Module 8

Methods of Proof: Contradiction

Indirect

Proof by Contradiction $\neg P \rightarrow F_0$

We want to prove P :

Proof by contrations.

1. Claim $\neg P$
2. Begin a direct proof of $\neg P$
3. Real goal : end up with two contradictory statements.

   i) q
   ⋮
   v) $\neg q$
4. Recognise contradition $(q \wedge \neg q) \Rightarrow F_0$
5. Conclusion : Because $\neg P \Rightarrow F_0$, P is true.

<u>Ex 1</u>: Prove $\sqrt{2}$ is irrational $P : \sqrt{2} \notin \mathbb{Q}$ ← Set of rational numbers (p/q)

<u>Proof by contradition:</u>

(i) $\sqrt{2} \in \mathbb{Q}$	Premise.
(ii) $\exists p, q \in \mathbb{Z}$ such that $\sqrt{2} = p/q$	defination of $\mathbb{Q}$
(iii) p/q is irreducible	restriction
(iv) $2 = p^2/q^2$	(ii), algebra
(v) $2q^2 = p^2$	algebra
(vi) $\underline{p^2 \in \mathbb{Z}_E}$, therefore $p \in \mathbb{Z}_E$	(v), defination of even $(\mathbb{Z}_E)$
(vii) Let $K \in \mathbb{Z}$	define
(viii) $p = 2K$	(vi), (vii), algebra
(ix) $2q^2 = (2K)^2$	(viii), (v), substitution
(x) $2q^2 = 4K^2$	algebra

Ex 2. Prove no integer is both even and odd.

(xi) $q^2 = 2K^2$ — algebra

(xii) $q^2 \in \mathbb{Z}_E$, therefore $q \in \mathbb{Z}_E$ — algebra

(xiii) P/q is reducible — (vi), (xii)

(xiv) P/q is reducible $\wedge$ P/q is irreducible — (iii), (xiii) Contradiction.

Conclusion, $\neg \mathbb{P} \Rightarrow F_0$

Therefore $\mathbb{P}$ is true.

Ex 2. Prove no Integer is both even and odd

Ex2: Prove there is an infinite number of even integers.

$P: \forall n \in \mathbb{Z}, \neg(n \in \mathbb{Z}_E \wedge n \in \mathbb{Z}_O)$

Proof by Contradition :

$\neg P: \neg(\forall n \in \mathbb{Z}, \neg(n \in \mathbb{Z}_E \wedge n \in \mathbb{Z}_O))$

$: \exists n, n \in \mathbb{Z}_E \wedge n \in \mathbb{Z}_O$

(i) $n \in \mathbb{Z}_E$ — Primise

(ii) $n \in \mathbb{Z}_O$ — Primise

(iii) Let $k_1, k_2 \in \mathbb{Z}$ — define

(iv) $n = 2k_1$, $n = 2k_2 + 1$ — (i), (ii), defination of odd and even

(v) $2k_1 = 2k_2 + 1$ — equality.

Ex 2. Prove no Integer is both even and odd

Ex 2: Prove there is an infinite number of even integers.

Assume:

$p, q \in \mathbb{Z}$

$p-q \in \mathbb{Z}$

(vi) $2k_1 - 2k_2 = 1$ — algebra

(vii) $2(k_1 - k_2) = 1$ — algebra, factoring

(viii) $k_1 - k_2 = 1/2$ — algebra

(ix) $k_1 - k_2 \in \mathbb{Z}$, $k_1 - k_2 = 1/2 \notin \mathbb{Z}$ — (iii), (viii), $k_1, k_2 \in \mathbb{Z}$, $k_1 - k_2 \in \mathbb{Z}$

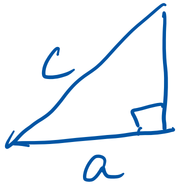
Conclusion: $\neg \mathbb{P} \Rightarrow F_0$

Therefore, $\mathbb{P}$ is true.

Ex 3: **Prove the hypotenuse of a right triangle is less than the sum of the lengths of the other two sides.**

$\mathbb{P}: \forall a,b,c \in \mathbb{R}^+$ such that $a^2+b^2=c^2$, $c < a+b$

Assumptions: Pyth. Theorem



$\Rightarrow c^2 = a^2+b^2$

a, b are the legs of right Δ and c is the hypotunuse

Proof by Condradiction:

$\neg\mathbb{P}: \exists a,b,c \in \mathbb{R}^+$ such that $a^2+b^2=c^2$, $c \geq a+b$

(i) $a,b,c \in \mathbb{R}^+$	Premise
(ii) $c \geq a+b$	Premise
(iii) Let $k \in \mathbb{R}$, $k \geq 0$	Defining.
(iv) $c = a+b+k$	def, (ii), (iii)
(v) $c^2 = a^2+b^2$	Pythagores theorem
(vi) $a^2+b^2 = (a+b+k)^2$	(iv), (v), substitution
(vii) $\cancel{a^2}+\cancel{b^2} = \cancel{a^2}+\cancel{b^2}+k^2+2ab+2bk+2ak$	algebra

$(a+b+k)^2$
$= a^2+b^2+k^2+2ab+2ak+2bk.$

Ex 3: **Prove the hypotenuse of a right triangle is less than the sum of the lengths of the other two sides.**

(viii) $0 = k^2 + 2ab + 2bk + 2ak$ algebra

(ix) $a = 0$ or $b = 0$ algebra, assume $k = 0$.

(x) $(a = 0 \vee b = 0) \wedge (a, b) \in \mathbb{R}^+$ (i), (ix), contradition.

Conclusion

$\neg \mathbb{P} \rightarrow F_0$

Therefore, $\mathbb{P}$ is True.

Ex 4: Prove there is an infinite number of even integers.

$\mathbb{P}: |\mathbb{Z}_E| = \infty$ $\qquad$ $\mathbb{P}: \nexists K \in \mathbb{Z}, |\mathbb{Z}_E| = K$.

Proof by contradiction

$\neg \mathbb{P}: \exists K \in \mathbb{Z}, |\mathbb{Z}_E| = K$

(i) because $\mathbb{Z}_E$ is finite, $\exists z_{max}$ largest element of $\mathbb{Z}_E$ $\qquad$ Property of finite sets

(ii) $\forall z \in \mathbb{Z}, (z > z_{max}) \rightarrow z \notin \mathbb{Z}_E$ $\qquad$ defination of max.

(iii) Let $z = z_{max} + 2$ $\qquad$ $\dfrac{\begin{array}{c} p \\ p \to q \end{array}}{q}$ $\qquad$ def^n

(iv) $z > z_{max}$ $\qquad$ (iii), Property of add^n

(v) $\boxed{z \notin \mathbb{Z}_E}$ $\qquad$ (ii), (iv) modus Ponens

(vi) Let $K_{max} \in \mathbb{Z}$, $z_{max} = 2K_{max}$ $\qquad$ (i), defination of even set $\mathbb{Z}_E$.

Ex 4: **Prove there is an infinite number of even integers.**

(vii) $z = 2k_{max} + 2$ — (vi), (iii) substitution.

(viii) $z = 2(k_{max} + 1)$ — (vii), factoring.

(ix) $\boxed{z \in \mathbb{Z}_E}$ — (viii), def^n of $\mathbb{Z}_E$, $k_{max}+1 \in \mathbb{Z}$

(x) $z \notin \mathbb{Z}_E \wedge z \in \mathbb{Z}_E$ — (v), (ix) contradiction.

Conclusion:

$\boxed{\neg P \rightarrow F_0, \text{ P is true.}}$