Introduction to Proof Methods
Part 2:
Indirect Proof Using Contradiction, Equivalent Statements, and Counterexamples

Mathematical Logic – First Term 2022-2023

MZI

School of Computing
Telkom University

SoC Tel-U

December 2022

Acknowledgements

This slide is compiled using the materials in the following sources:

1. *Discrete Mathematics and Its Applications* (Chapter 1), 8th Edition, 2019, by K. H. Rosen (primary reference).
2. *Discrete Mathematics with Applications* (Chapter 4), 5th Edition, 2018, by S. S. Epp.
3. Discrete Mathematics 1 (2012) slides at Fasilkom UI by B. H. Widjaja.
4. Discrete Mathematics 1 (2010) slides at Fasilkom UI by A. A. Krisnadhi.

Some figures are excerpted from those sources. This slide is intended for internal academic purpose in SoC Telkom University. No slides are ever free from error nor incapable of being improved. Please convey your comments and corrections (if any) to `<pleasedontspam>@telkomuniversity.ac.id`.

Contents

Contents

Indirect Proofs by Contradiction

Theorem

There exists no largest integer.

How do we proof above theorem?

Indirect Proofs by Contradiction

Theorem

There exists no largest integer.

How do we proof above theorem? The above statement cannot be proven using direct proof nor indirect proof by contraposition.

Indirect Proofs by Contradiction

Indirect Proofs by Contradiction

Suppose we want to prove that a statement p is true. An indirect proof by contradiction can be used to prove the truth of p in following way:

Indirect Proofs by Contradiction

Suppose we want to prove that a statement p is true. An indirect proof by contradiction can be used to prove the truth of p in following way:

1. first, assume that $\neg p$ is **true**

Indirect Proofs by Contradiction

Suppose we want to prove that a statement p is true. An indirect proof by contradiction can be used to prove the truth of p in following way:

1. first, assume that $\neg p$ is **true**
2. construct subsequent statements using rules of inference until...

Indirect Proofs by Contradiction

Suppose we want to prove that a statement p is true. An indirect proof by contradiction can be used to prove the truth of p in following way:

1. first, assume that $\neg p$ is **true**
2. construct subsequent statements using rules of inference until...
3. we obtain statement r and statement $\neg r$

Indirect Proofs by Contradiction

Suppose we want to prove that a statement p is true. An indirect proof by contradiction can be used to prove the truth of p in following way:

1. first, assume that $\neg p$ is **true**
2. construct subsequent statements using rules of inference until...
3. we obtain statement r and statement $\neg r$
4. as a result, using conjunction rule, we have $r \wedge \neg r$ which is a contradiction

Indirect Proofs by Contradiction

Suppose we want to prove that a statement p is true. An indirect proof by contradiction can be used to prove the truth of p in following way:

1. first, assume that $\neg p$ is **true**
2. construct subsequent statements using rules of inference until...
3. we obtain statement r and statement $\neg r$
4. as a result, using conjunction rule, we have $r \wedge \neg r$ which is a contradiction
5. consequently, we infer that $\neg p \rightarrow (r \wedge \neg r)$ is **true**

Indirect Proofs by Contradiction

Suppose we want to prove that a statement p is true. An indirect proof by contradiction can be used to prove the truth of p in following way:

1. first, assume that $\neg p$ is **true**
2. construct subsequent statements using rules of inference until...
3. we obtain statement r and statement $\neg r$
4. as a result, using conjunction rule, we have $r \wedge \neg r$ which is a contradiction
5. consequently, we infer that $\neg p \rightarrow (r \wedge \neg r)$ is **true**
6. because $\neg p \rightarrow (r \wedge \neg r)$ is **true**, and $(r \wedge \neg r)$ is **false**, we infer that

Indirect Proofs by Contradiction

Suppose we want to prove that a statement p is true. An indirect proof by contradiction can be used to prove the truth of p in following way:

1. first, assume that $\neg p$ is **true**
2. construct subsequent statements using rules of inference until...
3. we obtain statement r and statement $\neg r$
4. as a result, using conjunction rule, we have $r \wedge \neg r$ which is a contradiction
5. consequently, we infer that $\neg p \rightarrow (r \wedge \neg r)$ is **true**
6. because $\neg p \rightarrow (r \wedge \neg r)$ is **true**, and $(r \wedge \neg r)$ is **false**, we infer that $\neg p$ **is false;** since $\neg p$ is **false**, we conclude that p is **true**.

Examples of Indirect Proofs by Contradiction

Theorem

There exists no largest integer.

Proof (Sketch)

Examples of Indirect Proofs by Contradiction

Theorem

There exists no largest integer.

Proof (Sketch)

1. Suppose there exists a largest integer, let's denote this integer by M.

Examples of Indirect Proofs by Contradiction

Theorem

There exists no largest integer.

Proof (Sketch)

1. Suppose there exists a largest integer, let's denote this integer by M.
2. Since M is the largest integer, then $M \geq n$ for all integers n.

Examples of Indirect Proofs by Contradiction

Theorem

There exists no largest integer.

Proof (Sketch)

1. Suppose there exists a largest integer, let's denote this integer by M.
2. Since M is the largest integer, then $M \geq n$ for all integers n.
3. Let $N = M + 1$,

Examples of Indirect Proofs by Contradiction

Theorem

There exists no largest integer.

Proof (Sketch)

1. Suppose there exists a largest integer, let's denote this integer by M.
2. Since M is the largest integer, then $M \geq n$ for all integers n.
3. Let $N = M + 1$, N is an integer (because M and 1 are both integers and the set of integers is closed under addition) and $N > M$.

Examples of Indirect Proofs by Contradiction

Theorem

There exists no largest integer.

