P \Rightarrow Q \Rightarrow R \equiv (P \wedge Q) \Rightarrow R$

Example III

Suppose n is an odd integer. Then $n = 4j+1$ for some $j \in \mathbb{Z}$, or $n = 4i-1$ for some $i \in \mathbb{Z}$

Pf: Suppose n is odd.

Then $n = 2m+1$ for some $m \in \mathbb{Z}$

Case 1: If m is even, then $m = 2j$ for some $j \in \mathbb{Z}$, and so $2(2j)+1 = 4j+1$

Case 2: If m is odd, then $m = 2k+1$ for some $k \in \mathbb{Z}$, and so $2(2k+1)+1 = 4k+3 = 4(k+1)-1 = 4i-1$

(III) Contrapositive proof of $P \Rightarrow Q$ (Indirect Proof)

Pf: Assume $\sim Q$

⋮

Therefore $\sim P$

Thus, $\sim Q \Rightarrow \sim P$

Thus, $P \Rightarrow Q$

Example IV

Let $x, y > 0$ with $x - 4y < y - 3x$. Prove that if $\overset{P}{3x > 2y}$, then $\overset{Q}{12x^2 + 10y^2 < 24xy}$

Pf: Assume $12x^2 + 10y^2 \geq 24xy$

Since $xy > 0$, then $24xy > 23xy$

This is $0 < 12x^2 - 23xy + 10y^2 = (4x-5y)(3x-2y)$

Since $x - 4y < y - 3x$, $4x - 5y < 0$

Hence, $3x - 2y < 0$.

Thus $3x - 2y < 0$ so $3x \leq 2y$

Hence, if $3x > 2y$, then $12x^2 + 10y^2 < 24xy$

(III) Contradiction proof of $P \Rightarrow Q$ (Indirect proof)

To prove $P \Rightarrow Q$, assume $P \wedge \sim Q$, show that $P \wedge \sim Q$ is impossible.

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

Pf: Assume $\sim P$

⋮

Therefore, Q

⋮

Therefore, $\sim Q$

Hence, $Q \wedge \sim Q$ a contradiction (write $\rightarrow\!\!\!\!\times$)

Thus, P.

Example V

The set of prime is infinite.

Pf: Suppose the set of prime is finite.

Let $P_1, P_2, \cdots, P_n$ be all primes.

Let $n = (P_1 \cdot P_2 \cdots P_n) + 1$

Then $n > 1$, and $n \in \mathbb{N}$, so n has a prime devisor q

Since q is prime, $\overset{Q}{q > 1}$.

Since $P_1, P_2, \cdots, P_n$ are all primes, $q \in \{P_1, P_2, \cdots, P_n\}$

Thus, $q \mid P_1 P_2 \cdots P_k$.

Since $q \mid n$, $q \mid (n - P_1 P_2 \cdots P_n)$. This is $q \mid 1$.

Hence, $\overset{\sim Q}{q = 1}$ ($\rightarrow\!\!\!\!\times$)

Thus, the set of prime is infinite.

Example VI

Let $x, y > 0$ with $x - 4y < y - 3x$. Prove that if $\overset{P}{3x > 2y}$, then $\overset{Q}{12x^2 + 10y^2 < 24xy}$

Pf: Assume $\overset{P}{3x > 2y}$ and $\overset{\sim Q}{12x^2 + 10y^2 \geq 24xy}$

Then $4x - 5y < 0$ and $3x - 2y > 0$

So, $0 > (4x - 5y)(3x - 2y) = 12x^2 - 23xy + 10y^2$

Then, $12x^2+10y^2<23xy$

But $12x^2+10y^2 \geq 24xy > 23xy$ ($\because x,y>0$) $\longrightarrow\!\!\!\!\leftarrow$

Thus, if $3x>2y$, then $12x^2+10y^2<24xy$

(IV) Proof by cases

Example VII

Let x be a real number. Prove that $-|x| \leq x \leq |x|$

Pf: Case1: Suppose $x \geq 0$, $x=|x|$

Since $x \geq 0$, $-x \leq x$, then $-x \leq x \leq x$

So, $-|x| \leq x \leq |x|$

Case2: Suppose $x<0$, $x=|-x|$

Since $x<0$, $x \leq -x$

Then $x \leq x \leq -x$ (this is $-(-x) \leq x \leq -x$)

So, $-|x| \leq x \leq |x|$.

