# Review for Exam 1

# Fundamentals

(Sec 2 & Sec 3)

- Logical connectives $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$
- Tautologies
- Proof techniques
- Quantifiers $\forall$, $\exists$, free vs. bound var., order matters w/ mixed quan.
- De Morgan's Laws and Distributive Laws

- Cond. proof
- proof by contradiction
- proof by contraposition

See the summary at the end of Sec 4.

- $\neg P \Rightarrow Q \wedge R$ means $(\neg P) \Rightarrow (Q \wedge R)$
- $\Rightarrow$ (conditional)
  - $\neg (P \Rightarrow Q)$
  - Drinks vs Ages
  - Cards
  - "vacuously true"

# Definitions (Sec. 4)

Write down the definitions of the following sentences exactly as provided in the textbook. Write down preambles whenever needed, such as "Let $a, b, m \in \mathbb{Z}$.".

- $x$ is even.
- $x$ is odd.
- $x$ is rational.
- $x$ is irrational.
- $d$ divides $x$.
- $x$ is a prime number.
- $a$ is congruent to $b$ modulo $m$.

# Tautologies (Cond'l proof exercise)

## Example 1

Use the method of conditional proof to explain in words why the sentence

$$\underbrace{[P \Rightarrow (Q \Rightarrow R)]}_{A_1} \Rightarrow \underbrace{[\underbrace{(P \Rightarrow Q)}_{A_2} \Rightarrow \underbrace{(\underbrace{P}_{A_3} \Rightarrow \underbrace{R}_{C_3})}_{C_2}]}_{C_1}$$

is a tautology. Be explicit about discharging assumptions.

Proof A1: Suppose $A_1 : P \Rightarrow (Q \Rightarrow R)$ is true. (WTS: $C_1 : (P \Rightarrow Q) \Rightarrow (P \Rightarrow R)$ is true.)

A2: Suppose $A_2 : P \Rightarrow Q$ is true. (WTS: $C_2 : P \Rightarrow R$ is true.)

A3: Suppose $A_3 : P$ is true. (WTS: $C_3 : R$ is true.)

Proof | A1: Suppose $A_1 : P \Rightarrow (Q \Rightarrow R)$ is true. (WTS: $C_1 : (P \Rightarrow Q) \Rightarrow (P \Rightarrow R)$ is true.)

A2: Suppose $A_2 : P \Rightarrow Q$ is true. (WTS: $C_2 : P \Rightarrow R$ is true.)

A3: Suppose $A_3 : P$ is true. (WTS: $C_3 : R$ is true.)

From A2 and A3, we see $Q$ is true, by modus ponens.

From A1 and A3, we see $Q \Rightarrow R$ is true, by modus ponens.

From this and the fact that $Q$ is true, we see $R$ is true, by modus ponens.

We have shown $C_3$ is true under A1, A2, and A3.

Discharging A3, $C_2$ is true under A1 and A2.

Discharging A2, $C_1$ is true under A1 alone.

Finally discharging A1, $A_1 \Rightarrow C_1$ is true under no assumption. Hence it is a tautology. $\square$

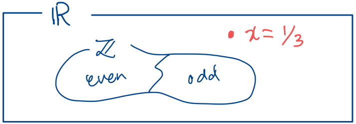
# Dichotomies and the Universe of Discourse

Let $x \in \mathbb{Z}$.

- If $x$ is odd, then $x$ is not even. T
- If $x$ is not even, then $x$ is odd. T


Let $x \in \mathbb{R}$.

- If $x$ is odd, then $x$ is not even. T
- If $x$ is not even, then $x$ is odd. F



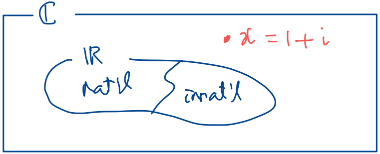

---

Let $x \in \mathbb{R}$.

- If $x$ is rational, then $x$ is not irrational. T
- If $x$ is not irrational, then $x$ is rational. T


Let $x \in \mathbb{C}$.

- If $x$ is rational, then $x$ is not irrational. T
- If $x$ is not irrational, then $x$ is rational. F



## Example 2 (Cf. S04E12.)

It is known that $\pi$ is an irrational number. From this, prove that $\pi + 2e$ is irrational or $\pi - 3e$ is irrational.

P Q

Proof (by contradiction) Suppose $\pi+2e$ is not irrational
and $\pi-3e$ is not irrational.

Since both $\pi+2e$ and $\pi-3e$ are real,
$\pi+2e$ is rational and $\pi-3e$ is rational.

Since the product of two rational numbers is rational,
$\frac{3}{5}(\pi+2e)$ is rational and $\frac{2}{5}(\pi-3e)$ is rational.

Since the sum of two rational numbers is rational,
$$\frac{3}{5}(\pi+2e)+\frac{2}{5}(\pi-3e) = \frac{3\pi+6e+2\pi-6e}{5} = \frac{5\pi}{5} = \pi$$
is rational. But since $\pi$ is real and $\pi$ is irrational, $\pi$ is not rational.
This is a contradiction.

WTS: $P \vee Q$

Proof by contradiction.

$$\neg(P \vee Q)$$
$$\equiv (\neg P) \wedge (\neg Q)$$

# Classical Showcases of Proof by Contradiction

- $\sqrt{2}$ is irrational. Quiz 4 : $\sqrt{3}$ is irrational.
- There are infinitely many prime numbers. (S04E16)

$n < q \leq n! + 1$

# When Prime Divides Product

**Euclid's Lemma (Remark 4.50)**

Let $p$ be a prime number and let $x, y \in \mathbb{Z}$. If $p \mid xy$, then $p \mid x$ or $p \mid y$.

In general, we have:

> Let $d \in \mathbb{N}$ and let $x, y \in \mathbb{Z}$. If $d \mid xy$, then there exist $d_1, d_2 \in \mathbb{N}$ such that $d_1 \mid x$, $d_2 \mid y$, and $d = d_1 d_2$.

The converse of Remark 4.50 is also true.

# Congruence

## Example 3 (S04E26(b))

Let $m, a_1, b_1, a_2$, and $b_2$ be integers. Suppose that

$$a_1 \equiv b_1 \mod m \quad \text{and} \quad a_2 \equiv b_2 \mod m.$$

Prove that $a_1 a_2 \equiv b_1 b_2 \mod m$.

# Induction

- Principle of mathematical induction.
- Declaration, base case, induction step, and conclusion.
- Inductive hypothesis.
- Proving $(\forall x \in \mathbb{Z})P(x)$.

# Induction Examples

For each $n \in \mathbb{N}$,

- $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$
- $1^2 + 2^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$
- $1^3 + 2^3 + \cdots + n^3 = \dfrac{n^2(n+1)^2}{4}$

For each $n \in \mathbb{N}$,

- 3 divides $4^n - 1$.

For each $x \in \mathbb{Z}$,

- $x$ is even or $x$ is odd.

Prove by induction that for each $n \in \mathbb{N}$,

5 divides $8^n - 3^n$.

Prove by induction that for each $n \in \mathbb{N}$,

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}.$$