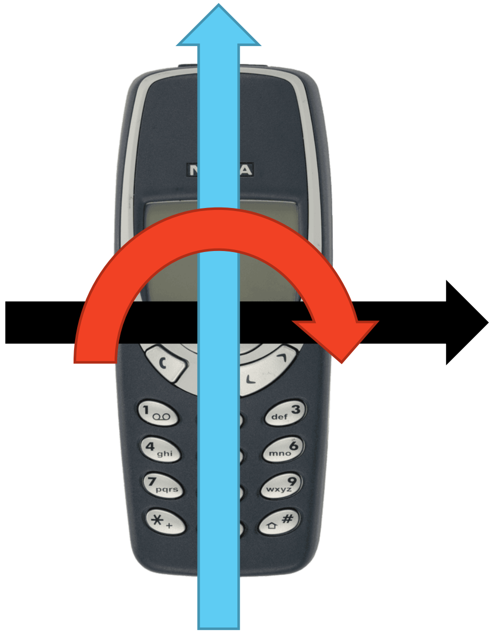
Mathematics for Robotics (ROB-GY 6013 Section A)

- **Week 1:**
    - Phone Flipping Activity
    - Syllabus
    - Notation
    - Logic
    - Direct Proof Techniques
- **Week 2:**
    - Recap and finish Indirect Proofs
    - Abstract Linear Algebra

Flip Phone



$$\mathcal{M} = \{I, H, V, T\}$$

- Let $\mathcal{M}$ be the set of "moves"
  - I (Idle, don't move)
  - H (Flip phone horizontally)
  - V (Flip phone vertically)
  - T (Twist phone 180 degrees)

Made up symbol for this binary operation

⇛	I	H	V	T
I	I	H	V	T
H	H	I	T	V
V	V	T	I	H
T	T	V	H	I

$$H \Rrightarrow V = T$$

Klein four-group

$$\mathcal{S} = \{1, 3, 5, 7\}$$

- Binary operation chosen as multiplication modulo 8

$(\times)$ $mod\ 8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

- Same pattern as before!
- Suggests deeper link between certain kinds of rotations and certain kinds of integer multiplication
  - They are both the Klein four-group!
  - Good way to start a Mathematics for Robotics course

Some recurring themes

- We live under the **shadow of real analysis**
    - Less emphasis on real analysis in this course, but that does not mean we are afraid of it
    - We will note when it pops up and move on
- We will ***try*** to think like a mathematician
    - **Thoughtfulness**
    - **Patience**
    - **Precision**

How to Argue with Mathematicians*

- **Vocabulary** (Notation)
- **Grammar** (More Notation/Logic)
- **Writing** (Proofs)

*As in how to structure mathematical arguments

Vocabulary: Common Sets

$\mathbb{N} = \{1, 2, 3, \cdots\}$ Natural numbers or counting numbers

$\mathbb{Z} = \mathcal{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$ Integers or whole numbers

$\mathbb{Q} = \left\{ \frac{m}{q} \mid m, q \in \mathbb{Z}, q \neq 0, \text{no common factors (reduce all fractions)} \right\}$ Rational numbers

$\mathbb{R}$ = Real numbers **are extremely tricky to define/construct!**

$\mathbb{C} = \{\alpha + j\beta \mid \alpha, \beta \in \mathbb{R}, j^2 = -1\}$ Complex numbers

Vocabulary: Logic

$\forall$ means "for every", "for all", "for each" **Universal Quantifier**

$\exists$ means "for some", "there exist(s)", "there is/are", "for at least one" **Existential Quantifier**

$\in$ means "element of" as in "$x \in A$", i.e., x is an element of the set A

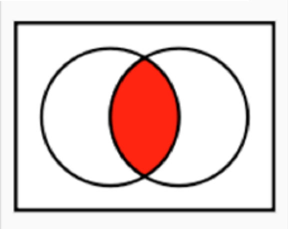
$\sim$ denotes "logical not". You will also often see $\neg$. We'll use both in these notes.

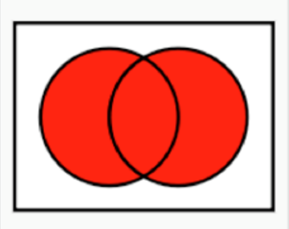
$p \implies q$ means "if the logical or mathematical statement p is true, then the statement q is true"

$p \iff q$ means "p is true if, and only if , q is true". While p iff q is another way to write $p \iff q$

Logical and: $p_1 \wedge p_2$ *Logical or*: $p_1 \vee p_2$

Intersection





Union

Vocabulary: Logic

$p \iff q$ is logically equivalent to

(a) $p \implies q$ and

(b) $q \implies p$

The *contrapositive* of $p \implies q$ is $\sim q \implies \sim p$

The *converse* of $p \implies q$ is $q \implies p$. It is very important to note that in general, $(p \implies q)$ *DOES NOT IMPLY* $(q \implies p)$, and vice-versa. If they did, we would not need $p \iff q$.

Sentences

- “Every family has one family member that all other family members dislike”

$$\forall F\ \exists y \in F \text{ such that } \forall x \in F \setminus \{y\}\ \ x \text{ dislikes } y$$

- Every real number is arbitrarily close to a rational number

$$\forall x \in \mathbb{R} \text{ and } \forall(\epsilon \in \mathbb{R}, \epsilon > 0)\ ,\ \exists q \in \mathbb{Q}\ \text{ s.t. } |x - q| < \epsilon$$

- Every real number can be approximated by a rational number up to any numerical precision (number of decimal places)

$$\forall x \in \mathbb{R} \text{ and } \forall n \in \mathbb{N}\ ,\ \exists q \in \mathbb{Q}\ \text{ s.t. } |x - q| < 1/10^n$$

$$\pi \approx 3.14159...$$

True Sentences

- Truth Tables and Venn Diagrams
- De Morgan's Laws (basically flip everyone)

$$\sim(A \wedge B) = (\sim A \vee \sim B)$$

$$\sim(A \vee B) = (\sim A \wedge \sim B)$$

- Existential and Universal quantifiers are negations of each other
  - "All swans are white" vs. "Some/at least one swan is black"
- Inverse, Converse, Contrapositive
  - Contrapositive is equivalent to original conditional statement

Definitions

- Definitions are biconditionals (if and only type statements)
  - They say the same thing in two (or more) different-sounding ways
- Definition of odd number:

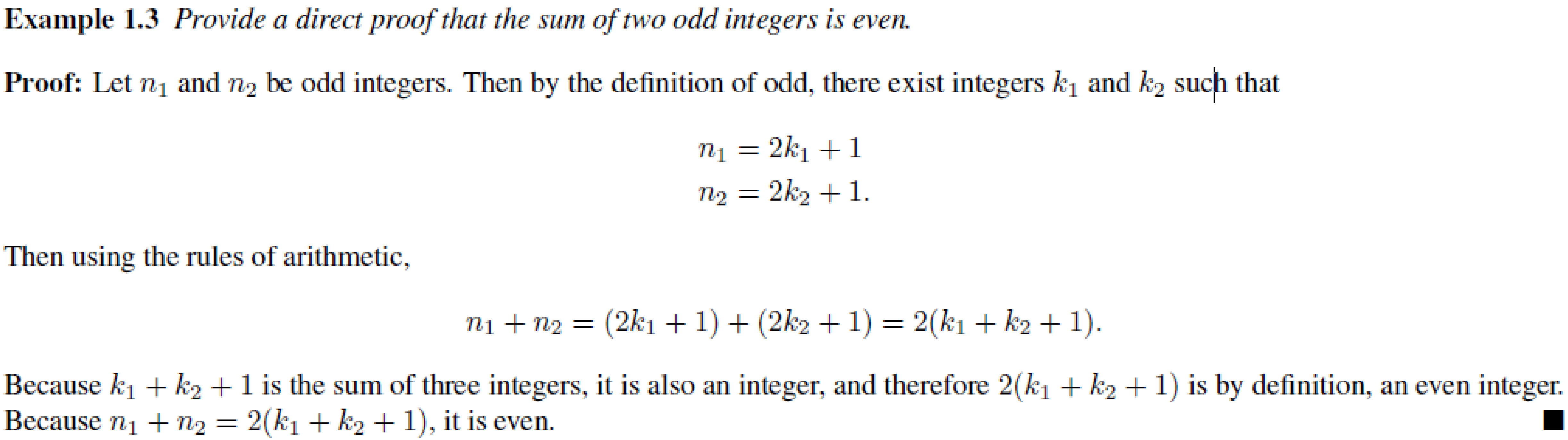
$$(n \text{ is odd}) \Leftrightarrow (\exists k \in \mathbb{Z} \mid n = 2k+1)$$

- Definition of even number:

$$(n \text{ is even}) \Leftrightarrow (\exists k \in \mathbb{Z} \mid n = 2k)$$

- In a proof, we might start with the left-hand side of the definition to get to the right-hand side (e.g., trying to show something is even) or the opposite direction (e.g., we know something is odd and are trying to get something out of that knowledge)

Proofs: Recipes for Truth



Example 1.3 *Provide a direct proof that the sum of two odd integers is even.*

Proof: Let n_1 and n_2 be odd integers. Then by the definition of odd, there exist integers k_1 and k_2 such that

$$n_1 = 2k_1 + 1$$
$$n_2 = 2k_2 + 1.$$

Then using the rules of arithmetic,

$$n_1 + n_2 = (2k_1 + 1) + (2k_2 + 1) = 2(k_1 + k_2 + 1).$$

Because $k_1 + k_2 + 1$ is the sum of three integers, it is also an integer, and therefore $2(k_1 + k_2 + 1)$ is by definition, an even integer. Because $n_1 + n_2 = 2(k_1 + k_2 + 1)$, it is even. ■

- Build outward from things you know/assume to be true: **axioms, definitions, and theorems** with some exceptions when you temporarily assume things that you don’t know to be true as part of the proof techniques

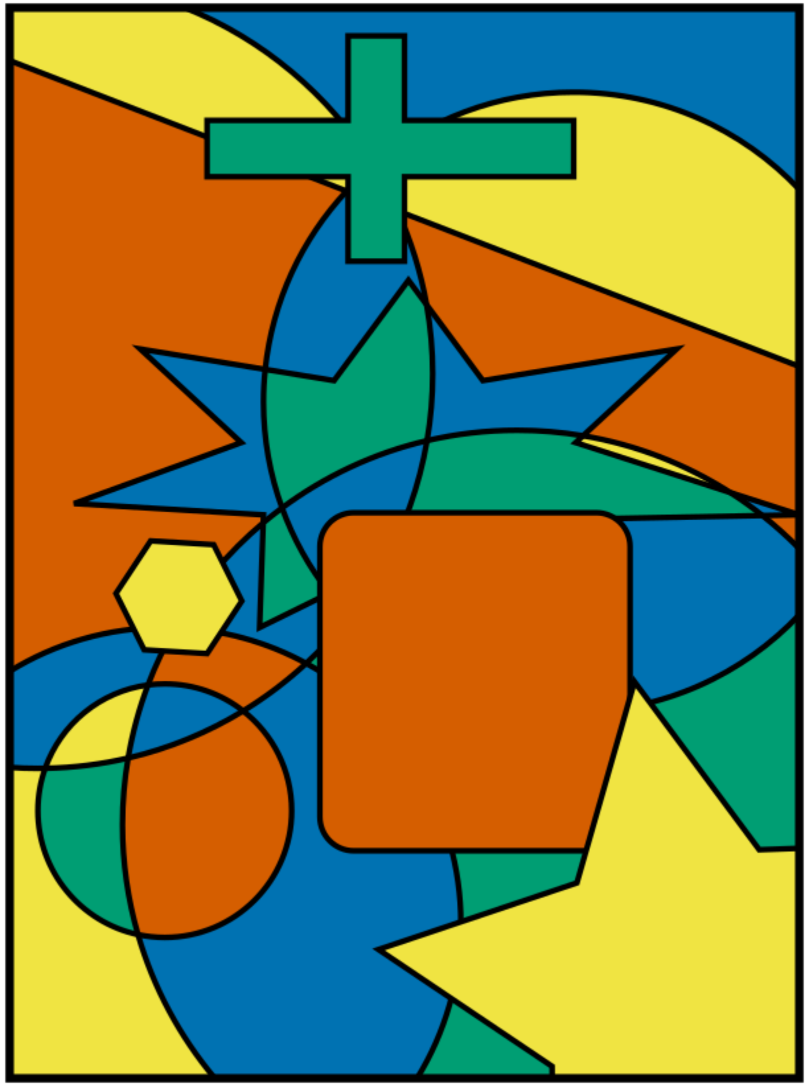
Style

- Abbreviations
  - iff (if and only if, for biconditionals)
  - s.t. or | (such that)

- End your proof with style!
  - End with QED (stands for quod erat demonstratum, Latin for **“which was to be demonstrated”**)
  - End with ■ also known as Halmos or tombstone

Special Direct Proof Techniques

- Proof by Exhaustion (**Four-color Theorem, Theorems involving Rubik's Cubes**)
- Proof by Mathematical Induction
  - First Principle or Standard Induction (Sum of $1 + 3 + \ldots + (2n - 1) = n^2$)
  - Second Principle or Strong Induction (Fundamental Theorem of Arithmetic)
  - Both are equivalent but are used in different cases!



First Principle of Induction (Standard Induction)

Let $P(n)$ denote a statement about the natural numbers with the following properties:

(a) **Base case:** Prove that $P(1)$ is true

(b) **Induction step:** Assume **induction hypothesis** ($P(k)$) is true.
Prove that if $P(k)$ is true,
then $P(k+1)$ must be true.

By the **(first)** principle of mathematical induction the statement $P(n)$ holds for every natural number n. **QED.**

Example 1.6 *Let's prove the **Claim:** For all* $n \geq 1$, $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.

Proof:

- Step 0: Write down $P(k)$: $1 + 3 + 5 + \cdots + (2k - 1) = k^2$.

- Step 1: Check the base case, $P(1)$: For $k = 1$, we have that $1 = 1^2$, and hence the base case is true.

- Step 2: Show the induction hypothesis is true. That is, using the fact that $P(k)$ is true, show that $P(k + 1)$ is true. Often, this involves re-writing $P(k + 1)$ as a sum of terms that show up in $P(k)$ and another term.