Thus in all cases, $-|x| \leq x \leq |x|$

(V) Two part proof of $P \Longleftrightarrow Q$

Pf: (1) Show $P \Longrightarrow Q$

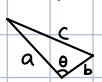
(2) Show $Q \Longrightarrow P$

Therefore, $P \Longleftrightarrow Q$

(VI) Biconditional proof of $P \Longleftrightarrow Q$

Pf: $P \Longleftrightarrow R_1 \Longleftrightarrow R_2 \Longleftrightarrow \cdots \Longleftrightarrow R_n \Longleftrightarrow Q$

Example VIII



Prove that the triangle is a right angle with hypothenuse $\Longleftrightarrow a^2+b^2=c^2$

Pf: By the law of consines, $a^2+b^2=c^2-2ab\cos\theta$, where $\theta (0<\theta<\pi)$ is the angle between the sides of a and b.

Hence, $a^2+b^2=c^2 \Longleftrightarrow 2ab\cos\theta=0 \Longleftrightarrow \cos\theta=0 \Longleftrightarrow \theta=\frac{\pi}{2} \Longleftrightarrow$ A right triangle with hypothenuse C.

§1-6 Proofs Involving Quantifiers

(I) Proof of $(\forall x)P(x)$ [U] domain

(A) Direct Proof

Pf: Given any x in the domain U

⋮

Hence, $P(x)$ is T.

Thus, $\forall x \in U$, $P(x)$ is T.

Thm1: If $a,b,c \in \mathbb{Z}$, $c|a$ and $c|b$, then $c|(ax+by)$ for all $x,y \in \mathbb{Z}$

Pf: Let $a,b,c \in \mathbb{Z}$

Suppose that $c|a$ and $c|b$. We want to claim "$\forall x,y \in \mathbb{Z}$, $c|(ax+by)$"

Since $c|a$ and $c|b$, $\exists k,m \in \mathbb{Z}$ s.t. $a=ck$ and $b=c$

Given any $x,y \in \mathbb{Z}$, we have $ax+by=(ck)x+(cm)y=c(kx+my)$

Since $kx+my \in \mathbb{Z}$ $c|(ax+by)$

Thus $\forall x,y \in \mathbb{Z}$, $c|(ax+by)$ #

(B) Proof by contradiction

Pf: Suppose $\sim(\forall x)P(x)$ [U]

Then $(\exists x)\sim P(x)$ [U]

Let $t \in U$ s.t. $\sim P(t)$

⋮

Thus, $Q \wedge \sim Q$ —×—

Thus, $(\exists x)\sim P(x)$ [U] is F, so $(\forall x)P(x)$ [U] is T.

Example I

Prove that $\forall x \in (0, \frac{\pi}{2})$, $\underbrace{\sin x + \cos x > 1}_{P(x)}$

Pf: Suppose $\exists t \in (0, \frac{\pi}{2})$ s.t. $\sin t + \cos t \leq 1$

Since $\forall x \in (0, \frac{\pi}{2})$, $\sin x > 0$ and $\cos x > 0$, we have $\sin t \cos t > 0$ and $0 < \sin t + \cos t \leq 1$

$0 < (\sin t + \cos t)^2 \leq 1^2 = 1 \Rightarrow 0 < \sin^2 t + \cos^2 t + 2\sin t \cos t \leq 1 \Rightarrow 0 < 1 + 2\sin t \cos t \leq 1$

$\Rightarrow -1 < 2\sin t \cos t \leq 0 \Rightarrow \sin t \cos t < 0$ —×—

Thus, $\forall x \in (0, \frac{\pi}{2})$, $\sin x + \cos x > 1$.

(II) Proof of $(\exists x)P(x)$ (U)

(A) Constructive proof (Direct proof)

Pf: Find $t \in U$ s.t. $P(t)$ is T.

