

# **Discrete Structures and Matrix Algebra**

Propositional Logic

## **Syllabus:**

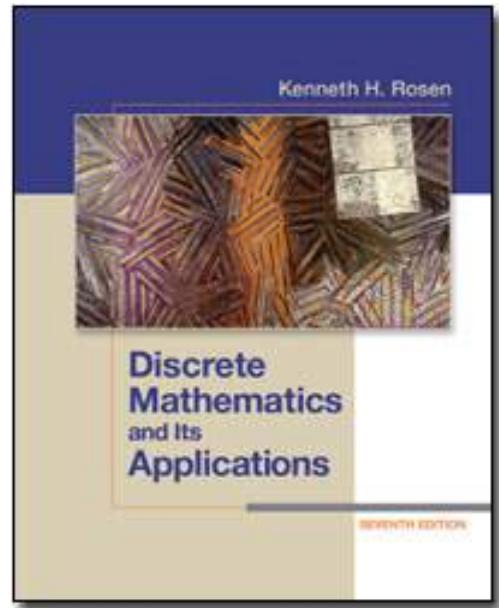
- 1. Unit – 1 [10 Hours]: Mathematical Logic - Propositions, Predicates and Quantifiers, Logical Statements, Equivalence of Statements, Converse, Contrapositive and Inverse Statements, Tautology and Contradiction, Mathematical Inference, Various Proof Strategies, Disprove, Normal Forms;**
- 2. Unit – 2 [8 Hours]: Sets - Basic Set Operations, Functions, Cardinality, Countable and Uncountable Sets, Sequence & Summations; Induction - Principle of Induction, Strong Induction; Recursion - Recursive Algorithms, Recursive Definition of Sets, Structural Induction;**
- 3. Unit – 3 [7 Hours]: Counting techniques - Sum and Product Rule, Inclusion and Exclusion Principles, Pigeonhole Principle, Generalized Pigeonhole Principle, Permutation, Combination, Recurrence Relation, Solving Homogeneous and Non Homogeneous Recurrence Relations, Binomial Coefficients and Identities;**
- 4. Unit – 4 [7 Hours]: Relations - Relations, Equivalence and Partial Order Relations, Partition and Equivalence Classes, Closure of Relation, Representation and Operation on Relations, Posets, Totally Ordered Sets, Well-Ordered Sets, Least and Maximum Elements, Least Upper Bound, Greatest Lower Bound, Lattice;**
- 5. Unit – 5 [9 Hours]: Solving Linear Equations Solving  $Ax = b$ , Elimination with Matrices, Multiplication and Inverse Matrices, Factorization into  $A = LU$ , Transposes and Permutations; Vector Spaces and Subspaces - Spaces of Vectors, Column Space, Null Space, Row Space, Left Null Space, Independence, Basis, and Dimension, Rank and Row Reduced Form, Invertible Matrices;**
- 6. Unit – 6 [7 Hours]: Orthogonality – Orthogonal Vectors and Spaces, Projections, Orthogonal Bases and Gram-Schmidt; Eigen Values and Eigen vectors - Diagonalization, Spectral Decomposition, Symmetric Matrices, Positive Definiteness, Singular Value Decomposition**

# Text Book

Now 8<sup>th</sup> Edition may be available.

PDF for free download of the 7<sup>th</sup> edition is available in the Internet (search for it).

Textbook:



Kenneth H. Rosen.  
*Discrete Mathematics  
and Its Applications,  
7th Edition.* McGraw  
Hill, 2012.

# Evaluation Plan

- Class participation quizzes – 15%
  - Scheduled quizzes – 25%
  - Assignments – 10%
  - Mid – 20%
  - End – 30%
- 
- This may be modified as per the CC meeting.

# Objectives: Discrete Mathematics

We will focus on two major goals:

- Basic tools and techniques in discrete mathematics
  - Propositional logic
  - Set Theory
  - Simple algorithms
  - Induction, recursion
  - Counting techniques (Combinatorics)
- Precise and rigorous mathematical reasoning
  - Writing proofs

# Unit 1 Syllabus

- **Unit – 1** [10 Hours]: Mathematical Logic -  
Propositions, Predicates and Quantifiers, Logical  
Statements, Equivalence of Statements, Converse,  
Contrapositive and Inverse Statements, Tautology  
and Contradiction, Mathematical Inference, Various  
Proof Strategies, Disprove, Normal Forms;

# To do well you should:

- Study with pen and paper
- Ask for help immediately
- Practice, practice, practice...
- Ask questions in class
- Keep up with the class
- Read the book, not just the slides

# Logic and reasoning?

- Logic is the basis of all mathematical reasoning,
- It has practical applications to the design of computing machines,
- Applied to many from artificial intelligence, to computer programming, to programming languages, and to other areas of computer science, as well as to many other fields of study.

# Reasoning about problems

- Is the number of primes finite?
- There exists integers  $a,b,c$  that satisfy the equation  $a^2+b^2 = c^2$
- The program below that I wrote works correctly for all possible inputs.....

# why Proofs?

Everyone knows that proofs are important throughout mathematics, but many people find it surprising how important proofs are in computer science.

- In fact, proofs are used to verify that computer programs produce the correct output for all possible input values,
- to show that algorithms always produce the correct result,
- to establish the security of a system, and
- to create artificial intelligence.

# Tools for reasoning: Logic

## Ch. 1: Introduction to Propositional Logic

- Truth values, truth tables
- Boolean logic:  $\vee \wedge \neg$
- Implications:  $\rightarrow \leftrightarrow$

# Why study propositional logic?

- A formal mathematical “language” for precise reasoning.
- Start with propositions.
- Add other constructs like negation, conjunction, disjunction, implication etc.
- All of these are based on ideas we use daily to reason about things.

# Example of a formal language: Arithmetic

---

E.g., the language of arithmetic

- $x+2 \geq y$  is a sentence;
- $2x+y > \{\}$  is not a sentence
- $x+2 \geq y$  is true iff the number  $x+2$  is no less than the number  $y$
- $x+2 \geq y$  is true in a world where  $x = 7, y = 1$
- $x+2 \geq y$  is false in a world where  $x = 0, y = 6$

**Sentence, statement are interchangeably used. In the following slides it becomes clear.**

# Propositional Logic

# Propositions

- Declarative sentence
- Must be either True or False.

## Propositions:

- Sri City is in Chittoor District.
- Sri City is a City.
- All students at IIIT Sri City are Computer Sc. majors.

## Not propositions:

- Do you like this class?
- There are x students in this class.

# Propositions

- A statement that has a truth value
- Which of the following are propositions?
  - Capital of India is New Delhi.
  - Ron Paul would be a great president.
  - Turn your homework in on Wednesday.
  - Why are we taking this class?
  - If  $n$  is an integer greater than two, then the equation  $a^n + b^n = c^n$  has no solutions in non-zero integers  $a$ ,  $b$ , and  $c$ .
  - Every even integer greater than two can be written as the sum of two primes
  - This statement is false

- The area of logic that deals with propositions is called the **propositional calculus** or **propositional logic**. It was first developed systematically by the Greek philosopher Aristotle more than 2300 years ago.

- We now turn our attention to methods for producing new propositions from those that we already have.
- These methods were discussed by the English mathematician George Boole in 1854 in his book *The Laws of Thought*.
- Many mathematical statements are constructed by combining one or more propositions.
- New propositions, called **compound propositions**, are formed from existing propositions using logical operators.

# Propositions

- Truth value: True or False
- Variables: p,q,r,s,...
- Negation:
- $\neg p$  (“not p”)
- Truth tables

p	$\neg p$
T	F
F	T

# DEFINITION 1

Let  $p$  be a proposition. The negation of  $p$ , denoted by  $\neg p$  (also denoted by  $\bar{p}$ ), is the statement

$\neg p$ : “it is not the case that  $p$  is true”

EXAMPLE 3. Find the negation of the proposition.

“Michael’s PC runs Linux”

**Solution:** The negation is

**“It is not the case that Michael’s PC runs Linux.”**

This negation can be more simply expressed as

**“Michael’s PC does not run Linux.”**

# negating propositions

$\neg p$ : “it is not the case that  $p$  is true”

$p$ : “it rained more than 10 mm in Sri City yesterday”

$p$ : “John has many iPads”

Negate the above. Can you simplify it (in English)

# Conjunction

DEFINITION 2. Let  $p$  and  $q$  be propositions. The conjunction of  $p$  and  $q$ , denoted by  $p \wedge q$ , is the proposition

“ $p$  and  $q$ .” The conjunction  $p \wedge q$  is true when both  $p$  and  $q$  are true and is false otherwise.

# Disjunction

DEFINITION 3. Let  $p$  and  $q$  be propositions. The disjunction of  $p$  and  $q$ , denoted by  $p \vee q$ , is the proposition

“ $p$  or  $q$ .” The disjunction  $p \vee q$  is false when both  $p$  and  $q$  are false and is true otherwise.

# Conjunction, Disjunction

- Conjunction:  $p \wedge q$  ["and"]
- Disjunction:  $p \vee q$  ["or"]

$p$	$q$	$p \wedge q$	$p \vee q$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	F

# Exclusive OR (XOR)

- $p \oplus q$  – T if p and q have different truth values, F otherwise
- Colloquially, we often use OR ambiguously – “A student can attend section A or section B” implies XOR (??!), but
  - “students can take MATH 301 if they have taken MATH 232 or MATH 101” usually means the normal OR (so a student who has taken both is still eligible for MATH 301).

# Conditional

- $p \rightarrow q$  [“if p then q”]
- $p$ : *hypothesis*,  $q$ : *conclusion*
- E.g.: “If you submit a homework late, it will not be graded”; “If you get 100% in this course, you will get ‘O’ grade”.
- Someone got 90%, now will he get ‘O’ or not?

**TABLE 4** The Truth Table for the Exclusive Or of Two Propositions.

$p$	$q$	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

**TABLE 5** The Truth Table for the Conditional Statement  $p \rightarrow q$ .

$p$	$q$	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

# Conditional - 2

- $p \rightarrow q$  ["if p then q"]
- Truth table:

$p$	$q$	$p \rightarrow q$	$\neg p \vee q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Note the truth table of  $\neg p \vee q$

# Logical Equivalence

- $p \rightarrow q$  and  $\neg p \vee q$  are logically equivalent
- Truth tables are the simplest way to prove such facts.
- We will learn other ways later.

Because conditional statements play such an essential role in mathematical reasoning, a variety of terminology is used to express  $p \rightarrow q$ . You will encounter most if not all of the following ways to express this conditional statement:

“if  $p$ , then  $q$ ”

“if  $p$ ,  $q$ ”

“ $p$  is sufficient for  $q$ ”

“ $q$  if  $p$ ”

“ $q$  when  $p$ ”

“a necessary condition for  $p$  is  $q$ ”

“ $q$  unless  $\neg p$ ”

“ $p$  implies  $q$ ”

“ $p$  only if  $q$ ”

“a sufficient condition for  $q$  is  $p$ ”

“ $q$  whenever  $p$ ”

“ $q$  is necessary for  $p$ ”

“ $q$  follows from  $p$ ”

- TRICKY: Is  $p \rightarrow q$  TRUE if  $p$  is FALSE?

- TRICKY: Is  $p \rightarrow q$  TRUE if  $p$  is FALSE?  
**YES!!**

- TRICKY: Is  $p \rightarrow q$  TRUE if  $p$  is FALSE?  
**YES!!**

If horses can fly then I am the  
President of USA.

**Is the above statement true?**

- TRICKY: Is  $p \rightarrow q$  TRUE if  $p$  is FALSE?  
**YES!!**

If horses can fly then I am the  
President of USA.

**Is the above statement true?**

B'cos “horses can fly” is False, the  
statement is True

# Look at this code.

**EXAMPLE 8** What is the value of the variable  $x$  after the statement

**if**  $2 + 2 = 4$  **then**  $x := x + 1$

if  $x = 0$  before this statement is encountered? (The symbol  $:=$  stands for assignment. The statement  $x := x + 1$  means the assignment of the value of  $x + 1$  to  $x$ .)

*Solution:* Because  $2 + 2 = 4$  is true, the assignment statement  $x := x + 1$  is executed. Hence,  $x$  has the value  $0 + 1 = 1$  after this statement is encountered. 

# Unit 1: Propositional Logic

# Contrapositive

- Contrapositive of  $p \rightarrow q$  is  $\neg q \rightarrow \neg p$
- Any conditional and its contrapositive are logically equivalent (have the same truth table) – Check by writing down the truth table.
- E.g. The contrapositive of “If you get 100% in this course, you will get an O” is “If you do not get an O in this course, you did not get 100%”.

## E.g.: Proof using contrapositive

Prove: If  $x^2$  is even,  $x$  is even

- Proof 1:  $x^2 = 2a$  for some integer  $a$ .  
Since 2 is prime, 2 must divide  $x$ .
- Proof 2: if  $x$  is not even,  $x$  is odd.  
Therefore  $x^2$  is odd. This is the  
contrapositive of the original assertion.

# Converse

- Converse of  $p \rightarrow q$  is  $q \rightarrow p$
- Not logically equivalent to conditional
- Ex 1: “If you get 100% in this course, you will get an A+” and “If you get an A+ in this course, you scored 100%” are not equivalent.
- Ex 2: If you won the lottery, you are rich.

# Other conditionals

## Inverse:

- inverse of  $p \rightarrow q$  is  $\neg p \rightarrow \neg q$
- How is this related to the converse?

## Biconditional:

- “If and only if”
- True if  $p, q$  have same truth values, false otherwise. Q: How is this related to XOR?
- Can also be defined as  $(p \rightarrow q) \wedge (q \rightarrow p)$

# Biconditional

**TABLE 6** The Truth Table for the Biconditional  $p \leftrightarrow q$ .

$p$	$q$	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

**EXAMPLE 11** Construct the truth table of the compound proposition

$$(p \vee \neg q) \rightarrow (p \wedge q).$$

**EXAMPLE 11** Construct the truth table of the compound proposition

$$(p \vee \neg q) \rightarrow (p \wedge q).$$

**TABLE 7** The Truth Table of  $(p \vee \neg q) \rightarrow (p \wedge q)$ .

$p$	$q$	$\neg q$	$p \vee \neg q$	$p \wedge q$	$(p \vee \neg q) \rightarrow (p \wedge q)$
T	T				
T	F				
F	T				
F	F				

**EXAMPLE 11** Construct the truth table of the compound proposition

$$(p \vee \neg q) \rightarrow (p \wedge q).$$

**TABLE 7** The Truth Table of  $(p \vee \neg q) \rightarrow (p \wedge q)$ .

$p$	$q$	$\neg q$	$p \vee \neg q$	$p \wedge q$	$(p \vee \neg q) \rightarrow (p \wedge q)$
T	T	F			
T	F	T			
F	T	F			
F	F	T			

**EXAMPLE 11** Construct the truth table of the compound proposition

$$(p \vee \neg q) \rightarrow (p \wedge q).$$

**TABLE 7** The Truth Table of  $(p \vee \neg q) \rightarrow (p \wedge q)$ .

$p$	$q$	$\neg q$	$p \vee \neg q$	$p \wedge q$	$(p \vee \neg q) \rightarrow (p \wedge q)$
T	T	F	T		
T	F	T	T		
F	T	F	F		
F	F	T	T		

**EXAMPLE 11** Construct the truth table of the compound proposition

$$(p \vee \neg q) \rightarrow (p \wedge q).$$

**TABLE 7** The Truth Table of  $(p \vee \neg q) \rightarrow (p \wedge q)$ .

$p$	$q$	$\neg q$	$p \vee \neg q$	$p \wedge q$	$(p \vee \neg q) \rightarrow (p \wedge q)$
T	T	F	T	T	
T	F	T	T	F	
F	T	F	F	F	
F	F	T	T	F	

**EXAMPLE 11** Construct the truth table of the compound proposition

$$(p \vee \neg q) \rightarrow (p \wedge q).$$

**TABLE 7** The Truth Table of  $(p \vee \neg q) \rightarrow (p \wedge q)$ .

$p$	$q$	$\neg q$	$p \vee \neg q$	$p \wedge q$	$(p \vee \neg q) \rightarrow (p \wedge q)$
T	T	F	T	T	T
T	F	T	T	F	F
F	T	F	F	F	T
F	F	T	T	F	F

# Example

- Q16(c)  $1+1=3$  if and only if monkeys can fly.
- Is this True statement?

# Readings and notes

- Read pages 1-12.
- Think about the notion of truth tables.
- Master the rationale behind the definition of conditionals.
- Practice translating English sentences to propositional logic statements.

# Next

## Ch. 1.2, 1.3: Propositional Logic - contd

- Compound propositions, precedence rules
- Tautologies and logical equivalences
- Read only the first section called “Translating English Sentences” in 1.2.

# Unit 1: Propositional Logic

# Excercise

12. Let  $p$ ,  $q$ , and  $r$  be the propositions

$p$  : You have the flu.

$q$  : You miss the final examination.

$r$  : You pass the course.

Express each of these propositions as an English sentence.

a)  $p \rightarrow q$

b)  $\neg q \leftrightarrow r$

c)  $q \rightarrow \neg r$

d)  $p \vee q \vee r$

e)  $(p \rightarrow \neg r) \vee (q \rightarrow \neg r)$

f)  $(p \wedge q) \vee (\neg q \wedge r)$

16. Determine whether these biconditionals are true or false.

- a)  $2 + 2 = 4$  if and only if  $1 + 1 = 2$ .
- b)  $1 + 1 = 2$  if and only if  $2 + 3 = 4$ .
- c)  $1 + 1 = 3$  if and only if monkeys can fly.
- d)  $0 > 1$  if and only if  $2 > 1$ .

17. Determine whether each of these conditional statements is true or false.

- a) If  $1 + 1 = 2$ , then  $2 + 2 = 5$ .
- b) If  $1 + 1 = 3$ , then  $2 + 2 = 4$ .
- c) If  $1 + 1 = 3$ , then  $2 + 2 = 5$ .
- d) If monkeys can fly, then  $1 + 1 = 3$ .

29. How many rows appear in a truth table for each of these compound propositions?

- a)  $p \rightarrow \neg p$
- b)  $(p \vee \neg r) \wedge (q \vee \neg s)$

**TABLE 8**  
Precedence of  
Logical  
Operators.

<i>Operator</i>	<i>Precedence</i>
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

# Compound Propositions

- Example:  $p \wedge q \vee r$ : Could be interpreted as  $(p \wedge q) \vee r$  or  $p \wedge (q \vee r)$
- precedence order:  $\neg \wedge \vee \rightarrow \leftrightarrow$  (IMP!)  
(Overruled by brackets)
- We use this order to compute truth values of compound propositions.

$\neg p \wedge q$  and  $\neg(p \wedge q)$  are different.

Note, putting braces like  $(\neg p) \wedge q$  is not needed.

Compare this with  $-5 + -6$ . See  $-(5 + -6)$  is different.

We do not need  $(-5) + (-6)$  **(Why?)**

$p \vee q \rightarrow r$  is the same as  $(p \vee q) \rightarrow r$

$p \wedge q \vee r$  means  $(p \wedge q) \vee r$       rather than  
 $p \wedge (q \vee r)$

# Tautology

- A compound proposition that is always TRUE, e.g.  $q \vee \neg q$
- Logical equivalence redefined:  $p, q$  are logical equivalences if  $p \leftrightarrow q$  is a tautology. Symbolically  $p \equiv q$ .
- Intuition:  $p \leftrightarrow q$  is true precisely when  $p, q$  have the same truth values.

# Contradiction and contingency

Contradiction is always false

Contingency may be true may be false based on actual assignment of truth value to elements.

# Propositional Logic

# Tautology

- A compound proposition that is always TRUE, e.g.  $q \vee \neg q$
- Logical equivalence redefined:  $p, q$  are logical equivalences if  $p \leftrightarrow q$  is a tautology. Symbolically  $p \equiv q$ .
- Intuition:  $p \leftrightarrow q$  is true precisely when  $p, q$  have the same truth values.

# Contradiction and contingency

Contradiction is always false

Contingency may be true may be false based on actual assignment of truth value to elements.

35. Construct a truth table for each of these compound propositions.

a)  $p \rightarrow \neg q$

b)  $\neg p \leftrightarrow q$

c)  $(p \rightarrow q) \vee (\neg p \rightarrow q)$

d)  $(p \rightarrow q) \wedge (\neg p \rightarrow q)$

e)  $(p \leftrightarrow q) \vee (\neg p \leftrightarrow q)$

f)  $(\neg p \leftrightarrow \neg q) \leftrightarrow (p \leftrightarrow q)$

Which are Tautologies? Contradictions? Contingencies

# Logic and Bit operations

<i>Truth Value</i>	<i>Bit</i>
T	1
F	0

Boolean variable is just like any other variable but can have either 1 or 0.

Computer bit operations correspond to the logical connectives. By replacing true by a 1 and false by a 0 in the truth tables for the operators  $\wedge$ ,  $\vee$ , and  $\oplus$ , the tables shown in Table 9 for the corresponding bit operations are obtained.

We will also use the notation OR, AND, and XOR for the operators  $\vee$ ,  $\wedge$ , and  $\oplus$ , as is done in various programming languages.

**TABLE 9** Table for the Bit Operators *OR*, *AND*, and *XOR*.

$x$	$y$	$x \vee y$	$x \wedge y$	$x \oplus y$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

## DEFINITION 7

A bit string is a sequence of zero or more bits. The length of this string is the number of bits in the string.

Eg: 101010011 is a bit string of length nine.

# Bitwise operations

Just extensions of **and, or** etc logical operations.

01 1011 0110

11 0001 1101

-----

11 1011 1111 bitwise OR

01 0001 0100 bitwise AND

10 1010 1011 bitwise XOR

# Exercise

44. Evaluate each of these expressions.

- a)  $1\ 1000 \wedge (0\ 1011 \vee 1\ 1011)$
- b)  $(0\ 1111 \wedge 1\ 0101) \vee 0\ 1000$
- c)  $(0\ 1010 \oplus 1\ 1011) \oplus 0\ 1000$
- d)  $(1\ 1011 \vee 0\ 1010) \wedge (1\ 0001 \vee 1\ 1011)$

50. An ancient Sicilian legend says that the barber in a remote town who can be reached only by traveling a dangerous mountain road shaves those people, and only those people, who do not shave themselves. Can there be such a barber?

Answer: Such a barber cannot exist!!

why??

Such a barber, if exist, should

1. shave himself
2. does not shave himself

Such a barber, if exist, should

1. shave himself, or (this is xor)
2. does not shave himself

# Manipulating Propositions

- Compound propositions can be simplified by using simple rules.
- Read page 25 - 28.
- Some are obvious, e.g. Identity, Domination, Idempotence, double negation, commutativity, associativity
- Less obvious: Distributive, De Morgan's laws, Absorption

# 1.3 Propositional Equivalences

- **DEFINITION 1**
- A compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it, is called a *tautology*.
- A compound proposition that is always false is called a *contradiction*.
- A compound proposition that is neither a tautology nor a contradiction is called a *contingency*.

**TABLE 1** Examples of a Tautology  
and a Contradiction.

$p$	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
T	F	T	F
F	T	T	F

# Logical Equivalences

- **DEFINITION 2**
- The compound propositions  $p$  and  $q$  are called *logically equivalent* if  $p \leftrightarrow q$  is a tautology.
- The notation  $p \equiv q$  denotes that  $p$  and  $q$  are logically equivalent.

- **Remark:** The symbol  $\equiv$  is not a logical connective, and  $p \equiv q$  is not a compound proposition,
- But rather is the statement that  $p \leftrightarrow q$  is a tautology. The symbol  $\leftrightarrow$  is sometimes used instead of  $\equiv$  to denote logical equivalence.

# De Morgan's Laws

$$\neg(q \vee r) \equiv \neg q \wedge \neg r$$

Intuition – For the LHS to be true: neither  $q$  nor  $r$  can be true. This is the same as saying  $q$  and  $r$  must be false.

$$\neg(q \wedge r) \equiv \neg q \vee \neg r$$

Intuition – For the LHS to be true:  $q \wedge r$  must be false. This is the same as saying  $q$  or  $r$  must be false.

Proof: use truth tables.

**TABLE 3** Truth Tables for  $\neg(p \vee q)$  and  $\neg p \wedge \neg q$ .

$p$	$q$	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

- **EXAMPLE 3** Show that  $p \rightarrow q$  and  $\neg p \vee q$  are logically equivalent.
- *Solution:* We construct the truth table for these compound propositions in Table 4. Because the truth values of  $\neg p \vee q$  and  $p \rightarrow q$  agree, they are logically equivalent.

**TABLE 4** Truth Tables for  $\neg p \vee q$  and  $p \rightarrow q$ .

$p$	$q$	$\neg p$	$\neg p \vee q$	$p \rightarrow q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

# Distributive Laws

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$

Intuition (not a proof!) – For the LHS to be true: p must be true and q or r must be true. This is the same as saying p and q must be true or p and r must be true.

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$

Intuition (less obvious) – For the LHS to be true: p must be true or both q and r must be true. This is the same as saying p or q must be true and p or r must be true.

Proof: use truth tables.

**TABLE 5** A Demonstration That  $p \vee (q \wedge r)$  and  $(p \vee q) \wedge (p \vee r)$  Are Logically Equivalent.

$p$	$q$	$r$	$q \wedge r$	$p \vee (q \wedge r)$	$p \vee q$	$p \vee r$	$(p \vee q) \wedge (p \vee r)$
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	T	T	T	T
F	T	T	T	T	T	T	T
F	T	F	F	F	T	F	F
F	F	T	F	F	F	T	F
F	F	F	F	F	F	F	F

TABLE 6 Logical Equivalences.

<i>Equivalence</i>	<i>Name</i>
$p \wedge T \equiv p$ $p \vee F \equiv p$	Identity laws
$p \vee T \equiv T$ $p \wedge F \equiv F$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv T$ $p \wedge \neg p \equiv F$	Negation laws

**TABLE 7** Logical Equivalences Involving Conditional Statements.

$p \rightarrow q \equiv \neg p \vee q$
$p \rightarrow q \equiv \neg q \rightarrow \neg p$
$p \vee q \equiv \neg p \rightarrow q$
$p \wedge q \equiv \neg(p \rightarrow \neg q)$
$\neg(p \rightarrow q) \equiv p \wedge \neg q$
$(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$
$(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$
$(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$
$(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

**TABLE 8** Logical Equivalences Involving Biconditional Statements.

$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$
$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$
$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

Furthermore, note that De Morgan's laws extend to

$$\neg(p_1 \vee p_2 \vee \cdots \vee p_n) \equiv (\neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_n)$$

and

$$\neg(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \equiv (\neg p_1 \vee \neg p_2 \vee \cdots \vee \neg p_n).$$

**EXAMPLE 6** Show that  $\neg(p \rightarrow q)$  and  $p \wedge \neg q$  are logically equivalent.

- We can use truth table.
- But a simple and elegant way is to use identities progressively and get the required result.

$\neg(p \rightarrow q) \equiv \neg(\neg p \vee q)$ , Since  $p \rightarrow q \equiv \neg p \vee q$   
 $\equiv \neg(\neg p) \wedge \neg q$  by the second De Morgan law  
 $\equiv p \wedge \neg q$  by the double negation law

# Propositional Logic

- **EXAMPLE 7** Show that  $\neg(p \vee (\neg p \wedge q))$  and  $\neg p \wedge \neg q$  are logically equivalent by developing a series of logical equivalences.

- **EXAMPLE 7** Show that  $\neg(p \vee (\neg p \wedge q))$  and  $\neg p \wedge \neg q$  are logically equivalent by developing a series of logical equivalences.

$$\begin{aligned}
 \neg(p \vee (\neg p \wedge q)) &\equiv \neg p \wedge \neg(\neg p \wedge q) && \text{by the second De Morgan law} \\
 &\equiv \neg p \wedge [\neg(\neg p) \vee \neg q] && \text{by the first De Morgan law} \\
 &\equiv \neg p \wedge (p \vee \neg q) && \text{by the double negation law} \\
 &\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) && \text{by the second distributive law} \\
 &\equiv F \vee (\neg p \wedge \neg q) && \text{because } \neg p \wedge p \equiv F \\
 &\equiv (\neg p \wedge \neg q) \vee F && \text{by the commutative law for disjunction} \\
 &\equiv \neg p \wedge \neg q && \text{by the identity law for } F
 \end{aligned}$$

- **EXAMPLE 7** Show that  $\neg(p \vee (\neg p \wedge q))$  and  $\neg p \wedge \neg q$  are logically equivalent by developing a series of logical equivalences.

$$\begin{aligned}
 \neg(p \vee (\neg p \wedge q)) &\equiv \neg p \wedge \neg(\neg p \wedge q) && \text{by the second De Morgan law} \\
 &\equiv \neg p \wedge [\neg(\neg p) \vee \neg q] && \text{by the first De Morgan law} \\
 &\equiv \neg p \wedge (p \vee \neg q) && \text{by the double negation law} \\
 &\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) && \text{by the second distributive law} \\
 &\equiv F \vee (\neg p \wedge \neg q) && \text{because } \neg p \wedge p \equiv F \\
 &\equiv (\neg p \wedge \neg q) \vee F && \text{by the commutative law for disjunction} \\
 &\equiv \neg p \wedge \neg q && \text{by the identity law for } F
 \end{aligned}$$

Consequently  $\neg(p \vee (\neg p \wedge q))$  and  $\neg p \wedge \neg q$  are logically equivalent.