  For us,
  $$P(k + 1) : 1 + 3 + 5 + \cdots + (2k - 1) + (2(k + 1) - 1) = (k + 1)^2.$$
  For the induction step, we assume that
  $$P(k) := 1 + 3 + 5 + \cdots + (2k - 1) = k^2$$
  is true and thus $P(k + 1)$ is true if, and only if
  $$k^2 + (2(k + 1) - 1) = (k + 1)^2.$$
  Using the known (and accepted) rules of algebra, we check that
  $$k^2 + (2(k + 1) - 1) = k^2 + 2k + 2 - 1 = k^2 + 2k + 1 = (k + 1)^2,$$
  and hence $P(k + 1)$ is true. Because we have shown that $P(1)$ is true and for all $k \geq 1$, $P(k) \implies P(k + 1)$, by the Principle of Induction, we conclude that for all $k \geq 1$,
  $$1 + 3 + 5 + \cdots + (2k - 1) = k^2.$$

■

Second Principle of Induction (Strong Induction)

Let $P(n)$ denote a statement about the natural numbers with the following properties:

(a) **Base case:** Prove that $P(1)$ is true

(b) **Induction step:** Assume **induction hypothesis** ($P(j)$ **is true for** $1 \leq j \leq k$).
Prove that if $P(j)$ **is true for** $1 \leq j \leq k$,
then $P(k+1)$ must be true.

By the **(second)** principle of mathematical induction the statement $P(n)$ holds for every natural number n. **QED.**”

Example 1.11 *Let's prove the* ***Theorem****: (Fundamental Theorem of Arithmetic) Every natural number $n \geq 2$ can be factored as a product of one or more primes.*

Proof:

- Step 0: We write down the statements. For $k \geq 2$, $P(k)$: there exist $i_k \geq 1$ and prime numbers $p_1, p_2, \ldots, p_{i_k}$ such that the product $p_1 \cdots p_{i_k} = k$.
- Step 1: Check the base case, $P(2)$: For $k = 2$, we have that $2 = 2$, and hence the base case is true.
- Step 2: Show the induction hypothesis is true. That is, using the fact that $P(j)$ is true for $1 \leq j \leq k$, show that $P(k+1)$ is true, that is, $k+1$ can be expressed as a product of primes. There are two cases:

  (a) Case 1: $k+1$ is prime. In this case, we are done because $k+1$ is already the product of one prime, namely itself.

  (b) Case 2: $k+1$ is composite. Then, there exist two natural numbers a and b, $2 \leq a, b \leq k$, such that $k+1 = a \cdot b$.

  Because a and b are natural numbers that are greater than or equal to 2 and less than or equal to k, by the induction step:

  $$\begin{aligned} P(a) &\implies a = p_1 \cdot p_2 \cdot \cdots \cdot p_{i_a}, \text{ for some primes } p_i \\ P(b) &\implies b = q_1 \cdot q_2 \cdot \cdots \cdot q_{j_b}, \text{ for some primes } q_j \end{aligned}$$

  Hence, $a \cdot b = (p_1 \cdot p_2 \cdot \cdots \cdot p_{i_a}) \cdot (q_1 \cdot q_2 \cdot \cdots \cdot q_{j_b})$, which is a product of primes.

■

Proposition Any postage of 8¢ or more is possible using 3¢ and 5¢ stamps.

Proof. We will use strong induction.

(1) This holds for postages of 8, 9 and 10 cents: For 8¢, use one 3¢ stamp and one 5¢ stamp. For 9¢, three 3¢ stamps. For 10¢, two 5¢ stamps.

(2) Let $k \geq 10$, and for each $8 \leq m \leq k$, assume a postage of m cents can be obtained exactly with 3¢ and 5¢ stamps. (That is, assume statements $S_8, S_9, \ldots, S_k$ are all true.) We must show that S_{k+1} is true, that is, $(k+1)$-cents postage can be achieved with 3¢ and 5¢ stamps. By assumption, S_{k-2} is true. Thus we can get $(k-2)$-cents postage with 3¢ and 5¢ stamps. Now just add one more 3¢ stamp, and we have $(k-2)+3 = k+1$ cents postage with 3¢ and 5¢ stamps. ■

Note on our Strong Induction proofs

- We genuinely needed the strong induction part to “reach back” into some $P(j)$ where j was not k.
- The Fundamental Theorem of Arithmetic actually says that any factorization natural number greater than or equal to 2 has a unique prime factorization. But we are going by the textbook.

Standard and Strong Induction are Equivalent

Equivalence of Strong and Ordinary Induction: Let $P(k)$ be the set of logical statements that are used with Strong Induction. Then the induction step is equivalent to

$$(P(1) \wedge P(2) \wedge \cdots \wedge P(k)) \implies P(k+1), \tag{1.1}$$

because we assume that $P(j)$ is true for $1 \leq j \leq k$. Next, you can note that (1.1) is equivalent to

$$P(1) \wedge P(2) \wedge \cdots \wedge P(k) \implies P(1) \wedge P(2) \wedge \cdots \wedge P(k) \wedge P(k+1), \tag{1.2}$$

because if $P(1) \wedge P(2) \wedge \cdots \wedge P(k) = \mathbf{T}$, then

$$(P(1) \wedge P(2) \wedge \cdots \wedge P(k) \wedge P(k+1) = \mathbf{T}) \iff (P(k+1) = \mathbf{T}).$$

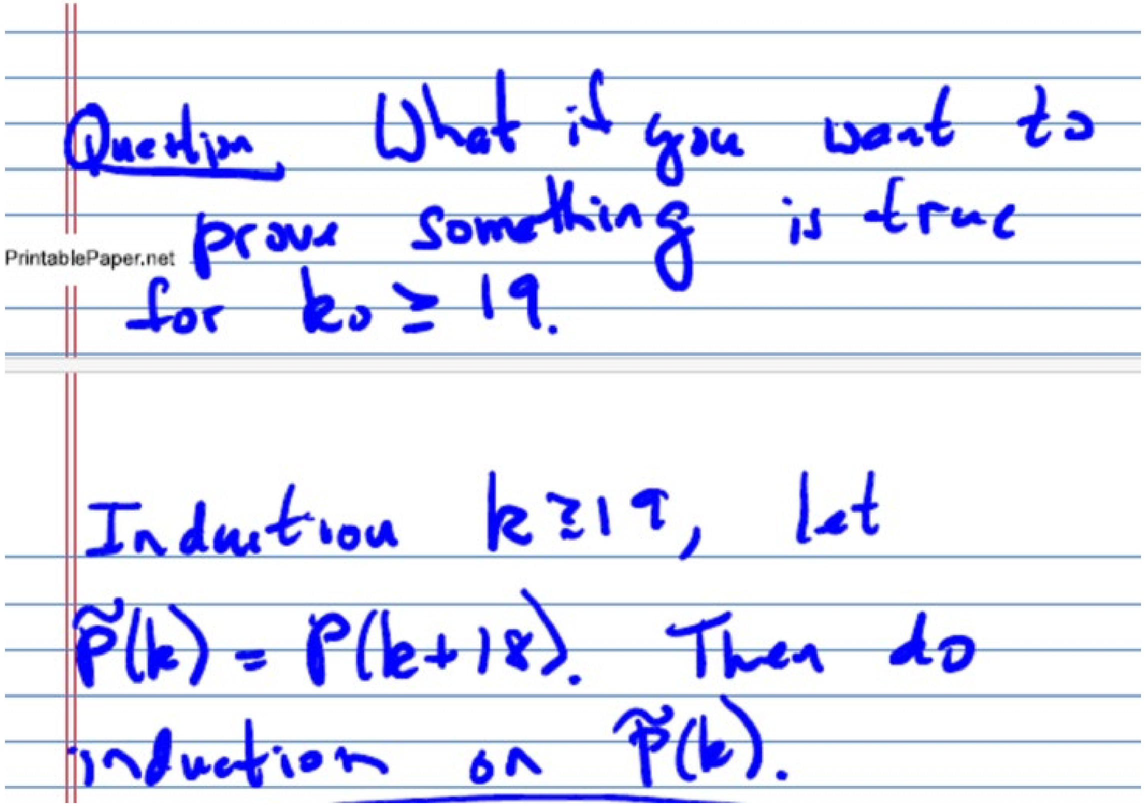
It follows that Ordinary Induction on

$$Q(k) := P(1) \wedge P(2) \wedge \cdots \wedge P(k)$$

is equivalent to Strong Induction on $P(k)$.