Proof (Sketch)

1. Suppose there exists a largest integer, let's denote this integer by M.
2. Since M is the largest integer, then $M \geq n$ for all integers n.
3. Let $N = M + 1$, N is an integer (because M and 1 are both integers and the set of integers is closed under addition) and $N > M$.
4. This contradicts to our supposition that M is the largest integer (number 1). □

Proof

Examples of Indirect Proofs by Contradiction

Theorem

There exists no largest integer.

Proof (Sketch)

1. Suppose there exists a largest integer, let's denote this integer by M.
2. Since M is the largest integer, then $M \geq n$ for all integers n.
3. Let $N = M + 1$, N is an integer (because M and 1 are both integers and the set of integers is closed under addition) and $N > M$.
4. This contradicts to our supposition that M is the largest integer (number 1). □

Proof

Suppose there exists a largest integer M.

Examples of Indirect Proofs by Contradiction

Theorem

There exists no largest integer.

Proof (Sketch)

1. Suppose there exists a largest integer, let's denote this integer by M.
2. Since M is the largest integer, then $M \geq n$ for all integers n.
3. Let $N = M + 1$, N is an integer (because M and 1 are both integers and the set of integers is closed under addition) and $N > M$.
4. This contradicts to our supposition that M is the largest integer (number 1). □

Proof

Suppose there exists a largest integer M. Since M is the largest integer, then $M \geq n$ for all integers n.

Examples of Indirect Proofs by Contradiction

Theorem

There exists no largest integer.

Proof (Sketch)

1. Suppose there exists a largest integer, let's denote this integer by M.
2. Since M is the largest integer, then $M \geq n$ for all integers n.
3. Let $N = M + 1$, N is an integer (because M and 1 are both integers and the set of integers is closed under addition) and $N > M$.
4. This contradicts to our supposition that M is the largest integer (number 1). □

Proof

Suppose there exists a largest integer M. Since M is the largest integer, then $M \geq n$ for all integers n. Let $N = M + 1$,

Examples of Indirect Proofs by Contradiction

Theorem

There exists no largest integer.

Proof (Sketch)

1. Suppose there exists a largest integer, let's denote this integer by M.
2. Since M is the largest integer, then $M \geq n$ for all integers n.
3. Let $N = M + 1$, N is an integer (because M and 1 are both integers and the set of integers is closed under addition) and $N > M$.
4. This contradicts to our supposition that M is the largest integer (number 1). □

Proof

Suppose there exists a largest integer M. Since M is the largest integer, then $M \geq n$ for all integers n. Let $N = M + 1$, N is an integer and $N > M$.

Examples of Indirect Proofs by Contradiction

Theorem

There exists no largest integer.

Proof (Sketch)

1. Suppose there exists a largest integer, let's denote this integer by M.
2. Since M is the largest integer, then $M \geq n$ for all integers n.
3. Let $N = M + 1$, N is an integer (because M and 1 are both integers and the set of integers is closed under addition) and $N > M$.
4. This contradicts to our supposition that M is the largest integer (number 1).

□

Proof

Suppose there exists a largest integer M. Since M is the largest integer, then $M \geq n$ for all integers n. Let $N = M + 1$, N is an integer and $N > M$. This contradicts to our supposition that M is the largest integer. Therefore, there exists no largest integer.

□

Exercise 4

Theorem (Theorem 4.1)

Among 37 people in one group, at least four of them born in the same month.

Theorem (Theorem 4.2)

There is no integer which is even and odd simultaneously.

Proof (Proof of Theorem 4.1)

We have 12 months in a year.

Proof (Proof of Theorem 4.1)

We have 12 months in a year. Suppose the statement that at least four people in the group of 37 people born in the same month is false, then we have

Proof (Proof of Theorem 4.1)

We have 12 months in a year. Suppose the statement that at least four people in the group of 37 people born in the same month is false, then we have at most three people in the group of 37 people born in the same month.

Proof (Proof of Theorem 4.1)

We have 12 months in a year. Suppose the statement that at least four people in the group of 37 people born in the same month is false, then we have at most three people in the group of 37 people born in the same month. Consequently, the number of people in the group is at most

Proof (Proof of Theorem 4.1)

We have 12 months in a year. Suppose the statement that at least four people in the group of 37 people born in the same month is false, then we have at most three people in the group of 37 people born in the same month. Consequently, the number of people in the group is at most $3 \cdot 12 = 36$, which contradicts to the fact that there are 37 people in the group. Therefore, among 37 people in one group, at least four of them born in the same month. □

Proof (Proof of Theorem 4.2)

Proof (Proof of Theorem 4.1)

We have 12 months in a year. Suppose the statement that at least four people in the group of 37 people born in the same month is false, then we have at most three people in the group of 37 people born in the same month. Consequently, the number of people in the group is at most $3 \cdot 12 = 36$, which contradicts to the fact that there are 37 people in the group. Therefore, among 37 people in one group, at least four of them born in the same month. □

Proof (Proof of Theorem 4.2)

Suppose m is an integer which is even and odd simultaneously,

Proof (Proof of Theorem 4.1)

We have 12 months in a year. Suppose the statement that at least four people in the group of 37 people born in the same month is false, then we have at most three people in the group of 37 people born in the same month. Consequently, the number of people in the group is at most $3 \cdot 12 = 36$, which contradicts to the fact that there are 37 people in the group. Therefore, among 37 people in one group, at least four of them born in the same month. $\square$

Proof (Proof of Theorem 4.2)

Suppose m is an integer which is even and odd simultaneously, then there exists integers k and ℓ such that $m = 2k = 2\ell + 1$.