# Using the laws

- Q: Is  $p \rightarrow (p \rightarrow q)$  a tautology?
- Can use truth tables
- Can write a compound proposition and simplify

# Propositional Satisfiability

- A compound proposition is **satisfiable** if there is an assignment of truth values to its variables that makes it true.
- When no such assignments exists, that is, when the compound proposition is false for all assignments of truth values to its variables, the compound proposition is **unsatisfiable**.

# Read Page 32 and 33

32 1 / The Foundations: Logic and Proofs

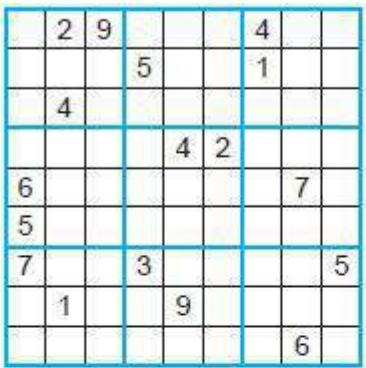


FIGURE 1 A  $9 \times 9$  Sudoku puzzle.

## Applications of Satisfiability

Many problems, in diverse areas such as robotics, software testing, computer-aided design, machine vision, integrated circuit design, computer networking, and genetics, can be modeled in terms of propositional satisfiability. Although most of these applications are beyond the scope of this book, we will study one application here. In particular, we will show how to use propositional satisfiability to model Sudoku puzzles.

**SUDOKU** A Sudoku puzzle is represented by a  $9 \times 9$  grid made up of nine  $3 \times 3$  subgrids, known as blocks, as shown in Figure 1. For each puzzle, some of the 81 cells, called given cells,

- **Solving Satisfiability Problems**
- A truth table can be used to determine whether a compound proposition is satisfiable, or equivalently, whether its negation is a tautology (see Exercise 60). This can be done by hand for a compound proposition with a small number of variables, but when the number of variables grows, this becomes impractical. For instance, there are  $2^{20} = 1,048,576$  rows in the truth table
- for a compound proposition with 20 variables. Clearly, you need a computer to determine whether a compound proposition in 20 variables is satisfiable or not.

- **61.** Determine whether each of these compound propositions is satisfiable.
  - a)  $(p \vee \neg q) \wedge (\neg p \vee q) \wedge (\neg p \vee \neg q)$
  - b)  $(p \rightarrow q) \wedge (p \rightarrow \neg q) \wedge (\neg p \rightarrow q) \wedge (\neg p \rightarrow \neg q)$
  - c)  $(p \leftrightarrow q) \wedge (\neg p \leftrightarrow q)$

# Limitations of Propositional Logic

- What can we NOT express using propositions?

Ex: How do you make a statement about all even integers?

If  $x > 2$  then  $x^2 > 4$

- A more general language: Predicate logic (Sec 1.4)

# Predicate Logic

## Predicates

Statements involving variables, such as

“ $x > 3$ ,” “ $x = y + 3$ ,” “ $x + y = z$ ,” and

“computer  $x$  is under attack by an intruder,” and

“computer  $x$  is functioning properly,”

are often found in mathematical assertions, in computer programs, and in system specifications.

These are neither true nor false, hence are not propositions.

# Predicate

Once an appropriate value is assigned to  $x$ ,  
“ $x > 3$ ,” will become a proposition.

So predicate is like a variable.  
Proposition is like a constant.

# Predicate

$x > 3$  can be expressed as Greater-than-three( $x$ ).

Greater-than-three( $x$ ) is True when  $x = 4$

Greater-than-three( $x$ ) if False when  $x = 2$

We can denote Greater-than-three( $x$ ) by  $P(x)$

Here, Greater-than-three and  $P$  are called predicates.

Predicate is actually like a function called “propositional function” whose value depends on its arguments.

$x > y$  can be expressed as  $GT(x, y)$ .

It has a truth value at each point  $(x, y)$

So better say, Whenever  $x$  is a number  $\text{GT}(x+1, x)$  is True.

(we believe, there is no confusion about what is a “number” and what it means “ $x+1$ ” )

# Have you noted?

“ $\text{GT}(3, 2)$ ” is a proposition

similarly

“Whenever  $x$  is a number  $\text{GT}(x+1, x)$ ” is a proposition.

The statement  $P(x)$  is also said to be the value of the propositional function  $P$  at  $x$ .

Obviously the value is either True or False.

Let  $R(x, y, z)$  denote the statement “ $x + y = z$ .”  
When values are assigned to the variables  $x$ ,  $y$ , and  $z$ ,  
this statement has a truth value.

EXAMPLE 5. What are the truth values of the propositions  $R(1, 2, 3)$  and  $R(0, 0, 1)$ ?

Let  $R(x, y, z)$  denote the statement “ $x + y = z$ .” When values are assigned to the variables  $x$ ,  $y$ , and  $z$ , this statement has a truth value.

EXAMPLE 5. What are the truth values of the propositions  $R(1, 2, 3)$  and  $R(0, 0, 1)$ ?

Solution: The proposition  $R(1, 2, 3)$  is obtained by setting  $x = 1$ ,  $y = 2$ , and  $z = 3$  in the statement  $R(x, y, z)$ . We see that  $R(1, 2, 3)$  is the statement

“ $1 + 2 = 3$ ,” which is true.

Also note that  $R(0, 0, 1)$ , which is the statement  
“ $0 + 0 = 1$ ,” is false.

In general, a statement involving the  $n$  variables  $x_1, x_2, \dots, x_n$  can be denoted by  $P(x_1, x_2, \dots, x_n)$ .

A statement of the form  $P(x_1, x_2, \dots, x_n)$  is the value of the propositional function  $P$  at the  $n$ -tuple  $(x_1, x_2, \dots, x_n)$ , and  $P$  is also called an  **$n$ -place predicate** or a  **$n$ -ary predicate**.

# Predicate Logic

- A predicate is a proposition that is a function of one or more variables.  
E.g.:  $P(x)$ :  $x$  is an even number. So  $P(1)$  is false,  $P(2)$  is true,....
- Examples of predicates:
  - Domain characters -  $\text{IsAlpha}(x)$  : TRUE iff  $x$  is an alphabetical character.
  - Domain floating point numbers -  $\text{IsInt}(x)$ : TRUE iff  $x$  is an integer.
  - Domain integers:  $\text{Prime}(x)$  - TRUE if  $x$  is prime, FALSE otherwise.

# Predicate Calculus

# Quantifiers

- describes the values of a variable that make the predicate true. E.g.  $\exists x P(x)$
- Domain or universe: range of values of a variable (sometimes implicit)

The area of logic that deals with predicates and quantifiers is called the **predicate calculus**.

# Two Popular Quantifiers

- Universal:  $\forall x P(x)$  – “ $P(x)$  for all  $x$  in the domain”
- Existential:  $\exists x P(x)$  – “ $P(x)$  for some  $x$  in the domain” or “there exists  $x$  such that  $P(x)$  is TRUE”.
- Either is meaningless if the domain is not known/specifyed.
- Examples (domain real numbers)
  - $\forall x (x^2 \geq 0)$
  - $\exists x (x > 1)$
  - $(\forall x > 1) (x^2 > x)$  – quantifier with restricted domain

# Using Quantifiers

Domain integers:

- Using implications: The cube of all negative integers is negative.

$$\forall x (x < 0) \rightarrow (x^3 < 0)$$

- Expressing sums :

$$\forall n (\sum_{i=1}^n i = n(n+1)/2)$$

Aside:  $\Sigma$  is summation notation

**TABLE 1** Quantifiers.

<i>Statement</i>	<i>When True?</i>	<i>When False?</i>
$\forall x P(x)$	$P(x)$ is true for every $x$ .	There is an $x$ for which $P(x)$ is false.
$\exists x P(x)$	There is an $x$ for which $P(x)$ is true.	$P(x)$ is false for every $x$ .

# Quantifiers with Restricted Domains

## EXAMPLE 17

What do the statements  $\forall x < 0 (x^2 > 0)$ ,  $\forall y = 0 (y^3 = 0)$ , and  $\exists z > 0 (z^2 = 2)$  mean, where the domain in each case consists of the real numbers?

The statement  $\forall x < 0 (x^2 > 0)$  states that for every real number  $x$  with  $x < 0$ ,  $x^2 > 0$ .

This statement is the same  
as  $\forall x(x < 0 \rightarrow x^2 > 0)$ .

The statement  $\forall y = 0 (y^3 = 0)$  states that for every real number  $y$  with  $y = 0$ , we have  
 $y^3 = 0$ .

Note that this statement is equivalent to

$$\forall y(y = 0 \rightarrow y^3 = 0).$$

Finally, the statement  $\exists z > 0 (z^2 = 2)$  states that there exists a real number  $z$  with  $z > 0$  such that  $z^2 = 2$ .

This statement is equivalent to

$$\exists z(z > 0 \wedge z^2 = 2).$$

# Precedence of Quantifiers

- $\forall \ \exists$  have higher precedence than operators from Propositional Logic; so  $\forall x P(x) \vee Q(x)$  is **not** logically equivalent to  $\forall x (P(x) \vee Q(x))$
- $\exists x (P(x) \wedge Q(x)) \vee \forall x R(x)$   
Say  $P(x)$ :  $x$  is odd,  $Q(x)$ :  $x$  is divisible by 3,  $R(x)$ :  $(x=0) \vee (2x > x)$

# Binding Variables

When a quantifier is used on the variable  $x$ , we say that this occurrence of the variable is **bound**.

An occurrence of a variable that is not bound by a quantifier and which is not set to a particular value is said to be **free**.

All the variables that occur in a propositional function must be bound or set equal to a particular value to turn it into a proposition.

This can be done using a combination of universal quantifiers, existential quantifiers, and value assignments.

# Scope

The part of a logical expression to which a quantifier is applied is called the **scope** of that quantifier.

Consequently, a variable is free if it is outside the scope of all quantifiers in the formula that specify the variable.

## EXAMPLE 18

In the statement  $\exists x(x + y = 1)$ , the variable  $x$  is bound by the existential quantification  $\exists x$ , but the variable  $y$  is *free*

In the statement  $\exists x(P(x) \wedge Q(x)) \vee \forall xR(x)$ , all variables are bound.

Observe that we could have written our statement using two different variables  $x$  and  $y$ , as  $\exists x(P(x) \wedge Q(x)) \vee \forall yR(y)$ , because the scopes of the two quantifiers do not overlap.

# Predicate Calculus

- Logical Equivalence:  $P \equiv Q$  iff they have same truth value no matter which **domain** is used and no matter which **predicates** are assigned to predicate variables.

# Negation of Quantifiers

- “There is no student who can ...”
- “Not all professors are bad....”
- “There is no Toronto Raptor that can dunk like Vince ...”
- $\neg \forall x P(x) \equiv \exists x \neg P(x)$  why?
- $\neg \exists x P(x) \equiv \forall x \neg P(x)$
- Careful: The negation of “Every Canadian loves Hockey” is NOT “No Canadian loves Hockey”! Many, many students make this mistake!

# De Morgan's laws for quantifiers

**TABLE 2** De Morgan's Laws for Quantifiers.

<i>Negation</i>	<i>Equivalent Statement</i>	<i>When Is Negation True?</i>	<i>When False?</i>
$\neg\exists x P(x)$	$\forall x \neg P(x)$	For every $x$ , $P(x)$ is false.	There is an $x$ for which $P(x)$ is true.
$\neg\forall x P(x)$	$\exists x \neg P(x)$	There is an $x$ for which $P(x)$ is false.	$P(x)$ is true for every $x$ .

What are the negations of the statements  
 $\forall x(x^2 > x)$  and  $\exists x(x^2 = 2)$ ?

What are the negations of the statements  
 $\forall x(x^2 > x)$  and  $\exists x(x^2 = 2)$ ?

$$\neg \forall x(x^2 > x) \equiv \exists x \neg(x^2 > x).$$

What are the negations of the statements  
 $\forall x(x^2 > x)$  and  $\exists x(x^2 = 2)$ ?

$$\neg \forall x(x^2 > x) \equiv \exists x \neg(x^2 > x).$$

$$\neg \exists x(x^2 = 2) \equiv \forall x \neg(x^2 = 2).$$

# Exercise

35. Find a counterexample, if possible, to these universally quantified statements, where the domain for all variables consists of all integers. This is a way to disprove the claim.

- a)  $\forall x(x^2 \geq x)$
- b)  $\forall x(x > 0 \vee x < 0)$
- c)  $\forall x(x = 1)$

43. Determine whether  $\forall x(P(x) \rightarrow Q(x))$  and  $\forall xP(x) \rightarrow \forall xQ(x)$  are logically equivalent. Justify your answer.

43. Determine whether  $\forall x(P(x) \rightarrow Q(x))$  and  $\forall xP(x) \rightarrow \forall xQ(x)$  are logically equivalent. Justify your answer.

**No.** There is a difference in the scope of the quantifier.

Note  $\forall xP(x) \rightarrow \forall xQ(x) \equiv \forall xP(x) \rightarrow \forall yQ(y)$

52. As mentioned in the text, the notation  $\exists !xP(x)$  denotes “There exists a unique  $x$  such that  $P(x)$  is true.” If the domain consists of all integers, what are the truth values of these statements?

- a)  $\exists !x(x > 1)$
- b)  $\exists !x(x^2 = 1)$
- c)  $\exists !x(x + 3 = 2x)$
- d)  $\exists !x(x = x + 1)$

# Nested Quantifiers

- $\forall x \exists y p(x,y)$  is actually  $\forall x (\exists y ( p(x,y) ) ).$
- $\forall \exists$  have higher precedence than operators from Propositional Logic; so  
 $\forall x P(x) \vee Q(x)$  is **not** logically equivalent to  
 $\forall x (P(x) \vee Q(x))$

# Nested Quantifiers

- Allows simultaneous quantification of many variables.

- E.g. – domain integers,

$$\exists x \exists y \exists z (x^2 + y^2 = z^2)$$

- $\forall n < 3 \exists x \exists y \exists z (x^n + y^n = z^n)$  (Fermat's Last Theorem)

- Domain real numbers:

$$\forall x \forall y \exists z (x < z < y) \vee (y < z < x)$$
 Is this true?

# Nested Quantifiers - 2

$\forall x \exists y (x + y = 0)$  is true over the integers

- Assume an arbitrary integer  $x$ .
- To show that there exists a  $y$  that satisfies the requirement of the predicate, choose  $y = -x$ . Clearly  $y$  is an integer, and thus is in the domain.
- So  $x + y = x + (-x) = x - x = 0$ .
- Since we assumed nothing about  $x$  (other than it is an integer), the argument holds for any integer  $x$ .
- Therefore, the predicate is TRUE.

## EXAMPLE 1

Assume that the domain for the variables  $x$  and  $y$  consists of all real numbers. The statement  $\forall x \forall y (x + y = y + x)$  says that  $x + y = y + x$  for all real numbers  $x$  and  $y$ . This is the commutative law for addition of real numbers.

$$\forall x \forall y P(x, y) \equiv \forall y \forall x P(x, y)$$

$$\exists x \exists y Q(x, y) \equiv \exists y \exists x Q(x, y)$$

$$\forall x \exists y P(x, y) \not\equiv \exists y \forall x P(x, y)$$

**TABLE 1** Quantifications of Two Variables.

<i>Statement</i>	<i>When True?</i>	<i>When False?</i>
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	$P(x, y)$ is true for every pair $x, y$ .	There is a pair $x, y$ for which $P(x, y)$ is false.
$\forall x \exists y P(x, y)$	For every $x$ there is a $y$ for which $P(x, y)$ is true.	There is an $x$ such that $P(x, y)$ is false for every $y$ .
$\exists x \forall y P(x, y)$	There is an $x$ for which $P(x, y)$ is true for every $y$ .	For every $x$ there is a $y$ for which $P(x, y)$ is false.
$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$	There is a pair $x, y$ for which $P(x, y)$ is true.	$P(x, y)$ is false for every pair $x, y$ .

## EXAMPLE 5.

Let  $Q(x, y, z)$  be the statement “ $x + y = z$ .” What are the truth values of the statements:

$\forall x \forall y \exists z Q(x, y, z)$  and  $\exists z \forall x \forall y Q(x, y, z)$ , where the domain of all variables consists of all real numbers?

# Predicate Calculus

# Translating Mathematical Statements into Statements

EXAMPLE 6. Translate the statement “The sum of two positive integers is always positive” into a logical expression.

# Translating Mathematical Statements into Statements

EXAMPLE 6. Translate the statement “The sum of two positive integers is always positive” into a logical expression.

$$\forall x \forall y ( (x > 0) \wedge (y > 0) \rightarrow (x + y > 0) ),$$

where the domain for both variables consists of all integers.

EXAMPLE 7 Translate the statement “Every real number except zero has a multiplicative inverse.” (A multiplicative inverse of a real number  $x$  is a real number  $y$  such that  $xy = 1$ .)

**EXAMPLE 7.** Translate the statement “Every real number except zero has a multiplicative inverse.” (A multiplicative inverse of a real number  $x$  is a real number  $y$  such that  $xy = 1$ .)

*Solution:* We first rewrite this as “For every real number  $x$  except zero,  $x$  has a multiplicative inverse.” We can rewrite this as “For every real number  $x$ , if  $x \neq 0$ , then there exists a real number  $y$  such that  $xy = 1$ .” This can be rewritten as

$$\forall x((x \neq 0) \rightarrow \exists y(xy = 1)).$$



# Exercise

9. Let  $L(x, y)$  be the statement “ $x$  loves  $y$ ,” where the domain for both  $x$  and  $y$  consists of all people in the world. Use quantifiers to express each of these statements.
- a) Everybody loves Jerry.
  - b) Everybody loves somebody.
  - c) There is somebody whom everybody loves.
  - d) Nobody loves everybody.
  - e) There is somebody whom Lydia does not love.
  - f) There is somebody whom no one loves.
  - g) There is exactly one person whom everybody loves.
  - h) There are exactly two people whom Lynn loves.
  - i) Everyone loves himself or herself.
  - j) There is someone who loves no one besides himself or herself.

**28.** Determine the truth value of each of these statements if the domain of each variable consists of all real numbers.

a)  $\forall x \exists y (x^2 = y)$

b)  $\forall x \exists y (x = y^2)$

c)  $\exists x \forall y (xy = 0)$

d)  $\exists x \exists y (x + y \neq y + x)$

e)  $\forall x (x \neq 0 \rightarrow \exists y (xy = 1))$

f)  $\exists x \forall y (y \neq 0 \rightarrow xy = 1)$

g)  $\forall x \exists y (x + y = 1)$

h)  $\exists x \exists y (x + 2y = 2 \wedge 2x + 4y = 5)$

i)  $\forall x \exists y (x + y = 2 \wedge 2x - y = 1)$

j)  $\forall x \forall y \exists z (z = (x + y)/2)$

## **1.6**

## **Rules of Inference**

---

Rules of inference which are templates for constructing valid arguments.

Rules of inference are our basic tools for establishing the truth of statements.

# Proof, argument, valid, conclusion

- **Proofs** in mathematics are valid arguments that establish the truth of mathematical statements.
- By an **argument**, we mean a sequence of statements that end with a conclusion.
- **Conclusion** is also a statement.
- By **valid**, we mean that the conclusion, or final statement of the argument, must follow from the truth of the preceding statements, or premises, of the argument.

That is, an argument is valid *if and only if* it is impossible for all the premises to be true and the conclusion to be false.

# Valid Arguments in Propositional Logic

“If you have a current password, then you can log onto the network.”

“You have a current password.”

Therefore,

“You can log onto the network.”

$$\begin{array}{c} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$

The statement  $((p \rightarrow q) \wedge p) \rightarrow q$   
is a tautology

**TABLE 1** Rules of Inference.

<i>Rule of Inference</i>	<i>Tautology</i>	<i>Name</i>
$\begin{array}{c} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$	$(p \wedge (p \rightarrow q)) \rightarrow q$	Modus ponens
$\begin{array}{c} \neg q \\ p \rightarrow q \\ \hline \therefore \neg p \end{array}$	$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$	Modus tollens
$\begin{array}{c} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}$	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$	Hypothetical syllogism
$\begin{array}{c} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$	$((p \vee q) \wedge \neg p) \rightarrow q$	Disjunctive syllogism
$\begin{array}{c} p \\ \hline \therefore p \vee q \end{array}$	$p \rightarrow (p \vee q)$	Addition
$\begin{array}{c} p \wedge q \\ \hline \therefore p \end{array}$	$(p \wedge q) \rightarrow p$	Simplification
$\begin{array}{c} p \\ q \\ \hline \therefore p \wedge q \end{array}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$\begin{array}{c} p \vee q \\ \neg p \vee r \\ \hline \therefore q \vee r \end{array}$	$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$	Resolution

# Using Rules of Inference to Build Arguments

EXAMPLE 6. Show that the premises “It is not sunny this afternoon and it is colder than yesterday,” “We will go swimming only if it is sunny,” “If we do not go swimming, then we will take a canoe trip,” and “If we take a canoe trip, then we will be home by sunset” lead to the conclusion “We will be home by sunset.”

## Solution:

Let  $p$  : “It is sunny this afternoon,”

$q$  : “It is colder than yesterday,”

$r$  : “We will go swimming,”

$s$  : “We will take a canoe trip,” and

$t$  : “We will be home by sunset.”

Then the premises become

$\neg p \wedge q$ ,  $r \rightarrow p$ ,  $\neg r \rightarrow s$ , and  $s \rightarrow t$ .

The conclusion is simply  $t$ . We need to give a valid argument with premises  $\neg p \wedge q$ ,  $r \rightarrow p$ ,  $\neg r \rightarrow s$ , and  $s \rightarrow t$  and conclusion  $t$ .

# Argument to show that premises give the conclusion

Step	Reason
1. $\neg p \wedge q$	Premise
2. $\neg p$	Simplification using (1)
3. $r \rightarrow p$	Premise
4. $\neg r$	Modus tollens using (2) and (3)
5. $\neg r \rightarrow s$	Premise
6. $s$	Modus ponens using (4) and (5)
7. $s \rightarrow t$	Premise
8. $t$	Modus ponens using (6) and (7)

# Fallacies

$$\begin{array}{c} p \rightarrow q \\ q \\ \hline p \end{array}$$

fallacy of assuming the conclusion.

# fallacy of denying the hypothesis

$$\begin{array}{c} p \rightarrow q \\ \neg p \\ \hline \neg q \end{array}$$

# Rules of Inference for Quantified Statements

**TABLE 2** Rules of Inference for Quantified Statements.

<i>Rule of Inference</i>	<i>Name</i>
$\begin{array}{c} \forall x P(x) \\ \therefore P(c) \end{array}$	Universal instantiation
$\begin{array}{c} P(c) \text{ for an arbitrary } c \\ \therefore \forall x P(x) \end{array}$	Universal generalization
$\begin{array}{c} \exists x P(x) \\ \therefore P(c) \text{ for some element } c \end{array}$	Existential instantiation
$\begin{array}{c} P(c) \text{ for some element } c \\ \therefore \exists x P(x) \end{array}$	Existential generalization

## EXAMPLE 12

Show that the premises “Everyone in this discrete mathematics class has taken a course in computer science” and “Marla is a student in this class”

imply the conclusion  
“Marla has taken a course in computer science.”

**Solution:**

Let  $D(x)$  denote “ $x$  is in this discrete mathematics class,” and

let  $C(x)$  denote “ $x$  has taken a course in computer science.”

Then the premises are:  $\forall x(D(x) \rightarrow C(x))$  and  $D(\text{Marla})$ .

The conclusion is  $C(\text{Marla})$ .

The following steps can be used to establish the conclusion from the premises.

Step	Reason
1. $\forall x(D(x) \rightarrow C(x))$	Premise
2. $D(\text{Marla}) \rightarrow C(\text{Marla})$	Universal instantiation from (1)
3. $D(\text{Marla})$	Premise
4. $C(\text{Marla})$	Modus ponens from (2) and (3)

# Rules of Inference and Proof

# Resolution

Computer programs have been developed to automate the task of reasoning and proving theorems.

Many of these programs make use of a rule of inference known as **resolution**.

This rule of inference is based on the tautology  
 $((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$ .

The final disjunction in the resolution rule,  $q \vee r$ , is called the **resolvent**.

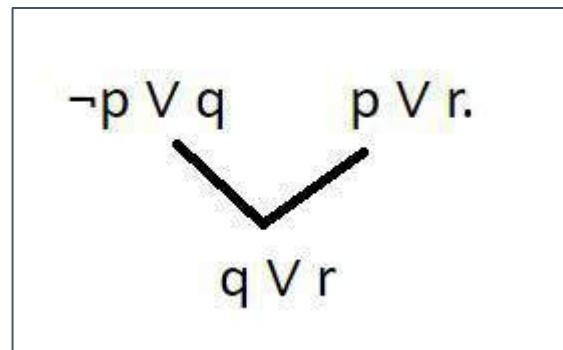
## EXAMPLE 8

Use resolution to show that the hypotheses “Jasmine is skiing or it is not snowing” and “It is snowing or Bart is playing hockey” imply that “Jasmine is skiing or Bart is playing hockey.”

Solution: Let  $p$  : “It is snowing,”  
 $q$  : “Jasmine is skiing,” and  
 $r$  : “Bart is playing hockey.”

The given hypotheses is:  $\neg p \vee q$  and  $p \vee r$ .

Using resolution, the proposition  $q \vee r$  is true. That is  
“Jasmine is skiing or Bart is playing hockey”.



# Clauses

Clause is a disjunction of variables or negation of variables.

Eg:  $p \vee q \vee r$ ,     $\neg p \vee q \vee r$ ,

$\neg p \vee \neg q \vee r$ ,     $\neg p \vee \neg q$ ,

$\neg p$ ,  $q$

# Conjunctive Normal form

This is the compound statement (formula) which is conjunction of clauses.

$$\text{Eg: } (p \vee q \vee r) \wedge (\neg p \vee q \vee r).$$

$$(\neg p \vee \neg q \vee r) \wedge (\neg p \vee \neg q).$$

$$\neg p \wedge q$$

Every formula has an equivalent formula which is in CNF.

- $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
- $\neg(p \vee q) \equiv \neg p \wedge \neg q$     Note,  $\neg p$  is a clause;  
similarly  $\neg q$  is a clause.
- $p \rightarrow q \equiv \neg p \vee q$

CNF and resolution is enough to do inferencing.

In Computer Programs where logic has to be used (like in AI applications) this method is often followed.

EXAMPLE 9. Show that the premises  $(p \wedge q) \vee r$  and  $r \rightarrow s$  imply the conclusion  $p \vee s$ .

$$(p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$$

$$r \rightarrow s \equiv \neg r \vee s$$

EXAMPLE 9. Show that the premises  $(p \wedge q) \vee r$  and  $r \rightarrow s$  imply the conclusion  $p \vee s$ .

$$(p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$$

$$r \rightarrow s \equiv \neg r \vee s$$

$$\begin{array}{ccc} p \vee r & & \neg r \vee s \\ \searrow & \swarrow & \\ p \vee s & & \end{array}$$

# Rules of Inference for Quantified Statements

**TABLE 2** Rules of Inference for Quantified Statements.

<i>Rule of Inference</i>	<i>Name</i>
$\frac{\forall x P(x)}{\therefore P(c)}$	Universal instantiation
$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$	Universal generalization
$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$	Existential instantiation
$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$	Existential generalization

# Combining Rules of Inference for Propositions and Quantified Statements

## Universal Modus Ponens

$\forall x(P(x) \rightarrow Q(x))$

$P(a)$ , where  $a$  is a particular element in the domain

---

$\therefore Q(a)$

# Example

Let  $P(n) : n > 4$

$Q(n) : n^2 < 2^n$

$\forall n(P(n) \rightarrow Q(n))$  is True

$P(100)$  is True

---

$Q(100)$  is True

i.e.,  $100^2 < 2^{100}$  is True

# Universal modus tollens

$\forall x(P(x) \rightarrow Q(x))$

$\neg Q(a)$ , where  $a$  is a particular element in the domain

---

$\therefore \neg P(a)$

# Identify the error

24. Identify the error or errors in this argument that supposedly shows that if  $\forall x(P(x) \vee Q(x))$  is true then  $\forall x P(x) \vee \forall x Q(x)$  is true.

1.  $\forall x(P(x) \vee Q(x))$  Premise
2.  $P(c) \vee Q(c)$  Universal instantiation from (1)
3.  $P(c)$  Simplification from (2)
4.  $\forall x P(x)$  Universal generalization from (3)
5.  $Q(c)$  Simplification from (2)
6.  $\forall x Q(x)$  Universal generalization from (5)
7.  $\forall x(P(x) \vee \forall x Q(x))$  Conjunction from (4) and (6)

- Formally, a **theorem** is a statement that can be shown to be true.
- A **proof** is a valid argument that establishes the truth of a theorem.
- The statements used in a proof can include **axioms (or postulates)**, other theorems (which are already proved).

- A less important theorem that is helpful in the proof of other results is called a **lemma**.

Complicated proofs are usually easier to understand when they are proved using a series of lemmas, where each lemma is proved individually.

A **corollary** is a theorem that can be established directly from a theorem that has been proved.

A **conjecture** is a statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert.

# Rules of Inference and Proof

# Proof Techniques

- Direct Proof

# Direct Proof

A direct proof of a conditional statement  $p \rightarrow q$  is constructed when the first step is the assumption that  $p$  is true;

subsequent steps are constructed using rules of inference, with the final step showing that  $q$  must also be true.

# Direct Proof

A direct proof shows that a conditional statement  $p \rightarrow q$  is true by showing that if  $p$  is true, then  $q$  must also be true, so that the combination  $p$  true and  $q$  false never occurs.