Other Notes on Induction

- The Base Case should start at $P(1)$ but we can replace the 1 with another positive integer and the machinery of the inductive proof still works



Question What if you want to prove something is true for $k_0 \geq 19$.

Induction $k \geq 19$, let $\tilde{P}(k) = P(k+18)$. Then do induction on $\tilde{P}(k)$.

Non-obvious Inductive Proof

Theorem: The sum of the angles in any convex polygon with n vertices is $(n-2)\cdot 180°$

Things we have:

- **Definition:** A convex polygon is a polygon where, for any two points in or on the polygon, the line between those points is contained within the polygon.
- **Theorem:** Any line drawn through a convex polygon splits that polygon into two convex polygons.
- **Theorem:** Angles in a triangle add up to 180°

Indirect Proof Techniques

- **Proof by Contrapositive**
- **Proof by Contradiction**

- Art and craft of proofs: picking which proof techniques to try

Proof by Contrapositive

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

Proof by Contrapositive

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

Proof. We will prove the **contrapositive**. ← (If n is *not* even, then n^2 is not even.)

Let n be an integer.

Suppose that n is not even, and thus odd.

Then, there exists an integer k such that $n = 2k + 1$

Then, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

Since $2k^2 + 2k$ is an integer, we see that n^2 is odd and therefore not even. ■

Proof by Contradiction

A logical contradiction is an assertion that is false for all possible values of its variables:

$$R \wedge (\sim R) = \boldsymbol{T}$$

If I assume a statement is true, and then derive a logical contradiction from that assumption, the assumption must be false.

We can use the above to our advantage!

$$\big(p \implies (\exists\, R \text{ such that } R \wedge (\sim R) = \mathbf{T})\big) \iff p = \mathbf{F}.$$

Euclid's Proof that $\sqrt{2}$ is irrational

- We define $p : \sqrt{2}$ is an irrational number.
- We start with the assumption $(\sim p = \mathbf{T})$, that is, $\sqrt{2}$ is a rational number.
- Based on that assumption, we can deduce there exist integers m and n, $n \neq 0$, such that $\sqrt{2} = \frac{m}{n}$ and m and n do not have a common factor.
- We now define ($R : m$ and n do not have a common factor) and know that $R = \mathbf{T}$.
- However, from $\sqrt{2} = \frac{m}{n}$, we show that m and n have 2 as a common factor.
- We now have $\sim R = \mathbf{T}$.
- Hence, $(R \wedge (\sim R)) = \mathbf{T}$, **which is a contradiction**.
- Conclusion: $\sim p = \mathbf{T}$ is impossible, and therefore $\sim p = \mathbf{F}$.
- Hence, $p = \mathbf{T}$ and we have proved that $\sqrt{2}$ is irrational. Pretty cool!

Proof: Our statement is $p : \sqrt{2}$ is irrational. We assume $\sim p : \sqrt{2}$ is rational. We seek to show that this leads to the existence of a statement R that is both true and false, a contradiction.

If $\sqrt{2}$ is rational, then there exist natural numbers m and n such that

- m and n have no common factors,
- $n \neq 0$, and

$$\sqrt{2} = \frac{m}{n}. \tag{1.3}$$

All we have done is apply the definition of a rational number. Next, we square both sides of (1.3) to arrive at

$$\left(2 = \frac{m^2}{n^2}\right) \implies \left(2n^2 = m^2\right) \implies \left(m^2 \text{ is even}\right).$$

From our result in Example 1.4, we deduce that m must be even, and hence there must exist an integer k such that $m = 2k$.

From $2n^2 = m^2$, we deduce that

$$\left(2n^2 = (2k)^2\right) \implies \left(2n^2 = 4k^2\right) \implies \left(n^2 = 2k^2\right) \implies n^2 \text{ is even}.$$

Once again appealing to our result in Example 1.4, we deduce that n must be even, and hence there must exist an integer j such that $n = 2j$.

Because both m and n are even, they have 2 as a common factor, which is a contradiction to m and n have no common factors.

Because we arrived at this contradiction from the statement "$\sqrt{2}$ is rational", we deduce that "$\sqrt{2}$ is rational" must be false. Hence, $\sqrt{2}$ is irrational. ■.

Proof by Contradiction

“It is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game.”

— **G.H. Hardy**

What is a…

- Scalar
- Vector
- Linear Combination
    - Linear Independence/Dependence

What is a scalar? A user’s perspective

- Quantity with only magnitude but no direction
- Practicality ($):

+ − × ÷

What is a ~~scalar~~ field?

- **Definition:** A **field** consists of a set, denoted by $\mathcal{F}$, of elements called **scalars** and two operations called **addition** “+” and **multiplication** “ $\cdot$ ”; the two operations are defined over $\mathcal{F}$ such that they satisfy the following conditions:
    - **Field Axioms** 1) – 7)

- We have seen binary operations before.

Definition 2.1 *(Chen, 2nd edition, page 8) : A* ***field*** *consists of a set, denoted by $\mathcal{F}$, of elements called* **scalars** *and two operations called addition "+" and multiplication "·"; the two operations are defined over $\mathcal{F}$ such that they satisfy the following conditions:*

1. *To every pair of elements α and β in $\mathcal{F}$, there correspond an element $\alpha + \beta$ in $\mathcal{F}$ called the* sum *of α and β, and an element $\alpha \cdot \beta$ (or simply $\alpha\beta$) in $\mathcal{F}$ called the* product *of α and β.*
2. *Addition and multiplication are respectively commutative: For any α and β in $\mathcal{F}$,*

$$\alpha + \beta = \beta + \alpha \qquad\qquad \alpha \cdot \beta = \beta \cdot \alpha$$

3. *Addition and multiplication are respectively associative: For any α, β, γ in $\mathcal{F}$,*

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \qquad\qquad (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$

4. *Multiplication is distributive with respect to addition: For any α, β, γ in $\mathcal{F}$,*

$$\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$$

5. *$\mathcal{F}$ contains an element, denoted by 0, and an element, denoted by 1, such that $\alpha + 0 = \alpha$ and $1 \cdot \alpha = \alpha$ for every α in $\mathcal{F}$.*
6. *To every α in $\mathcal{F}$, there is an element β in $\mathcal{F}$ such that $\alpha + \beta = 0$. The element β is called the* additive inverse.
7. *To every α in $\mathcal{F}$ which is not the element 0, there is an element γ in $\mathcal{F}$ such that $\alpha \cdot \gamma = 1$. The element γ is called the* multiplicative inverse.