Proof (Proof of Theorem 4.1)

We have 12 months in a year. Suppose the statement that at least four people in the group of 37 people born in the same month is false, then we have at most three people in the group of 37 people born in the same month. Consequently, the number of people in the group is at most $3 \cdot 12 = 36$, which contradicts to the fact that there are 37 people in the group. Therefore, among 37 people in one group, at least four of them born in the same month. $\square$

Proof (Proof of Theorem 4.2)

Suppose m is an integer which is even and odd simultaneously, then there exists integers k and ℓ such that $m = 2k = 2\ell + 1$. Hence, we have $2\,(k - \ell) = 1$, or $k - \ell = \frac{1}{2}$.

Proof (Proof of Theorem 4.1)

We have 12 months in a year. Suppose the statement that at least four people in the group of 37 people born in the same month is false, then we have at most three people in the group of 37 people born in the same month. Consequently, the number of people in the group is at most $3 \cdot 12 = 36$, which contradicts to the fact that there are 37 people in the group. Therefore, among 37 people in one group, at least four of them born in the same month. □

Proof (Proof of Theorem 4.2)

Suppose m is an integer which is even and odd simultaneously, then there exists integers k and ℓ such that $m = 2k = 2\ell + 1$. Hence, we have $2(k - \ell) = 1$, or $k - \ell = \frac{1}{2}$. This cannot be happened because the set of integers is closed under subtraction. Therefore, there is no integer which is even and odd simultaneously. □

Exercise 5

Theorem (Theorem 5)

There is no smallest odd integer.

Proof (Proof of Theorem 5)

Exercise 5

Theorem (Theorem 5)

There is no smallest odd integer.

Proof (Proof of Theorem 5)

Suppose there exists a smallest odd integer M.

Exercise 5

Theorem (Theorem 5)

There is no smallest odd integer.

Proof (Proof of Theorem 5)

Suppose there exists a smallest odd integer M. Then $M = 2k + 1$ for some integer k and $M \leq n$ for all odd integers n.

Exercise 5

Theorem (Theorem 5)

There is no smallest odd integer.

Proof (Proof of Theorem 5)

Suppose there exists a smallest odd integer M. Then $M = 2k + 1$ for some integer k and $M \leq n$ for all odd integers n. Let
$N =$

Exercise 5

Theorem (Theorem 5)

There is no smallest odd integer.

Proof (Proof of Theorem 5)

Suppose there exists a smallest odd integer M. Then $M = 2k + 1$ for some integer k and $M \leq n$ for all odd integers n. Let
$N = M - 2 = 2k - 1 = 2(k - 1) + 1$, N is odd and $N < M$.

Exercise 5

Theorem (Theorem 5)

There is no smallest odd integer.

Proof (Proof of Theorem 5)

Suppose there exists a smallest odd integer M. Then $M = 2k + 1$ for some integer k and $M \leq n$ for all odd integers n. Let $N = M - 2 = 2k - 1 = 2\,(k - 1) + 1$, N is odd and $N < M$. This means N is an odd integer smaller than M, and this contradicts to the assumption that M is the smallest odd integer. Therefore, there is no smallest odd integer. □

$\sqrt{2}$ is irrational

Theorem

$\sqrt{2}$ is irrational.

$\sqrt{2}$ is irrational

Theorem

$\sqrt{2}$ is irrational.

The above theorem means that $\sqrt{2}$ cannot be expressed in the form of $\frac{a}{b}$ where a and b are integers and $b \neq 0$.
To prove above theorem, we first consider following definition and lemmas.

Definition

$\sqrt{2}$ is irrational

Theorem

$\sqrt{2}$ is irrational.

The above theorem means that $\sqrt{2}$ cannot be expressed in the form of $\frac{a}{b}$ where a and b are integers and $b \neq 0$.
To prove above theorem, we first consider following definition and lemmas.

Definition

Suppose a and b are integers, not both zero. The *greatest common divisor* of a and b, denoted by $\gcd(a, b)$, is defined as the largest integer that divides both a and b.

Remark

$\sqrt{2}$ is irrational

Theorem

$\sqrt{2}$ is irrational.

The above theorem means that $\sqrt{2}$ cannot be expressed in the form of $\frac{a}{b}$ where a and b are integers and $b \neq 0$.
To prove above theorem, we first consider following definition and lemmas.

Definition

Suppose a and b are integers, not both zero. The *greatest common divisor* of a and b, denoted by $\gcd(a, b)$, is defined as the largest integer that divides both a and b.

Remark

In Bahasa Indonesia, you may familiar with the terminology FPB (*faktor persekutuan terbesar*).

For example, we have: $\gcd(8, 4) =$

$\sqrt{2}$ is irrational

Theorem

$\sqrt{2}$ is irrational.

The above theorem means that $\sqrt{2}$ cannot be expressed in the form of $\frac{a}{b}$ where a and b are integers and $b \neq 0$.
To prove above theorem, we first consider following definition and lemmas.

Definition

Suppose a and b are integers, not both zero. The *greatest common divisor* of a and b, denoted by $\gcd(a, b)$, is defined as the largest integer that divides both a and b.

Remark

In Bahasa Indonesia, you may familiar with the terminology FPB (*faktor persekutuan terbesar*).

For example, we have: $\gcd(8, 4) = 4$, $\gcd(12, 9) =$

$\sqrt{2}$ is irrational

Theorem

$\sqrt{2}$ is irrational.

The above theorem means that $\sqrt{2}$ cannot be expressed in the form of $\frac{a}{b}$ where a and b are integers and $b \neq 0$.
To prove above theorem, we first consider following definition and lemmas.

Definition

Suppose a and b are integers, not both zero. The *greatest common divisor* of a and b, denoted by $\gcd(a, b)$, is defined as the largest integer that divides both a and b.

Remark

In Bahasa Indonesia, you may familiar with the terminology FPB (*faktor persekutuan terbesar*).