In a direct proof, we assume that  $p$  is true and use axioms, definitions, and previously proven theorems, together with rules of inference, to show that  $q$  must also be true.

## DEFINITION 1

The integer  $n$  is *even* if there exists an integer  $k$  such that  $n = 2k$ , and  $n$  is *odd* if there exists an integer  $k$  such that  $n = 2k + 1$ . (Note that every integer is either even or odd, and no integer is both even and odd.) Two integers have the *same parity* when both are even or both are odd; they have *opposite parity* when one is even and the other is odd.

### DEFINITION 1

The integer  $n$  is *even* if there exists an integer  $k$  such that  $n = 2k$ , and  $n$  is *odd* if there exists an integer  $k$  such that  $n = 2k + 1$ . (Note that every integer is either even or odd, and no integer is both even and odd.) Two integers have the *same parity* when both are even or both are odd; they have *opposite parity* when one is even and the other is odd.

EXAMPLE 1. Give a direct proof of the theorem “If  $n$  is an odd integer, then  $n^2$  is odd.”

Can you state the theorem in the language of the first order logic?

What is the domain of  $n$ ?

### DEFINITION 1

The integer  $n$  is *even* if there exists an integer  $k$  such that  $n = 2k$ , and  $n$  is *odd* if there exists an integer  $k$  such that  $n = 2k + 1$ . (Note that every integer is either even or odd, and no integer is both even and odd.) Two integers have the *same parity* when both are even or both are odd; they have *opposite parity* when one is even and the other is odd.

EXAMPLE 1. Give a direct proof of the theorem “If  $n$  is an odd integer, then  $n^2$  is odd.”

$\forall n (P(n) \rightarrow Q(n))$ , where  $P(n)$  is “ $n$  is an odd integer” and  $Q(n)$  is “ $n^2$  is odd.”

Domain of  $n$  is Set of integers.

# Proof [Direct]

1. Let  $P(n)$  is true.
2. We have,  $n = 2k + 1$ , where  $k$  is an integer. [from def. of odd integers]
3. Now,  $n^2 = (2k + 1)^2$   
 $= 4k^2 + 4k + 1$   
 $= 2(2k^2 + 2k) + 1.$
1. Since,  $k$  is integer,  $2k^2 + 2k$  is an integer. [from integer properties]
2. Let  $2k^2 + 2k = m$ .
3. We have,  $n^2 = 2m + 1$ , where  $m$  is an integer.
4. So,  $n^2$  is odd [ from def. of odd integers] ie.,  $Q(n)$  is true.
5. Hence  $\forall n (P(n) \rightarrow Q(n))$  is true. QED.

# Note

1. Good to number your steps.
2. Each step should follow the previous step.
3. Better give explanation why and how the current step follows the previous. Use parentheses, appropriate words like “So,” “We know,” “Given”, so on.
4. Do not write unnecessary stories.
5. If the reason (for the current step from previous) is obvious then no need to give that obvious reason.

# Proof by Contraposition

$p \rightarrow q$  is equivalent to its contrapositive,  
 $\neg q \rightarrow \neg p$ .

So instead of proving  $p \rightarrow q$  you can prove  
 $\neg q \rightarrow \neg p$ .

## EXAMPLE 3

Prove that if  $n$  is an integer and  $3n + 2$  is odd, then  $n$  is odd.

First write the statement in FOL (first order logic).

## EXAMPLE 3

Prove that if  $n$  is an integer and  $3n + 2$  is odd, then  $n$  is odd.

First write the statement in FOL (first order logic).

Let the predicate  $\text{Int}(k)$  :  $k$  is an integer

Similarly,  $\text{Odd}(k)$  :  $k$  is odd.

$$\text{Int}(n) \wedge \text{Odd}(3n+2) \rightarrow \text{Odd}(n)$$

## EXAMPLE 3 [Page 83]

Prove that if  $n$  is an integer and  $3n + 2$  is odd, then  $n$  is odd.

First write the statement in FOL (first order logic).

Let the predicate  $\text{Int}(k)$  :  $k$  is an integer

Similarly,  $\text{Odd}(k)$  :  $k$  is odd.

$$\text{Int}(n) \wedge \text{Odd}(3n+2) \rightarrow \text{Odd}(n)$$

$\equiv \forall n(\text{Odd}(3n+2) \rightarrow \text{Odd}(n))$  where domain of  $n$  is implicit.

## Proof[Contraposition]:

Since,  $\text{Odd}(3n+2) \rightarrow \text{Odd}(n) \equiv$   
 $\neg \text{Odd}(n) \rightarrow \neg \text{Odd}(3n+2)$

We show  $\neg \text{Odd}(n) \rightarrow \neg \text{Odd}(3n+2)$

That is, we show  $\text{Even}(n) \rightarrow \text{Even}(3n+2)$ .

**[Def:Even]**  $\text{Even}(m) \rightarrow (m=2k)$  where k is an integer.

To show  $\text{Even}(n) \rightarrow \text{Even}(3n+2)$

Let  $\text{Even}(n)$  is True.

Let  $n = 2k$ , where  $k$  is an integer.

$$\begin{aligned}\text{We get, } 3n+2 &= 3(2k)+2 \\ &= 2(3k+1)\end{aligned}$$

Since,  $3k+1$  is an integer,

we get  $\text{Even}(3n+2)$  is True.

So,  $\text{Even}(n) \rightarrow \text{Even}(3n+2)$ . QED.

## VACUOUS AND TRIVIAL PROOFS [Page 84]

We can quickly prove that a conditional statement  $p \rightarrow q$  is true when we know that  $p$  is false.

So showing  $p$  is false is a proof for  $p \rightarrow q$  which is called a Vacuous proof.

Often students feel that this is a surprise !

## EXAMPLE 5

Show that the proposition  $P(0)$  is true, where  $P(n)$  is “If  $n > 1$ , then  $n^2 > n$ ” and the domain consists of all integers.

**Proof[Vacuous]:**

Let  $R(n) : n > 1$ , and

$S(n) : n^2 > n$ .

Since  $R(0)$  is False, we get  $P(0) : R(0) \rightarrow S(0)$  is True.

## EXAMPLE 5

Show that the proposition  $P(0)$  is true, where  $P(n)$  is “If  $n > 1$ , then  $n^2 > n$ ” and the domain consists of all integers.

**Proof[Vacuous]:**

Let  $R(n) : n > 1$ , and

$S(n) : n^2 > n$ .

Since  $R(0)$  is False, we get  $P(0) : R(0) \rightarrow S(0)$  is True.

**Remark:** The fact that the conclusion of this conditional statement,  $0^2 > 0$ , is false is irrelevant to the truth value of the conditional statement, because a conditional statement with a false hypothesis is guaranteed to be true.

# Trivial Proof

We can quickly prove that a conditional statement  $p \rightarrow q$  is true when we know that  $q$  is True.

So showing  $q$  is True is a proof for  $p \rightarrow q$  which is called a Trivial proof.

Often students feel that this also is a surprise !

# Read

1. Example 6 in Page 85
2. Definition 2, Examples 7 and 8 in Page 85.

# Proofs by Contradiction [page 86]

To show that the proposition  $p$  is True,

we can show that  $\neg p \rightarrow F$

That is, we can show:  $\neg p \rightarrow (r \wedge \neg r)$  for some statement  $r$ .

(why this should work?)

# Proof

# Proof by Contradiction ...

To show  $p \rightarrow q$

the proof by contradiction shows that

$(p \wedge \neg q) \rightarrow F$ .

That is,

1. Add negation of the conclusion to the premises.
2. Derive a contradiction.

## EXAMPLE 11

Give a proof by contradiction of the theorem  
“If  $3n + 2$  is odd, then  $n$  is odd.”

Proof[Contradiction]:

Assume Even( $n$ ) is True. And, now we need to show  
Odd( $3n+2$ )  $\wedge$  Even( $n$ ) leads to a contradiction.

We can write  $n = 2k$  where  $k$  is an integer.

Then  $3n+2 = 3(2k)+2 = 2(3k+1)$ .

So  $3n+2$  is even. ie.,  $\text{Even}(3n+2)$  is True.

So,  $\text{Odd}(3n+2) \wedge \text{Even}(3n+2)$  which is always False.

Hence,  $\text{Odd}(3n+2) \rightarrow \text{Odd}(n)$ .

QED.

# PROOFS OF EQUIVALENCE

- To prove a theorem that is a biconditional statement, that is, a statement of the form  $p \leftrightarrow q$ , we show that
- $p \rightarrow q$  and  $q \rightarrow p$  are both true.
- The validity of this approach is based on the tautology  $(p \leftrightarrow q) \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$ .
- That is,  $(p \leftrightarrow q) \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

## EXAMPLE 12

Prove the theorem “If  $n$  is an integer, then  $n$  is odd if and only if  $n^2$  is odd.”

Proof:

We need to prove  $\text{Odd}(n) \leftrightarrow \text{Odd}(n^2)$ .

We show

1.  $\text{Odd}(n) \rightarrow \text{Odd}(n^2)$ , and
2.  $\text{Odd}(n^2) \rightarrow \text{Odd}(n)$

$$1. \text{ Odd}(n) \rightarrow \text{Odd}(n^2)$$

Proof[Direct]:

$$\begin{aligned}\text{Odd}(n) &\rightarrow n=2k+1 \text{ for some integer } k \\ &\rightarrow n^2 = (2k+1)^2 = 4k^2 + 4k + 1 \\ &\rightarrow n^2 = 2(2k^2 + 2k) + 1 \\ &\rightarrow \text{Odd}(n^2), \quad \text{QED.}\end{aligned}$$

2.  $\text{Odd}(n^2) \rightarrow \text{Odd}(n)$

Proof[Contraposition]:

Contrapositive of  $\text{Odd}(n^2) \rightarrow \text{Odd}(n)$  is  
 $\text{Even}(n) \rightarrow \text{Even}(n^2)$ .

Can you complete this?

2.  $\text{Odd}(n^2) \rightarrow \text{Odd}(n)$

Proof[Contraposition]:

Contrapositive of  $\text{Odd}(n^2) \rightarrow \text{Odd}(n)$  is  
 $\text{Even}(n) \rightarrow \text{Even}(n^2)$ .

Can you complete this?

Direct proof is cumbersome, but contraposition is easy.  
Refer Example 8 of Page 85

Sometimes a theorem states that several propositions are equivalent. Such a theorem states that propositions  $p_1, p_2, p_3, \dots, p_n$  are equivalent. This can be written as

$$p_1 \leftrightarrow p_2 \leftrightarrow \dots \leftrightarrow p_n,$$

Sometimes a theorem states that several propositions are equivalent. Such a theorem states that propositions  $p_1, p_2, p_3, \dots, p_n$  are equivalent. This can be written as

$$p_1 \leftrightarrow p_2 \leftrightarrow \dots \leftrightarrow p_n.$$

One easy way is to show is to show

$$(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \dots \wedge (p_n \rightarrow p_1)$$

## EXAMPLE 13

Show that these statements about the integer  $n$  are equivalent:

$p_1$ :  $n$  is even.

$p_2$ :  $n - 1$  is odd.

$p_3$ :  $n^2$  is even.

Proof: We will show that these three statements are equivalent by showing that the conditional statements  $p_1 \rightarrow p_2$ ,  $p_2 \rightarrow p_3$ , and  $p_3 \rightarrow p_1$  are true.

## EXAMPLE 13

Show that these statements about the integer  $n$  are equivalent:

p1:  $n$  is even.

p2:  $n - 1$  is odd.

p3:  $n^2$  is even.

Proof: We will show that these three statements are equivalent by showing that the conditional statements  $p1 \rightarrow p2$ ,  $p2 \rightarrow p3$ , and  $p3 \rightarrow p1$  are true. **Read Page**

**88**

# COUNTEREXAMPLES

To show that  $\forall x P(x)$  is false,

we need only find a counterexample, that is, an example  $x$  for which  $P(x)$  is false.

This is useful to **disprove** a statement.

## EXAMPLE 14

Show that the statement “Every positive integer is the sum of the squares of two integers” is false.

## EXAMPLE 14

Show that the statement “Every positive integer is the sum of the squares of two integers” is false.

Proof[Counter example]:

Integer 3 cannot be written as the sum of the squares of two integers.

## EXAMPLE 14

Show that the statement “Every positive integer is the sum of the squares of two integers” is false.

Proof[Counter example]:

Integer 3 cannot be written as the sum of the squares of two integers.

Note, this is not complete yet. You need to show that 3 cannot be written as sum of two integer squares.

## EXAMPLE 14

Show that the statement “Every positive integer is the sum of the squares of two integers” is false.

Proof[Counter example]:

Integer 3 cannot be written as the sum of the squares of two integers.

Note, this is not complete yet. You need to show that 3 cannot be written as sum of two integer squares. This can be done by other techniques.

# Read.

## Mistakes in Proofs

There are many common errors made in constructing mathematical proofs. We will briefly describe some of these here. Among the most common errors are mistakes in arithmetic and basic algebra. Even professional mathematicians make such errors, especially when working with complicated formulae. Whenever you use such computations you should check them as carefully as possible. (You should also review any troublesome aspects of basic algebra, especially before you study Section 5.1.)



Each step of a mathematical proof needs to be correct and the conclusion needs to follow logically from the steps that precede it. Many mistakes result from the introduction of steps that do not logically follow from those that precede it. This is illustrated in Examples 15–17.

**EXAMPLE 15** What is wrong with this famous supposed “proof” that  $1 = 2$ ?

**“Proof:**” We use these steps, where  $a$  and  $b$  are two equal positive integers.

Step	Reason
1. $a = b$	Given
2. $a^2 = ab$	Multiply both sides of (1) by $a$
3. $a^2 - b^2 = ab - b^2$	Subtract $b^2$ from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Factor both sides of (3)
5. $a + b = b$	Divide both sides of (4) by $a - b$
6. $2b = b$	Replace $a$ by $b$ in (5) because $a = b$ and simplify

# Exercise

1. Use a direct proof to show that the sum of two odd integers is even.

6. Use a direct proof to show that the product of two odd numbers is odd.

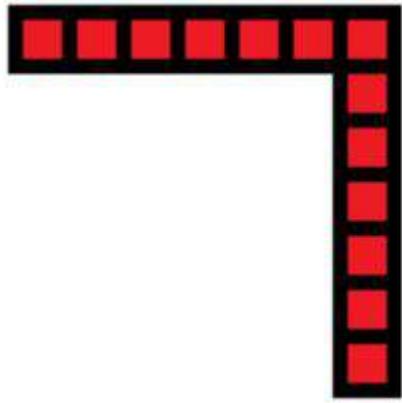
7. Use a direct proof to show that every odd integer is the difference of two squares.

7. Use a direct proof to show that every odd integer is the difference of two squares.

$$2k+1 = (k+1-k)(k+1+k)$$

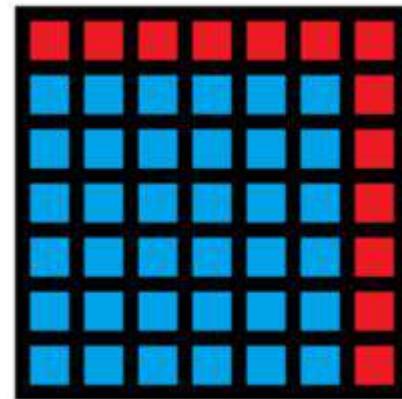
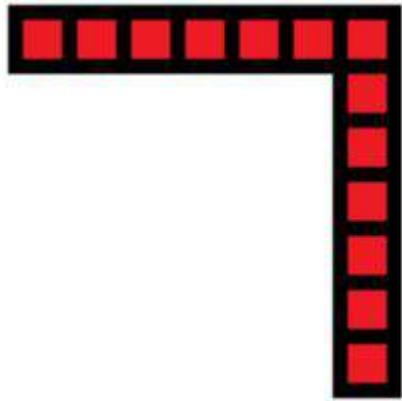
But you need to present this formally...

7. Use a direct proof to show that every odd integer is the difference of two squares.

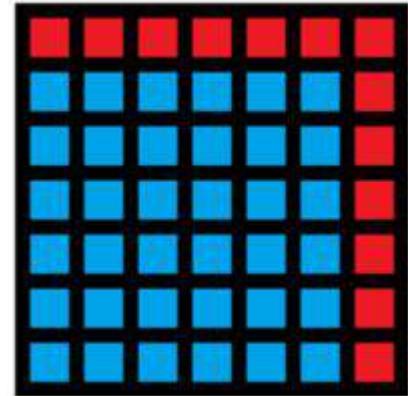
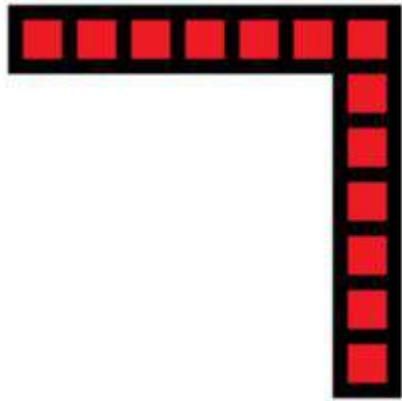


Evey odd number can be  
represented like this. Do you  
accept?

7. Use a direct proof to show that every odd integer is the difference of two squares.



7. Use a direct proof to show that every odd integer is the difference of two squares.



**do you get the intuition why the theorem is true ?!!**

# Can you prove this?

Every even integer greater than two is the sum of two prime numbers.

# Can you prove this?

Every even integer greater than two is the sum of two prime numbers.

Don't break your head. This is still an open problem called **Goldbach Conjecture**

[Conjecture is a belief, not a theorem]



42. Prove that these four statements about the integer  $n$  are equivalent: (i)  $n^2$  is odd, (ii)  $1 - n$  is even, (iii)  $n^3$  is odd, (iv)  $n^2 + 1$  is even.

**You can try (i)→(ii)→(iii)→(iv)→(i)**

# Exhaustive Proof and Proof by Cases

Sometimes we cannot prove a theorem using a single argument that holds for all possible cases.

We now introduce a method that can be used to prove a theorem, by considering different cases separately

To prove a conditional statement of the form  
 $(p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q$

the tautology

$$[(p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_n \rightarrow q)]$$

can be used as a rule of inference

## EXHAUSTIVE PROOF

Some theorems can be proved by examining a relatively small number of examples.

Such proofs are called exhaustive proofs, or proofs by exhaustion because these proofs proceed by exhausting all possibilities.

An exhaustive proof is a special type of proof by cases where each case involves checking a single example.

## Example 1

- Prove that  $n \leq 4 \rightarrow (n + 1)^3 \geq 3^n$
- Implicitly you should understand that n is from the set of integers.

## Example 1

- Prove that  $(n > 0 \wedge n \leq 4) \rightarrow (n + 1)^3 \geq 3^n$
- Implicitly you should understand that  $n$  is from the set of integers.
- Proof[Exhaustion]:

We have,  $n \in \{1, 2, 3, 4\}$ .

We show for each of  $n$  that the statement is true.

$$(n > 0 \wedge n \leq 4) \rightarrow (n + 1)^3 \geq 3^n$$

- $(n = 1) \rightarrow 2^3 \geq 3^1$  is True.
- $(n = 2) \rightarrow 3^3 \geq 3^2$  is True.
- Can you complete the proof?

## EXAMPLE 2

Prove that the only consecutive positive integers not exceeding 100 that are perfect powers are 8 and 9.

(An integer is a perfect power if it equals  $n^a$ , where  $a$  is an integer greater than 1.)

## EXAMPLE 2

Prove that the only consecutive positive integers not exceeding 100 that are perfect powers are 8 and 9.

(An integer is a perfect power if it equals  $n^a$ , where  $a$  is an integer greater than 1.)

Proof[Exhaustion]: How many cases are going to be there?

## EXAMPLE 2

Prove that the only consecutive positive integers not exceeding 100 that are perfect powers are 8 and 9.

(An integer is a perfect power if it equals  $n^a$ , where  $a$  is an integer greater than 1.)

Proof[Exhaustion]: Perfect squares not exceeding 100 are 1, 4, 9, 16, 25, 36, 49, 64, 81, and 100.

## EXAMPLE 2

Prove that the only consecutive positive integers not exceeding 100 that are perfect powers are 8 and 9.

(An integer is a perfect power if it equals  $n^a$ , where  $a$  is an integer greater than 1.)

Proof[Exhaustion]: Perfect squares not exceeding 100 are 1, 4, 9, 16, 25, 36, 49, 64, 81, and 100.

Can you complete the proof??

# Proof by cases

**EXAMPLE 3** Prove that if  $n$  is an integer, then  $n^2 \geq n$ .

# Proof by cases

**EXAMPLE 3** Prove that if  $n$  is an integer, then  $n^2 \geq n$ .

*Solution:* We can prove that  $n^2 \geq n$  for every integer by considering three cases, when  $n = 0$ , when  $n \geq 1$ , and when  $n \leq -1$ . We split the proof into three cases because it is straightforward to prove the result by considering zero, positive integers, and negative integers separately.

# Proof by cases [Page 93]

**EXAMPLE 3** Prove that if  $n$  is an integer, then  $n^2 \geq n$ .

*Solution:* We can prove that  $n^2 \geq n$  for every integer by considering three cases, when  $n = 0$ , when  $n \geq 1$ , and when  $n \leq -1$ . We split the proof into three cases because it is straightforward to prove the result by considering zero, positive integers, and negative integers separately.

*Case (i):* When  $n = 0$ , because  $0^2 = 0$ , we see that  $0^2 \geq 0$ . It follows that  $n^2 \geq n$  is true in this case.

*Case (ii):* When  $n \geq 1$ , when we multiply both sides of the inequality  $n \geq 1$  by the positive integer  $n$ , we obtain  $n \cdot n \geq n \cdot 1$ . This implies that  $n^2 \geq n$  for  $n \geq 1$ .

*Case (iii):* In this case  $n \leq -1$ . However,  $n^2 \geq 0$ . It follows that  $n^2 \geq n$ .

Because the inequality  $n^2 \geq n$  holds in all three cases, we can conclude that if  $n$  is an integer, then  $n^2 \geq n$ . 

# Unit 2

# Sets



GEORG CANTOR (1845–1918)

Cantor is considered  
the founder of set theory

# Syllabus for Unit 2

- Unit – 2 [8 Hours]: Sets - Basic Set Operations, Functions, Cardinality, Countable and Uncountable Sets, Sequence & Summations; Induction - Principle of Induction, Strong Induction; Recursion - Recursive Algorithms, Recursive Definition of Sets, Structural Induction;

# DEFINITION 1

- A set is an unordered collection of objects, called elements or members of the set.
- A set is said to contain its elements.
- We write  $a \in A$  to denote that  $a$  is an element of the set  $A$ .
- The notation  $a \notin A$  denotes that  $a$  is not an element of the set  $A$ .

# Representation of sets

- The notation  $\{a, b, c, d\}$  represents the set with the four elements a, b, c, and d. This way of describing a set is known as the **roster method**.

- Sometimes the **roster method** is used to describe a set without listing all its members.
- Some members of the set are listed, and then ellipses (...) are used when the general pattern of the elements is obvious

- Sometimes the **roster method** is used to describe a set without listing all its members.
- Some members of the set are listed, and then ellipses (...) are used when the general pattern of the elements is obvious
- The set of positive integers less than 100 can be denoted by {1, 2, 3,..., 99}.

# Set builder notation

- $O = \{x \mid x \text{ is an odd positive integer less than } 10\}$ ,

# Notation for commonly used sets

**N** = {0, 1, 2, 3, ...}, the set of **natural numbers**

**Z** = {..., -2, -1, 0, 1, 2, ...}, the set of **integers**

**Z<sup>+</sup>** = {1, 2, 3, ...}, the set of **positive integers**

**Q** = { $p/q \mid p \in \mathbf{Z}$ ,  $q \in \mathbf{Z}$ , and  $q \neq 0$ }, the set of **rational numbers**

**R**, the set of **real numbers**

**R<sup>+</sup>**, the set of **positive real numbers**

**C**, the set of **complex numbers**.

- $\mathbf{Q}^+ = \{x \in \mathbb{R} \mid x = p/q, \text{ for some positive integers } p \text{ and } q\}$ .

# Intervals are sets

Recall the notation for **intervals** of real numbers. When  $a$  and  $b$  are real numbers with  $a < b$ , we write

$$[a, b] = \{x \mid a \leq x \leq b\}$$

$$[a, b) = \{x \mid a \leq x < b\}$$

$$(a, b] = \{x \mid a < x \leq b\}$$

$$(a, b) = \{x \mid a < x < b\}$$

Note that  $[a, b]$  is called the **closed interval** from  $a$  to  $b$  and  $(a, b)$  is called the **open interval** from  $a$  to  $b$ .

## DEFINITION 2: Set Equality

- Two sets are equal if and only if they have the same elements.
- Therefore, if A and B are sets, then A and B are equal if and only if  $\forall x(x \in A \leftrightarrow x \in B)$ .
- We write  $A = B$  if A and B are **equal** sets.

## EXAMPLE 6

- The sets  $\{1, 3, 5\}$  and  $\{3, 5, 1\}$  are equal, because they have the same elements.
- Note that the order in which the elements of a set are listed does not matter.

# Duplicates does not matter

- Note also that it does not matter if an element of a set is listed more than once, so  $\{1, 3, 3, 3, 5, 5, 5, 5\}$  is the same as the set  $\{1, 3, 5\}$  because they have the same elements.

# THE EMPTY SET

- There is a special set that has no elements. This set is called the empty set, or null set, and is denoted by  $\emptyset$ .
- The empty set can also be denoted by { }
- For instance, the set of all positive integers that are greater than their squares is the null set.

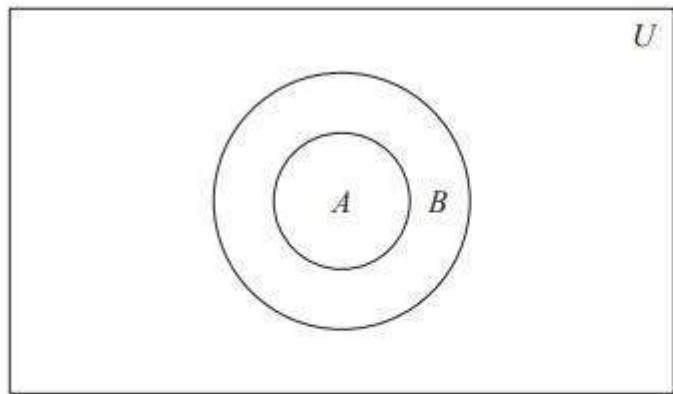
# $\emptyset$ Vs. $\{\emptyset\}$

- A common error is to confusion: Between set  $\emptyset$  with the set  $\{\emptyset\}$
- $\{\emptyset\}$  is a singleton set.
- Singleton set means that the set has only one element.

## DEFINITION 3: Subsets

- The set A is a subset of B if and only if every element of A is also an element of B.
- We use the notation  $A \subseteq B$  to indicate that A is a subset of the set B.

- We see that  $A \subseteq B$  if and only if the quantification  $\forall x(x \in A \rightarrow x \in B)$  is true.
- Note that to show that  $A$  is not a subset of  $B$  we need only find one element  $x \in A$  with  $x \notin B$ .
  - Such an  $x$  is a counterexample to disprove the claim that  $x \in A$  implies  $x \in B$ .



**FIGURE 2** Venn Diagram Showing that  $A$  Is a Subset of  $B$ .

## THEOREM 1

For every set  $S$ , (i)  $\emptyset \subseteq S$  and (ii)  $S \subseteq S$ .

- Proof for (i)[Direct]:

$\forall x(x \in \emptyset \rightarrow x \in S)$  is true. Because  $x \in \emptyset$  is always false. QED.

- Proof for (ii) is left as an exercise.

# Proper subset

- When we wish to emphasize that a set A is a subset of a set B but that  $A \neq B$ , we write  $A \subset B$  and say that A is a **proper subset** of B.
-

# Proper subset

- When we wish to emphasize that a set A is a subset of a set B but that  $A = B$ , we write  $A \subset B$  and say that A is a **proper subset** of B.
- That is, A is a proper subset of B if and only if  $\forall x(x \in A \rightarrow x \in B) \wedge \exists x(x \in B \wedge x \notin A)$

# The Size of a Set

- **DEFINITION 4**

Let  $S$  be a set. If there are exactly  $n$  distinct elements in  $S$  where  $n$  is a nonnegative integer, we say that  $S$  is a *finite set* and that  $n$  is the *cardinality* of  $S$ . The cardinality of  $S$  is denoted by  $|S|$ .

- Remark: The term cardinality comes from the common usage of the term cardinal number as the size of a finite set.

**EXAMPLE 10** Let  $A$  be the set of odd positive integers less than 10. Then  $|A| = 5$ .

**EXAMPLE 11** Let  $S$  be the set of letters in the English alphabet. Then  $|S| = 26$ .

**EXAMPLE 12** Because the null set has no elements, it follows that  $|\emptyset| = 0$ .

We will also be interested in sets that are not finite.

## DEFINITION 5

- A set is said to be *infinite* if it is not finite.
- **EXAMPLE 13** The set of positive integers is infinite.

# Power Set

- **DEFINITION 6** Given a set  $S$ , the power set of  $S$  is the set of all subsets of the set  $S$ . The power set of  $S$  is denoted by  $\mathcal{P}(S)$ .
- Note, in Computer Science and in other Engineering fields, this is also denoted by  $2^S$ .