Closure

Defi[illegible]*hen, 2nd edition, page 8) : A* ***field*** *consists of a set, denoted by $\mathcal{F}$, of elements called* ***scalars*** *and two operations* [illegible] *“+” and multiplication “·”; the two operations are defined over $\mathcal{F}$ such that they satisfy the following conditions:*

1. *To every pair of elements α and β in $\mathcal{F}$, there correspond an element $\alpha + \beta$ in $\mathcal{F}$ called the* sum *of α and β, and an element $\alpha \cdot \beta$ (or simply $\alpha\beta$) in $\mathcal{F}$ called the* product *of α and β.*
2. *Addition and multiplication are respectively commutative: For any α and β in $\mathcal{F}$,*

$$\alpha + \beta = \beta + \alpha \qquad\qquad \alpha \cdot \beta = \beta \cdot \alpha$$

3. *Addition and multiplication are respectively associative: For any α, β, γ in $\mathcal{F}$,*

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \qquad\qquad (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$

4. *Multiplication is distributive with respect to addition: For any α, β, γ in $\mathcal{F}$,*

$$\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$$

5. *$\mathcal{F}$ contains an element, denoted by 0, and an element, denoted by 1, such that $\alpha + 0 = \alpha$ and $1 \cdot \alpha = \alpha$ for every α in $\mathcal{F}$.*
6. *To every α in $\mathcal{F}$, there is an element β in $\mathcal{F}$ such that $\alpha + \beta = 0$. The element β is called the* additive inverse.
7. *To every α in $\mathcal{F}$ which is not the element 0, there is an element γ in $\mathcal{F}$ such that $\alpha \cdot \gamma = 1$. The element γ is called the* multiplicative inverse.

Closure

Commutativity

Def hen, 2nd page 8) : A ***field*** *consists of a set, denoted by $\mathcal{F}$, of elements called* ***scalars*** *and two operations* tion “·”; *the two operations are defined over $\mathcal{F}$ such that they satisfy the following conditions:*

1. *of elements α and β in $\mathcal{F}$, there correspond an element $\alpha + \beta$ in $\mathcal{F}$ called the* sum *of α and β, and an element (or simply $\alpha\beta$) in $\mathcal{F}$ called the* product *of α and β.*

2. *Addition and multiplication are respectively commutative: For any α and β in $\mathcal{F}$,*

$$\alpha + \beta = \beta + \alpha \qquad\qquad \alpha \cdot \beta = \beta \cdot \alpha$$

3. *Addition and multiplication are respectively associative: For any α, β, γ in $\mathcal{F}$,*

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \qquad\qquad (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$

4. *Multiplication is distributive with respect to addition: For any α, β, γ in $\mathcal{F}$,*

$$\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$$

5. *$\mathcal{F}$ contains an element, denoted by 0, and an element, denoted by 1, such that $\alpha + 0 = \alpha$ and $1 \cdot \alpha = \alpha$ for every α in $\mathcal{F}$.*
6. *To every α in $\mathcal{F}$, there is an element β in $\mathcal{F}$ such that $\alpha + \beta = 0$. The element β is called the* additive inverse.
7. *To every α in $\mathcal{F}$ which is not the element 0, there is an element γ in $\mathcal{F}$ such that $\alpha \cdot \gamma = 1$. The element γ is called the* multiplicative inverse.

Closure

Commutativity

Associativity

Defihen, 2nd page 8) : A ***field*** consists of a set, denoted by $\mathcal{F}$, of elements called ***scalars*** and two operations tion "$\cdot$"; the two operations are defined over $\mathcal{F}$ such that they satisfy the following conditions:

1. of elements α and β in $\mathcal{F}$, there correspond an element $\alpha + \beta$ in $\mathcal{F}$ called the sum of α and β, and an element (or simply $\alpha\beta$) in $\mathcal{F}$ called the product of α and β.

2. *Addition an on are respectively commutative: For any α and β in $\mathcal{F}$,*

$$\alpha + \beta = \beta + \alpha \qquad \alpha \cdot \beta = \beta \cdot \alpha$$

3. *Addition and multiplication are respectively associative: For any α, β, γ in $\mathcal{F}$,*

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \qquad (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$

4. *Multiplication is distributive with respect to addition: For any α, β, γ in $\mathcal{F}$,*

$$\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$$

5. *$\mathcal{F}$ contains an element, denoted by 0, and an element, denoted by 1, such that $\alpha + 0 = \alpha$ and $1 \cdot \alpha = \alpha$ for every α in $\mathcal{F}$.*

6. *To every α in $\mathcal{F}$, there is an element β in $\mathcal{F}$ such that $\alpha + \beta = 0$. The element β is called the* additive inverse.

7. *To every α in $\mathcal{F}$ which is not the element 0, there is an element γ in $\mathcal{F}$ such that $\alpha \cdot \gamma = 1$. The element γ is called the* multiplicative inverse.

Closure

Defi… hen, 2nd … page 8) : A ***field*** consists of a set, denoted by $\mathcal{F}$, of elements called **scalars** and two operations … tion "·"; the two operations are defined over $\mathcal{F}$ such that they satisfy the following conditions:

Commutativity

1. … of elements α and β in $\mathcal{F}$, there correspond an element $\alpha + \beta$ in $\mathcal{F}$ called the sum of α and β, and an element … (or simply $\alpha\beta$) in $\mathcal{F}$ called the product of α and β.

Associativity

2. Addition an… on are respectively commutative: For any α and β in $\mathcal{F}$,

$$\alpha + \beta = \beta + \alpha \qquad\qquad \alpha \cdot \beta = \beta \cdot \alpha$$

Distributivity

3. Addition an… on are respectively associative: For any α, β, γ in $\mathcal{F}$,

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \qquad\qquad (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$

4. Multiplication is distributive with respect to addition: For any α, β, γ in $\mathcal{F}$,

$$\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$$

5. $\mathcal{F}$ contains an element, denoted by 0, and an element, denoted by 1, such that $\alpha + 0 = \alpha$ and $1 \cdot \alpha = \alpha$ for every α in $\mathcal{F}$.

6. To every α in $\mathcal{F}$, there is an element β in $\mathcal{F}$ such that $\alpha + \beta = 0$. The element β is called the additive inverse.

7. To every α in $\mathcal{F}$ which is not the element 0, there is an element γ in $\mathcal{F}$ such that $\alpha \cdot \gamma = 1$. The element γ is called the multiplicative inverse.

Closure

Defi hen, 2nd page 8) : *A* ***field*** *consists of a set, denoted by* $\mathcal{F}$*, of elements called* **scalars** *and two operations* tion "·"; *the two operations are defined over* $\mathcal{F}$ *such that they satisfy the following conditions:*

Commutativity

1. *elements* α *and* β *in* $\mathcal{F}$*, there correspond an element* $\alpha + \beta$ *in* $\mathcal{F}$ *called the* sum *of* α *and* β*, and an element* *(or simply* $\alpha\beta$*) in* $\mathcal{F}$ *called the* product *of* α *and* β*.*

Associativity

2. *Addition* *on are respectively commutative: For any* α *and* β *in* $\mathcal{F}$*,*

$$\alpha + \beta = \beta + \alpha \qquad \alpha \cdot \beta = \beta \cdot \alpha$$

Distributivity

3. *Addition* *on are respectively associative: For any* α*,* β*,* γ *in* $\mathcal{F}$*,*

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \qquad (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$

4. *Multiplic* *ion is distributive with respect to addition: For any* α*,* β*,* γ *in* $\mathcal{F}$*,*

Identity

$$\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$$

5. $\mathcal{F}$ *contains an element, denoted by* 0*, and an element, denoted by* 1*, such that* $\alpha + 0 = \alpha$ *and* $1 \cdot \alpha = \alpha$ *for every* α *in* $\mathcal{F}$*.*
6. *To every* α *in* $\mathcal{F}$*, there is an element* β *in* $\mathcal{F}$ *such that* $\alpha + \beta = 0$*. The element* β *is called the* additive inverse.
7. *To every* α *in* $\mathcal{F}$ *which is not the element 0, there is an element* γ *in* $\mathcal{F}$ *such that* $\alpha \cdot \gamma = 1$*. The element* γ *is called the* multiplicative inverse.