Example II

There is an even prime natural

Pf: $2 \in \mathbb{N}$, prime, even #

(B) Indirect proof

Pf: Look for facts that imply that $\exists t \in U$ s.t. $P(t)$ is T.

Example III

Prove $r(x) = x^5 + x^2 - 1$ has a real zero (this is, $\exists x \in \mathbb{R}, r(x) = 0$)

Pf: We have $r(x)$ is continuous in $\mathbb{R}$ and $r(0) = -1 < 0$, $r(1) = 1 > 0$

By the Intermediate Value Theorem, $\exists t \in (0,1)$ s.t. $r(t) = 0$

(C) Proof by contradiction

Pf: Suppose $\sim(\exists x)P(x)$

Then $(\forall x) \sim P(x)$

⋮

Thus $Q \wedge \sim Q$ ⟶✕

Hence, $\sim(\exists x)P(x)$ is F. So, $(\exists x)P(x)$ is T.

Example IV

Let S be a set of 6 positive integers each less than or equal to 10.

Prove that $\exists$ a pair x, y in S s.t. $x + y = 11$

Pf: Suppose $\nexists x, y \in S$ s.t. $x + y = 11$

Then S may contain at most one element from each the sets

$\{1, 10\}$, $\{2, 9\}$, $\{3, 8\}$, $\{4, 7\}$, and $\{5, 6\}$

Thus, S contains at most 5 elements ⟶✕

Hence, $\exists x,y\in S$ s.t. $x+y=11$ #

(III) Proof of $(\exists!x)P(x)(U)$

Pf: (i) Prove that $(\exists x)P(x)(U)$ (existence, use (II)(A)(B)(C))

(ii) Prove that $(\forall y)(\forall z)(P(y)=P(z)\Rightarrow y=z)$ uniqueness

Assume that $y,z\in U$ s.t. $P(y)=P(z)$ are T

⋮

Thus $y=z$.

From (i) and (ii) $(\exists!x)(P(x))(U)$ is T

Example V

Prove that every nozero real number has a unique multiplicative inverse.

(that is, $(\forall x\in\mathbb{R})(x\neq 0\Rightarrow(\exists!y\in\mathbb{R})(xy=1))$)

Pf: (i) (existence)

Since $x\neq 0$, choose $y=\frac{1}{x}\in\mathbb{R}$. Then $x\cdot y=x\cdot\frac{1}{x}=1$

Hence, x has a multiplicative inverse.

(ii) uniqueness

Suppose that $w,z\in\mathbb{R}$ s.t. $x\cdot w=1$ and $x\cdot z=1$

Then $xw=xz\Rightarrow(xw-xz)=0\Rightarrow(w-z)x=0$

Since $x\neq 0$, $w-z=0$, so $w=z$

Def2: A consructive proof of $(\exists x)\sim P(x)$ names an object t in the domain s.t. $P(x)$ is F.

The object t is called a counterexample to $(\forall x)P(x)$

Example VI

$f(x)=|x|$ is a counterexample for "Every function that is continuous on 0 is differenciable at 0"

Thm3: Between any two rational number x and y there is a rational number z.

Pf: WLOG, we may assume that $x<y$.

Want to claim "$(\forall x\in\mathbb{Q})(\forall y\in\mathbb{Q})(x<y)\Rightarrow(\exists z\in\mathbb{Q})(x<z<y)$"

Since $x,y\in\mathbb{Q}$ write $x=\frac{p}{q}$, and $y=\frac{s}{t}$ for some $p,q,s,t\in\mathbb{Z}$, and $q,t\neq 0$

Choose $z=\frac{x+y}{2}$, then $z=\frac{x+y}{2}=\frac{1}{2}(\frac{p}{q}+\frac{r}{s})=\frac{1}{2}(\frac{ps+qr}{qs})=\frac{ps+qr}{2qs}$

Suppose $ps+qr, 2qs\in\mathbb{Z}$, and $2qs\neq 0$, we have $z\in\mathbb{Q}$

Moreover, $x=\frac{x+x}{2}<\frac{x+y}{2}=z<\frac{y+y}{2}=y$, so $x<z<y$

Note: (1) $(\forall x)(\forall y)P(x,y)\Leftrightarrow(\forall y)(\forall x)P(x,y)$