- 
- 

**EXAMPLE 14** What is the power set of the set  $\{0, 1, 2\}$ ?

- 
- 

**EXAMPLE 14** What is the power set of the set  $\{0, 1, 2\}$ ?

*Solution:* The power set  $\mathcal{P}(\{0, 1, 2\})$  is the set of all subsets of  $\{0, 1, 2\}$ . Hence,

$$\mathcal{P}(\{0, 1, 2\}) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}.$$

Note that the empty set and the set itself are members of this set of subsets.

- 
- 

**EXAMPLE 14** What is the power set of the set  $\{0, 1, 2\}$ ?

*Solution:* The power set  $\mathcal{P}(\{0, 1, 2\})$  is the set of all subsets of  $\{0, 1, 2\}$ . Hence,

$$\mathcal{P}(\{0, 1, 2\}) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}.$$

Note that the empty set and the set itself are members of this set of subsets.

$\mathcal{P}$

- Note that the book uses
- But, in these slides we might use  $\mathcal{P}$  or  $\mathbf{P}$  (for simplicity in typing).
- You can also write  $2^{\{0,1,2\}}$

EXAMPLE 15. What is the power set of the empty set? What is the power set of the set  $\{\emptyset\}$ ?

-

**EXAMPLE 15.** What is the power set of the empty set? What is the power set of the set  $\{\emptyset\}$ ?

- *Solution:* The empty set has exactly one subset, namely, itself. Consequently,  
$$\mathcal{P}(\emptyset) = \{\emptyset\}.$$

**EXAMPLE 15.** What is the power set of the empty set? What is the power set of the set  $\{\emptyset\}$ ?

- *Solution:* The empty set has exactly one subset, namely, itself. Consequently,  
$$\mathcal{P}(\emptyset) = \{\emptyset\}.$$

- The set  $\{\emptyset\}$  has exactly two subsets, namely,  $\emptyset$  and the set  $\{\emptyset\}$  itself. Therefore,  
$$\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}.$$

# Cartesian Products

- We need to define first the **ordered n-tuple**

# Cartesian Products

- We need to define first the **ordered n-tuple**
- DEFINITION 7

The *ordered n-tuple*  $(a_1, a_2, \dots, a_n)$  is the ordered collection that has  $a_1$  as its first element,  $a_2$  as its second element,  $\dots$ , and  $a_n$  as its  $n$ th element.

# Cartesian Products

- We need to define first the **ordered n-tuple**
- DEFINITION 7

The *ordered n-tuple*  $(a_1, a_2, \dots, a_n)$  is the ordered collection that has  $a_1$  as its first element,  $a_2$  as its second element,  $\dots$ , and  $a_n$  as its  $n$ th element.

We say that two ordered  $n$ -tuples are equal if and only if each corresponding pair of their elements is equal. In other words,  $(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_n)$  if and only if  $a_i = b_i$ , for  $i = 1, 2, \dots, n$ .

# Cartesian Products

- We need to define first the **ordered n-tuple**
- DEFINITION 7

The *ordered n-tuple*  $(a_1, a_2, \dots, a_n)$  is the ordered collection that has  $a_1$  as its first element,  $a_2$  as its second element,  $\dots$ , and  $a_n$  as its  $n$ th element.

We say that two ordered  $n$ -tuples are equal if and only if each corresponding pair of their elements is equal. In other words,  $(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_n)$  if and only if  $a_i = b_i$ , for  $i = 1, 2, \dots, n$ .

In particular, ordered 2-tuples are called **ordered pairs**. The ordered pairs  $(a, b)$  and  $(c, d)$  are equal if and only if  $a = c$  and  $b = d$ . Note that  $(a, b)$  and  $(b, a)$  are not equal unless  $a = b$ .

# Cartesian Products

- **DEFINITION 8**

Let  $A$  and  $B$  be sets. The *Cartesian product* of  $A$  and  $B$ , denoted by  $A \times B$ , is the set of all ordered pairs  $(a, b)$ , where  $a \in A$  and  $b \in B$ . Hence,

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

- Read examples in page 123
- Read Definition 9 in page 123

## EXAMPLE 20

- Suppose that  $A = \{1, 2\}$ . It follows that  $A^2 = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$  and  $A^3 = \{(1, 1, 1), (1, 1, 2), (1, 2, 1), (1, 2, 2), (2, 1, 1), (2, 1, 2), (2, 2, 1), (2, 2, 2)\}$ .
- For definition of  $A^n$ ,  
*where n is a positive integer read the text book*  
page 124

# Sets

# Relation

-

# Relation

- Subset of a Cartesian Product.
- $R \subseteq A \times B$
- R is called a relation from A to B.
- Note  $A \times B \neq B \times A$
- By default Relations are binary, unless other specified.
- In Databases called “relational databases” a table is nothing but a n-ary relation.

# Using Set Notation with Quantifiers

- **EXAMPLE 22**

What do the statements  $\forall x \in \mathbf{R} (x^2 \geq 0)$  and  $\exists x \in \mathbf{Z} (x^2 = 1)$  mean?

# Using Set Notation with Quantifiers

- **EXAMPLE 22**

What do the statements  $\forall x \in \mathbf{R} (x^2 \geq 0)$  and  $\exists x \in \mathbf{Z} (x^2 = 1)$  mean?

*Solution:* The statement  $\forall x \in \mathbf{R} (x^2 \geq 0)$  states that for every real number  $x$ ,  $x^2 \geq 0$ . This statement can be expressed as “The square of every real number is nonnegative.” This is a true statement.

# Using Set Notation with Quantifiers

- **EXAMPLE 22**

What do the statements  $\forall x \in \mathbf{R} (x^2 \geq 0)$  and  $\exists x \in \mathbf{Z} (x^2 = 1)$  mean?

*Solution:* The statement  $\forall x \in \mathbf{R} (x^2 \geq 0)$  states that for every real number  $x$ ,  $x^2 \geq 0$ . This statement can be expressed as “The square of every real number is nonnegative.” This is a true statement.

The statement  $\exists x \in \mathbf{Z} (x^2 = 1)$  states that there exists an integer  $x$  such that  $x^2 = 1$ . This statement can be expressed as “There is an integer whose square is 1.” This is also a true statement because  $x = 1$  is such an integer (as is  $-1$ ). ◀

# Truth Sets and Quantifiers

- The truth set of  $P(x)$  is denoted by  $\{x \in D \mid P(x)\}.$
- Here  $P$  is a predicate over the domain  $D.$

# EXAMPLE 23

What are the truth sets of the predicates  $P(x)$ ,  $Q(x)$ , and  $R(x)$ , where the domain is the set of integers and  $P(x)$  is “ $|x| = 1$ ,”  $Q(x)$  is “ $x^2 = 2$ ,” and  $R(x)$  is “ $|x| = x$ .”

# EXAMPLE 23

What are the truth sets of the predicates  $P(x)$ ,  $Q(x)$ , and  $R(x)$ , where the domain is the set of integers and  $P(x)$  is “ $|x| = 1$ ,”  $Q(x)$  is “ $x^2 = 2$ ,” and  $R(x)$  is “ $|x| = x$ .”

*Solution:* The truth set of  $P$ ,  $\{x \in \mathbf{Z} \mid |x| = 1\}$ , is the set of integers for which  $|x| = 1$ . Because  $|x| = 1$  when  $x = 1$  or  $x = -1$ , and for no other integers  $x$ , we see that the truth set of  $P$  is the set  $\{-1, 1\}$ .

# EXAMPLE 23

What are the truth sets of the predicates  $P(x)$ ,  $Q(x)$ , and  $R(x)$ , where the domain is the set of integers and  $P(x)$  is “ $|x| = 1$ ,”  $Q(x)$  is “ $x^2 = 2$ ,” and  $R(x)$  is “ $|x| = x$ .”

*Solution:* The truth set of  $P$ ,  $\{x \in \mathbf{Z} \mid |x| = 1\}$ , is the set of integers for which  $|x| = 1$ . Because  $|x| = 1$  when  $x = 1$  or  $x = -1$ , and for no other integers  $x$ , we see that the truth set of  $P$  is the set  $\{-1, 1\}$ .

The truth set of  $Q$ ,  $\{x \in \mathbf{Z} \mid x^2 = 2\}$ , is the set of integers for which  $x^2 = 2$ . This is the empty set because there are no integers  $x$  for which  $x^2 = 2$ .

# EXAMPLE 23

What are the truth sets of the predicates  $P(x)$ ,  $Q(x)$ , and  $R(x)$ , where the domain is the set of integers and  $P(x)$  is “ $|x| = 1$ ,”  $Q(x)$  is “ $x^2 = 2$ ,” and  $R(x)$  is “ $|x| = x$ .”

*Solution:* The truth set of  $P$ ,  $\{x \in \mathbf{Z} \mid |x| = 1\}$ , is the set of integers for which  $|x| = 1$ . Because  $|x| = 1$  when  $x = 1$  or  $x = -1$ , and for no other integers  $x$ , we see that the truth set of  $P$  is the set  $\{-1, 1\}$ .

The truth set of  $Q$ ,  $\{x \in \mathbf{Z} \mid x^2 = 2\}$ , is the set of integers for which  $x^2 = 2$ . This is the empty set because there are no integers  $x$  for which  $x^2 = 2$ .

The truth set of  $R$ ,  $\{x \in \mathbf{Z} \mid |x| = x\}$ , is the set of integers for which  $|x| = x$ . Because  $|x| = x$  if and only if  $x \geq 0$ , it follows that the truth set of  $R$  is  $\mathbf{N}$ , the set of nonnegative integers.

- Solve at least a few exercise problems in page 125
- Next, We briefly cover: 2.2 Set Operations which is mostly a repetition of your high school or +2 concepts.

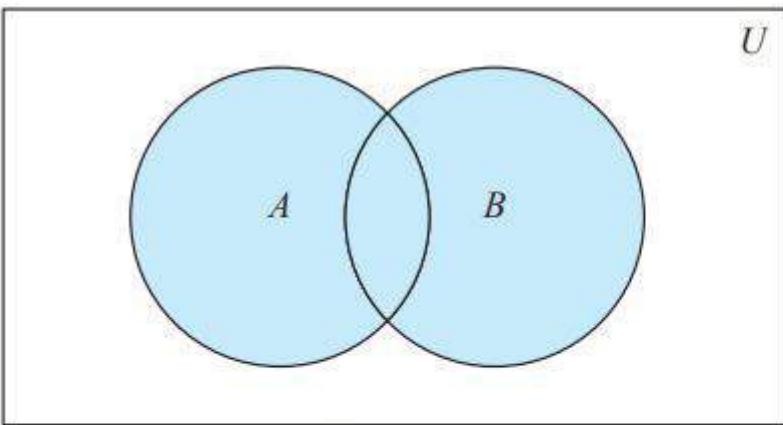
# Set Operations

# Pages 127

- Read about union, intersection, complement.

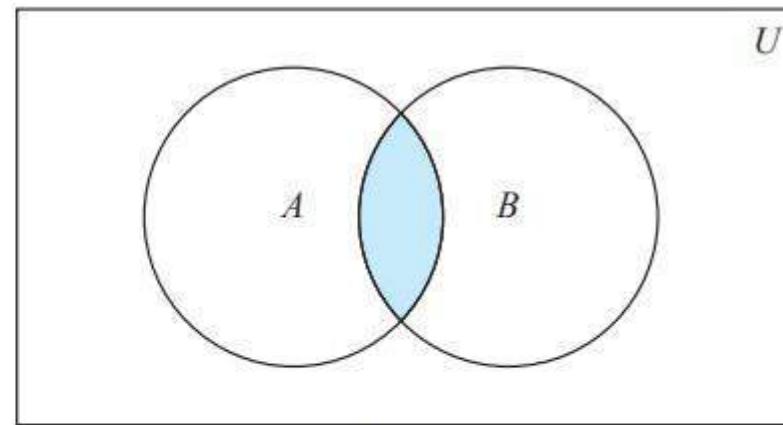
$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$



$A \cup B$  is shaded.

**FIGURE 1** Venn Diagram of the Union of  $A$  and  $B$ .



$A \cap B$  is shaded.

**FIGURE 2** Venn Diagram of the Intersection of  $A$  and  $B$ .

# DEFINITION 3

- 

Two sets are called *disjoint* if their intersection is the empty set.

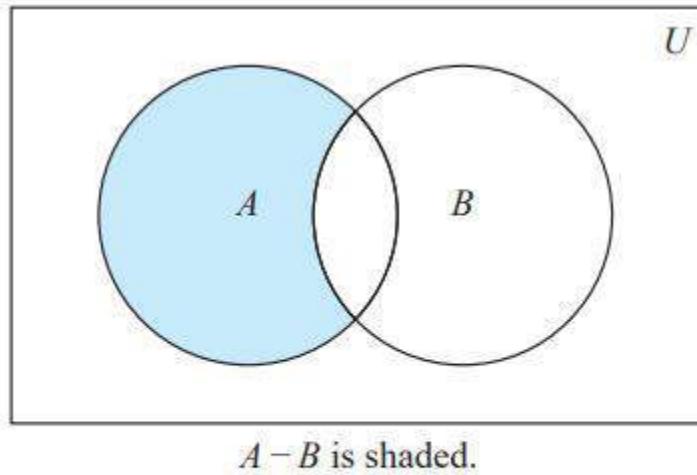
- $|A \cup B| = |A| + |B| - |A \cap B|.$
- But if A and B are disjoint then

$$|A \cup B| = |A| + |B|$$

# A – B

$$A - B = \{x \mid x \in A \wedge x \notin B\}.$$

**Remark:** The difference of sets  $A$  and  $B$  is sometimes denoted by  $A \setminus B$ .

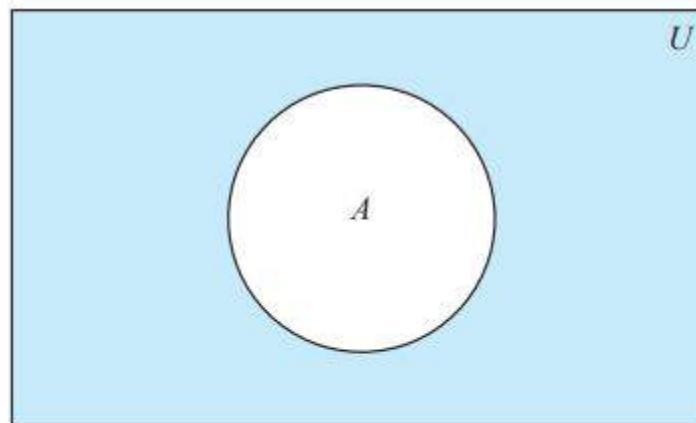


**FIGURE 3** Venn Diagram for  
the Difference of  $A$  and  $B$ .

# DEFINITION 5

- Complement.

Let  $U$  be the universal set. The *complement* of the set  $A$ , denoted by  $\bar{A}$ , is the complement of  $A$  with respect to  $U$ . Therefore, the complement of the set  $A$  is  $U - A$ .



$\bar{A}$  is shaded.

**FIGURE 4** Venn Diagram for the Complement of the Set  $A$ .

$$\overline{A} = \{x \in U \mid x \notin A\}.$$

Can you prove this?

- $A - B = A \cap \overline{B}.$

<i>Identity</i>	<i>Name</i>
$A \cap U = A$ $A \cup \emptyset = A$	Identity laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$(\overline{\overline{A}}) = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws

**EXAMPLE 10** Prove that  $\overline{A \cap B} = \overline{A} \cup \overline{B}$ .

• *Solution:* We will prove that the two sets  $\overline{A \cap B}$  and  $\overline{A} \cup \overline{B}$  are equal by showing that each set is a subset of the other.

We show (i)  $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$ , and  
(ii)  $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$

Read page 130 for this.

# Set builder notation and logical equivalences can be used...

- Show  $\overline{A \cap B} = \overline{A} \cup \overline{B}$ .

*Solution:* We can prove this identity with the following steps.

$$\begin{aligned}\overline{A \cap B} &= \{x \mid x \notin A \cap B\} && \text{by definition of complement} \\&= \{x \mid \neg(x \in (A \cap B))\} && \text{by definition of does not belong symbol} \\&= \{x \mid \neg(x \in A \wedge x \in B)\} && \text{by definition of intersection} \\&= \{x \mid \neg(x \in A) \vee \neg(x \in B)\} && \text{by the first De Morgan law for logical equivalences} \\&= \{x \mid x \notin A \vee x \notin B\} && \text{by definition of does not belong symbol} \\&= \{x \mid x \in \overline{A} \vee x \in \overline{B}\} && \text{by definition of complement} \\&= \{x \mid x \in \overline{A} \cup \overline{B}\} && \text{by definition of union} \\&= \overline{A} \cup \overline{B} && \text{by meaning of set builder notation}\end{aligned}$$

# Membership Tables

- Similar to Truth table in propositional logic.
- To indicate an element is in the set we use 1.
- To say an element is not in the set we use 0.

## EXAMPLE 13

Use a membership table to show that  
 $\cap (B \cup C) = (A \cap B) \cup (A \cap C)$ .

A

**TABLE 2** A Membership Table for the Distributive Property.

A	B	C	$B \cup C$	$A \cap (B \cup C)$	$A \cap B$	$A \cap C$	$(A \cap B) \cup (A \cap C)$
1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1
1	0	1	1	1	0	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

# EXAMPLE 14

Let  $A$ ,  $B$ , and  $C$  be sets. Show that

$$\overline{A \cup (B \cap C)} = (\overline{C} \cup \overline{B}) \cap \overline{A}.$$

*Solution:* We have

$$\begin{aligned}\overline{A \cup (B \cap C)} &= \overline{A} \cap \overline{(B \cap C)} && \text{by the first De Morgan law} \\ &= \overline{A} \cap (\overline{B} \cup \overline{C}) && \text{by the second De Morgan law} \\ &= (\overline{B} \cup \overline{C}) \cap \overline{A} && \text{by the commutative law for intersections} \\ &= (\overline{C} \cup \overline{B}) \cap \overline{A} && \text{by the commutative law for unions.}\end{aligned}$$

# Generalized Unions and Intersections

## DEFINITION 6

The *union* of a collection of sets is the set that contains those elements that are members of at least one set in the collection.

We use the notation

$$A_1 \cup A_2 \cup \dots \cup A_n = \bigcup_{i=1}^n A_i$$

to denote the union of the sets  $A_1, A_2, \dots, A_n$ .

# DEFINITION 7

The *intersection* of a collection of sets is the set that contains those elements that are members of all the sets in the collection.

We use the notation

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^n A_i$$

# EXAMPLE 16

For  $i = 1, 2, \dots$ , let  $A_i = \{i, i + 1, i + 2, \dots\}$ . Then,

$$\bigcup_{i=1}^n A_i = \bigcup_{i=1}^n \{i, i + 1, i + 2, \dots\} = \{1, 2, 3, \dots\},$$

and

$$\bigcap_{i=1}^n A_i =$$

# EXAMPLE 16

For  $i = 1, 2, \dots$ , let  $A_i = \{i, i + 1, i + 2, \dots\}$ . Then,

$$\bigcup_{i=1}^n A_i = \bigcup_{i=1}^n \{i, i + 1, i + 2, \dots\} = \{1, 2, 3, \dots\},$$

and

$$\bigcap_{i=1}^n A_i = \bigcap_{i=1}^n \{i, i + 1, i + 2, \dots\} = \{n, n + 1, n + 2, \dots\} = A_n.$$

# EXAMPLE 17

Suppose that  $A_i = \{1, 2, 3, \dots, i\}$  for  $i = 1, 2, 3, \dots$ . Then,

$$\bigcup_{i=1}^{\infty} A_i = \bigcup_{i=1}^{\infty} \{1, 2, 3, \dots, i\} = \{1, 2, 3, \dots\} = \mathbf{Z}^+$$

and

$$\bigcap_{i=1}^{\infty} A_i = \bigcap_{i=1}^{\infty} \{1, 2, 3, \dots, i\} = \{1\}.$$

# Exercises

5. Prove the complementation law in Table 1 by showing that  $\overline{\overline{A}} = A$ .
6. Prove the identity laws in Table 1 by showing that
  - a)  $A \cup \emptyset = A$ .
  - b)  $A \cap U = A$ .
7. Prove the domination laws in Table 1 by showing that
  - a)  $A \cup U = U$ .
  - b)  $A \cap \emptyset = \emptyset$ .
8. Prove the idempotent laws in Table 1 by showing that
  - a)  $A \cup A = A$ .
  - b)  $A \cap A = A$ .
9. Prove the complement laws in Table 1 by showing that
  - a)  $A \cup \overline{A} = U$ .
  - b)  $A \cap \overline{A} = \emptyset$ .
10. Show that
  - a)  $A - \emptyset = A$ .
  - b)  $\emptyset - A = \emptyset$ .

**29.** What can you say about the sets  $A$  and  $B$  if we know that

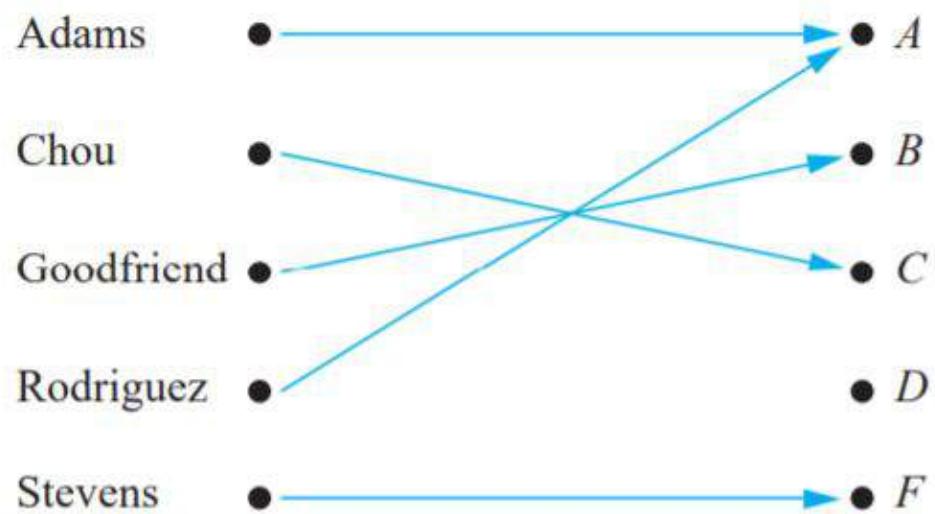
- a)  $A \cup B = A?$
- b)  $A \cap B = A?$
- c)  $A - B = A?$
- d)  $A \cap B = B \cap A?$
- e)  $A - B = B - A?$

**\*46.** Show that if  $A$ ,  $B$ , and  $C$  are sets, then

$$\begin{aligned}|A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| \\&\quad - |A \cap C| - |B \cap C| + |A \cap B \cap C|.\end{aligned}$$

## **2.3** Functions

Page 138, ...



**FIGURE 1** Assignment of Grades in a Discrete Mathematics Class.

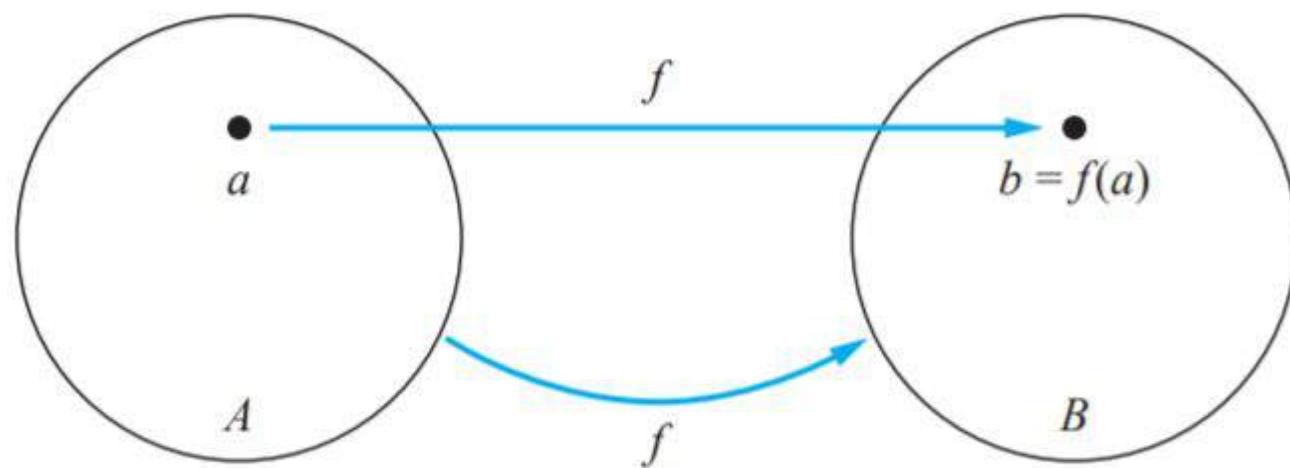
# DEFINITION 1

- Let A and B be nonempty sets.
- A function f from A to B is an assignment of exactly one element of B to each element of A.
- We write  $f(a) = b$  if b is the unique element of B assigned by the function f to the element a of A.
- If f is a function from A to B, we write  
$$f: A \rightarrow B.$$

Remark: Functions are sometimes also called  
*mappings* or *transformations*.

# DEFINITION 2

- If  $f$  is a function from  $A$  to  $B$ , we say that  $A$  is the *domain* of  $f$  and  $B$  is the codomain of  $f$ .
- If  $f(a) = b$ , we say that  $b$  is the *image* of  $a$  and  $a$  is a *preimage* of  $b$ .
- The *range*, or *image*, of  $f$  is the set of all images of elements of  $A$ . Also, if  $f$  is a function from  $A$  to  $B$ , we say that  $f$  *maps*  $A$  to  $B$ .



**FIGURE 2** The Function  $f$  Maps  $A$  to  $B$ .

## EXAMPLE 3

Let  $f$  be the function that assigns the last two bits of a bit string of length 2 or greater to that string. For example,  $f(11010) = 10$ . Then, the domain of  $f$  is the set of all bit strings of length 2 or greater, and both the codomain and range are the set  $\{00, 01, 10, 11\}$ .



- A function is called **real-valued** if its codomain is the set of real numbers, and
- it is called **integer-valued** if its codomain is the set of integers.
- Two real-valued functions or two integer valued functions with the same domain can be **added**, as well as **multiplied**.

# DEFINITION 3: Addition and Multiplication of two functions

Let  $f_1$  and  $f_2$  be functions from  $A$  to  $\mathbf{R}$ . Then  $f_1 + f_2$  and  $f_1 f_2$  are also functions from  $A$  to  $\mathbf{R}$  defined for all  $x \in A$  by

$$(f_1 + f_2)(x) = f_1(x) + f_2(x),$$

$$(f_1 f_2)(x) = f_1(x) f_2(x).$$

# EXAMPLE 6

Let  $f_1$  and  $f_2$  be functions from  $\mathbf{R}$  to  $\mathbf{R}$  such that  $f_1(x) = x^2$  and  $f_2(x) = x - x^2$ . What are the functions  $f_1 + f_2$  and  $f_1 f_2$ ?

## EXAMPLE 6

Let  $f_1$  and  $f_2$  be functions from  $\mathbf{R}$  to  $\mathbf{R}$  such that  $f_1(x) = x^2$  and  $f_2(x) = x - x^2$ . What are the functions  $f_1 + f_2$  and  $f_1 f_2$ ?

*Solution:* From the definition of the sum and product of functions, it follows that

$$(f_1 + f_2)(x) = f_1(x) + f_2(x) = x^2 + (x - x^2) = x$$

and

$$(f_1 f_2)(x) = x^2(x - x^2) = x^3 - x^4.$$



# DEFINITION 4

Let  $f$  be a function from  $A$  to  $B$  and let  $S$  be a subset of  $A$ . The *image* of  $S$  under the function  $f$  is the subset of  $B$  that consists of the images of the elements of  $S$ . We denote the image of  $S$  by  $f(S)$ , so

$$f(S) = \{t \mid \exists s \in S (t = f(s))\}.$$

We also use the shorthand  $\{f(s) \mid s \in S\}$  to denote this set.

# DEFINITION 4

Let  $f$  be a function from  $A$  to  $B$  and let  $S$  be a subset of  $A$ . The *image* of  $S$  under the function  $f$  is the subset of  $B$  that consists of the images of the elements of  $S$ . We denote the image of  $S$  by  $f(S)$ , so

$$f(S) = \{t \mid \exists s \in S (t = f(s))\}.$$

We also use the shorthand  $\{f(s) \mid s \in S\}$  to denote this set.

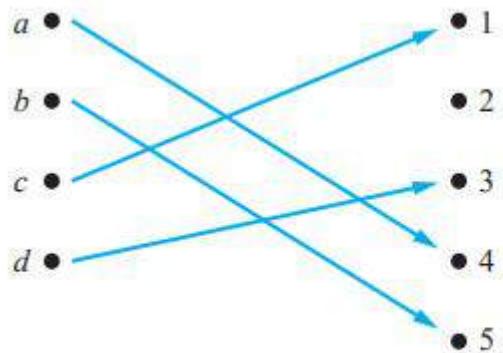
**Remark:** The notation  $f(S)$  for the image of the set  $S$  under the function  $f$  is potentially ambiguous. Here,  $f(S)$  denotes a set, and not the value of the function  $f$  for the set  $S$ .