Closure

Commutativity

Defi *hen, 2nd* *page 8) : A **field** consists of a set, denoted by $\mathcal{F}$, of elements called **scalars** and two operations* *tion "·"; the two operations are defined over $\mathcal{F}$ such that they satisfy the following conditions:*

of elements α and β in $\mathcal{F}$, there correspond an element $\alpha+\beta$ in $\mathcal{F}$ called the sum *of α and β, and an element* *(or simply $\alpha\beta$) in $\mathcal{F}$ called the* product *of α and β.*

Associativity

2. *Addition ar* *on are respectively commutative: For any α and β in $\mathcal{F}$,*

$$\alpha+\beta=\beta+\alpha \qquad \alpha\cdot\beta=\beta\cdot\alpha$$

Distributivity

3. *Addition an* *on are respectively associative: For any α, β, γ in $\mathcal{F}$,*

$$(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma) \qquad (\alpha\cdot\beta)\cdot\gamma=\alpha\cdot(\beta\cdot\gamma)$$

4. *Multiplic* *ion is distributive with respect to addition: For any α, β, γ in $\mathcal{F}$,*

$$\alpha\cdot(\beta+\gamma)=(\alpha\cdot\beta)+(\alpha\cdot\gamma)$$

Identity

Inverses

an element, denoted by 0, and an element, denoted by 1, such that $\alpha+0=\alpha$ and $1\cdot\alpha=\alpha$ for every α in $\mathcal{F}$.

6. *To every α in $\mathcal{F}$, there is an element β in $\mathcal{F}$ such that $\alpha+\beta=0$. The element β is called the* additive inverse.

7. *To every α in $\mathcal{F}$ which is not the element 0, there is an element γ in $\mathcal{F}$ such that $\alpha\cdot\gamma=1$. The element γ is called the* multiplicative inverse.

Definition 2.1 *(Chen, 2nd edition, page 8) : A* ***field*** *consists of a set, denoted by* $\mathcal{F}$*, of elements called* **scalars** *and two operations called addition "+" and multiplication "·"; the two operations are defined over* $\mathcal{F}$ *such that they satisfy the following conditions:*

1. *To every pair of elements* α *and* β *in* $\mathcal{F}$*, there correspond an element* $\alpha + \beta$ *in* $\mathcal{F}$ *called the* sum *of* α *and* β*, and an element* $\alpha \cdot \beta$ *(or simply* $\alpha\beta$*) in* $\mathcal{F}$ *called the* product *of* α *and* β.
2. *Addition and multiplication are respectively commutative: For any* α *and* β *in* $\mathcal{F}$,

$$\alpha + \beta = \beta + \alpha \qquad \qquad \alpha \cdot \beta = \beta \cdot \alpha$$

3. *Addition and multiplication are respectively associative: For any* α*,* β*,* γ *in* $\mathcal{F}$,

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \qquad \qquad (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$

4. *Multiplication is distributive with respect to addition: For any* α*,* β*,* γ *in* $\mathcal{F}$,

$$\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$$

5. $\mathcal{F}$ *contains an element, denoted by* 0*, and an element, denoted by* 1*, such that* $\alpha + 0 = \alpha$ *and* $1 \cdot \alpha = \alpha$ *for every* α *in* $\mathcal{F}$.
6. *To every* α *in* $\mathcal{F}$*, there is an element* β *in* $\mathcal{F}$ *such that* $\alpha + \beta = 0$*. The element* β *is called the* additive inverse.
7. *To every* α *in* $\mathcal{F}$ *which is not the element 0, there is an element* γ *in* $\mathcal{F}$ *such that* $\alpha \cdot \gamma = 1$*. The element* γ *is called the* multiplicative inverse.

Fields or Not?

- Canonical Example:

$$\mathbb{R}$$

- How to tell?

$$\mathbb{Z}, \mathbb{C}, \mathbb{Q}, \mathbb{N}$$

- Are all fields infinite?

Fields or Not?

- Canonical Example:

$$\mathbb{R}$$

- How to tell?

$$\mathbb{Z}, \mathbb{C}, \mathbb{Q}, \mathbb{N}, \mathbb{R}^{2\times 2}$$

Fields or Not?

- Canonical Example:

$$\mathbb{R}$$

- How to tell?

$$\cancel{\mathbb{Z}}, \mathbb{C}, \mathbb{Q}, \cancel{\mathbb{N}}, \cancel{\mathbb{R}^{2\times 2}}$$

$\underline{7}$ $\underline{5,6,7}$ $\underline{2,7}$ Axioms Failed

More Fields

- Are all fields infinite?
- Are there interesting fields?