For example, we have: $\gcd(8, 4) = 4$, $\gcd(12, 9) = 3$, $\gcd(-3, -6) =$

$\sqrt{2}$ is irrational

Theorem

$\sqrt{2}$ is irrational.

The above theorem means that $\sqrt{2}$ cannot be expressed in the form of $\frac{a}{b}$ where a and b are integers and $b \neq 0$.
To prove above theorem, we first consider following definition and lemmas.

Definition

Suppose a and b are integers, not both zero. The *greatest common divisor* of a and b, denoted by $\gcd(a, b)$, is defined as the largest integer that divides both a and b.

Remark

In Bahasa Indonesia, you may familiar with the terminology FPB (*faktor persekutuan terbesar*).

For example, we have: $\gcd(8, 4) = 4$, $\gcd(12, 9) = 3$, $\gcd(-3, -6) = 3$, and $\gcd(3, 0) =$

$\sqrt{2}$ is irrational

Theorem

$\sqrt{2}$ is irrational.

The above theorem means that $\sqrt{2}$ cannot be expressed in the form of $\frac{a}{b}$ where a and b are integers and $b \neq 0$.
To prove above theorem, we first consider following definition and lemmas.

Definition

Suppose a and b are integers, not both zero. The *greatest common divisor* of a and b, denoted by $\gcd(a, b)$, is defined as the largest integer that divides both a and b.

Remark

In Bahasa Indonesia, you may familiar with the terminology FPB (*faktor persekutuan terbesar*).

For example, we have: $\gcd(8, 4) = 4$, $\gcd(12, 9) = 3$, $\gcd(-3, -6) = 3$, and $\gcd(3, 0) = 3$.

Lemma (Lemma 6)

If r is a rational number, then r can be expressed in the form of $\frac{a}{b}$ with $\gcd(a, b) = 1$.

For example, $\frac{8}{18}$ can be expressed as

Lemma (Lemma 6)

If r is a rational number, then r can be expressed in the form of $\frac{a}{b}$ with $\gcd(a,b)=1$.

For example, $\frac{8}{18}$ can be expressed as $\frac{4}{9}$, observe that $\gcd(4,9)=1$. The rational number $\frac{a}{b}$ where $\gcd(a,b)=1$ is called the simplest form of such number .

Lemma (Lemma 7)

Let n be an integer, if n^2 is even, then n is even.

Proof

Left as an exercise.

The proof that $\sqrt{2}$ is irrational

Proof (Proof that $\sqrt{2}$ is irrational)

The proof that $\sqrt{2}$ is irrational

Proof (Proof that $\sqrt{2}$ is irrational)

Suppose $\sqrt{2}$ is not irrational,

The proof that $\sqrt{2}$ is irrational

Proof (Proof that $\sqrt{2}$ is irrational)

Suppose $\sqrt{2}$ is not irrational, then $\sqrt{2}$ is rational.

The proof that $\sqrt{2}$ is irrational

Proof (Proof that $\sqrt{2}$ is irrational)

Suppose $\sqrt{2}$ is not irrational, then $\sqrt{2}$ is rational. Therefore (according to Lemma 6) there exists integers a and b with $b \neq 0$ and $\gcd(a, b) = 1$ such that $\frac{a}{b} = \sqrt{2}$.

The proof that $\sqrt{2}$ is irrational

Proof (Proof that $\sqrt{2}$ is irrational)

Suppose $\sqrt{2}$ is not irrational, then $\sqrt{2}$ is rational. Therefore (according to Lemma 6) there exists integers a and b with $b \neq 0$ and $\gcd(a, b) = 1$ such that $\frac{a}{b} = \sqrt{2}$. By squaring both sides of this equation, we have $\frac{a^2}{b^2} = 2$, or equivalently $a^2 = 2b^2$.

The proof that $\sqrt{2}$ is irrational

Proof (Proof that $\sqrt{2}$ is irrational)

Suppose $\sqrt{2}$ is not irrational, then $\sqrt{2}$ is rational. Therefore (according to Lemma 6) there exists integers a and b with $b \neq 0$ and $\gcd(a, b) = 1$ such that $\frac{a}{b} = \sqrt{2}$. By squaring both sides of this equation, we have $\frac{a^2}{b^2} = 2$, or equivalently $a^2 = 2b^2$.

Observe that a^2 is even.

The proof that $\sqrt{2}$ is irrational

Proof (Proof that $\sqrt{2}$ is irrational)

Suppose $\sqrt{2}$ is not irrational, then $\sqrt{2}$ is rational. Therefore (according to Lemma 6) there exists integers a and b with $b \neq 0$ and $\gcd(a, b) = 1$ such that $\frac{a}{b} = \sqrt{2}$. By squaring both sides of this equation, we have $\frac{a^2}{b^2} = 2$, or equivalently $a^2 = 2b^2$.

Observe that a^2 is even. According to Lemma 7, a is also even, so $a = 2c$, for some integer c.

The proof that $\sqrt{2}$ is irrational

Proof (Proof that $\sqrt{2}$ is irrational)

Suppose $\sqrt{2}$ is not irrational, then $\sqrt{2}$ is rational. Therefore (according to Lemma 6) there exists integers a and b with $b \neq 0$ and $\gcd(a, b) = 1$ such that $\frac{a}{b} = \sqrt{2}$. By squaring both sides of this equation, we have $\frac{a^2}{b^2} = 2$, or equivalently $a^2 = 2b^2$.

Observe that a^2 is even. According to Lemma 7, a is also even, so $a = 2c$, for some integer c. By substituting this value to our previous fact, we have $(2c)^2 = 2b^2$, or $4c^2 = 2b^2$, and by dividing both sides by 2 we have $b^2 = 2c^2$.