## EXAMPLE 7

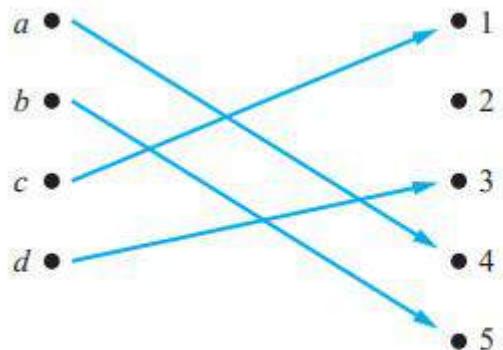
- Let  $A = \{a, b, c, d, e\}$  and  $B = \{1, 2, 3, 4\}$  with  $f(a) = 2$ ,  $f(b) = 1$ ,  $f(c) = 4$ ,  $f(d) = 1$ , and  $f(e) = 1$ .
- The image of the subset  $S = \{b, c, d\}$  is the set  $f(S) = \{1, 4\}$ .

# One-to-One and Onto Functions

- DEFINITION 5
- A function  $f$  is said to be **one-to-one**, or an injunction, if and only if  $f(a) = f(b)$  implies that  $a = b$  for all  $a$  and  $b$  in the domain of  $f$ .
- A function is said to be **injective** if it is one-to-one.



**FIGURE 3** A One-to-One Function.



**FIGURE 3 A One-to-One Function.**

Note that a function  $f$  is one-to-one if and only if  $f(a) \neq f(b)$  whenever  $a \neq b$ . This way of expressing that  $f$  is one-to-one is obtained by taking the contrapositive of the implication in the definition.

**Remark:** We can express that  $f$  is one-to-one using quantifiers as  $\forall a \forall b(f(a) = f(b) \rightarrow a = b)$  or equivalently  $\forall a \forall b(a \neq b \rightarrow f(a) \neq f(b))$ , where the universe of discourse is the domain of the function.

## EXAMPLE 8

- Determine whether the function  $f$  from  $\{a, b, c, d\}$  to  $\{1, 2, 3, 4, 5\}$  with  $f(a) = 4$ ,  $f(b) = 5$ ,  $f(c) = 1$ , and  $f(d) = 3$  is one-to-one.

## EXAMPLE 8

- Determine whether the function  $f$  from  $\{a, b, c, d\}$  to  $\{1, 2, 3, 4, 5\}$  with  $f(a) = 4$ ,  $f(b) = 5$ ,  $f(c) = 1$ , and  $f(d) = 3$  is one-to-one.
- Solution: The function  $f$  is one-to-one because  $f$  takes on different values at the four elements of its domain. This is illustrated in Figure 3.

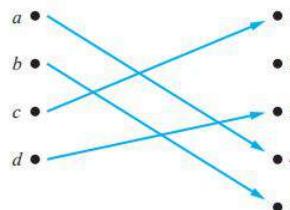


FIGURE 3 A One-to-One Function.

## EXAMPLE 9

Determine whether the function  $f(x) = x^2$  from the set of integers to the set of integers is one-to-one.

-

## EXAMPLE 9

Determine whether the function  $f(x) = x^2$  from the set of integers to the set of integers is one-to-one.

- No
- What if the domain is the set of positive integers ( $\mathbf{Z}^+$ )

## EXAMPLE 9

Determine whether the function  $f(x) = x^2$  from the set of integers to the set of integers is one-to-one.

- No
- What if the domain is the set of positive integers ( $\mathbf{Z}^+$ )
- Yes.

## EXAMPLE 10

- Determine whether the function  $f(x) = x + 1$  from the set of real numbers to itself is one-to-one.

## EXAMPLE 10

- Determine whether the function  $f(x) = x + 1$  from the set of real numbers to itself is one-to-one.
- Yes. Because  $x \neq y \rightarrow x + 1 \neq y + 1$

# DEFINITION 6

- A function  $f$  whose domain and codomain are subsets of the set of real numbers is called **increasing** if  $f(x) \leq f(y)$ , and **strictly increasing** if  $f(x) < f(y)$ , whenever  $x < y$  and  $x$  and  $y$  are in the domain of  $f$ .
- Similarly,  $f$  is called **decreasing** if  $f(x) \geq f(y)$ , and **strictly decreasing** if  $f(x) > f(y)$ , whenever  $x < y$  and  $x$  and  $y$  are in the domain of  $f$ . (The word **strictly** in this definition indicates a strict inequality.)

**Remark:** A function  $f$  is increasing if  $\forall x \forall y (x < y \rightarrow f(x) \leq f(y))$ , strictly increasing if  $\forall x \forall y (x < y \rightarrow f(x) < f(y))$ , decreasing if  $\forall x \forall y (x < y \rightarrow f(x) \geq f(y))$ , and strictly decreasing if  $\forall x \forall y (x < y \rightarrow f(x) > f(y))$ , where the universe of discourse is the domain of  $f$ .

# Onto function (Surjection)

A function  $f$  from  $A$  to  $B$  is called *onto*, or a *surjection*, if and only if for every element  $b \in B$  there is an element  $a \in A$  with  $f(a) = b$ . A function  $f$  is called *surjective* if it is onto.

**Remark:** A function  $f$  is onto if  $\forall y \exists x (f(x) = y)$ , where the domain for  $x$  is the domain of the function and the domain for  $y$  is the codomain of the function.

## EXAMPLE 12

Let  $f$  be the function from  $\{a, b, c, d\}$  to  $\{1, 2, 3\}$  defined by  $f(a) = 3$ ,  $f(b) = 2$ ,  $f(c) = 1$ , and  $f(d) = 3$ . Is  $f$  an onto function?

## EXAMPLE 12

Let  $f$  be the function from  $\{a, b, c, d\}$  to  $\{1, 2, 3\}$  defined by  $f(a) = 3$ ,  $f(b) = 2$ ,  $f(c) = 1$ , and  $f(d) = 3$ . Is  $f$  an onto function?

*Solution:* Because all three elements of the codomain are images of elements in the domain, we see that  $f$  is onto. This is illustrated in Figure 4. Note that if the codomain were  $\{1, 2, 3, 4\}$ , then  $f$  would not be onto.

# EXAMPLE 13

Is the function  $f(x) = x^2$  from the set of integers to the set of integers onto?

# EXAMPLE 13

Is the function  $f(x) = x^2$  from the set of integers to the set of integers onto?

*Solution:* The function  $f$  is not onto because there is no integer  $x$  with  $x^2 = -1$ , for instance.

## EXAMPLE 14

- Is the function  $f(x) = x + 1$  from the set of integers to the set of integers onto?

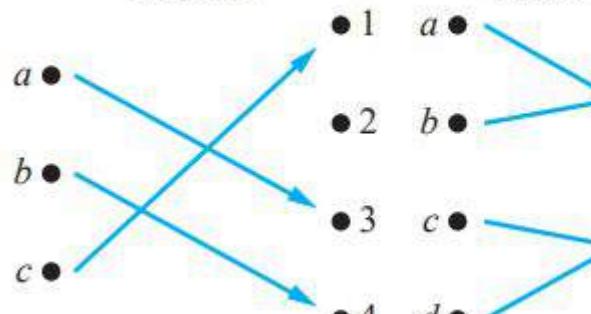
## EXAMPLE 14

- Is the function  $f(x) = x + 1$  from the set of integers to the set of integers onto?
- Solution: This function is onto, because for every integer  $y$  there is an integer  $x$  such that  $f(x) = y$ .
- To see this, note that  $f(x) = y$  if and only if  $x + 1 = y$ , which holds if and only if  $x = y - 1$ .

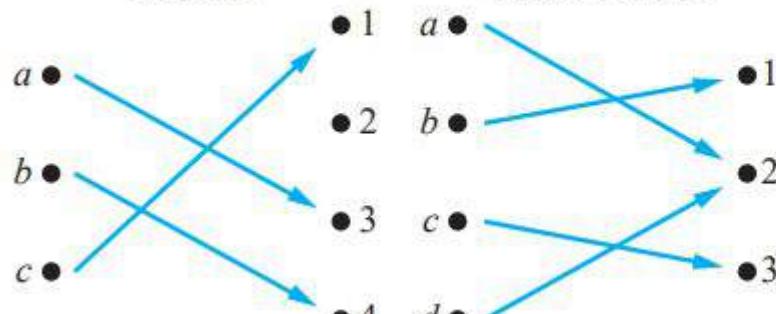
# DEFINITION 8

- The function  $f$  is a **one-to-one correspondence**, or a **bijection**, if it is both one-to-one and onto. We also say that such a function is **bijective**.

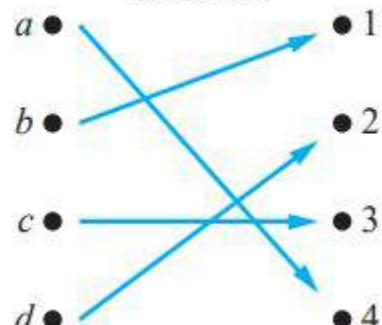
(a) One-to-one,  
not onto



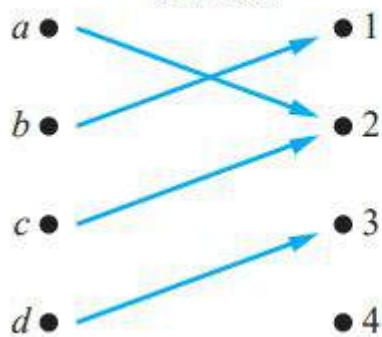
(b) Onto,  
not one-to-one



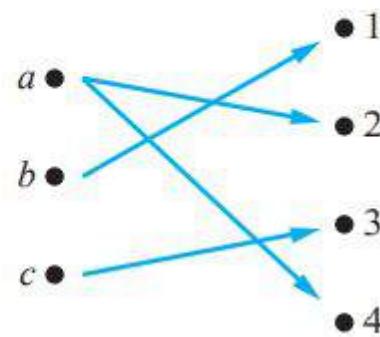
(c) One-to-one,  
and onto



(d) Neither one-to-one  
nor onto



(e) Not a function



# Identity function

- Let  $A$  be a set. The *identity function* on  $A$  is the function  $\iota_A : A \rightarrow A$ , where

$$\iota_A(x) = x$$

- The symbol  $\iota$  is called iota.
- In google forms we cannot type this so we use **identity(x) defined over A**

# Summary

Suppose that  $f : A \rightarrow B$ .

*To show that  $f$  is injective* Show that if  $f(x) = f(y)$  for arbitrary  $x, y \in A$  with  $x \neq y$ , then  $x = y$ .

*To show that  $f$  is not injective* Find particular elements  $x, y \in A$  such that  $x \neq y$  and  $f(x) = f(y)$ .

*To show that  $f$  is surjective* Consider an arbitrary element  $y \in B$  and find an element  $x \in A$  such that  $f(x) = y$ .

*To show that  $f$  is not surjective* Find a particular  $y \in B$  such that  $f(x) \neq y$  for all  $x \in A$ .

- Next...
  - Inverse Functions and
  - Compositions of Functions

# Inverse Functions and Compositions of Functions

# DEFINITION 9

- ***Inverse*** function

Let  $f$  be a one-to-one correspondence from the set  $A$  to the set  $B$ . The *inverse function* of  $f$  is the function that assigns to an element  $b$  belonging to  $B$  the unique element  $a$  in  $A$  such that  $f(a) = b$ . The inverse function of  $f$  is denoted by  $f^{-1}$ . Hence,  $f^{-1}(b) = a$  when  $f(a) = b$ .

# DEFINITION 9

- ***Inverse*** function

Let  $f$  be a one-to-one correspondence from the set  $A$  to the set  $B$ . The *inverse function* of  $f$  is the function that assigns to an element  $b$  belonging to  $B$  the unique element  $a$  in  $A$  such that  $f(a) = b$ . The inverse function of  $f$  is denoted by  $f^{-1}$ . Hence,  $f^{-1}(b) = a$  when  $f(a) = b$ .

**Remark:** Be sure not to confuse the function  $f^{-1}$  with the function  $1/f$ , which is the function that assigns to each  $x$  in the domain the value  $1/f(x)$ . Notice that the latter makes sense only when  $f(x)$  is a non-zero real number.

# DEFINITION 9

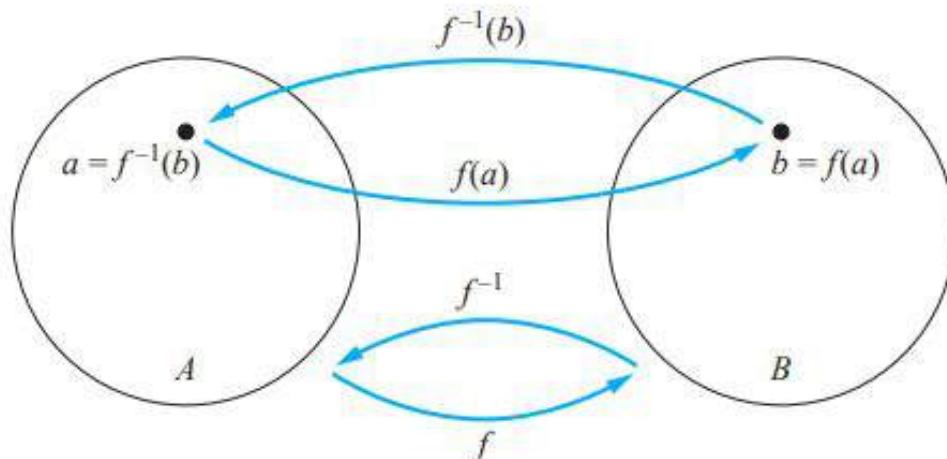
- ***Inverse*** function

Let  $f$  be a one-to-one correspondence from the set  $A$  to the set  $B$ . The *inverse function* of  $f$  is the function that assigns to an element  $b$  belonging to  $B$  the unique element  $a$  in  $A$  such that  $f(a) = b$ . The inverse function of  $f$  is denoted by  $f^{-1}$ . Hence,  $f^{-1}(b) = a$  when  $f(a) = b$ .

**Remark:** Be sure not to confuse the function  $f^{-1}$  with the function  $1/f$ , which is the function that assigns to each  $x$  in the domain the value  $1/f(x)$ . Notice that the latter makes sense only when  $f(x)$  is a non-zero real number.

If a function  $f$  is not a one-to-one correspondence,  
we cannot define an inverse function of  $f$ .

- A one-to-one correspondence is called invertible because we can define an inverse of this function. A function is not invertible if it is not a one-to-one correspondence, because the inverse of such a function does not exist.



**FIGURE 6** The Function  $f^{-1}$  Is the Inverse of Function  $f$ .

# EXAMPLE 19

- Let  $f : \mathbf{Z} \rightarrow \mathbf{Z}$  be such that  $f(x) = x + 1$ . Is  $f$  invertible, and if it is, what is its inverse?
-

# EXAMPLE 19

- Let  $f : \mathbf{Z} \rightarrow \mathbf{Z}$  be such that  $f(x) = x + 1$ . Is  $f$  invertible, and if it is, what is its inverse?
- Solution:* The function  $f$  has an inverse because it is a one-to-one correspondence, as follows from Examples 10 and 14. To reverse the correspondence, suppose that  $y$  is the image of  $x$ , so that  $y = x + 1$ . Then  $x = y - 1$ . This means that  $y - 1$  is the unique element of  $\mathbf{Z}$  that is sent to  $y$  by  $f$ . Consequently,  $f^{-1}(y) = y - 1$ . 

## EXAMPLE 20

- 

Let  $f$  be the function from  $\mathbf{R}$  to  $\mathbf{R}$  with  $f(x) = x^2$ . Is  $f$  invertible?

## EXAMPLE 20

- 

Let  $f$  be the function from  $\mathbf{R}$  to  $\mathbf{R}$  with  $f(x) = x^2$ . Is  $f$  invertible?

*Solution:* Because  $f(-2) = f(2) = 4$ ,  $f$  is not one-to-one. If an inverse function were defined, it would have to assign two elements to 4. Hence,  $f$  is not invertible. (Note we can also show that  $f$  is not invertible because it is not onto.) 

## EXAMPLE 20

- 

Let  $f$  be the function from  $\mathbf{R}$  to  $\mathbf{R}$  with  $f(x) = x^2$ . Is  $f$  invertible?

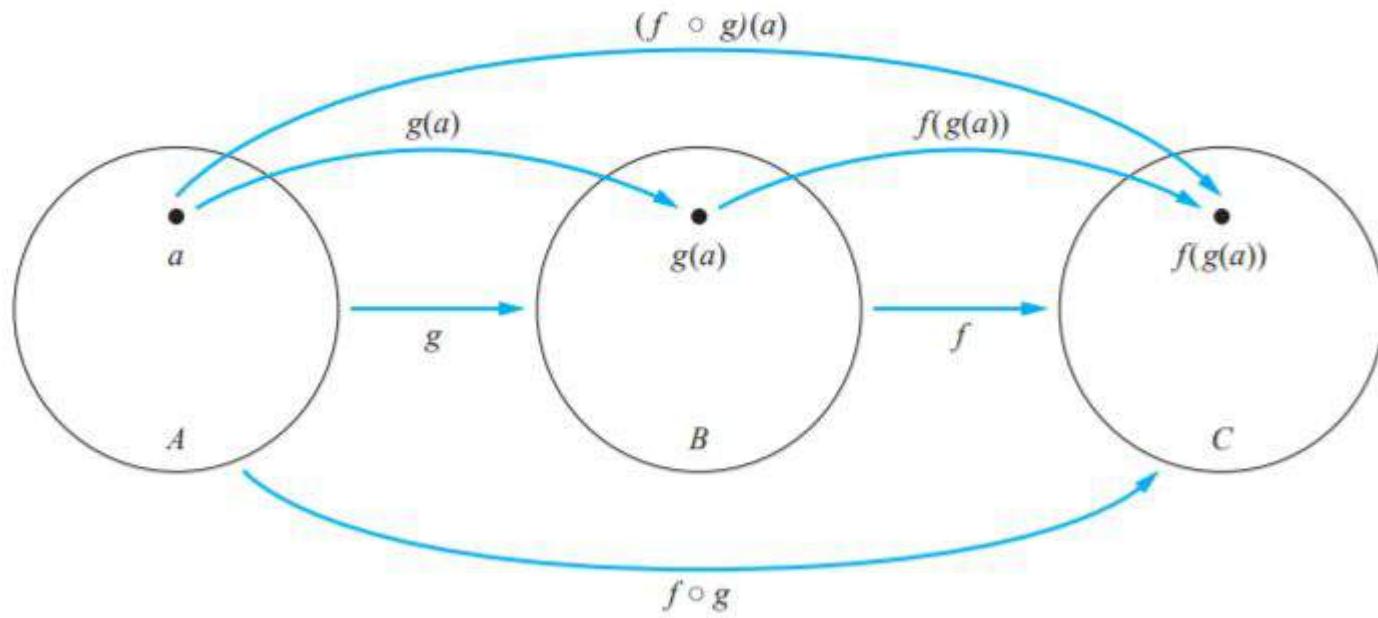
*Solution:* Because  $f(-2) = f(2) = 4$ ,  $f$  is not one-to-one. If an inverse function were defined, it would have to assign two elements to 4. Hence,  $f$  is not invertible. (Note we can also show that  $f$  is not invertible because it is not onto.) 

Show that if we restrict the function  $f(x) = x^2$  to a function from the set of all nonnegative real numbers to the set of all nonnegative real numbers, then  $f$  is invertible.

# Def. 10: Composition

Let  $g$  be a function from the set  $A$  to the set  $B$  and let  $f$  be a function from the set  $B$  to the set  $C$ . The *composition* of the functions  $f$  and  $g$ , denoted for all  $a \in A$  by  $f \circ g$ , is defined by

$$(f \circ g)(a) = f(g(a)).$$



**FIGURE 7** The Composition of the Functions  $f$  and  $g$ .

# EXAMPLE 23

Let  $f$  and  $g$  be the functions from the set of integers to the set of integers defined by  $f(x) = 2x + 3$  and  $g(x) = 3x + 2$ . What is the composition of  $f$  and  $g$ ? What is the composition of  $g$  and  $f$ ?

# EXAMPLE 23

Let  $f$  and  $g$  be the functions from the set of integers to the set of integers defined by  $f(x) = 2x + 3$  and  $g(x) = 3x + 2$ . What is the composition of  $f$  and  $g$ ? What is the composition of  $g$  and  $f$ ?

*Solution:* Both the compositions  $f \circ g$  and  $g \circ f$  are defined. Moreover,

$$(f \circ g)(x) = f(g(x)) = f(3x + 2) = 2(3x + 2) + 3 = 6x + 7$$

# EXAMPLE 23

Let  $f$  and  $g$  be the functions from the set of integers to the set of integers defined by  $f(x) = 2x + 3$  and  $g(x) = 3x + 2$ . What is the composition of  $f$  and  $g$ ? What is the composition of  $g$  and  $f$ ?

*Solution:* Both the compositions  $f \circ g$  and  $g \circ f$  are defined. Moreover,

$$(f \circ g)(x) = f(g(x)) = f(3x + 2) = 2(3x + 2) + 3 = 6x + 7$$

and

$$(g \circ f)(x) = g(f(x)) = g(2x + 3) = 3(2x + 3) + 2 = 6x + 11.$$



# composition is not commutative

**Remark:** Note that even though  $f \circ g$  and  $g \circ f$  are defined for the functions  $f$  and  $g$  in Example 23,  $f \circ g$  and  $g \circ f$  are not equal. In other words, the commutative law does not hold for the composition of functions.

When the composition of a function and its inverse is formed, in either order, an identity function is obtained.

Note, existence of inverse demands that the function must be a one-to-one correspondence.

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a,$$

and

$$(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b.$$

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a,$$

and

$$(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b.$$

Consequently  $f^{-1} \circ f = \iota_A$  and  $f \circ f^{-1} = \iota_B$ , where  $\iota_A$  and  $\iota_B$  are the identity functions on the sets  $A$  and  $B$ , respectively. That is,  $(f^{-1})^{-1} = f$ .

# Reading assignment

Read from page 148 to 151 about graph of a function and about ceiling and floor functions.

Also read about partial functions in page 151.

## **2.4**

## **Sequences and Summations**

---

# Sequences

## • DEFINITION 1

A *sequence* is a function from a subset of the set of integers (usually either the set  $\{0, 1, 2, \dots\}$  or the set  $\{1, 2, 3, \dots\}$ ) to a set  $S$ . We use the notation  $a_n$  to denote the image of the integer  $n$ . We call  $a_n$  a *term* of the sequence.

- We use the set  $\{1, 2, 3, \dots\}$

EXAMPLE 1

# EXAMPLE 1

---

Consider the sequence  $\{a_n\}$ , where

$$a_n = \frac{1}{n}.$$

The list of the terms of this sequence, beginning with  $a_1$ , namely,

$$a_1, a_2, a_3, a_4, \dots,$$

starts with

$$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots$$

# DEFINITION 2

A *geometric progression* is a sequence of the form

$$a, ar, ar^2, \dots, ar^n, \dots$$

where the *initial term*  $a$  and the *common ratio*  $r$  are real numbers.

**Remark:** A geometric progression is a discrete analogue of the exponential function

$$f(x) = ar^x.$$

## EXAMPLE 2

The sequences  $\{b_n\}$  with  $b_n = (-1)^n$ ,  $\{c_n\}$  with  $c_n = 2 \cdot 5^n$ , and  $\{d_n\}$  with  $d_n = 6 \cdot (1/3)^n$  are geometric progressions with initial term and common ratio equal to 1 and  $-1$ ; 2 and  $5$ ; and  $6$  and  $1/3$ , respectively, if we start at  $n = 0$ . The list of terms  $b_0, b_1, b_2, b_3, b_4, \dots$  begins with

$$1, -1, 1, -1, 1, \dots;$$

the list of terms  $c_0, c_1, c_2, c_3, c_4, \dots$  begins with

$$2, 10, 50, 250, 1250, \dots;$$

and the list of terms  $d_0, d_1, d_2, d_3, d_4, \dots$  begins with

$$6, 2, \frac{2}{3}, \frac{2}{9}, \frac{2}{27}, \dots$$



# DEFINITION 3

An *arithmetic progression* is a sequence of the form

$$a, a + d, a + 2d, \dots, a + nd, \dots$$

where the *initial term*  $a$  and the *common difference*  $d$  are real numbers.

**Remark:** An arithmetic progression is a discrete analogue of the linear function  $f(x) = dx + a$ .

# Read.

## Mistakes in Proofs

There are many common errors made in constructing mathematical proofs. We will briefly describe some of these here. Among the most common errors are mistakes in arithmetic and basic algebra. Even professional mathematicians make such errors, especially when working with complicated formulae. Whenever you use such computations you should check them as carefully as possible. (You should also review any troublesome aspects of basic algebra, especially before you study Section 5.1.)



Each step of a mathematical proof needs to be correct and the conclusion needs to follow logically from the steps that precede it. Many mistakes result from the introduction of steps that do not logically follow from those that precede it. This is illustrated in Examples 15–17.

**EXAMPLE 15** What is wrong with this famous supposed “proof” that  $1 = 2$ ?

**“Proof:**” We use these steps, where  $a$  and  $b$  are two equal positive integers.

Step	Reason
1. $a = b$	Given
2. $a^2 = ab$	Multiply both sides of (1) by $a$
3. $a^2 - b^2 = ab - b^2$	Subtract $b^2$ from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Factor both sides of (3)
5. $a + b = b$	Divide both sides of (4) by $a - b$
6. $2b = b$	Replace $a$ by $b$ in (5) because $a = b$ and simplify

summations

# Notation

- For a given sequence  $\{a_n\}$  to mean  $a_m + a_{m+1} + \dots + a_n$  we use the notation

$$\sum_{j=m}^n a_j, \quad \sum_{j=m}^n a_j, \quad \text{or} \quad \sum_{m \leq j \leq n} a_j$$

- (read as the sum from  $j = m$  to  $j = n$  of  $a_j$ ) **of summation**, and the choice of the letter  $j$  as the variable is arbitrary; that is, we could have used any other letter, such as  $i$  or  $k$ .

$$\sum_{j=m}^n a_j = \sum_{i=m}^n a_i = \sum_{k=m}^n a_k.$$

- $m$  is the lower limit, and  $n$  is the upper limit for the index of summation.

## EXAMPLE 18

- What is the value of  $\sum_{j=1}^5 j^2$ ?

# EXAMPLE 18

- What is the value of  $\sum_{j=1}^5 j^2$ ?

*Solution:* We have

$$\begin{aligned}\sum_{j=1}^5 j^2 &= 1^2 + 2^2 + 3^2 + 4^2 + 5^2 \\&= 1 + 4 + 9 + 16 + 25 \\&= 55.\end{aligned}$$

- Sometimes it is useful to shift the index of summation in a sum. This is often done when two sums need to be added but their indices of summation do not match.

- 

$$\sum_{j=1}^5 j^2 = \sum_{k=0}^4 (k+1)^2.$$

# THEOREM 1

If  $a$  and  $r$  are real numbers and  $r \neq 0$ , then

$$\sum_{j=0}^n ar^j = \begin{cases} \frac{ar^{n+1} - a}{r - 1} & \text{if } r \neq 1 \\ (n + 1)a & \text{if } r = 1. \end{cases}$$

# Proof:

Let

$$S_n = \sum_{j=0}^n ar^j.$$

We have,

$$rS_n = r \sum_{j=0}^n ar^j$$

substituting summation formula for  $S$

$$= \sum_{j=0}^n ar^{j+1}$$

by the distributive property

$$= \sum_{k=1}^{n+1} ar^k$$

shifting the index of summation, with  $k = j + 1$

$$= \left( \sum_{k=0}^n ar^k \right) + (ar^{n+1} - a)$$

removing  $k = n + 1$  term and adding  $k = 0$  term

$$= S_n + (ar^{n+1} - a)$$

substituting  $S$  for summation formula

From these equalities, we see that

$$rS_n = S_n + (ar^{n+1} - a).$$

Solving for  $S_n$  shows that if  $r \neq 1$ , then

$$S_n = \frac{ar^{n+1} - a}{r - 1}.$$

If  $r = 1$ , then the  $S_n = \sum_{j=0}^n ar^j = \sum_{j=0}^n a = (n + 1)a$ .

**TABLE 2** Some Useful Summation Formulae.

<i>Sum</i>	<i>Closed Form</i>
$\sum_{k=0}^n ar^k \ (r \neq 0)$	$\frac{ar^{n+1} - a}{r - 1}, r \neq 1$
$\sum_{k=1}^n k$	$\frac{n(n + 1)}{2}$
$\sum_{k=1}^n k^2$	$\frac{n(n + 1)(2n + 1)}{6}$
$\sum_{k=1}^n k^3$	$\frac{n^2(n + 1)^2}{4}$
$\sum_{k=0}^{\infty} x^k,  x  < 1$	$\frac{1}{1 - x}$
$\sum_{k=1}^{\infty} kx^{k-1},  x  < 1$	$\frac{1}{(1 - x)^2}$

# EXAMPLE 23

Find  $\sum_{k=50}^{100} k^2$ .

# EXAMPLE 23

Find  $\sum_{k=50}^{100} k^2$ .

*Solution:* First note that because  $\sum_{k=1}^{100} k^2 = \sum_{k=1}^{49} k^2 + \sum_{k=50}^{100} k^2$ , we have

$$\sum_{k=50}^{100} k^2 = \sum_{k=1}^{100} k^2 - \sum_{k=1}^{49} k^2.$$

Using the formula  $\sum_{k=1}^n k^2 = n(n+1)(2n+1)/6$  from Table 2 (and proved in Exercise 38), we see that

$$\sum_{k=50}^{100} k^2 = \frac{100 \cdot 101 \cdot 201}{6} - \frac{49 \cdot 50 \cdot 99}{6} = 338,350 - 40,425 = 297,925.$$



# SOME INFINITE SERIES

- **EXAMPLE 24:**

*(Requires calculus)* Let  $x$  be a real number with  $|x| < 1$ . Find  $\sum_{n=0}^{\infty} x^n$ .