More Fields

- Are all fields infinite? **No**
- Are there “*interesting*” fields? **Yes**

Finite Field {0,1}

+	**0**	**1**
0	0	1
1	1	0

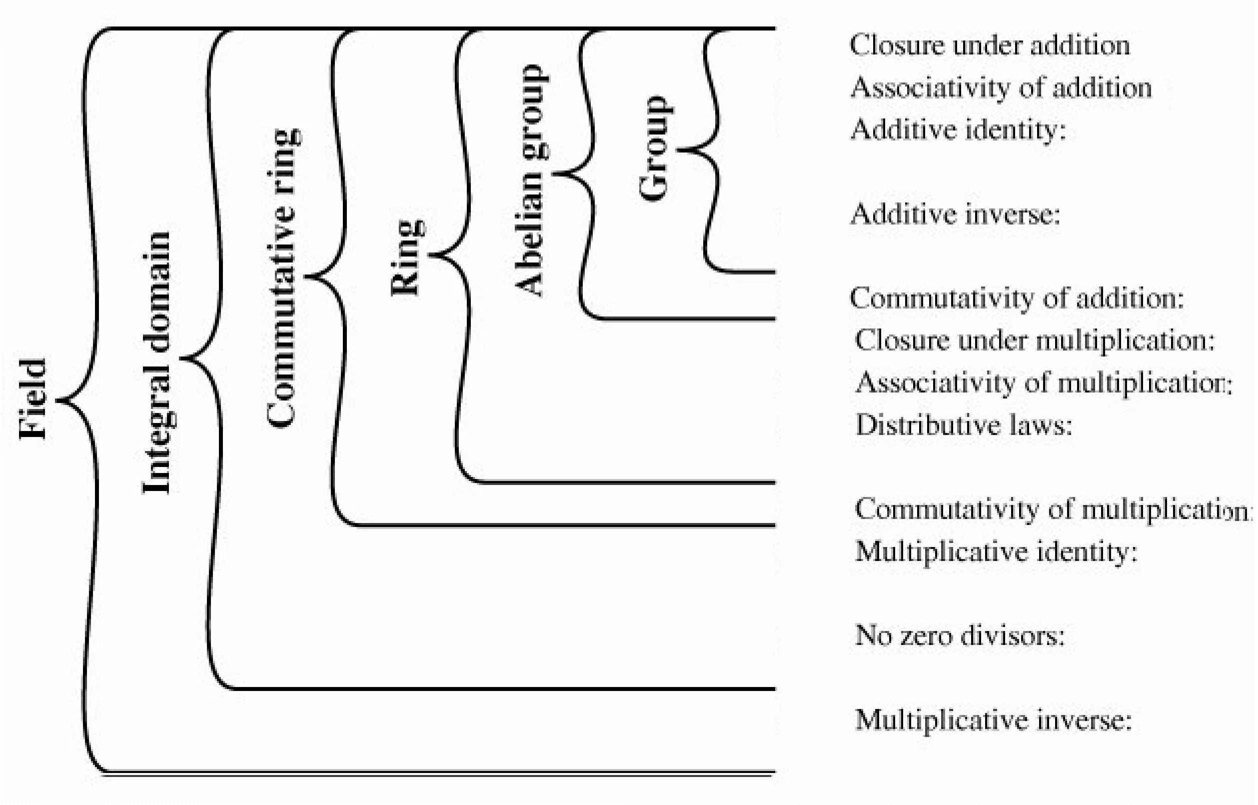
•	**0**	**1**
0	0	0
1	0	1

Levels of thinking

- Field Axioms
- Scalar as magnitude
- “Like $\mathbb{R}$ ”

Levels of thinking

- **Field Axioms: Thinking like a mathematician**
  - **What if I start dropping axioms — it is no longer a field — but do I get something else?**
    - **Yes, rings, groups, etc.**
- Scalar as magnitude
- “Like $\mathbb{R}$ ”



What is a vector? A user’s perspective

- Quantity with magnitude and direction
- Practicality (physics):

$+ \quad - \quad \bullet \quad \times$

What is a vector (or linear) space?

- **Definition:** A **vector space** (or, **linear space**) over a field $\mathcal{F}$, denoted by $(\mathcal{X},\mathcal{F})$, consists of a set, denoted by $\mathcal{X}$, of elements called **vectors**, a field $\mathcal{F}$, and two operations called **vector addition** and **scalar multiplication**. The two operations are defined over $\mathcal{X}$ and $\mathcal{F}$ such that they satisfy all the following conditions:
  - **Vector Axioms** 1) – 10)

- These axioms look familiar
- The definition of vectors builds on the definition of scalars

Definition 2.2 *(Chen 2nd Edition, page 9) A* ***vector space (or, linear space)*** *over a field $\mathcal{F}$, denoted by $(\mathcal{X}, \mathcal{F})$, consists of a set, denoted by $\mathcal{X}$, of elements called* ***vectors****, a field $\mathcal{F}$, and two operations called* ***vector addition*** *and* ***scalar multiplication****. The two operations are defined over $\mathcal{X}$ and $\mathcal{F}$ such that they satisfy all the following conditions:*

1. *To every pair of vectors v^1 and v^2 in $\mathcal{X}$, there corresponds a vector $v^1 + v^2$ in $\mathcal{X}$, called the sum of v^1 and v^2*[1].
2. *Addition is commutative: For any v^1, v^2 in $\mathcal{X}$, $v^1 + v^2 = v^2 + v^1$.*
3. *Addition is associative: For any v^1, v^2, and v^3 in $\mathcal{X}$, $\left(v^1 + v^2\right) + v^3 = v^1 + \left(v^2 + v^3\right)$.*
4. *$\mathcal{X}$ contains a vector, denoted by $\boldsymbol{0}$, such that $\boldsymbol{0} + v = v$ for every v in $\mathcal{X}$. The vector $\boldsymbol{0}$ is called the zero vector or the origin.*
5. *To every v in $\mathcal{X}$, there is a vector $\bar{v}$ in $\mathcal{X}$, such that $v + \bar{v} = 0$.*
6. *To every α in $\mathcal{F}$, and every v in $\mathcal{X}$, there corresponds a vector $\alpha \cdot v$ in $\mathcal{X}$ called the* scalar product *of α and v.*
7. *Scalar multiplication is associative: For any α, β in $\mathcal{F}$ and any v in $\mathcal{X}$, $\alpha \cdot (\beta \cdot x) = (\alpha \cdot \beta) \cdot x$*
8. *Scalar multiplication is distributive with respect to vector addition: For any α in $\mathcal{F}$ and any v^1, v^2 in $\mathcal{X}$, $\alpha \cdot \left(v^1 + v^2\right) = \alpha \cdot v^1 + \alpha \cdot v^2$.*
9. *Scalar multiplication is distributive with respect to scalar addition: For any α, β in $\mathcal{F}$ and any v in $\mathcal{X}$, $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$.*
10. *For any v in $\mathcal{X}$, $1 \cdot v = v$, where 1 is the element 1 in $\mathcal{F}$.*

---

[1] We use superscripts v^1, v^2, v^3 to denote different *vectors*. The superscripts *do not* denote powers.

Definition 2.2 *(Chen 2nd Edition, page 9) A* ***vector space (or, linear space)*** *over a field $\mathcal{F}$, denoted by $(\mathcal{X}, \mathcal{F})$, consists of a set, denoted by $\mathcal{X}$, of elements called* ***vectors****, a field $\mathcal{F}$, and two operations called* ***vector addition*** *and* ***scalar multiplication****. The two operations are defined over $\mathcal{X}$ and $\mathcal{F}$ such that they satisfy all the following conditions:*

1. *To every pair of vectors v^1 and v^2 in $\mathcal{X}$, there corresponds a vector $v^1 + v^2$ in $\mathcal{X}$, called the sum of v^1 and v^2*[1].
2. *Addition is commutative: For any v^1, v^2 in $\mathcal{X}$, $v^1 + v^2 = v^2 + v^1$.*
3. *Addition is associative: For any v^1, v^2, and v^3 in $\mathcal{X}$, $(v^1 + v^2) + v^3 = v^1 + (v^2 + v^3)$.*
4. *$\mathcal{X}$ contains a vector, denoted by $\mathbf{0}$, such that $\mathbf{0} + v = v$ for every v in $\mathcal{X}$. The vector $\mathbf{0}$ is called the zero vector or the origin.*
5. *To every v in $\mathcal{X}$, there is a vector $\bar{v}$ in $\mathcal{X}$, such that $v + \bar{v} = 0$.*
6. *To every α in $\mathcal{F}$, and every v in $\mathcal{X}$, there corresponds a vector $\alpha \cdot v$ in $\mathcal{X}$ called the* scalar product *of α and v.*
7. *Scalar multiplication is associative: For any α, β in $\mathcal{F}$ and any v in $\mathcal{X}$, $\alpha \cdot (\beta \cdot x) = (\alpha \cdot \beta) \cdot x$* ← Typo in book!
8. *Scalar multiplication is distributive with respect to vector addition: For any α in $\mathcal{F}$ and any v^1, v^2 in $\mathcal{X}$, $\alpha \cdot (v^1 + v^2) = \alpha \cdot v^1 + \alpha \cdot v^2$.*
9. *Scalar multiplication is distributive with respect to scalar addition: For any α, β in $\mathcal{F}$ and any v in $\mathcal{X}$, $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$.*
10. *For any v in $\mathcal{X}$, $1 \cdot v = v$, where 1 is the element 1 in $\mathcal{F}$.*

---

[1] We use superscripts v^1, v^2, v^3 to denote different *vectors*. The superscripts *do not* denote powers.

