3.4 Arguments with Quantified Statements

Universal Instantiation
The **rule of universal instantiation** states that if $\forall x \in S, P(x)$ is true, then $P(a)$ is true for any $a \in S$. This allows deductive reasoning from general to specific.

Universal Modus Ponens The argument form:

- $\forall x, P(x) \to Q(x)$
- $P(a)$
- $\therefore Q(a)$

is called **universal modus ponens**. It is a **valid** argument form.

Valid Arguments
An argument form is **valid** if the conclusion is true when premises are true for any predicate substitution.

An argument is valid if its form is valid.

Example:

- If an infinite series converges then its terms go to 0
- The series $\sum_{n=1}^{\infty} \frac{n^2}{n!}$ converges
- $\therefore \lim_{n\to\infty} \frac{n^2}{n!} = 0$

This is **valid** by universal modus ponens.

Universal modus tollens is also a valid argument form.

4.1 Direct Proof and Counterexamples Part 1: Introduction

Even and Odd Integers

An integer n is **even** if $\exists k \in \mathbb{Z} : n = 2k$.

An integer n is **odd** if $\exists k \in \mathbb{Z} : n = 2k + 1$.

- 0 is even, since $0 = 2 \cdot 0$.
- If $a, b \in \mathbb{Z}$, then $6a - 8b + 11$ is odd. Proof: $6a - 8b + 11 = 2(3a - 4b) + 1$.
- -75 is odd, since $-75 = 2(-38) + 1$.
- Every integer is either even or odd.
- No integer can be both even and odd.

Primes and Composites

A positive integer $n > 1$ is **prime** if $\nexists r, s \in \mathbb{Z}$ such that $1 < r, s < n$ and $n = rs$.

A positive integer $n > 1$ is **composite** if $\exists r, s \in \mathbb{Z}$ such that $1 < r, s < n$ and $n = rs$.

- 1 is neither prime nor composite.
- 2 is prime.
- Every integer > 1 is prime or composite.

Proofs of Existential Statements

To prove $\exists x \in D : P(x)$, exhibit $x \in D$ with $P(x)$ true.

- $\exists n \in \mathbb{Z} : n = a^2 + b^2 = c^2 + d^2$, where $a, b, c, d \in \mathbb{Z}$. Proof: Let $n = 50$. Then $n = 1^2 + 7^2 = 5^2 + 5^2$.
- Let $r, s \in \mathbb{Z}$. Then $\exists k \in \mathbb{Z} : 8r - 14s = 2k$. Proof: Let $k = 4r - 7s$.

To disprove $\forall x \in D : P(x) \implies Q(x)$, exhibit a **counterexample**: $x \in D$ with $P(x)$ true and $Q(x)$ false.

Proof by Exhaustion

Verify $P(x)$ for all x in small finite D.

- $\forall n \in 2\mathbb{Z}, 4 \leq n \leq 26 : n = p + q$ for primes p, q. Proof: verify for $n = 4, 6, \ldots, 26$.

Fails for large/infinite D.

Proof by Generalizing from a Generic Particular

To prove $\forall x \in D : P(x)$ for large/infinite D:

1. Let x be an arbitrary, generic element of D.
2. Prove $P(x)$ holds for this generic x.

Let $D =$ odd integers, $E =$ even integers. Prove:

$$\forall m, n \in D : m + n \in E$$

Proof:

Let $m, n \in D$. Write $m = 2p + 1, n = 2q + 1$ for integers p, q. Then $m + n = 2(p + q) + 2 \in E$.

Naming p, q is **existential instantiation**.

4.3 Direct Proof and Counterexamples Part 3: Rational Numbers)

Rational Numbers

A real number r is called **rational** if it can be expressed as a quotient $\frac{a}{b}$ of integers a and b, where $b \neq 0$.

A real number that is not rational is called **irrational**.

- $\frac{13}{4}$ is rational, since it is a quotient of integers.
- $\frac{2}{0}$ is not rational, since we cannot divide by 0 in the real numbers.
- -7 is rational, since $-7 = \frac{-7}{1}$.
- 0 is rational, since $0 = \frac{0}{42}$.
- 2.913 is rational, since $2.913 = \frac{2913}{1000}$. In general, any terminating decimal is rational.
- $0.242424\ldots$ is rational. This repeating decimal can be written as the infinite series $0.24 + 0.0024 + 0.000024 + \cdots$. This is a geometric series with first term $a = 0.24$ and common ratio $r = 0.01$. By the formula for the sum of an infinite geometric series, this repeating decimal is equal to $\frac{a}{1-r} = \frac{24}{99} = \frac{8}{33}$, which is rational.

Proofs Involving Rational Numbers

If r and s are rational numbers, then $r - s$ is rational.

Let r, s be rational numbers. Then there exist integers a, b, c, d with $b, d \neq 0$ such that $r = \frac{a}{b}$ and $s = \frac{c}{d}$. Then $r - s = \frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd}$.

Now $ad - bc$ and bd are integers, and $bd \neq 0$. Therefore, $r - s$ is rational.

If c is a root of a cubic polynomial with rational coefficients, then c is a root of a cubic polynomial with integer coefficients.

Let c be a root of $r_3x^3 + r_2x^2 + r_1x + r_0$, where r_i are rational. Then $r_i = \frac{a_i}{b_i}$ for integers a_i, b_i with $b_i \neq 0$. Plugging in c gives $\frac{a_3}{b_3}c^3 + \frac{a_2}{b_2}c^2 + \frac{a_1}{b_1}c + \frac{a_0}{b_0} = 0$. Multiplying by $b_3b_2b_1b_0$ gives $a_3c^3 + a_2c^2 + a_1c + a_0 = 0$, a cubic polynomial with integer coefficients that has c as a root.