# SOME INFINITE SERIES

- **EXAMPLE 24:**

(Requires calculus) Let  $x$  be a real number with  $|x| < 1$ . Find  $\sum_{n=0}^{\infty} x^n$ .

*Solution:* By Theorem 1 with  $a = 1$  and  $r = x$  we see that  $\sum_{n=0}^k x^n = \frac{x^{k+1} - 1}{x - 1}$ . Because  $|x| < 1$ ,  $x^{k+1}$  approaches 0 as  $k$  approaches infinity. It follows that

$$\sum_{n=0}^{\infty} x^n = \lim_{k \rightarrow \infty} \frac{x^{k+1} - 1}{x - 1} = \frac{0 - 1}{x - 1} = \frac{1}{1 - x}.$$



# EXAMPLE 25

(Requires calculus) Differentiating both sides of the equation

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1-x},$$

from Example 24 we find that

$$\sum_{k=1}^{\infty} kx^{k-1} = \frac{1}{(1-x)^2}.$$

(This differentiation is valid for  $|x| < 1$  by a theorem about infinite series.)

# 2.5 Cardinality of Sets

Page 170, ...

# DEFINITION 1

- The sets A and B have the same cardinality if and only if there is a one-to-one correspondence from A to B.
- When A and B have the same cardinality, we write  $|A|=|B|$ .

# DEFINITION 2

- If there is a one-to-one function from A to B, the cardinality of A is less than or the same as the cardinality of B and we write  $|A| \leq |B|$ .
- Moreover, when  $|A| \leq |B|$  and A and B have different cardinality, we say that the cardinality of A is less than the cardinality of B and we write  $|A| < |B|$ .

## DEFINITION 3: Countable Sets

- A set that is either finite or has the same cardinality as the set of positive integers is called countable.
- A set that is not countable is called uncountable.
-

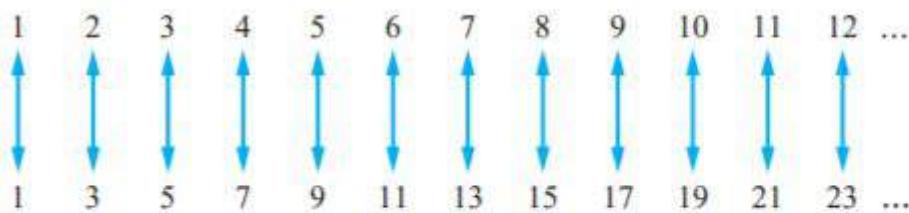
- When an infinite set  $S$  is countable, we denote the cardinality of  $S$  by  $\aleph_0$  (where  $\aleph$  is aleph, the first letter of the Hebrew alphabet).
- We write  $|S| = \aleph_0$  and say that  $S$  has cardinality “aleph null.”

# EXAMPLE 1

- Show that the set of odd positive integers is a countable set.

# EXAMPLE 1

- Show that the set of odd positive integers is a countable set.
- $f(n) = 2n - 1$  is a one-to-one correspondence between these odd positive integers and set of integers.



**FIGURE 1** A One-to-One Correspondence Between  $\mathbb{Z}^+$  and the Set of Odd Positive Integers.

## EXAMPLE 3

- Show that the set of all integers is countable.

## EXAMPLE 3

- Show that the set of all integers is countable.
- We can list all integers in a sequence by starting with 0 and alternating between positive and negative integers:

$0, 1, -1, 2, -2, \dots$

$0, 1, -1, 2, -2, \dots$

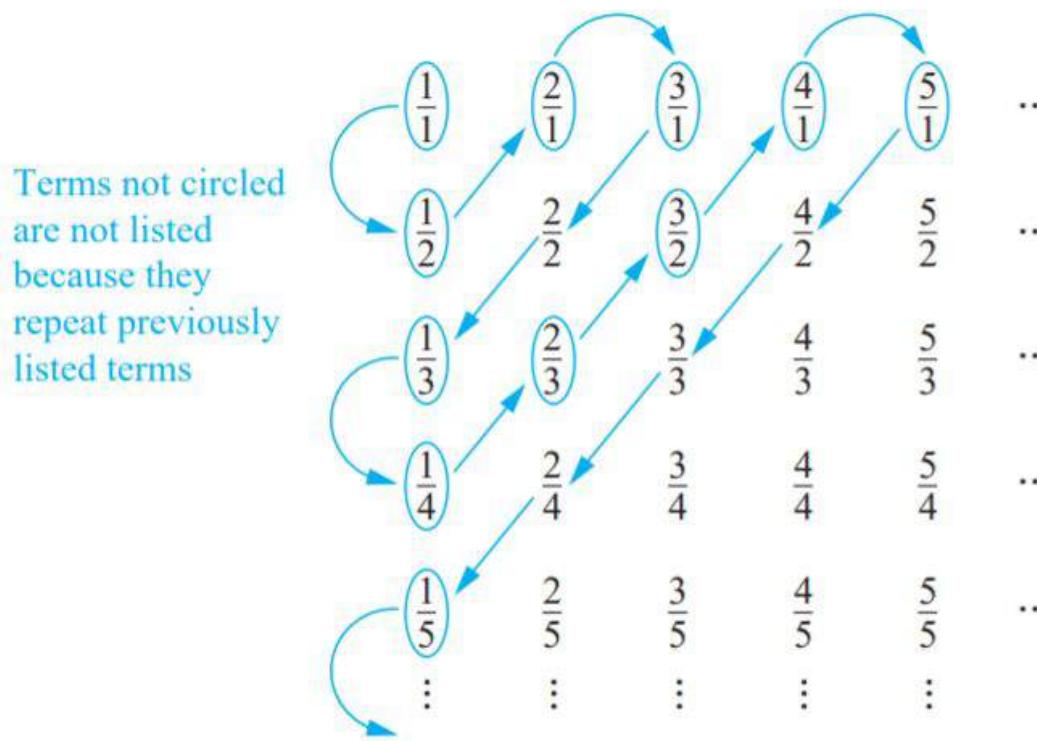
- $f(n) = n/2$  when  $n$  is even and  
 $f(n) = -(n - 1)/2$  when  $n$  is odd.
- Recall,  $n$  is from  $\{1, 2, 3, \dots\}$

## EXAMPLE 4

Show that the set of positive rational numbers is countable.

## EXAMPLE 4

Show that the set of positive rational numbers is countable.



**FIGURE 3** The Positive Rational Numbers Are Countable.

# Rationals are countable

- The key to listing the rational numbers in a sequence is to first list the positive rational numbers  $p/q$  with  $p + q = 2$ , followed by those with  $p + q = 3$ , followed by those with  $p + q = 4$ , and so on, following the path shown in Figure 3.

# Rationals are countable...

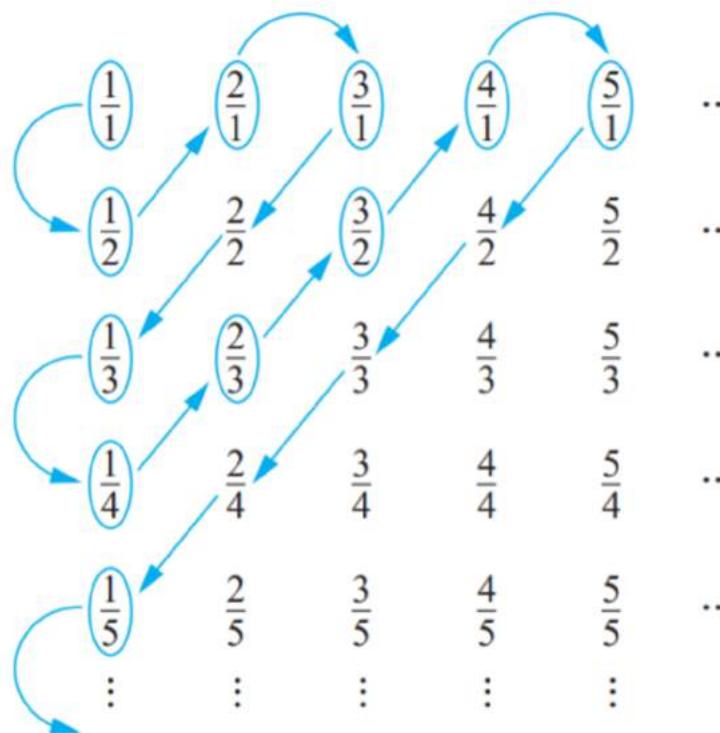
- Whenever we encounter a number  $p/q$  that is already listed, we do not list it again. For example, when we come to  $2/2 = 1$  we do not list it because we have already listed  $1/1 = 1$ .
- The initial terms in the list of positive rational numbers we have constructed are  $1, 1/2, 2, 3, 1/3, 1/4, 2/3, 3/2, 4, 5$ , and so on.

# Cardinality and Recursion

## EXAMPLE 4

Show that the set of positive rational numbers is countable.

Terms not circled  
are not listed  
because they  
repeat previously  
listed terms



**FIGURE 3** The Positive Rational Numbers Are Countable.

# Rationals is countable

- The key to listing the rational numbers in a sequence is to first list the positive rational numbers  $p/q$  with  $p + q = 2$ , followed by those with  $p + q = 3$ , followed by those with  $p + q = 4$ , and so on, following the path shown in Figure 3.

# Rationals is countable...

- Whenever we encounter a number  $p/q$  that is already listed, we do not list it again. For example, when we come to  $2/2 = 1$  we do not list it because we have already listed  $1/1 = 1$ .
- The initial terms in the list of positive rational numbers we have constructed are  $1, 1/2, 2, 3, 1/3, 1/4, 2/3, 3/2, 4, 5$ , and so on.

# An uncountable set

- EXAMPLE 5: Show that the set of real numbers is an uncountable set.

# An uncountable set

- EXAMPLE 5: Show that the set of real numbers is an uncountable set.
- we use an important proof method, introduced in 1879 by **Georg Cantor** and known as the **Cantor diagonalization** argument, to prove that the set of real numbers is not countable. This proof method is used extensively in mathematical logic and in the theory of computation.

- Let us assume that we can enumerate the real numbers between 0 and 1

- Let us assume that we can enumerate the real numbers between 0 and 1

$$r_1 = 0.d_{11}d_{12}d_{13}d_{14} \dots$$

$$r_2 = 0.d_{21}d_{22}d_{23}d_{24} \dots$$

$$r_3 = 0.d_{31}d_{32}d_{33}d_{34} \dots$$

$$r_4 = 0.d_{41}d_{42}d_{43}d_{44} \dots$$

⋮

where  $d_{ij} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ . (For example, if  $r_1 = 0.23794102 \dots$ , we have  $d_{11} = 2$ ,  $d_{12} = 3$ ,  $d_{13} = 7$ , and so on.)

- Let us assume that we can enumerate the real numbers between 0 and 1

$$r_1 = 0.d_{11}d_{12}d_{13}d_{14} \dots$$

$$r_2 = 0.d_{21}d_{22}d_{23}d_{24} \dots$$

$$r_3 = 0.d_{31}d_{32}d_{33}d_{34} \dots$$

$$r_4 = 0.d_{41}d_{42}d_{43}d_{44} \dots$$

⋮

where  $d_{ij} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ . (For example, if  $r_1 = 0.23794102 \dots$ , we have  $d_{11} = 2$ ,  $d_{12} = 3$ ,  $d_{13} = 7$ , and so on.)

Then, form a new real number with decimal expansion

$r = 0.d_1d_2d_3d_4 \dots$ , where the decimal digits are determined by the following rule:

$$d_i = \begin{cases} 4 & \text{if } d_{ii} \neq 4 \\ 5 & \text{if } d_{ii} = 4. \end{cases}$$

$r$  is not in the list

- Why?

# THEOREM 1

- If  $A$  and  $B$  are countable sets, then  $A \cup B$  is also countable.

# THEOREM 1

- If A and B are countable sets, then  $A \cup B$  is also countable.
- Proof[by exhaustion].
  - There are 3 cases.

# Case 1

- A and B are finite.
- Can you complete the proof for this case?

## Case 2

- One of A and B is finite and the other is countably infinite.
- Without loss of generality (WLOG) we can assume that B is finite with m elements, and A is countably infinite.

## Case 2

- One of A and B is finite and the other is countably infinite.
- Without loss of generality (WLOG) we can assume that B is finite with m elements, and A is countably infinite.
- Can you complete this case?

## Case 3

- Both A and B are countably infinite.

## Case 3

- Both  $A$  and  $B$  are countably infinite.

*Case (iii):* Because both  $A$  and  $B$  are countably infinite, we can list their elements as  $a_1, a_2, a_3, \dots, a_n, \dots$  and  $b_1, b_2, b_3, \dots, b_n, \dots$ , respectively. By alternating terms of these two sequences we can list the elements of  $A \cup B$  in the infinite sequence  $a_1, b_1, a_2, b_2, a_3, b_3, \dots, a_n, b_n, \dots$ . This means  $A \cup B$  must be countably infinite.

EQD.

# THEOREM 2

**SCHRÖDER-BERNSTEIN THEOREM** If  $A$  and  $B$  are sets with  $|A| \leq |B|$  and  $|B| \leq |A|$ , then  $|A| = |B|$ . In other words, if there are one-to-one functions  $f$  from  $A$  to  $B$  and  $g$  from  $B$  to  $A$ , then there is a one-to-one correspondence between  $A$  and  $B$ .

- The proof is complex. Ref the book Pages 174-5

## EXAMPLE 6

- Show that the  $|(0, 1)| = |(0, 1]|$ .
- Without Schröder-Bernstein theorem, it might have been a difficult task.
- But with the theorem's help, it is quite easy.

We find one-to-one function between the sets in both ways.

Finding a one-to-one function from  $(0, 1)$  to  $(0, 1]$  is simple. Because  $(0, 1) \subset (0, 1]$ ,  $f(x) = x$  is a one-to-one function from  $(0, 1)$  to  $(0, 1]$ .

We find one-to-one function between the sets in both ways.

Finding a one-to-one function from  $(0, 1)$  to  $(0, 1]$  is simple. Because  $(0, 1) \subset (0, 1]$ ,  $f(x) = x$  is a one-to-one function from  $(0, 1)$  to  $(0, 1]$ .

Finding a one-to-one function from  $(0, 1]$  to  $(0, 1)$  is also not difficult. The function  $g(x) = x/2$  is clearly one-to-one and maps  $(0, 1]$  to  $(0, 1/2] \subset (0, 1)$ . As we have found one-to-one functions from  $(0, 1)$  to  $(0, 1]$  and from  $(0, 1]$  to  $(0, 1)$ , the Schröder-Bernstein theorem tells us that  $|(0, 1)| = |(0, 1]|$ . 

- Read the book pages 175-6 for computable functions and continuum hypothesis

# DEFINITION 4: Recurrence Relation

A *recurrence relation* for the sequence  $\{a_n\}$  is an equation that expresses  $a_n$  in terms of one or more of the previous terms of the sequence, namely,  $a_0, a_1, \dots, a_{n-1}$ , for all integers  $n$  with  $n \geq n_0$ , where  $n_0$  is a nonnegative integer.

# DEFINITION 4: Recurrence Relation

A *recurrence relation* for the sequence  $\{a_n\}$  is an equation that expresses  $a_n$  in terms of one or more of the previous terms of the sequence, namely,  $a_0, a_1, \dots, a_{n-1}$ , for all integers  $n$  with  $n \geq n_0$ , where  $n_0$  is a nonnegative integer.

A sequence is called a *solution* of a recurrence relation if its terms satisfy the recurrence relation. (A recurrence relation is said to *recursively define* a sequence. We will explain this alternative terminology in Chapter 5.)

## EXAMPLE 5

Let  $\{a_n\}$  be a sequence that satisfies the recurrence relation  $a_n = a_{n-1} + 3$  for  $n = 1, 2, 3, \dots$ , and suppose that  $a_0 = 2$ . What are  $a_1$ ,  $a_2$ , and  $a_3$ ?

## EXAMPLE 5

Let  $\{a_n\}$  be a sequence that satisfies the recurrence relation  $a_n = a_{n-1} + 3$  for  $n = 1, 2, 3, \dots$ , and suppose that  $a_0 = 2$ . What are  $a_1$ ,  $a_2$ , and  $a_3$ ?

*Solution:* We see from the recurrence relation that  $a_1 = a_0 + 3 = 2 + 3 = 5$ . It then follows that  $a_2 = 5 + 3 = 8$  and  $a_3 = 8 + 3 = 11$ .

## EXAMPLE 5

Let  $\{a_n\}$  be a sequence that satisfies the recurrence relation  $a_n = a_{n-1} + 3$  for  $n = 1, 2, 3, \dots$ , and suppose that  $a_0 = 2$ . What are  $a_1$ ,  $a_2$ , and  $a_3$ ?

*Solution:* We see from the recurrence relation that  $a_1 = a_0 + 3 = 2 + 3 = 5$ . It then follows that  $a_2 = 5 + 3 = 8$  and  $a_3 = 8 + 3 = 11$ . 

- Sequence: 2, 5, 8, 11, ...
- This is what type of sequence?

# The Initial Condition

- The initial conditions for a recursively defined sequence specify first one or few terms of the sequence.
- The recurrence relation takes-over after the initial conditions, to give other terms of the sequence.

# the Fibonacci sequence

The *Fibonacci sequence*,  $f_0, f_1, f_2, \dots$ , is defined by the initial conditions  $f_0 = 0, f_1 = 1$ , and the recurrence relation

$$f_n = f_{n-1} + f_{n-2}$$

for  $n = 2, 3, 4, \dots$

# The Fibonacci sequence

The *Fibonacci sequence*,  $f_0, f_1, f_2, \dots$ , is defined by the initial conditions  $f_0 = 0, f_1 = 1$ , and the recurrence relation

$$f_n = f_{n-1} + f_{n-2}$$

for  $n = 2, 3, 4, \dots$

- Sequence: 0, 1, 1, 2, 3, 5, 8, ...

## EXAMPLE 8: Factorials

- Notation:  $a_n = n!$
- Initial condition:  $a_1 = 1.$
- Recurrence relation:  $n! = n(n - 1)!$
- That is,  $a_n = na_{n-1}$

# Closed Formula

- Explicit formula for  $a_n$  which is a function of  $n$ .

## Example 9

- The sequence  $\{a_n\}$  is given by  $a_n = 2a_{n-1} - a_{n-2}$
- Initial condition:  $a_1 = 3$  and  $a_2 = 6$
- Can you find the closed form for  $a_n$  ?

## Example 9

- The sequence  $\{a_n\}$  is given by  $a_n = 2a_{n-1} - a_{n-2}$
- Initial condition:  $a_1 = 3$  and  $a_2 = 6$
- Can you find the closed form for  $a_n$  ?
- To have some understanding find few initial terms.... May be we get a pattern ...

## Example 9

- The sequence  $\{a_n\}$  is given by  $a_n = 2a_{n-1} - a_{n-2}$
- Initial condition:  $a_1 = 3$  and  $a_2 = 6$
- Can you find the closed form for  $a_n$  ?
- To have some understanding find few initial terms.... May be we get a pattern ...
- 3, 6, 9, 12, ...

## Example 9

- The sequence  $\{a_n\}$  is given by  $a_n = 2a_{n-1} - a_{n-2}$
- Initial condition:  $a_1 = 3$  and  $a_2 = 6$
- Can you find the closed form for  $a_n$  ?
- To have some understanding find few initial terms.... May be we get a pattern ...
- $3, 6, 9, 12, \dots$
- So,  $a_n = 3n$

# Continued...

- The sequence  $\{a_n\}$  is given by  $a_n = 2a_{n-1} - a_{n-2}$
- Instead of initial condition:  $a_1 = 3$  and  $a_2 = 6$ , we give the following initial condition
- $a_1 = 5, a_2 = 5$ .

# Continued...

- The sequence  $\{a_n\}$  is given by 
$$a_n = 2a_{n-1} - a_{n-2}$$
- Instead of initial condition:  $a_1 = 3$  and  $a_2 = 6$ , we give the following initial condition
- $a_1 = 5, a_2 = 5$ .
- Can you find the closed form?

# Continued...

- The sequence  $\{a_n\}$  is given by  $a_n = 2a_{n-1} - a_{n-2}$
- Instead of initial condition:  $a_1 = 3$  and  $a_2 = 6$ , we give the following initial condition
- $a_1 = 5, a_2 = 5.$
- Can you find the closed form?
- The sequence: 5, 5, 5, 5, ...
- So,  $a_n = 5.$

Let  $\{a_n\}$  be a sequence that satisfies the recurrence relation  $a_n = a_{n-1} + 3$  for  $n = 1, 2, 3, \dots$ , and suppose that  $a_0 = 2$ . What are  $a_1$ ,  $a_2$ , and  $a_3$ ?

- Can you find the closed form?

Let  $\{a_n\}$  be a sequence that satisfies the recurrence relation  $a_n = a_{n-1} + 3$  for  $n = 1, 2, 3, \dots$ , and suppose that  $a_0 = 2$ . What are  $a_1$ ,  $a_2$ , and  $a_3$ ?

- Can you find the closed form?

$$a_1 = 2 + 3$$

$$a_2 = (2 + 3) + 3 = 2 + 2 \cdot 3$$

$$a_3 = 2 + 3 \cdot 3$$

⋮

$$a_n = 2 + 3 \cdot n$$

- This method is called **forward substitution**.

- This method is called **forward substitution**.
- In similar lines, starting with  $a_n$  and going back to the initial conditions ... is called **backward substitution**.
- Read pages 159 and 160.

# **Structural Induction**

- To prove results about recursively defined sets, we generally use some form of mathematical induction.
- Example 10 illustrates the connection between recursively defined sets and mathematical induction.

## EXAMPLE 10

- Show that the set  $S$  defined in Example 5 by specifying that  $3 \in S$  and that if  $x \in S$  and  $y \in S$ , then  $x + y \in S$ , is the set of all positive integers that are multiples of 3.

# EXAMPLE 10

- Show that the set  $S$  defined in Example 5 by specifying that  $3 \in S$  and that if  $x \in S$  and  $y \in S$ , then  $x + y \in S$ , is the set of all positive integers that are multiples of 3.
- Proof: Let  $A$  be the set of positive integers divisible by 3.

Part 1: Show that  $A \subseteq S$

Part 2: Show that  $S \subseteq A$

TST  $A \subseteq S$

$A$  is positive integers divisible by 3.

$$3 \in S \wedge (x \in S \wedge y \in S \rightarrow x + y \in S)$$

- We need to show  $a \in A \rightarrow a \in S$
- Let  $P(k) : 3k$  for some positive  $k$  is in the set  $S$ .
- Basis:  $P(1)$  is true. Since  $3 \cdot 1 = 3 \in S$
- IH:  $P(k) \rightarrow P(k + 1)$
- $P(k) \rightarrow 3k$  is in  $S$ .  
 $\rightarrow 3(k + 1) = 3k + 3$  is divisible by 3  
 $\rightarrow 3k + 3 \in S$ , since  $3k \in S$  and  $3 \in S$   
 $\rightarrow P(k + 1)$ .

$$\text{TST } S \subseteq A$$

- Left as exercise. You can see the text book.
- This is using mathematical induction.
- You can see the difficulty.

# But Structural induction may be easy.

- **BASIS STEP:** Show that the result holds for all elements specified in the basis step of the recursive definition to be in the set.
- **RECURSIVE STEP:** Show that if the statement is true for each of the elements used to construct new elements in the recursive step of the definition, the result holds for these new elements.

- Every element is built up recursively... So to show  $P(s)$  for all  $s \in S$ ...  
Show  $P(b)$  for all base case elements  $b$ .
- Show if  $P()$  holds for every named element in the recursive rule, then  $P()$  holds for the new element (repeat for each rule).

Let  $S$  be:

Basis:  $6 \in S, 15 \in S$

Recursive: if  $x, y \in S$  then  $x + y \in S$ .

Show that every element of  $S$  is divisible by 3.

Let  $P(x)$  be  $x$  is divisible by 3

We show  $P(x)$  holds for all  $x \in S$  by structural induction.

Base Cases:

$6 = 2 \cdot 3$  so  $3|6$ , and  $P(6)$  holds.  $15 = 5 \cdot 3$ , so  $3|15$  and

$P(15)$  holds.

Inductive Hypothesis: Suppose  $P(x)$  and  $P(y)$  for arbitrary  $x, y$ . Inductive Step: By IH  $3|x$  and  $3|y$ . So  $x = 3n$  and  $y = 3m$  for integers  $m, n$ .

Adding the equations,  $x + y = 3(n + m)$ . Since  $n, m$  are integers, we have  $3|(x + y)$  by definition of divides. This gives  $P(x + y)$ . We conclude  $P(x) \forall x \in S$  by the principle of structural induction.

# **Strings**

# DEFINITION 1

The set  $\Sigma^*$  of *strings* over the alphabet  $\Sigma$  is defined recursively by

*BASIS STEP:*  $\lambda \in \Sigma^*$  (where  $\lambda$  is the empty string containing no symbols).

*RECURSIVE STEP:* If  $w \in \Sigma^*$  and  $x \in \Sigma$ , then  $wx \in \Sigma^*$ .

# EXAMPLE 7

**Length of a String** Give a recursive definition of  $l(w)$ , the length of the string  $w$ .

*Solution:* The length of a string can be recursively defined by

$$l(\lambda) = 0;$$

$$l(wx) = l(w) + 1 \text{ if } w \in \Sigma^* \text{ and } x \in \Sigma.$$

# Properties over strings, how to establish them?

- Suppose that  $P(w)$  is a propositional function over the set of strings  $w \in \Sigma^*$ .
- To use structural induction to prove that  $P(w)$  holds for all strings  $w \in \Sigma^*$ ,
- we need to complete both a basis step and a recursive step. These steps are:
- **BASIS STEP:** Show that  $P(\lambda)$  is true.
- **RECURSIVE STEP:** Assume that  $P(w)$  is true, where  $w \in \Sigma^*$ . Show that if  $x \in \Sigma$ , then  $P(wx)$  must also be true.

# EXAMPLE 12

- Use structural induction to prove that  $l(xy) = l(x) + l(y)$ , where  $x$  and  $y$  belong to  $\Sigma^*$ , the set of strings over the alphabet  $\Sigma$ .

# EXAMPLE 12

Use structural induction to prove that  $l(xy) = l(x) + l(y)$ , where  $x$  and  $y$  belong to  $\Sigma^*$ , the set of strings over the alphabet  $\Sigma$ .

**EXAMPLE 12** Use structural induction to prove that  $l(xy) = l(x) + l(y)$ , where  $x$  and  $y$  belong to  $\Sigma^*$ , the set of strings over the alphabet  $\Sigma$ .

**Solution:** We will base our proof on the recursive definition of the set  $\Sigma^*$  given in Definition 1 and the definition of the length of a string in Example 7, which specifies that  $l(\lambda) = 0$  and  $l(wx) = l(w) + 1$  when  $w \in \Sigma^*$  and  $x \in \Sigma$ . Let  $P(y)$  be the statement that  $l(xy) = l(x) + l(y)$  whenever  $x$  belongs to  $\Sigma^*$ .

**BASIS STEP:** To complete the basis step, we must show that  $P(\lambda)$  is true. That is, we must show that  $l(x\lambda) = l(x) + l(\lambda)$  for all  $x \in \Sigma^*$ . Because  $l(x\lambda) = l(x) = l(x) + 0 = l(x) + l(\lambda)$  for every string  $x$ , it follows that  $P(\lambda)$  is true.

**RECURSIVE STEP:** To complete the inductive step, we assume that  $P(y)$  is true and show that this implies that  $P(ya)$  is true whenever  $a \in \Sigma$ . What we need to show is that  $l(xya) = l(x) + l(ya)$  for every  $a \in \Sigma$ . To show this, note that by the recursive definition of  $l(w)$  (given in Example 7), we have  $l(xya) = l(xy) + 1$  and  $l(ya) = l(y) + 1$ . And, by the inductive hypothesis,  $l(xy) = l(x) + l(y)$ . We conclude that  $l(xya) = l(x) + l(y) + 1 = l(x) + l(ya)$ . 

**For want of time, let us close Unit2  
here.**

# **DSMA-Unit 3**

All the slides are prepared by quoting and taking as it is from the book: Kenneth H. Rosen, Discrete Mathematics and applications, TataMcGraw Hill, 7<sup>th</sup> Edition, 2012, ISBN: 978-0-07-338309-5

# **Syllabus (7 Hours)**

Counting techniques - Sum and Product Rule, Inclusion and Exclusion Principles, Pigeonhole Principle, Generalized Pigeonhole Principle, Permutation, Combination, Recurrence Relation, Solving Homogeneous and Non Homogeneous Recurrence Relations, Binomial Coefficients and Identities;

# Counting

Combinatorics, the study of arrangements of objects, is an important part of discrete mathematics. This subject was studied as long ago as the seventeenth century, when combinatorial questions arose in the study of gambling games. Enumeration, the counting of objects with certain properties, is an important part of combinatorics.

Applications: Probability Theory, Mathematical Biology, Algorithms

### **Basic Counting Principles: THE PRODUCT RULE**

The product rule applies when a procedure is made up of separate tasks.

Suppose that a procedure can be broken down into a sequence of two tasks. If there are  $n_1$  ways to do the first task and for each of these ways of doing the first task, there are  $n_2$  ways to do the second task, then there are  $n_1n_2$  ways to do the procedure.