The proof that $\sqrt{2}$ is irrational

Proof (Proof that $\sqrt{2}$ is irrational)

Suppose $\sqrt{2}$ is not irrational, then $\sqrt{2}$ is rational. Therefore (according to Lemma 6) there exists integers a and b with $b \neq 0$ and $\gcd(a,b) = 1$ such that $\frac{a}{b} = \sqrt{2}$. By squaring both sides of this equation, we have $\frac{a^2}{b^2} = 2$, or equivalently $a^2 = 2b^2$.

Observe that a^2 is even. According to Lemma 7, a is also even, so $a = 2c$, for some integer c. By substituting this value to our previous fact, we have $(2c)^2 = 2b^2$, or $4c^2 = 2b^2$, and by dividing both sides by 2 we have $b^2 = 2c^2$.

Observe that b^2 is even.

The proof that $\sqrt{2}$ is irrational

Proof (Proof that $\sqrt{2}$ is irrational)

Suppose $\sqrt{2}$ is not irrational, then $\sqrt{2}$ is rational. Therefore (according to Lemma 6) there exists integers a and b with $b \neq 0$ and $\gcd(a, b) = 1$ such that $\frac{a}{b} = \sqrt{2}$. By squaring both sides of this equation, we have $\frac{a^2}{b^2} = 2$, or equivalently $a^2 = 2b^2$.

Observe that a^2 is even. According to Lemma 7, a is also even, so $a = 2c$, for some integer c. By substituting this value to our previous fact, we have $(2c)^2 = 2b^2$, or $4c^2 = 2b^2$, and by dividing both sides by 2 we have $b^2 = 2c^2$.

Observe that b^2 is even. Based on Lemma 7, b is also even, so $b = 2d$, for some integer d.

The proof that $\sqrt{2}$ is irrational

Proof (Proof that $\sqrt{2}$ is irrational)

Suppose $\sqrt{2}$ is not irrational, then $\sqrt{2}$ is rational. Therefore (according to Lemma 6) there exists integers a and b with $b \neq 0$ and $\gcd(a, b) = 1$ such that $\frac{a}{b} = \sqrt{2}$. By squaring both sides of this equation, we have $\frac{a^2}{b^2} = 2$, or equivalently $a^2 = 2b^2$.

Observe that a^2 is even. According to Lemma 7, a is also even, so $a = 2c$, for some integer c. By substituting this value to our previous fact, we have $(2c)^2 = 2b^2$, or $4c^2 = 2b^2$, and by dividing both sides by 2 we have $b^2 = 2c^2$.

Observe that b^2 is even. Based on Lemma 7, b is also even, so $b = 2d$, for some integer d. As a result, we have $\gcd(a, b) = \gcd(2c, 2d) \geq 2$,

The proof that $\sqrt{2}$ is irrational

Proof (Proof that $\sqrt{2}$ is irrational)

Suppose $\sqrt{2}$ is not irrational, then $\sqrt{2}$ is rational. Therefore (according to Lemma 6) there exists integers a and b with $b \neq 0$ and $\gcd(a, b) = 1$ such that $\frac{a}{b} = \sqrt{2}$. By squaring both sides of this equation, we have $\frac{a^2}{b^2} = 2$, or equivalently $a^2 = 2b^2$.

Observe that a^2 is even. According to Lemma 7, a is also even, so $a = 2c$, for some integer c. By substituting this value to our previous fact, we have $(2c)^2 = 2b^2$, or $4c^2 = 2b^2$, and by dividing both sides by 2 we have $b^2 = 2c^2$.

Observe that b^2 is even. Based on Lemma 7, b is also even, so $b = 2d$, for some integer d. As a result, we have $\gcd(a, b) = \gcd(2c, 2d) \geq 2$, which contradicts to our previous assumption that $\gcd(a, b) = 1$.

The proof that $\sqrt{2}$ is irrational

Proof (Proof that $\sqrt{2}$ is irrational)

Suppose $\sqrt{2}$ is not irrational, then $\sqrt{2}$ is rational. Therefore (according to Lemma 6) there exists integers a and b with $b \neq 0$ and $\gcd(a, b) = 1$ such that $\frac{a}{b} = \sqrt{2}$. By squaring both sides of this equation, we have $\frac{a^2}{b^2} = 2$, or equivalently $a^2 = 2b^2$.

Observe that a^2 is even. According to Lemma 7, a is also even, so $a = 2c$, for some integer c. By substituting this value to our previous fact, we have $(2c)^2 = 2b^2$, or $4c^2 = 2b^2$, and by dividing both sides by 2 we have $b^2 = 2c^2$.

Observe that b^2 is even. Based on Lemma 7, b is also even, so $b = 2d$, for some integer d. As a result, we have $\gcd(a, b) = \gcd(2c, 2d) \geq 2$, which contradicts to our previous assumption that $\gcd(a, b) = 1$. Therefore, $\sqrt{2}$ is irrational. □

Challenging Problems

Exercise

Determine the truth of these following statements. The notation ${}^{a}\log_b$ denotes a real number (if exists) such that $a^{{}^{a}\log b} = b$ (e.g.: ${}^{2}\log 8 = 3$, ${}^{3}\log 9 = 2$).

1. ${}^{2}\log 3$ is irrational.
2. $\sqrt[3]{2}$ is irrational.
3. If a is even and b is odd, then ${}^{a}\log b$ is irrational.

Contents

Proving Equivalent Statements

- Suppose there is a theorem (or lemma/proposition) in a biconditional statement: "p if and only if q", or $p \leftrightarrow q$.
- The statement $p \leftrightarrow q$ is equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$, therefore to show that $p \leftrightarrow q$ is true, we can do this by proving that $p \rightarrow q$ is true **and** $q \rightarrow p$ is true.

Theorem

Suppose n is an integer, then n is odd if and only if $5n + 6$ is odd.