Vector Spaces or not?

- Main Example:

$$(\mathbb{R}^n, \mathbb{R})$$

- How to tell?

$$(\mathbb{R}, \mathbb{C}) \quad (\mathbb{C}, \mathbb{R}) \quad (\mathbb{Q}, \mathbb{R})$$

$$(\mathbb{R}, \mathbb{R}) \quad (\mathbb{C}, \mathbb{C}) \quad (\mathbb{Q}, \mathbb{Q})$$

Vector Spaces or not?

- Main Example:

$$(\mathbb{R}^n, \mathbb{R})$$

- How to tell?

$$\cancel{(\mathbb{R}, \mathbb{C})} \quad (\mathbb{C}, \mathbb{R}) \quad \cancel{(\mathbb{Q}, \mathbb{R})}$$

$$(\mathbb{R}, \mathbb{R}) \quad (\mathbb{C}, \mathbb{C}) \quad (\mathbb{Q}, \mathbb{Q})$$

Vector Spaces $(\mathcal{X}, \mathcal{F})$

- $\mathcal{X} = \mathcal{F}^n$

  The set of n-tuples $\mathcal{F}^n := \left\{ \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \middle| \alpha_i \in \mathcal{F}, 1 \leq i \leq n \right\},$

  where vector addition and scalar multiplication are defined as:

$$(a)\ \textit{Vector Addition:}\ \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} + \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = \begin{bmatrix} \alpha_1 + \beta_1 \\ \vdots \\ \alpha_n + \beta_n \end{bmatrix}$$

$$(b)\ \textit{Scalar Multiplication:}\ \alpha \cdot x = \begin{bmatrix} \alpha x_1 \\ \vdots \\ \alpha x_n \end{bmatrix}$$

Vector Spaces $(\mathcal{X}, \mathcal{F})$

- $\mathcal{X} = \mathcal{F}^{n\times m}$
  The set of *n* x m matrices with coefficients in $\mathcal{F}$

$$\mathcal{F}^{n\times m} := \left\{ \begin{bmatrix} A_{1,1} & \dots & A_{1,m} \\ \vdots & \ddots & \vdots \\ A_{n,1} & \dots & A_{n,m} \end{bmatrix} \middle| A_{i,j} \in \mathcal{F},\ 1 \le i \le n,\ 1 \le j \le m \right\},$$

where vector addition and scalar multiplication are defined as:

$$[A+B]_{ij} := [A]_{ij} + [B]_{ij}$$

$$\alpha \in \mathbb{R},\ [\alpha A]_{ij} := \alpha [A]_{ij}$$

- Matrices can be viewed as vectors

Interesting Vector Spaces $(\mathcal{X},\mathcal{F})$

- $\mathcal{X}=\mathcal{F}$

  Every field forms a vector space over **itself**. $(\mathcal{F},\mathcal{F})$

  e.g., $(\mathbb{R},\mathbb{R})$ $(\mathbb{C},\mathbb{C})$ $(\mathbb{Q},\mathbb{Q})$

- $\mathcal{X}=\{f:D\to\mathbb{R}\}$ where $D\subset\mathbb{R}$, and $\mathcal{F}=\mathbb{R}$

  The set of all real-valued functions on *D*, where vector addition and scalar multiplication are defined as:

$$(a)\ \ \forall\ f,g\in\mathcal{X},\ define\ f+g\in\mathcal{X}\ by\ \forall t\in D,\ (f+g)(t):=f(t)+g(t);$$

$$(b)\ \ \forall\ f\in\mathcal{X}\ and\ \alpha\in\mathbb{R},\ define\ \alpha\cdot f\in\mathcal{X}\ by\ \forall t\in D,(\alpha\cdot f)(t):=\alpha\cdot f(t).$$

Interesting Vector Spaces $(\mathcal{X}, \mathcal{F})$

- $\mathcal{X} = \{f : D \to \mathbb{R}\}$ where $D \subset \mathbb{R}$, and $\mathcal{F} = \mathbb{R}$

  The set of all real-valued functions on *D*, where vector addition and scalar multiplication are defined as:

$$(a)\ \forall\ f, g \in \mathcal{X},\ define\ f + g \in \mathcal{X}\ by\ \forall t \in D,\ (f+g)(t) := f(t) + g(t);$$

$$(b)\ \forall\ f \in \mathcal{X}\ and\ \alpha \in \mathbb{R},\ define\ \alpha \cdot f \in \mathcal{X}\ by\ \forall t \in D, (\alpha \cdot f)(t) := \alpha \cdot f(t).$$

- Let’s check Vector Axiom 8 $\alpha \cdot (f+g) = \alpha \cdot f + \alpha \cdot g$
  - We will use the definition of a function evaluated at a point *t*
  - And then rely on the known definitions about real numbers

Let $t \in D$*, then*

(a) *LHS:* $[\alpha \cdot (f+g)](t) := \alpha \cdot [f+g](t) = \alpha \cdot [f(t)+g(t)] = \alpha \cdot f(t) + \alpha \cdot g(t)$

(b) *RHS:* $[\alpha \cdot f + \alpha \cdot g](t) := [\alpha \cdot f](t) + [\alpha \cdot g](t) = \alpha \cdot f(t) + \alpha \cdot g(t)$

(c) *Hence, LHS = RHS and we are done.*

Levels of thinking

- Vector Axioms
- Vectors as magnitude with direction
- Expand your perspective to allow for functions

Subspaces

- **Definition:** Let $(\mathcal{X},\mathcal{F})$ be a vector space, and let $\mathcal{Y}$ be a subset of $\mathcal{X}$. Then $\mathcal{Y}$ is a **subspace** if using the rules of vector addition and scalar multiplication defined in $(\mathcal{X},\mathcal{F})$, we have that $(\mathcal{Y},\mathcal{F})$ is a vector space.

- Note on subsets (proper/strict vs. otherwise)
- The definition builds on definition of a vector space

Subspaces

- **Definition:** Let $(\mathcal{X},\mathcal{F})$ be a vector space, and let $\mathcal{Y}$ be a subset of $\mathcal{X}$. Then $\mathcal{Y}$ is a **subspace** if using the rules of vector addition and scalar multiplication defined in $(\mathcal{X},\mathcal{F})$, we have that $(\mathcal{Y},\mathcal{F})$ is a vector space.

- (**Proposition 2.8 in the book**) The following are equivalent (TFAE)

(a) $(\mathcal{Y},\mathcal{F})$ *is a subspace of* $(\mathcal{X},\mathcal{F})$.

(b) $\forall v^1, v^2 \in \mathcal{Y}, v^1 + v^2 \in \mathcal{Y}$ *(closed under vector addition),*
and $\forall y \in \mathcal{Y}$ *and* $\alpha \in \mathcal{F}, \alpha y \in \mathcal{Y}$ *(closed under scalar multiplication).*

(c) $\forall v^1, v^2 \in \mathcal{Y}, \forall \alpha \in \mathcal{F}, \alpha \cdot v^1 + v^2 \in \mathcal{Y}.$

(d) $\forall v^1, v^2 \in \mathcal{Y}, \forall \alpha_1, \alpha_2 \in \mathcal{F}, \alpha_1 \cdot v^1 + \alpha_2 \cdot v^2 \in \mathcal{Y}.$

Interesting Subspaces?

- Think about it