## Example 1

A new company with just two employees, Sanchez and Patel, rents a floor of a building with 12 offices. How many ways are there to assign different offices to these two employees?

# Example 1

**A new company with just two employees, Sanchez and Patel, rents a floor of a building with 12 offices. How many ways are there to assign different offices to these two employees?**

Solution: The procedure of assigning offices to these two employees consists of assigning an office to Sanchez, which can be done in 12 ways, then assigning an office to Patel different from the office assigned to Sanchez, which can be done in 11 ways. By the product rule, there are  $12 \cdot 11 = 132$  ways to assign offices to these two employees.

## Example 2

The chairs of an auditorium are to be labeled with an uppercase English letter followed by a positive integer not exceeding 100. What is the largest number of chairs that can be labeled differently?

## Example 2

**The chairs of an auditorium are to be labeled with an uppercase English letter followed by a positive integer not exceeding 100. What is the largest number of chairs that can be labeled differently?**

**Solution:** The procedure of labeling a chair consists of two tasks, namely, assigning to the seat one of the 26 uppercase English letters, and then assigning to it one of the 100 possible integers. The product rule shows that there are  $26 \cdot 100 = 2600$  different ways that a chair can be labeled. Therefore, the largest number of chairs that can be labeled differently is 2600.

# Extended Product Rule

An extended version of the product rule is often useful. Suppose that a procedure is carried out by performing the tasks  $T_1, T_2, \dots, T_m$  in sequence. If each task  $T_i, i = 1, 2, \dots, n$ , can be done in  $n_i$  ways, regardless of how the previous tasks were done, then there are  $n_1 \cdot n_2 \cdot \dots \cdot n_m$  ways to carry out the procedure. This version of the product rule can be proved by mathematical induction from the product rule for two tasks (see Exercise 72).

## Example 3

**How many different license plates can be made if each plate contains a sequence of three uppercase English letters followed by three digits (and no sequences of letters are prohibited, even if they are obscene)?**

## Example 3

**How many different license plates can be made if each plate contains a sequence of three uppercase English letters followed by three digits (and no sequences of letters are prohibited, even if they are obscene)?**

**Solution:** There are 26 choices for each of the three uppercase English letters and ten choices for each of the three digits. Hence, by the product rule there are a total of  $26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 = 17,576,000$  possible license plates.

# Questions

**How many functions are there from a set with m elements to a set with n elements?**

# Questions

**Use the product rule to show that the number of different subsets of a finite set  $S$  is  $2^{|S|}$ .**

## Sum Rule

**THE SUM RULE:** If a task can be done either in one of  $n_1$  ways or in one of  $n_2$  ways, where none of the set of  $n_1$  ways is the same as any of the set of  $n_2$  ways, then there are  $n_1 + n_2$  ways to do the task.

## **Example 4**

Suppose that either a member of the mathematics faculty or a student who is a mathematics major is chosen as a representative to a university committee. How many different choices are there for this representative if there are 37 members of the mathematics faculty and 83 mathematics majors and no one is both a faculty member and a student?

## Example 4

Suppose that either a member of the mathematics faculty or a student who is a mathematics major is chosen as a representative to a university committee. How many different choices are there for this representative if there are 37 members of the mathematics faculty and 83 mathematics majors and no one is both a faculty member and a student?

**Solution:** There are 37 ways to choose a member of the mathematics faculty and there are 83 ways to choose a student who is a mathematics major. Choosing a member of the mathematics faculty is never the same as choosing a student who is a mathematics major because no one is both a faculty member and a student. By the sum rule it follows that there are  $37 + 83 = 120$  possible ways to pick this representative.

We can extend the sum rule to more than two tasks. Suppose that a task can be done in one of  $n_1$  ways, in one of  $n_2$  ways,  $\dots$ , or in one of  $n_m$  ways, where none of the set of  $n_i$  ways of doing the task is the same as any of the set of  $n_j$  ways, for all pairs  $i$  and  $j$  with  $1 \leq i < j \leq m$ . Then the number of ways to do the task is  $n_1 + n_2 + \dots + n_m$ . This extended version of the sum rule is often useful in counting problems, as Examples 13 and 14 show. This version of the sum rule can be proved using mathematical induction from the sum rule for two sets. (This is Exercise 71.)

## Example 5

A student can choose a computer project from one of three lists. The three lists contain 23, 15, and 19 possible projects, respectively. No project is on more than one list. How many possible projects are there to choose from?

## Example 5

A student can choose a computer project from one of three lists. The three lists contain 23, 15, and 19 possible projects, respectively. No project is on more than one list. How many possible projects are there to choose from?

**Solution:** The student can choose a project by selecting a project from the first list, the second list, or the third list. Because no project is on more than one list, by the sum rule there are  $23 + 15 + 19 = 57$  ways to choose a project.

The sum rule can be phrased in terms of sets as: If  $A_1, A_2, \dots, A_m$  are pairwise disjoint finite sets, then the number of elements in the union of these sets is the sum of the numbers of elements in the sets. To relate this to our statement of the sum rule, note there are  $|A_i|$  ways to choose an element from  $A_i$  for  $i = 1, 2, \dots, m$ . Because the sets are pairwise disjoint, when we select an element from one of the sets  $A_i$ , we do not also select an element from a different set  $A_j$ . Consequently, by the sum rule, because we cannot select an element from two of these sets at the same time, the number of ways to choose an element from one of the sets, which is the number of elements in the union, is

$$|A_1 \cup A_2 \cup \dots \cup A_m| = |A_1| + |A_2| + \dots + |A_m| \text{ when } A_i \cap A_j = \emptyset \text{ for all } i, j.$$

# Counting

# Combination of Sum and Product Rule

## EXAMPLE 16

Each user on a computer system has a password, which is six to eight characters long, where each character is an uppercase letter or a digit. Each password must contain at least one digit. How many possible passwords are there?

*Solution:* Let  $P$  be the total number of possible passwords, and let  $P_6$ ,  $P_7$ , and  $P_8$  denote the number of possible passwords of length 6, 7, and 8, respectively. By the sum rule,  $P = P_6 + P_7 + P_8$ . We will now find  $P_6$ ,  $P_7$ , and  $P_8$ . Finding  $P_6$  directly is difficult. To find  $P_6$  it is easier to find the number of strings of uppercase letters and digits that are six characters long, including those with no digits, and subtract from this the number of strings with no digits. By the product rule, the number of strings of six characters is  $36^6$ , and the number of strings with no digits is  $26^6$ . Hence,

$$P_6 = 36^6 - 26^6 = 2,176,782,336 - 308,915,776 = 1,867,866,560.$$

Similarly, we have

$$P_7 = 36^7 - 26^7 = 78,364,164,096 - 8,031,810,176 = 70,332,353,920$$

and

$$\begin{aligned}P_8 &= 36^8 - 26^8 = 2,821,109,907,456 - 208,827,064,576 \\&= 2,612,282,842,880.\end{aligned}$$

Consequently,

$$P = P_6 + P_7 + P_8 = 2,684,483,063,360.$$

# THE SUBTRACTION RULE

**If a task can be done in either  $n_1$  ways or  $n_2$  ways, then the number of ways to do the task is  $n_1 + n_2$  minus the number of ways to do the task that are common to the two different ways.**

The subtraction rule is also known as the principle of inclusion–exclusion, especially when it is used to count the number of elements in the union of two sets. Suppose that  $A_1$  and  $A_2$  are sets. Then, there are  $|A_1|$  ways to select an element from  $A_1$  and  $|A_2|$  ways to select an element from  $A_2$ . The number of ways to select an element from  $A_1$  or from  $A_2$ , that is, the number of ways to select an element from their union, is the sum of the number of ways to select an element from  $A_1$  and the number of ways to select an element from  $A_2$ , minus the number of ways to select an element that is in both  $A_1$  and  $A_2$ . Because there are  $|A_1 \cup A_2|$  ways to select an element in either  $A_1$  or in  $A_2$ , and  $|A_1 \cap A_2|$  ways to select an element common to both sets, we have  $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$ .

## Question 1

A computer company receives 350 applications from computer graduates for a job planning a line of new Web servers. Suppose that 220 of these applicants majored in computer science, 147 majored in business, and 51 majored both in computer science and in business. How many of these applicants majored neither in computer science nor in business?

## Question 2

How many positive integers between 50 and 100

- a) are divisible by 7?
- b) are divisible by 11?
- c) are divisible by both 7 and 11?

# The Pigeonhole Principle

Suppose that a flock of 20 pigeons flies into a set of 19 pigeonholes to roost. Because there are 20 pigeons but only 19 pigeonholes, at least one of these 19 pigeonholes must have at least two pigeons in it. To see why this is true, note that if each pigeonhole had at most one pigeon in it, at most 19 pigeons, one per hole, could be accommodated. This illustrates a general principle called the pigeonhole principle, which states that if there are more pigeons than pigeonholes, then there must be at least one pigeonhole with at least two pigeons in it.

# The Pigeonhole Principle

**If  $k$  is a positive integer and  $k + 1$  or more objects are placed into  $k$  boxes, then there is at least one box containing two or more of the objects.**

**Proof:** We prove the pigeonhole principle using a proof by contraposition. Suppose that none of the  $k$  boxes contains more than one object. Then the total number of objects would be at most  $k$ . This is a contradiction, because there are at least  $k + 1$  objects.

The pigeonhole principle is also called the Dirichlet drawer principle, after the nineteenth-century German mathematician G. Lejeune Dirichlet, who often used this principle in his work.

## Corollary 1

**A function  $f$  from a set with  $k + 1$  or more elements to a set with  $k$  elements is not one-to-one.**

## Corollary 1

**A function  $f$  from a set with  $k + 1$  or more elements to a set with  $k$  elements is not one-to-one.**

**Proof:** Suppose that for each element  $y$  in the codomain of  $f$  we have a box that contains all elements  $x$  of the domain of  $f$  such that  $f(x) = y$ . Because the domain contains  $k + 1$  or more elements and the codomain contains only  $k$  elements, the pigeonhole principle tells us that one of these boxes contains two or more elements  $x$  of the domain. This means that  $f$  cannot be one-to-one.

## Example 1

**Among any group of 367 people, there must be at least two with the same birthday, because there are only 366 possible birthdays.**

# Examples

## Example 1

**Among any group of 367 people, there must be at least two with the same birthday, because there are only 366 possible birthdays.**

## Example 2

**In any group of 27 English words, there must be at least two that begin with the same letter, because there are 26 letters in the English alphabet.**

## Example 3

**How many students must be in a class to guarantee that at least two students receive the same score on the final exam, if the exam is graded on a scale from 0 to 100 points?**

## Example 3

**How many students must be in a class to guarantee that at least two students receive the same score on the final exam, if the exam is graded on a scale from 0 to 100 points?**

**Solution:** There are 101 possible scores on the final. The pigeonhole principle shows that among any 102 students there must be at least 2 students with the same score.

# The Generalized Pigeonhole Principle

The pigeonhole principle states that there must be at least two objects in the same box when there are more objects than boxes. However, even more can be said when the number of objects exceeds a multiple of the number of boxes. For instance, among any set of 21 decimal digits there must be 3 that are the same. This follows because when 21 objects are distributed into 10 boxes, one box must have more than 2 objects.

**THE GENERALIZED PIGEONHOLE PRINCIPLE:** If  $N$  objects are placed into  $k$  boxes, then there is at least one box containing at least  $[N/k]$  objects.

# Proof

**Proof:** We will use a proof by contraposition. Suppose that none of the boxes contains more than  $\lceil N/k \rceil - 1$  objects. Then, the total number of objects is at most

$$k \left( \left\lceil \frac{N}{k} \right\rceil - 1 \right) < k \left( \left( \frac{N}{k} + 1 \right) - 1 \right) = N,$$

where the inequality  $\lceil N/k \rceil < (N/k) + 1$  has been used. This is a contradiction because there are a total of  $N$  objects. 

# Examples

## Example 4

Among 100 people there are at least  $[100/12] = 9$  who were born in the same month.

## Example 5

What is the minimum number of students required in a discrete mathematics class to be sure that at least six will receive the same grade, if there are five possible grades, A, B, C, D, and F?

# Solution

The minimum number of students needed to ensure that at least six students receive the same grade is the smallest integer  $N$  such that  $[N/5] = 6$ . The smallest such integer is  $N = 5 \cdot 5 + 1 = 26$ . If you have only 25 students, it is possible for there to be five who have received each grade so that no six students have received the same grade. Thus, 26 is the minimum number of students needed to ensure that at least six students will receive the same grade.

Show that among any  $n + 1$  positive integers not exceeding  $2n$  there must be an integer that divides one of the other integers.

**Solution:** Write each of the  $n + 1$  integers  $a_1, a_2, \dots, a_{n+1}$  as a power of 2 times an odd integer. In other words, let  $a_j = 2^{k_j}q_j$  for  $j = 1, 2, \dots, n + 1$ , where  $k_j$  is a nonnegative integer and  $q_j$  is odd. The integers  $q_1, q_2, \dots, q_{n+1}$  are all odd positive integers less than  $2n$ . Because there are only  $n$  odd positive integers less than  $2n$ , it follows from the pigeonhole principle that two of the integers  $q_1, q_2, \dots, q_{n+1}$  must be equal. Therefore, there are distinct integers  $i$  and  $j$  such that  $q_i = q_j$ . Let  $q$  be the common value of  $q_i$  and  $q_j$ . Then,  $a_i = 2^{k_i}q$  and  $a_j = 2^{k_j}q$ . It follows that if  $k_i < k_j$ , then  $a_i$  divides  $a_j$ ; while if  $k_i > k_j$ , then  $a_j$  divides  $a_i$ .



# Permutations and Combinations

# Introduction

Many counting problems can be solved by finding the number of ways to arrange a specified number of distinct elements of a set of a particular size, where the order of these elements matters. Many other counting problems can be solved by finding the number of ways to select a particular number of elements from a set of a particular size, where the order of the elements selected does not matter. For example, in how many ways can we select three students from a group of five students to stand in line for a picture? How many different committees of three students can be formed from a group of four students?

Permutation and Combination help us solving these kinds of problems.

# Permutations

**Ex 1: In how many ways can we select three students from a group of five students to stand in line for a picture? In how many ways can we arrange all five of these students in a line for a picture?**

**Solution:** First, note that the order in which we select the students matters. There are five ways to select the first student to stand at the start of the line. Once this student has been selected, there are four ways to select the second student in the line. After the first and second students have been selected, there are three ways to select the third student in the line. By the product rule, there are  $5 \cdot 4 \cdot 3 = 60$  ways to select three students from a group of five students to stand in line for a picture. To arrange all five students in a line for a picture, we select the first student in five ways, the second in four ways, the third in three ways, the fourth in two ways, and the fifth in one way. Consequently, there are  $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$  ways to arrange all five students in a line for a picture.

Example 1 illustrates how ordered arrangements of distinct objects can be counted. This leads to some terminology.

A **permutation** of a set of distinct objects is an ordered arrangement of these objects. We also are interested in ordered arrangements of some of the elements of a set. An ordered arrangement of  $r$  elements of a set is called an  $r$ -permutation.

Let  $S = \{1, 2, 3\}$ . The ordered arrangement  $3, 1, 2$  is a permutation of  $S$ . The ordered arrangement  $3, 2$  is a 2-permutation of  $S$ .

The number of  $r$ -permutations of a set with  $n$  elements is denoted by  $P(n,r)$ . We can find  $P(n,r)$  using the product rule.

**Ex. 2.** Let  $S = \{a, b, c\}$ . The 2-permutations of  $S$  are the ordered arrangements  $a,b; a,c; b,a; b,c; c,a;$  and  $c,b$ . Consequently, there are six 2-permutations of this set with three elements. There are always six 2-permutations of a set with three elements. There are three ways to choose the first element of the arrangement. There are two ways to choose the second element of the arrangement, because it must be different from the first element. Hence, by the product rule, we see that  $P(3, 2) = 3 \cdot 2 = 6$ .

We now use the product rule to find a formula for  $P(n,r)$  whenever  $n$  and  $r$  are positive integers with  $1 \leq r \leq n$ .

# Theorem 1

**If  $n$  is a positive integer and  $r$  is an integer with  $1 \leq r \leq n$ , then there are  $P(n, r) = n(n - 1)(n - 2) \cdots (n - r + 1)$   $r$ -permutations of a set with  $n$  distinct elements.**

**Proof:** We will use the product rule to prove that this formula is correct. The first element of the permutation can be chosen in  $n$  ways because there are  $n$  elements in the set. There are  $n - 1$  ways to choose the second element of the permutation, because there are  $n - 1$  elements left in the set after using the element picked for the first position. Similarly, there are  $n - 2$  ways to choose the third element, and so on, until there are exactly  $n - (r - 1) = n - r + 1$  ways to choose the  $r$ th element. Consequently, by the product rule, there are  $n(n-1)(n-2)\cdots(n-r+1)$   $r$ -permutations of the set.

Note that  $P(n, 0) = 1$  whenever  $n$  is a nonnegative integer because there is exactly one way to order zero elements. That is, there is exactly one list with no elements in it, namely the empty list.

**COROLLARY 1**

If  $n$  and  $r$  are integers with  $0 \leq r \leq n$ , then  $P(n, r) = \frac{n!}{(n - r)!}$ .

**Proof:** When  $n$  and  $r$  are integers with  $1 \leq r \leq n$ , by Theorem 1 we have

$$P(n, r) = n(n - 1)(n - 2) \cdots (n - r + 1) = \frac{n!}{(n - r)!}$$

Because  $\frac{n!}{(n - 0)!} = \frac{n!}{n!} = 1$  whenever  $n$  is a nonnegative integer, we see that the formula  $P(n, r) = \frac{n!}{(n - r)!}$  also holds when  $r = 0$ . 

By Theorem 1 we know that if  $n$  is a positive integer, then  $P(n, n) = n!$ . We will illustrate this result with some examples.

**Ex.3. How many ways are there to select a first-prize winner, a second-prize winner, and a third-prize winner from 100 different people who have entered a contest?**

**Solution:** Because it matters which person wins which prize, the number of ways to pick the three prize winners is the number of ordered selections of three elements from a set of 100 elements, that is, the number of 3-permutations of a set of 100 elements. Consequently, the answer is  $P(100,3) = 100 \cdot 99 \cdot 98 = 970,200$ .

**Ex. 3.** Suppose that a saleswoman has to visit eight different cities. She must begin her trip in a specified city, but she can visit the other seven cities in any order she wishes. How many possible orders can the saleswoman use when visiting these cities?

**Solution:** The number of possible paths between the cities is the number of permutations of seven elements, because the first city is determined, but the remaining seven can be ordered arbitrarily. Consequently, there are  $7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5040$  ways for the saleswoman to choose her tour. If, for instance, the saleswoman wishes to find the path between the cities with minimum distance, and she computes the total distance for each possible path, she must consider a total of 5040 paths!

**Ex. 4. How many permutations of the letters ABCDEFGH contain the string ABC ?**

**Solution:** Because the letters ABC must occur as a block, we can find the answer by finding the number of permutations of six objects, namely, the block ABC and the individual letters D, E, F , G, and H . Because these six objects can occur in any order, there are  $6! = 720$  permutations of the letters ABCDEFGH in which ABC occurs as a block.

# Combination

We now turn our attention to counting unordered selections of objects.

**Ex. 5. How many different committees of three students can be formed from a group of four students?**

**Solution:** To answer this question, we need to only find the number of subsets with three elements from the set containing the four students. We see that there are four such subsets, one for each of the four students, because choosing three students is the same as choosing one of the four students to leave out of the group. This means that there are four ways to choose the three students for the committee, where the order in which these students are chosen does not matter.

Many counting problems can be solved by finding the number of subsets of a particular size of a set with  $n$  elements, where  $n$  is a positive integer.

An  $r$ -combination of elements of a set is an unordered selection of  $r$  elements from the set. Thus, an  $r$ -combination is simply a subset of the set with  $r$  elements.

**Ex. 6.** Let  $S$  be the set  $\{1, 2, 3, 4\}$ . Then  $\{1, 3, 4\}$  is a 3-combination from  $S$ . (Note that  $\{4, 1, 3\}$  is the same 3-combination as  $\{1, 3, 4\}$ , because the order in which the elements of a set are listed does not matter.)

The number of  $r$ -combinations of a set with  $n$  distinct elements is denoted by  $C(n, r)$ . Note that  $C(n, r)$  is also denoted by  $\binom{n}{r}$  and is called a **binomial coefficient**.

**Ex. 7.** We see that  $C(4, 2) = 6$ , because the 2-combinations of  $\{a, b, c, d\}$  are the six subsets  $\{a, b\}$ ,  $\{a, c\}$ ,  $\{a, d\}$ ,  $\{b, c\}$ ,  $\{b, d\}$ , and  $\{c, d\}$ .

We can determine the number of  $r$ -combinations of a set with  $n$  elements using the formula for the number of  $r$ -permutations of a set. To do this, note that the  $r$ -permutations of a set can be obtained by first forming  $r$ -combinations and then ordering the elements in these combinations. The proof of Theorem 2, which gives the value of  $C(n, r)$ , is based on this observation.

## THEOREM 2

The number of  $r$ -combinations of a set with  $n$  elements, where  $n$  is a nonnegative integer and  $r$  is an integer with  $0 \leq r \leq n$ , equals

$$C(n, r) = \frac{n!}{r!(n-r)!}.$$

**Proof:** The  $P(n, r)$   $r$ -permutations of the set can be obtained by forming the  $C(n, r)$   $r$ -combinations of the set, and then ordering the elements in each  $r$ -combination, which can be done in  $P(r, r)$  ways. Consequently, by the product rule,

$$P(n, r) = C(n, r) \cdot P(r, r).$$

This implies that

$$C(n, r) = \frac{P(n, r)}{P(r, r)} = \frac{n!/(n-r)!}{r!/(r-r)!} = \frac{n!}{r!(n-r)!}.$$

## Alternative Expression

$$C(n, r) = \frac{n!}{r!(n-r)!} = \frac{n(n-1)\cdots(n-r+1)}{r!}$$

**Ex. 8. How many poker hands of five cards can be dealt from a standard deck of 52 cards? Also, how many ways are there to select 47 cards from a standard deck of 52 cards?**

*Solution:* Because the order in which the five cards are dealt from a deck of 52 cards does not matter, there are

$$C(52, 5) = \frac{52!}{5!47!}$$

different hands of five cards that can be dealt. To compute the value of  $C(52, 5)$ , first divide the numerator and denominator by  $47!$  to obtain

$$C(52, 5) = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}.$$

$$C(52, 5) = 26 \cdot 17 \cdot 10 \cdot 49 \cdot 12 = 2,598,960.$$

Consequently, there are 2,598,960 different poker hands of five cards that can be dealt from a standard deck of 52 cards.

Note that there are

$$C(52, 47) = \frac{52!}{47!5!}$$

different ways to select 47 cards from a standard deck of 52 cards. We do not need to compute this value because  $C(52, 47) = C(52, 5)$ . (Only the order of the factors  $5!$  and  $47!$  is different in the denominators in the formulae for these quantities.) It follows that there are also 2,598,960 different ways to select 47 cards from a standard deck of 52 cards. ◀

**COROLLARY 2**

Let  $n$  and  $r$  be nonnegative integers with  $r \leq n$ . Then  $C(n, r) = C(n, n - r)$ .

***Proof:*** From Theorem 2 it follows that

$$C(n, r) = \frac{n!}{r! (n - r)!}$$

and

$$C(n, n - r) = \frac{n!}{(n - r)! [n - (n - r)]!} = \frac{n!}{(n - r)! r!}.$$

Hence,  $C(n, r) = C(n, n - r)$ . 

**Ex. 9. How many ways are there to select five players from a 10-member tennis team to make a trip to a match at another school?**

*Solution:* The answer is given by the number of 5-combinations of a set with 10 elements. By Theorem 2, the number of such combinations is

$$C(10, 5) = \frac{10!}{5! 5!} = 252.$$



## **Ex. 10. How many bit strings of length n contain exactly r 1s?**

**Solution:** The positions of r 1s in a bit string of length n form an r-combination of the set  $\{1, 2, 3, \dots, n\}$ . Hence, there are  $C(n, r)$  bit strings of length n that contain exactly r 1s.

**Ex. 11.** Suppose that there are 9 faculty members in the mathematics department and 11 in the computer science department. How many ways are there to select a committee to develop a discrete mathematics course at a school if the committee is to consist of three faculty members from the mathematics department and four from the computer science department?

**Solution:** By the product rule, the answer is the product of the number of 3-combinations of a set with nine elements and the number of 4-combinations of a set with 11 elements. By Theorem 2, the number of ways to select the committee is

$$C(9, 3) \cdot C(11, 4) = \frac{9!}{3!6!} \cdot \frac{11!}{4!7!} = 84 \cdot 330 = 27,720.$$



# Recurrence Relation

Recall that a recursive definition of a sequence specifies one or more initial terms and a rule for determining subsequent terms from those that precede them. Also, recall that a rule of the latter sort is called a recurrence relation and that a sequence is called a solution of a recurrence relation if its terms satisfy the recurrence relation.

- **Notation:**  $a_n = n!$
- **Initial condition:**  $a_1 = 1.$
- **Recurrence relation:**  $n! = n(n - 1)!$
- **That is,**  $a_n = na_{n-1}$

A *recurrence relation* for the sequence  $\{a_n\}$  is an equation that expresses  $a_n$  in terms of one or more of the previous terms of the sequence, namely,  $a_0, a_1, \dots, a_{n-1}$ , for all integers  $n$  with  $n \geq n_0$ , where  $n_0$  is a nonnegative integer.

A sequence is called a *solution* of a recurrence relation if its terms satisfy the recurrence relation. (A recurrence relation is said to *recursively define* a sequence. We will explain this alternative terminology in Chapter 5.)

In this section we will show that such relations can be used to study and to solve counting problems. For example, suppose that the number of bacteria in a colony doubles every hour. If a colony begins with five bacteria, how many will be present in  $n$  hours? To solve this problem,

let  $a_n$  be the number of bacteria at the end of  $n$  hours. Because the number of bacteria doubles every hour, the relationship  $a_n = 2a_{n-1}$  holds whenever  $n$  is a positive integer. This recurrence relation, together with the initial condition  $a_0 = 5$ , uniquely determines  $a_n$  for all nonnegative integers  $n$ . We can find a formula for  $a_n$  using the iterative approach followed in Chapter 2, namely that  $a_n = 5 \cdot 2^n$  for all nonnegative integers  $n$ .

# Applications of Recurrence Relation

- Finance
- Optimization
- Algorithms
- Mathematics and Counting

We can use recurrence relations to model a wide variety of problems

## Example

Find a recurrence relation and give initial conditions for the number of bit strings of length  $n$  that do not have two consecutive 0s. How many such bit strings are there of length five?

**Solution:** Let  $a_n$  denote the number of bit strings of length  $n$  that do not have two consecutive 0s. To obtain a recurrence relation for  $\{a_n\}$ , note that by the sum rule, the number of bit strings of length  $n$  that do not have two consecutive 0s equals the number of such bit strings ending with a 0 plus the number of such bit strings ending with a 1. We will assume that  $n \geq 3$ , so that the bit string has at least three bits.

The bit strings of length  $n$  ending with 1 that do not have two consecutive 0s are precisely the bit strings of length  $n - 1$  with no two consecutive 0s with a 1 added at the end. Consequently, there are  $a_{n-1}$  such bit strings.

Bit strings of length  $n$  ending with a 0 that do not have two consecutive 0s must have 1 as their  $(n - 1)$ st bit; otherwise they would end with a pair of 0s. It follows that the bit strings of length  $n$  ending with a 0 that have no two consecutive 0s are precisely the bit strings of length  $n - 2$  with no two consecutive 0s with 10 added at the end. Consequently, there are  $a_{n-2}$  such bit strings.

We conclude, as illustrated in Figure 4, that

$$a_n = a_{n-1} + a_{n-2}$$

for  $n \geq 3$ .

The initial conditions are  $a_1 = 2$ , because both bit strings of length one, 0 and 1 do not have consecutive 0s, and  $a_2 = 3$ , because the valid bit strings of length two are 01, 10, and 11. To obtain  $a_5$ , we use the recurrence relation three times to find that

$$a_3 = a_2 + a_1 = 3 + 2 = 5,$$

$$a_4 = a_3 + a_2 = 5 + 3 = 8,$$

$$a_5 = a_4 + a_3 = 8 + 5 = 13.$$

**Remark:** Note that  $\{a_n\}$  satisfies the same recurrence relation as the Fibonacci sequence. Because  $a_1 = f_3$  and  $a_2 = f_4$  it follows that  $a_n = f_{n+2}$ .

# Solving Linear Recurrence Relations

A wide variety of recurrence relations occur in models. Some of these recurrence relations can be solved using iteration or some other ad hoc technique. However, one important class of recurrence relations can be explicitly solved in a systematic way. These are recurrence relations that express the terms of a sequence as linear combinations of previous terms.

A *linear homogeneous recurrence relation of degree k with constant coefficients* is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where  $c_1, c_2, \dots, c_k$  are real numbers, and  $c_k \neq 0$ .

The recurrence relation in the definition is linear because the right-hand side is a sum of previous terms of the sequence each multiplied by a function of  $n$ . The recurrence relation is homogeneous because no terms occur that are not multiples of the  $a_j$ 's. The coefficients of the terms of the sequence are all constants, rather than functions that depend on  $n$ . The degree is  $k$  because  $a_n$  is expressed in terms of the previous  $k$  terms of the sequence.