Proof

Proving Equivalent Statements

- Suppose there is a theorem (or lemma/proposition) in a biconditional statement: "p if and only if q", or $p \leftrightarrow q$.
- The statement $p \leftrightarrow q$ is equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$, therefore to show that $p \leftrightarrow q$ is true, we can do this by proving that $p \rightarrow q$ is true **and** $q \rightarrow p$ is true.

Theorem

Suppose n is an integer, then n is odd if and only if $5n + 6$ is odd.

Proof

$(\Rightarrow)$ We first show that if n is odd, then $5n + 6$ is odd.

Proving Equivalent Statements

- Suppose there is a theorem (or lemma/proposition) in a biconditional statement: "p if and only if q", or $p \leftrightarrow q$.
- The statement $p \leftrightarrow q$ is equivalent to $(p \to q) \wedge (q \to p)$, therefore to show that $p \leftrightarrow q$ is true, we can do this by proving that $p \to q$ is true **and** $q \to p$ is true.

Theorem

Suppose n is an integer, then n is odd if and only if $5n + 6$ is odd.

Proof

$(\Rightarrow)$ We first show that if n is odd, then $5n + 6$ is odd. Assume n is odd, then $n = 2k + 1$, for some integer k. We have $5n + 6 = 5(2k + 1) + 6 = 2(5k + 5) + 1$. Therefore $5n + 6$ is odd.

Proving Equivalent Statements

- Suppose there is a theorem (or lemma/proposition) in a biconditional statement: "p if and only if q", or $p \leftrightarrow q$.
- The statement $p \leftrightarrow q$ is equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$, therefore to show that $p \leftrightarrow q$ is true, we can do this by proving that $p \rightarrow q$ is true **and** $q \rightarrow p$ is true.

Theorem

Suppose n is an integer, then n is odd if and only if $5n + 6$ is odd.

Proof

$(\Rightarrow)$ We first show that if n is odd, then $5n + 6$ is odd. Assume n is odd, then $n = 2k + 1$, for some integer k. We have
$5n + 6 = 5\,(2k + 1) + 6 = 2\,(5k + 5) + 1$. Therefore $5n + 6$ is odd.
$(\Leftarrow)$ We will show that if $5n + 6$ is odd, then n is odd.

Proving Equivalent Statements

- Suppose there is a theorem (or lemma/proposition) in a biconditional statement: "p if and only if q", or $p \leftrightarrow q$.
- The statement $p \leftrightarrow q$ is equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$, therefore to show that $p \leftrightarrow q$ is true, we can do this by proving that $p \rightarrow q$ is true **and** $q \rightarrow p$ is true.

Theorem

Suppose n is an integer, then n is odd if and only if $5n + 6$ is odd.

Proof

($\Rightarrow$) We first show that if n is odd, then $5n + 6$ is odd. Assume n is odd, then $n = 2k + 1$, for some integer k. We have $5n + 6 = 5(2k + 1) + 6 = 2(5k + 5) + 1$. Therefore $5n + 6$ is odd.
($\Leftarrow$) We will show that if $5n + 6$ is odd, then n is odd. This statement is equivalent to its contrapositive, that is, if n is even, then $5n + 6$ is even.

Proving Equivalent Statements

- Suppose there is a theorem (or lemma/proposition) in a biconditional statement: "p if and only if q", or $p \leftrightarrow q$.
- The statement $p \leftrightarrow q$ is equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$, therefore to show that $p \leftrightarrow q$ is true, we can do this by proving that $p \rightarrow q$ is true **and** $q \rightarrow p$ is true.

Theorem

Suppose n is an integer, then n is odd if and only if $5n + 6$ is odd.

Proof

$(\Rightarrow)$ We first show that if n is odd, then $5n + 6$ is odd. Assume n is odd, then $n = 2k + 1$, for some integer k. We have
$5n + 6 = 5\,(2k + 1) + 6 = 2\,(5k + 5) + 1$. Therefore $5n + 6$ is odd.
$(\Leftarrow)$ We will show that if $5n + 6$ is odd, then n is odd. This statement is equivalent to its contrapositive, that is, if n is even, then $5n + 6$ is even. Assume n even, then $n = 2\ell$, for some integer ℓ. We have
$5n + 6 = 5\,(2\ell) + 6 = 2\,(5\ell + 3)$. Therefore $5n + 6$ is even. $\square$

Exercise 6

Exercise

Prove or disprove following statement. Let n be an integer:

1. n is odd if and only if $7n + 4$ is odd,
2. $n + 5$ is even if and only if $3n + 2$ is odd.

Contents

Counterexamples

Recall that in order to show that a statement of the form $\forall x P(x)$ is false, it is sufficient to provide a counterexample, i.e., an element c in the universe of discourse that makes $P(c)$ is false.

Exercise

Prove or disprove following statements:

1. If x is a nonzero real number, then $x^2 \geq 1$.
2. Suppose x, y, and z are integers. If $xy = 0$ and $yz = 0$, then $xz = 0$.

Solution:

Counterexamples

Recall that in order to show that a statement of the form $\forall x P(x)$ is false, it is sufficient to provide a counterexample, i.e., an element c in the universe of discourse that makes $P(c)$ is false.

Exercise

Prove or disprove following statements:

1. If x is a nonzero real number, then $x^2 \geq 1$.
2. Suppose x, y, and z are integers. If $xy = 0$ and $yz = 0$, then $xz = 0$.

Solution:

1. The statement is false, choose $x =$

Counterexamples

Recall that in order to show that a statement of the form $\forall x P(x)$ is false, it is sufficient to provide a counterexample, i.e., an element c in the universe of discourse that makes $P(c)$ is false.