(2) $(\exists x)(\exists y)P(x,y)\Leftrightarrow(\exists y)(\exists x)P(x,y)$

(3) $((\forall x)P(x)\vee(\forall x)Q(x))\Rightarrow(\forall x)(P(x)\vee Q(x))$

(4) $(\forall x)(P(x)\Rightarrow Q(x))\Rightarrow((\forall x)P(x)\Rightarrow(\forall x)Q(x))$

(5) $(\forall x)(P(x)\wedge Q(x))\Leftrightarrow((\forall x)P(x)\wedge(\forall x)Q(x))$

(6) $(\exists x)(\forall y)P(x,y)\Rightarrow(\forall y)(\exists x)P(x,y)$

Example VII

Show by example that (3), (4), (6) "$\Leftarrow$" are not valid.

(4): $P(x)$: x is odd. $Q(x)$: x is even

$((\forall x\in\mathbb{Z})P(x)\overset{T}{\Rightarrow}(\forall x\in\mathbb{Z})Q(x))\not\Rightarrow(\forall x\in\mathbb{Z})(P(x)\overset{F}{\Rightarrow}Q(x))$

§1-8 Proofs from Number Theory

Thm1: The Division Algorithm

Suppose $a,b\in\mathbb{Z}$ and $a\neq 0$. Then $\exists!\, q,r\in\mathbb{Z}$ s.t. $b=aq+r$ with $0\leq r<|a|$

Pf: See 2-5 (In this case, if $0<a\leq b$, then $q\in\mathbb{N}$)

Def2: Let $a,b\in\mathbb{Z}$, and $a\neq 0$. The integer d is the greatest common divisor of a and b, write $d=\gcd(a,b)$ if

(i) $d|a$ and $d|b$

(ii) $c|a$ and $c|b\Rightarrow c\leq d$

Thm3: Let $a,b\in\mathbb{Z}$, and $a\neq 0$.

Then $\gcd(a,b)$ is the smallest positive linear combinations of a and b (the form $ax+by$, where $x,y\in\mathbb{Z}$)

e.g. $\gcd(12,18)=6$, $12(-1)+18(1)=6\leq 12x+18y$ if $12x+18y>0$ for some $x,y\in\mathbb{Z}$

Pf: Let $d=as+bt$ be the smallest linear combination of a and b.

Want to claim "$d=\gcd(a,b)$"

(i) Claim that $d|a$ and $d|b$:

By the Division Algorithm, $\exists q, r \in \mathbb{Z}$ s.t. $a = dq + r$, $0 \le r < d$

Then $r = a - dq = a - (as+bt)q = a - asq - btq = a(1-sq) + b(-tq)$ (linear combination of a,b)

But $0 \le r < d$ and d is the smallest positive linear combination

Hence, $r = 0$.

This is $a = dq$, so $d|a$.

Replacing a by b, similarly, $d|b$

Thus $d|a$ and $d|b$.

(ii) Claim that $c|a$ and $c|b \Rightarrow c \le d$

Suppose $c|a$ and $c|b$, by I-6 Thm1, $c|d$.

Since $d > 0$, we get $c \le d$

By (i) and (ii), $d = \gcd(a,b)$ #

Lemma4: Let $a,b \in \mathbb{N}$, if $b = aq + r$ for some $q, r \in \mathbb{Z}$, then $\gcd(a,b) = \gcd(r,a)$

Pf: Let $d = \gcd(a,b)$ and $e = \gcd(r,a)$

Want to claim "$d = e$"

The case $e \le d$:

Since $b = aq + r$ and $e|r$, $e|a$, we have $e|(aq+r)$

Thus, $e|b$.

Then $e|b$ and $e|a$. So $e \le \gcd(a,b) = d$

The case $e \ge d$:

We have $b = aq + r \Rightarrow r = b - aq$

Since $d = \gcd(a,b)$, we have $d|(b - aq) \Rightarrow d|r$

Thus, $d|a$ and $d|r$, so $d \le \gcd(r,a) = e$

Thus, $d = e$.

Thm5: (Euclid's Algorithm)

Let $a,b\in\mathbb{N}$ with $a\le b$.