Exercise

Prove or disprove following statements:

1. If x is a nonzero real number, then $x^2 \geq 1$.
2. Suppose x, y, and z are integers. If $xy = 0$ and $yz = 0$, then $xz = 0$.

Solution:

1. The statement is false, choose $x = \frac{1}{2}$, then $x^2 = \frac{1}{4} \ngeq 1$.

Counterexamples

Recall that in order to show that a statement of the form $\forall x P(x)$ is false, it is sufficient to provide a counterexample, i.e., an element c in the universe of discourse that makes $P(c)$ is false.

Exercise

Prove or disprove following statements:

1. If x is a nonzero real number, then $x^2 \geq 1$.
2. Suppose x, y, and z are integers. If $xy = 0$ and $yz = 0$, then $xz = 0$.

Solution:

1. The statement is false, choose $x = \frac{1}{2}$, then $x^2 = \frac{1}{4} \ngeq 1$.
2. The statement is false, choose $x =$

Counterexamples

Recall that in order to show that a statement of the form $\forall x P(x)$ is false, it is sufficient to provide a counterexample, i.e., an element c in the universe of discourse that makes $P(c)$ is false.

Exercise

Prove or disprove following statements:

1. If x is a nonzero real number, then $x^2 \geq 1$.
2. Suppose x, y, and z are integers. If $xy = 0$ and $yz = 0$, then $xz = 0$.

Solution:

1. The statement is false, choose $x = \frac{1}{2}$, then $x^2 = \frac{1}{4} \not\geq 1$.
2. The statement is false, choose $x = 1$, $y =$

Counterexamples

Recall that in order to show that a statement of the form $\forall x P\left(x\right)$ is false, it is sufficient to provide a counterexample, i.e., an element c in the universe of discourse that makes $P\left(c\right)$ is false.

Exercise

Prove or disprove following statements:

1. If x is a nonzero real number, then $x^2 \geq 1$.
2. Suppose x, y, and z are integers. If $xy = 0$ and $yz = 0$, then $xz = 0$.

Solution:

1. The statement is false, choose $x = \frac{1}{2}$, then $x^2 = \frac{1}{4} \ngeq 1$.
2. The statement is false, choose $x = 1$, $y = 0$, and $z =$

Counterexamples

Recall that in order to show that a statement of the form $\forall x P(x)$ is false, it is sufficient to provide a counterexample, i.e., an element c in the universe of discourse that makes $P(c)$ is false.

Exercise

Prove or disprove following statements:

1. If x is a nonzero real number, then $x^2 \geq 1$.
2. Suppose x, y, and z are integers. If $xy = 0$ and $yz = 0$, then $xz = 0$.

Solution:

1. The statement is false, choose $x = \frac{1}{2}$, then $x^2 = \frac{1}{4} \ngeq 1$.
2. The statement is false, choose $x = 1$, $y = 0$, and $z = 2$, then $xy = 0$, $yz = 0$, yet $xz = 2$.

Contents

Proof Strategy

"*Begin at the beginning... and go on till you come to the end: then stop.*"
-Lewis Carrol, *Alice's Adventures in Wonderland*, 1865

When we need to verify the truth of a particular statement, we can do following steps:

1. translate each of the terms according to its definition,

Proof Strategy

"*Begin at the beginning... and go on till you come to the end: then stop.*"
-Lewis Carrol, *Alice's Adventures in Wonderland*, 1865

When we need to verify the truth of a particular statement, we can do following steps:

1. translate each of the terms according to its definition,
2. analyze the meaning of the hypothesis and conclusion in the statement,

Proof Strategy

"*Begin at the beginning... and go on till you come to the end: then stop.*"
-Lewis Carrol, *Alice's Adventures in Wonderland*, 1865

When we need to verify the truth of a particular statement, we can do following steps:

1. translate each of the terms according to its definition,
2. analyze the meaning of the hypothesis and conclusion in the statement,
3. observe the correlation between hypothesis and its conclusion,

Proof Strategy

"Begin at the beginning... and go on till you come to the end: then stop."
-Lewis Carrol, *Alice's Adventures in Wonderland*, 1865

When we need to verify the truth of a particular statement, we can do following steps:

1. translate each of the terms according to its definition,
2. analyze the meaning of the hypothesis and conclusion in the statement,
3. observe the correlation between hypothesis and its conclusion,
4. try one of the proof methods to prove the statement, when we encounter an implication $(p \rightarrow q)$, we do:

Proof Strategy

"*Begin at the beginning... and go on till you come to the end: then stop.*"
-Lewis Carrol, *Alice's Adventures in Wonderland*, 1865

When we need to verify the truth of a particular statement, we can do following steps:

1. translate each of the terms according to its definition,
2. analyze the meaning of the hypothesis and conclusion in the statement,
3. observe the correlation between hypothesis and its conclusion,
4. try one of the proof methods to prove the statement, when we encounter an implication $(p \to q)$, we do:
    1. try direct proof; if it failed

Proof Strategy

"*Begin at the beginning... and go on till you come to the end: then stop.*"
-Lewis Carrol, *Alice's Adventures in Wonderland*, 1865

When we need to verify the truth of a particular statement, we can do following steps:

1. translate each of the terms according to its definition,
2. analyze the meaning of the hypothesis and conclusion in the statement,
3. observe the correlation between hypothesis and its conclusion,
4. try one of the proof methods to prove the statement, when we encounter an implication $(p \rightarrow q)$, we do:
    1. try direct proof; if it failed
    2. try indirect proof by contraposition; if it failed

Proof Strategy

"*Begin at the beginning... and go on till you come to the end: then stop.*"
-Lewis Carrol, *Alice's Adventures in Wonderland*, 1865

When we need to verify the truth of a particular statement, we can do following steps:

1. translate each of the terms according to its definition,
2. analyze the meaning of the hypothesis and conclusion in the statement,
3. observe the correlation between hypothesis and its conclusion,
4. try one of the proof methods to prove the statement, when we encounter an implication $(p \rightarrow q)$, we do:
    1. try direct proof; if it failed
    2. try indirect proof by contraposition; if it failed
    3. try indirect proof by contradiction

Proof Strategy

"*Begin at the beginning... and go on till you come to the end: then stop.*"
-Lewis Carrol, *Alice's Adventures in Wonderland*, 1865

When we need to verify the truth of a particular statement, we can do following steps:

1. translate each of the terms according to its definition,
2. analyze the meaning of the hypothesis and conclusion in the statement,
3. observe the correlation between hypothesis and its conclusion,
4. try one of the proof methods to prove the statement, when we encounter an implication $(p \rightarrow q)$, we do:
    1. try direct proof; if it failed
    2. try indirect proof by contraposition; if it failed
    3. try indirect proof by contradiction
5. if the proof methods failed; probably the statement is false and try to guess a counterexample instead.

Contents

Some Mistakes in Mathematical “Proofs”

What’s wrong with these “theorem” and “proof”?

“Theorem”

$1 = -1$

“Proof”

Observe that $1 =$

Some Mistakes in Mathematical “Proofs”

What’s wrong with these “theorem” and “proof”?

“Theorem”

$1 = -1$

“Proof”

Observe that $1 = \sqrt{1} =$

Some Mistakes in Mathematical "Proofs"

What's wrong with these "theorem" and "proof"?

"Theorem"

$1 = -1$

"Proof"

Observe that $1 = \sqrt{1} = \sqrt{(-1)(-1)} =$

Some Mistakes in Mathematical "Proofs"

What's wrong with these "theorem" and "proof"?

"Theorem"

$1 = -1$

"Proof"

Observe that $1 = \sqrt{1} = \sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1} =$

Some Mistakes in Mathematical "Proofs"

What's wrong with these "theorem" and "proof"?

"Theorem"

$1 = -1$

"Proof"

Observe that $1 = \sqrt{1} = \sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1} = \left(\sqrt{-1}\right)^2$

Some Mistakes in Mathematical "Proofs"

What's wrong with these "theorem" and "proof"?

"Theorem"

$1 = -1$

"Proof"

Observe that $1 = \sqrt{1} = \sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1} = \left(\sqrt{-1}\right)^2 = -1.$ □

Some Mistakes in Mathematical “Proofs”

What’s wrong with these “theorem” and “proof”?

“Theorem”

$1 = -1$

“Proof”

Observe that $1 = \sqrt{1} = \sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1} = \left(\sqrt{-1}\right)^2 = -1.$ □

An error occurs in the use of the fact that $\sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1}$, the property $\sqrt{ab} = \sqrt{a}\sqrt{b}$ can only be used when at least one of a or b is positive. This type of error is an example of *mathematical fallacy*.

Are following theorem and proof correct?

Theorem

If n^2 is even, then n is even.

Proof (?)

Assume that n^2 is even, then $n^2 = 2k$ for some integer k. Suppose $n = 2\ell$ for some integer ℓ, then we have $n^2 = 4\ell^2 = 2\left(2\ell^2\right)$. Thus, we conclude that n is even. □

Are following theorem and proof correct?

Theorem

If n^2 is even, then n is even.

Proof (?)

Assume that n^2 is even, then $n^2 = 2k$ for some integer k. Suppose $n = 2\ell$ for some integer ℓ, then we have $n^2 = 4\ell^2 = 2\left(2\ell^2\right)$. Thus, we conclude that n is even. □

The above theorem is true, and one of its proof can be obtained using indirect proof by contraposition.

Are following theorem and proof correct?

Theorem

If n^2 is even, then n is even.

Proof (?)

Assume that n^2 is even, then $n^2 = 2k$ for some integer k. Suppose $n = 2\ell$ for some integer ℓ, then we have $n^2 = 4\ell^2 = 2\left(2\ell^2\right)$. Thus, we conclude that n is even. □

The above theorem is true, and one of its proof can be obtained using indirect proof by contraposition.
However, "the proof" is incorrect because the statement "suppose $n = 2\ell$ for some integer ℓ" occurs out of nowhere (there is no justification).

Are following theorem and proof correct?

Theorem

If n^2 is even, then n is even.

Proof (?)

Assume that n^2 is even, then $n^2 = 2k$ for some integer k. Suppose $n = 2\ell$ for some integer ℓ, then we have $n^2 = 4\ell^2 = 2\left(2\ell^2\right)$. Thus, we conclude that n is even. □

The above theorem is true, and one of its proof can be obtained using indirect proof by contraposition.
However, "the proof" is incorrect because the statement "suppose $n = 2\ell$ for some integer ℓ" occurs out of nowhere (there is no justification). No argument has been given to show that n can be written as 2ℓ for some integer ℓ. Instead, this is what we are supposed to prove.

Are following theorem and proof correct?

Theorem

If n^2 is even, then n is even.

Proof (?)

Assume that n^2 is even, then $n^2 = 2k$ for some integer k. Suppose $n = 2\ell$ for some integer ℓ, then we have $n^2 = 4\ell^2 = 2\left(2\ell^2\right)$. Thus, we conclude that n is even. □

The above theorem is true, and one of its proof can be obtained using indirect proof by contraposition.

However, "the proof" is incorrect because the statement "suppose $n = 2\ell$ for some integer ℓ" occurs out of nowhere (there is no justification). No argument has been given to show that n can be written as 2ℓ for some integer ℓ. Instead, this is what we are supposed to prove.

This type of error, which occurs when we use the statement equivalent to the statement being proved (within the prove of itself), is an example of *circular reasoning*.