Then there exist two list of positive integers $q_1,q_2,\cdots,q_{k+1}$ and $r_1,r_2,\cdots,r_{k+1}$ such that

(i) $a>r_1>r_2>\cdots>r_k>0$

(ii) $b=aq_1+r_1$

$a=r_1q_2+r_2$

$r_1=r_2q_3+r_3$

$r_2=r_3q_4+r_4$

$\vdots$

$r_{k-1}=r_kq_{k+1}+r_{k+1}$ (this is $r_{k+1}=0$)

Moreover, $\gcd(a,b)=r_k$

Pf: By the Divison Algorithm, for $0<a\le b$, $\exists q_1\in\mathbb{N}, r_1\in\mathbb{Z}$ such that $b=aq_1+r_1$, $0\le r_1<a$

If $r_1=0$, the lists are done.

If $0<r_1<a$, $\exists q_2\in\mathbb{N}$, $r_2\in\mathbb{Z}$ such that $a=r_1q_2+r_2$, $0\le r_2<r_1$

If $r_2=0$, the lists are done.

If $0<r_2<r_1$, $\exists q_3\in\mathbb{N}$, $r_3\in\mathbb{Z}$ such that $r_1=r_2q_3+r_3$, $0\le r_3<r_2$

Continuing in this fashion, we get a decreasing sequence of nonnegative integers $r_1>r_2>r_3>\cdots$

The list must end, so there exists an integer k such that $r_{k+1}=0$

Thus $a>r_1>r_2>\cdots>r_k>r_{k+1}=0$

Finally, we claim that $r_k=\gcd(a,b)$

By Lemma4, $\gcd(a,b)=\gcd(a,r_1)=\gcd(r_1,r_2)=\cdots=\gcd(r_k,r_{k-1})=\gcd(r_k,0)=r_k$

Example I

Find $\gcd(32,12)$.

Sol: $32=12\times2+8\Rightarrow12=8\times1+4\Rightarrow8=4\times2+0$

Then $\gcd(32,12)=4$

Example II

Write $\gcd(44,104)$ as a linear combination of 44 and 104.

Use Euclids Algorithm to find $\gcd(44,104)$.

$104=44\times2+16\Rightarrow16=104-44\times2$ ——(3)

$44 = 16\times2 + 12 \Rightarrow 12 = 44 - 16\times2$ —— (2)

$16 = 12\times1 + 4 \Rightarrow 4 = 16 - 12\times1$ —— (1)

$12 = 4\times3 + 0$ gcd(44, 104)

By (1) and (2), $4 = 16 - (44 - 16\times2) = 16\times3 - 44$ —— (4)

By (3) and (4), $4 = (104 - 44\times2)\times3 - 44 = 104\times3 + 44\times(-7)$

Def4: We say that nozero integers a and b are relatively prime or coprime if gcd(a,b) = 1

Lemma5: (Euclid's Lemma)

Let $a, b, p \in \mathbb{Z}$. If p is prime and $p \mid (ab)$, then $p \mid a$ or $p \mid b$.

Pf: Suppose that p is prime and $p \mid (a \cdot b)$

Assume that $p \nmid a$. Then gcd(p, a) = 1 (a, p are coprime)

Thus $\exists s, t \in \mathbb{Z}$ s.t. $as + pt = 1 \Rightarrow b(as + pt) = b \Rightarrow b = bas + bpt$

Since $p \mid (ab)$, we have $p \mid (abs)$ and so $p \mid (abs + bpt)$

This is $p \mid b$.

Thus, $p \mid a$ or $p \mid b$.

Rmk6: Let $a, b, p \in \mathbb{Z}$ and p be prime:

Euclid's Lemma $\Leftrightarrow$ If $p \mid (a, b)$ and $p \nmid a$, then $p \mid b$. (by $(r \Rightarrow (q \vee s)) \Leftrightarrow ((r \wedge \sim q) \Rightarrow s)$)

$\Leftrightarrow$ If $p \nmid a$ and $p \nmid b$ then $p \nmid (ab)$ (by $r \Rightarrow q \Leftrightarrow (\sim q \Rightarrow \sim r)$)