A consequence of the second principle of mathematical induction is that a sequence satisfying the recurrence relation in the definition is uniquely determined by this recurrence relation and the  $k$  initial conditions

$$a_0 = C_0, a_1 = C_1, \dots, a_{k-1} = C_{k-1}.$$

Recurrence relation:  $a_n = a_{n-1} + a_{n-2}$

Initial Condition:  $a_0 = 0$

Possible Solutions: 0, 2, 2, 4, 6, 10, 16,...

0, 0, 0, 0, 0, 0,...

Both the above sequence satisfy the above two conditions.

As this is a recurrence relation of degree 2, we need to specify  $a_0 = 0$  and  $a_1 = 1$  to get unique sequence as:

0, 1, 1, 2, 3, 5,...

## Examples of linear homogeneous recurrence relations with constant coefficients.

The recurrence relation  $P_n = (1.11)P_{n-1}$  is a linear homogeneous recurrence relation of degree one. The recurrence relation  $f_n = f_{n-1} + f_{n-2}$  is a linear homogeneous recurrence relation of degree two. The recurrence relation  $a_n = a_{n-5}$  is a linear homogeneous recurrence relation of degree five. 

## Not linear homogeneous recurrence relations with constant coefficients.

The recurrence relation  $a_n = a_{n-1} + a_{n-2}^2$  is not linear. The recurrence relation  $H_n = 2H_{n-1} + 1$  is not homogeneous. The recurrence relation  $B_n = nB_{n-1}$  does not have constant coefficients. 

Linear homogeneous recurrence relations are studied for two reasons. First, they often occur in modeling of problems. Second, they can be systematically solved.

# Solving Linear Homogeneous Recurrence Relations with Constant Coefficients

The basic approach for solving linear homogeneous recurrence relations is to look for solutions of the form  $a_n = r^n$ , where  $r$  is a constant. Note that  $a_n = r^n$  is a solution of the recurrence relation  $a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k}$  if and only if

$$r^n = c_1r^{n-1} + c_2r^{n-2} + \cdots + c_kr^{n-k}.$$

When both sides of this equation are divided by  $r^{n-k}$  and the right-hand side is subtracted from the left, we obtain the equation

$$r^k - c_1r^{k-1} - c_2r^{k-2} - \cdots - c_{k-1}r - c_k = 0.$$

Consequently, the sequence  $\{a_n\}$  with  $a_n = r^n$  is a solution if and only if  $r$  is a solution of this last equation. We call this the **characteristic equation** of the recurrence relation. The solutions of this equation are called the **characteristic roots** of the recurrence relation. As we will see, these characteristic roots can be used to give an explicit formula for all the solutions of the recurrence relation.

We will first develop results that deal with linear homogeneous recurrence relations with constant coefficients of degree two. Proofs of all these theorems are not complicated but long hence are not provided here. Please see Page 515 for the proof. We now turn our attention to linear homogeneous recurrence relations of degree two. First, consider the case when there are two distinct characteristic roots.

Let  $c_1$  and  $c_2$  be real numbers. Suppose that  $r^2 - c_1r - c_2 = 0$  has two distinct roots  $r_1$  and  $r_2$ . Then the sequence  $\{a_n\}$  is a solution of the recurrence relation  $a_n = c_1a_{n-1} + c_2a_{n-2}$  if and only if  $a_n = \alpha_1r_1^n + \alpha_2r_2^n$  for  $n = 0, 1, 2, \dots$ , where  $\alpha_1$  and  $\alpha_2$  are constants.

**Note:** The characteristic roots of a linear homogeneous recurrence relation with constant coefficients may be complex numbers. Theorem 1 (and also subsequent theorems in this section) still applies in this case. Recurrence relations with complex characteristic roots will not be discussed here.

**Example 1.**

What is the solution of the recurrence relation

$$a_n = a_{n-1} + 2a_{n-2}$$

with  $a_0 = 2$  and  $a_1 = 7$ ?

**Solution:** Theorem 1 can be used to solve this problem. The characteristic equation of the recurrence relation is  $r^2 - r - 2 = 0$ . Its roots are  $r = 2$  and  $r = -1$ . Hence, the sequence  $\{a_n\}$  is a solution to the recurrence relation if and only if

$$a_n = \alpha_1 2^n + \alpha_2 (-1)^n,$$

for some constants  $\alpha_1$  and  $\alpha_2$ . From the initial conditions, it follows that

$$a_0 = 2 = \alpha_1 + \alpha_2,$$

$$a_1 = 7 = \alpha_1 \cdot 2 + \alpha_2 \cdot (-1).$$

Solving these two equations shows that  $\alpha_1 = 3$  and  $\alpha_2 = -1$ . Hence, the solution to the recurrence relation and initial conditions is the sequence  $\{a_n\}$  with

$$a_n = 3 \cdot 2^n - (-1)^n.$$



# Problem

**Find an explicit formula for the Fibonacci numbers**

Recall that the sequence of Fibonacci numbers satisfies the recurrence relation  $f_n = f_{n-1} + f_{n-2}$  and also satisfies the initial conditions

$$f_0 = 0 \text{ and } f_1 = 1.$$

**Solution:** Recall that the sequence of Fibonacci numbers satisfies the recurrence relation  $f_n = f_{n-1} + f_{n-2}$  and also satisfies the initial conditions  $f_0 = 0$  and  $f_1 = 1$ . The roots of the characteristic equation  $r^2 - r - 1 = 0$  are  $r_1 = (1 + \sqrt{5})/2$  and  $r_2 = (1 - \sqrt{5})/2$ . Therefore, from Theorem 1 it follows that the Fibonacci numbers are given by

$$f_n = \alpha_1 \left( \frac{1 + \sqrt{5}}{2} \right)^n + \alpha_2 \left( \frac{1 - \sqrt{5}}{2} \right)^n,$$

for some constants  $\alpha_1$  and  $\alpha_2$ . The initial conditions  $f_0 = 0$  and  $f_1 = 1$  can be used to find these constants. We have

$$f_0 = \alpha_1 + \alpha_2 = 0,$$

$$f_1 = \alpha_1 \left( \frac{1 + \sqrt{5}}{2} \right) + \alpha_2 \left( \frac{1 - \sqrt{5}}{2} \right) = 1.$$

The solution to these simultaneous equations for  $\alpha_1$  and  $\alpha_2$  is

$$\alpha_1 = 1/\sqrt{5}, \quad \alpha_2 = -1/\sqrt{5}.$$

Consequently, the Fibonacci numbers are given by

$$f_n = \frac{1}{\sqrt{5}} \left( \frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left( \frac{1 - \sqrt{5}}{2} \right)^n.$$





Theorem 1 does not apply when there is one characteristic root of multiplicity two.

Theorem 2 shows how to handle this case.

## Theorem 2

Let  $c_1$  and  $c_2$  be real numbers with  $c_2 \neq 0$ . Suppose that  $r^2 - c_1r - c_2 = 0$  has only one root  $r_0$ . A sequence  $\{a_n\}$  is a solution of the recurrence relation  $a_n = c_1a_{n-1} + c_2a_{n-2}$  if and only if  $a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n$ , for  $n = 0, 1, 2, \dots$ , where  $\alpha_1$  and  $\alpha_2$  are constants.

## Example 2

What is the solution of the recurrence relation

$$a_n = 6a_{n-1} - 9a_{n-2}$$

with initial conditions  $a_0 = 1$  and  $a_1 = 6$ ?

**Solution:** The only root of  $r^2 - 6r + 9 = 0$  is  $r = 3$ . Hence, the solution to this recurrence relation is

$$a_n = \alpha_1 3^n + \alpha_2 n 3^n$$

for some constants  $\alpha_1$  and  $\alpha_2$ . Using the initial conditions, it follows that

$$a_0 = 1 = \alpha_1,$$

$$a_1 = 6 = \alpha_1 \cdot 3 + \alpha_2 \cdot 3.$$

Solving these two equations shows that  $\alpha_1 = 1$  and  $\alpha_2 = 1$ . Consequently, the solution to this recurrence relation and the initial conditions is

$$a_n = 3^n + n 3^n.$$



We will now state the general result about the solution of linear homogeneous recurrence relations with constant coefficients, where the degree may be greater than two, under the assumption that the characteristic equation has distinct roots.

Let  $c_1, c_2, \dots, c_k$  be real numbers. Suppose that the characteristic equation

$$r^k - c_1 r^{k-1} - \cdots - c_k = 0$$

has  $k$  distinct roots  $r_1, r_2, \dots, r_k$ . Then a sequence  $\{a_n\}$  is a solution of the recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

if and only if

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \cdots + \alpha_k r_k^n$$

for  $n = 0, 1, 2, \dots$ , where  $\alpha_1, \alpha_2, \dots, \alpha_k$  are constants.

### Example 3

Find the solution to the recurrence relation

$$a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$$

with the initial conditions  $a_0 = 2$ ,  $a_1 = 5$ , and  $a_2 = 15$ .

*Solution:* The characteristic polynomial of this recurrence relation is

$$r^3 - 6r^2 + 11r - 6.$$

The characteristic roots are  $r = 1$ ,  $r = 2$ , and  $r = 3$ , because  $r^3 - 6r^2 + 11r - 6 = (r - 1)(r - 2)(r - 3)$ . Hence, the solutions to this recurrence relation are of the form

$$a_n = \alpha_1 \cdot 1^n + \alpha_2 \cdot 2^n + \alpha_3 \cdot 3^n.$$

To find the constants  $\alpha_1$ ,  $\alpha_2$ , and  $\alpha_3$ , use the initial conditions. This gives

$$a_0 = 2 = \alpha_1 + \alpha_2 + \alpha_3,$$

$$a_1 = 5 = \alpha_1 + \alpha_2 \cdot 2 + \alpha_3 \cdot 3,$$

$$a_2 = 15 = \alpha_1 + \alpha_2 \cdot 4 + \alpha_3 \cdot 9.$$

When these three simultaneous equations are solved for  $\alpha_1$ ,  $\alpha_2$ , and  $\alpha_3$ , we find that  $\alpha_1 = 1$ ,  $\alpha_2 = -1$ , and  $\alpha_3 = 2$ . Hence, the unique solution to this recurrence relation and the given initial conditions is the sequence  $\{a_n\}$  with

$$a_n = 1 - 2^n + 2 \cdot 3^n.$$



We now state the most general result about linear homogeneous recurrence relations with constant coefficients, allowing the characteristic equation to have multiple roots. The key point is that for each root  $r$  of the characteristic equation, the general solution has a summand of the form  $P(n)r^n$ , where  $P(n)$  is a polynomial of degree  $m - 1$ , with  $m$  the multiplicity of this root.

Let  $c_1, c_2, \dots, c_k$  be real numbers. Suppose that the characteristic equation

$$r^k - c_1 r^{k-1} - \cdots - c_k = 0$$

has  $t$  distinct roots  $r_1, r_2, \dots, r_t$  with multiplicities  $m_1, m_2, \dots, m_t$ , respectively, so that  $m_i \geq 1$  for  $i = 1, 2, \dots, t$  and  $m_1 + m_2 + \cdots + m_t = k$ . Then a sequence  $\{a_n\}$  is a solution of the recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

if and only if

$$\begin{aligned} a_n = & (\alpha_{1,0} + \alpha_{1,1} n + \cdots + \alpha_{1,m_1-1} n^{m_1-1}) r_1^n \\ & + (\alpha_{2,0} + \alpha_{2,1} n + \cdots + \alpha_{2,m_2-1} n^{m_2-1}) r_2^n \\ & + \cdots + (\alpha_{t,0} + \alpha_{t,1} n + \cdots + \alpha_{t,m_t-1} n^{m_t-1}) r_t^n \end{aligned}$$

for  $n = 0, 1, 2, \dots$ , where  $\alpha_{i,j}$  are constants for  $1 \leq i \leq t$  and  $0 \leq j \leq m_i - 1$ .

## Example 4

Find the solution to the recurrence relation

$$a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3}$$

with initial conditions  $a_0 = 1$ ,  $a_1 = -2$ , and  $a_2 = -1$ .

**Solution:** The characteristic equation of this recurrence relation is

$$r^3 + 3r^2 + 3r + 1 = 0.$$

Because  $r^3 + 3r^2 + 3r + 1 = (r + 1)^3$ , there is a single root  $r = -1$  of multiplicity three of the characteristic equation. By Theorem 4 the solutions of this recurrence relation are of the form

$$a_n = \alpha_{1,0}(-1)^n + \alpha_{1,1}n(-1)^n + \alpha_{1,2}n^2(-1)^n.$$

To find the constants  $\alpha_{1,0}$ ,  $\alpha_{1,1}$ , and  $\alpha_{1,2}$ , use the initial conditions. This gives

$$a_0 = 1 = \alpha_{1,0},$$

$$a_1 = -2 = -\alpha_{1,0} - \alpha_{1,1} - \alpha_{1,2},$$

$$a_2 = -1 = \alpha_{1,0} + 2\alpha_{1,1} + 4\alpha_{1,2}.$$

The simultaneous solution of these three equations is  $\alpha_{1,0} = 1$ ,  $\alpha_{1,1} = 3$ , and  $\alpha_{1,2} = -2$ . Hence, the unique solution to this recurrence relation and the given initial conditions is the sequence  $\{a_n\}$  with

$$a_n = (1 + 3n - 2n^2)(-1)^n.$$



# Linear Nonhomogeneous Recurrence Relations with Constant Coefficients

We have seen how to solve linear homogeneous recurrence relations with constant coefficients. Is there a relatively simple technique for solving a linear, but not homogeneous, recurrence relation with constant coefficients, such as  $a_n = 3a_{n-1} + 2n$ ? We will see that the answer is yes for certain families of such recurrence relations.

The recurrence relation  $a_n = 3a_{n-1} + 2n$  is an example of a **linear nonhomogeneous recurrence relation with constant coefficients**, that is, a recurrence relation of the form

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k} + F(n),$$

where  $c_1, c_2, \dots, c_k$  are real numbers and  $F(n)$  is a function not identically zero depending only on  $n$ . The recurrence relation

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k}$$

is called the **associated homogeneous recurrence relation**. It plays an important role in the solution of the nonhomogeneous recurrence relation.

Each of the recurrence relations  $a_n = a_{n-1} + 2^n$ ,  $a_n = a_{n-1} + a_{n-2} + n^2 + n + 1$ ,  $a_n = 3a_{n-1} + n3^n$ , and  $a_n = a_{n-1} + a_{n-2} + a_{n-3} + n!$  is a linear nonhomogeneous recurrence relation with constant coefficients. The associated linear homogeneous recurrence relations are  $a_n = a_{n-1}$ ,  $a_n = a_{n-1} + a_{n-2}$ ,  $a_n = 3a_{n-1}$ , and  $a_n = a_{n-1} + a_{n-2} + a_{n-3}$ , respectively. 

The key fact about linear nonhomogeneous recurrence relations with constant coefficients is that every solution is the sum of a particular solution and a solution of the associated linear homogeneous recurrence relation, as Theorem 5 shows.

## Theorem 5

If  $\{a_n^{(p)}\}$  is a particular solution of the nonhomogeneous linear recurrence relation with constant coefficients

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n),$$

then every solution is of the form  $\{a_n^{(p)} + a_n^{(h)}\}$ , where  $\{a_n^{(h)}\}$  is a solution of the associated homogeneous recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}.$$

**Proof:** Because  $\{a_n^{(p)}\}$  is a particular solution of the nonhomogeneous recurrence relation, we know that

$$a_n^{(p)} = c_1 a_{n-1}^{(p)} + c_2 a_{n-2}^{(p)} + \cdots + c_k a_{n-k}^{(p)} + F(n).$$

Now suppose that  $\{b_n\}$  is a second solution of the nonhomogeneous recurrence relation, so that

$$b_n = c_1 b_{n-1} + c_2 b_{n-2} + \cdots + c_k b_{n-k} + F(n).$$

Subtracting the first of these two equations from the second shows that

$$b_n - a_n^{(p)} = c_1(b_{n-1} - a_{n-1}^{(p)}) + c_2(b_{n-2} - a_{n-2}^{(p)}) + \cdots + c_k(b_{n-k} - a_{n-k}^{(p)}).$$

It follows that  $\{b_n - a_n^{(p)}\}$  is a solution of the associated homogeneous linear recurrence, say,  $\{a_n^{(h)}\}$ . Consequently,  $b_n = a_n^{(p)} + a_n^{(h)}$  for all  $n$ . 

By Theorem 5, we see that the key to solving nonhomogeneous recurrence relations with constant coefficients is finding a particular solution. Then every solution is a sum of this solution and a solution of the associated homogeneous recurrence relation. Although there is no general method for finding such a solution that works for every function  $F(n)$ , there are techniques that work for certain types of functions  $F(n)$ , such as polynomials and powers of constants.

Find all solutions of the recurrence relation  $a_n = 3a_{n-1} + 2n$ . What is the solution with  $a_1 = 3$ ?

**Solution:** To solve this linear nonhomogeneous recurrence relation with constant coefficients, we need to solve its associated linear homogeneous equation and to find a particular solution for the given nonhomogeneous equation. The associated linear homogeneous equation is  $a_n = 3a_{n-1}$ . Its solutions are  $a_n^{(h)} = \alpha 3^n$ , where  $\alpha$  is a constant.

We now find a particular solution. Because  $F(n) = 2n$  is a polynomial in  $n$  of degree one, a reasonable trial solution is a linear function in  $n$ , say,  $p_n = cn + d$ , where  $c$  and  $d$  are constants. To determine whether there are any solutions of this form, suppose that  $p_n = cn + d$  is such a solution. Then the equation  $a_n = 3a_{n-1} + 2n$  becomes  $cn + d = 3(c(n - 1) + d) + 2n$ . Simplifying and combining like terms gives  $(2 + 2c)n + (2d - 3c) = 0$ . It follows that  $cn + d$  is a solution if and only if  $2 + 2c = 0$  and  $2d - 3c = 0$ . This shows that  $cn + d$  is a solution if and only if  $c = -1$  and  $d = -3/2$ . Consequently,  $a_n^{(p)} = -n - 3/2$  is a particular solution.

By Theorem 5 all solutions are of the form

$$a_n = a_n^{(p)} + a_n^{(h)} = -n - \frac{3}{2} + \alpha \cdot 3^n,$$

where  $\alpha$  is a constant.

To find the solution with  $a_1 = 3$ , let  $n = 1$  in the formula we obtained for the general solution. We find that  $3 = -1 - 3/2 + 3\alpha$ , which implies that  $\alpha = 11/6$ . The solution we seek is  $a_n = -n - 3/2 + (11/6)3^n$ .

Find all solutions of the recurrence relation

$$a_n = 5a_{n-1} - 6a_{n-2} + 7^n.$$

**Solution:** This is a linear nonhomogeneous recurrence relation. The solutions of its associated homogeneous recurrence relation

$$a_n = 5a_{n-1} - 6a_{n-2}$$

are  $a_n^{(h)} = \alpha_1 \cdot 3^n + \alpha_2 \cdot 2^n$ , where  $\alpha_1$  and  $\alpha_2$  are constants. Because  $F(n) = 7^n$ , a reasonable trial solution is  $a_n^{(p)} = C \cdot 7^n$ , where  $C$  is a constant. Substituting the terms of this sequence into the recurrence relation implies that  $C \cdot 7^n = 5C \cdot 7^{n-1} - 6C \cdot 7^{n-2} + 7^n$ . Factoring out  $7^{n-2}$ , this equation becomes  $49C = 35C - 6C + 49$ , which implies that  $20C = 49$ , or that  $C = 49/20$ . Hence,  $a_n^{(p)} = (49/20)7^n$  is a particular solution. By Theorem 5, all solutions are of the form

$$a_n = \alpha_1 \cdot 3^n + \alpha_2 \cdot 2^n + (49/20)7^n.$$



In previous two examples, we made an educated guess that there are solutions of a particular form. In both cases we were able to find particular solutions. This was not an accident. Whenever  $F(n)$  is the product of a polynomial in  $n$  and the  $n$ th power of a constant, we know exactly what form a particular solution has, as stated in Theorem 6.

## Theorem 6

Suppose that  $\{a_n\}$  satisfies the linear nonhomogeneous recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n),$$

where  $c_1, c_2, \dots, c_k$  are real numbers, and

$$F(n) = (b_t n^t + b_{t-1} n^{t-1} + \cdots + b_1 n + b_0) s^n,$$

where  $b_0, b_1, \dots, b_t$  and  $s$  are real numbers. When  $s$  is not a root of the characteristic equation of the associated linear homogeneous recurrence relation, there is a particular solution of the form

$$(p_t n^t + p_{t-1} n^{t-1} + \cdots + p_1 n + p_0) s^n.$$

When  $s$  is a root of this characteristic equation and its multiplicity is  $m$ , there is a particular solution of the form

$$n^m (p_t n^t + p_{t-1} n^{t-1} + \cdots + p_1 n + p_0) s^n.$$

## Example

What form does a particular solution of the linear nonhomogeneous recurrence relation  $a_n = 6a_{n-1} - 9a_{n-2} + F(n)$  have when  $F(n) = 3^n$ ,  $F(n) = n3^n$ ,  $F(n) = n^22^n$ , and  $F(n) = (n^2 + 1)3^n$ ?

**Solution:** The associated linear homogeneous recurrence relation is  $a_n = 6a_{n-1} - 9a_{n-2}$ . Its characteristic equation,  $r^2 - 6r + 9 = (r - 3)^2 = 0$ , has a single root, 3, of multiplicity two. To apply Theorem 6, with  $F(n)$  of the form  $P(n)s^n$ , where  $P(n)$  is a polynomial and  $s$  is a constant, we need to ask whether  $s$  is a root of this characteristic equation.

Because  $s = 3$  is a root with multiplicity  $m = 2$  but  $s = 2$  is not a root, Theorem 6 tells us that a particular solution has the form  $p_0n^23^n$  if  $F(n) = 3^n$ , the form  $n^2(p_1n + p_0)3^n$  if  $F(n) = n3^n$ , the form  $(p_2n^2 + p_1n + p_0)2^n$  if  $F(n) = n^22^n$ , and the form  $n^2(p_2n^2 + p_1n + p_0)3^n$  if  $F(n) = (n^2 + 1)3^n$ . ◀

Care must be taken when  $s = 1$  when solving recurrence relations of the type covered by Theorem 6. In particular, to apply this theorem with  $F(n) = b_t n_t + b_{t-1} n_{t-1} + \cdots + b_1 n + b_0$ , the parameter  $s$  takes the value  $s = 1$  (even though the term  $1^n$  does not explicitly appear). By the theorem, the form of the solution then depends on whether 1 is a root of the characteristic equation of the associated linear homogeneous recurrence relation.

Example:

Let  $a_n$  be the sum of the first  $n$  positive integers, so that

$$a_n = \sum_{k=1}^n k.$$

Note that  $a_n$  satisfies the linear nonhomogeneous recurrence relation

$$a_n = a_{n-1} + n.$$

(To obtain  $a_n$ , the sum of the first  $n$  positive integers, from  $a_{n-1}$ , the sum of the first  $n - 1$  positive integers, we add  $n$ .) Note that the initial condition is  $a_1 = 1$ .

The associated linear homogeneous recurrence relation for  $a_n$  is

$$a_n = a_{n-1}.$$

The solutions of this homogeneous recurrence relation are given by  $a_n^{(h)} = c(1)^n = c$ , where  $c$  is a constant. To find all solutions of  $a_n = a_{n-1} + n$ , we need find only a single particular solution. By Theorem 6, because  $F(n) = n = n \cdot (1)^n$  and  $s = 1$  is a root of degree one of the characteristic equation of the associated linear homogeneous recurrence relation, there is a particular solution of the form  $n(p_1n + p_0) = p_1n^2 + p_0n$ .

Inserting this into the recurrence relation gives  $p_1n^2 + p_0n = p_1(n-1)^2 + p_0(n-1) + n$ . Simplifying, we see that  $n(2p_1 - 1) + (p_0 - p_1) = 0$ , which means that  $2p_1 - 1 = 0$  and  $p_0 - p_1 = 0$ , so  $p_0 = p_1 = 1/2$ . Hence,

$$a_n^{(p)} = \frac{n^2}{2} + \frac{n}{2} = \frac{n(n+1)}{2}$$

is a particular solution. Hence, all solutions of the original recurrence relation  $a_n = a_{n-1} + n$  are given by  $a_n = a_n^{(h)} + a_n^{(p)} = c + n(n+1)/2$ . Because  $a_1 = 1$ , we have  $1 = a_1 = c + 1 \cdot 2/2 = c + 1$ , so  $c = 0$ . It follows that  $a_n = n(n+1)/2$ .

# Binomial Coefficients and Identities

As we remarked in Section 6.3, the number of  $r$ -combinations from a set with  $n$  elements is often denoted by  $\binom{n}{r}$ . This number is also called a **binomial coefficient** because these numbers occur as coefficients in the expansion of powers of binomial expressions such as  $(a + b)^n$ . We will discuss the **binomial theorem**, which gives a power of a binomial expression as a sum of terms involving binomial coefficients. We will prove this theorem using a combinatorial proof.

## Example

The expansion of  $(x + y)^3$  can be found using combinatorial reasoning instead of multiplying the three terms out. When  $(x + y)^3 = (x + y)(x + y)(x + y)$  is expanded, all products of a term in the first sum, a term in the second sum, and a term in the third sum are added. Terms of the form  $x^3$ ,  $x^2y$ ,  $xy^2$ , and  $y^3$  arise. To obtain a term of the form  $x^3$ , an  $x$  must be chosen in each of the sums, and this can be done in only one way. Thus, the  $x^3$  term in the product has a coefficient of 1. To obtain a term of the form  $x^2y$ , an  $x$  must be chosen in two of the three sums (and consequently a  $y$  in the other sum). Hence, the number of such terms is the number of 2-combinations of three objects, namely,  $\binom{3}{2}$ . Similarly, the number of terms of the form  $xy^2$  is the number of ways to pick one of the three sums to obtain an  $x$  (and consequently take a  $y$  from each of the other two sums). This can be done in  $\binom{3}{1}$  ways. Finally, the only way to obtain a  $y^3$  term is to choose the  $y$  for each of the three sums in the product, and this can be done in exactly one way. Consequently, it follows that

$$\begin{aligned}(x + y)^3 &= (x + y)(x + y)(x + y) = (xx + xy + yx + yy)(x + y) \\&= xxx + xxy + xyx + xyy + yxx + yxy + yyx + yyy \\&= x^3 + 3x^2y + 3xy^2 + y^3.\end{aligned}$$



**THE BINOMIAL THEOREM** Let  $x$  and  $y$  be variables, and let  $n$  be a nonnegative integer. Then

$$(x + y)^n = \sum_{j=0}^n \binom{n}{j} x^{n-j} y^j = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \cdots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n.$$

**Proof:** We use a combinatorial proof. The terms in the product when it is expanded are of the form  $x^{n-j} y^j$  for  $j = 0, 1, 2, \dots, n$ . To count the number of terms of the form  $x^{n-j} y^j$ , note that to obtain such a term it is necessary to choose  $n - j$  xs from the  $n$  sums (so that the other  $j$  terms in the product are ys). Therefore, the coefficient of  $x^{n-j} y^j$  is  $\binom{n}{n-j}$ , which is equal to  $\binom{n}{j}$ . This proves the theorem. ◀

## Example

What is the expansion of  $(x + y)^4$ ?

## Example

What is the expansion of  $(x + y)^4$ ?

*Solution:* From the binomial theorem it follows that

$$\begin{aligned}(x + y)^4 &= \sum_{j=0}^4 \binom{4}{j} x^{4-j} y^j \\&= \binom{4}{0} x^4 + \binom{4}{1} x^3 y + \binom{4}{2} x^2 y^2 + \binom{4}{3} x y^3 + \binom{4}{4} y^4 \\&= x^4 + 4x^3 y + 6x^2 y^2 + 4x y^3 + y^4.\end{aligned}$$

What is the coefficient of  $x^{12}y^{13}$  in the expansion of  $(x + y)^{25}$ ?

*Solution:* From the binomial theorem it follows that this coefficient is

$$\binom{25}{13} = \frac{25!}{13! 12!} = 5,200,300.$$

**What is the coefficient of  $x^{12}y^{13}$  in the expansion of  $(2x - 3y)^{25}$ ?**

What is the coefficient of  $x^{12}y^{13}$  in the expansion of  $(2x - 3y)^{25}$ ?

**Solution:** First, note that this expression equals  $(2x + (-3y))^{25}$ . By the binomial theorem, we have

$$(2x + (-3y))^{25} = \sum_{j=0}^{25} \binom{25}{j} (2x)^{25-j} (-3y)^j.$$

Consequently, the coefficient of  $x^{12}y^{13}$  in the expansion is obtained when  $j = 13$ , namely,

$$\binom{25}{13} 2^{12} (-3)^{13} = -\frac{25!}{13! 12!} 2^{12} 3^{13}.$$



# Identities

We can prove some useful identities using the binomial theorem.

Let  $n$  be a nonnegative integer. Then

$$\sum_{k=0}^n \binom{n}{k} = 2^n.$$

**Proof:** Using the binomial theorem with  $x = 1$  and  $y = 1$ , we see that

$$2^n = (1 + 1)^n = \sum_{k=0}^n \binom{n}{k} 1^k 1^{n-k} = \sum_{k=0}^n \binom{n}{k}.$$

This is the desired result. 

# Alternative Method

**Proof:** A set with  $n$  elements has a total of  $2^n$  different subsets. Each subset has zero elements, one element, two elements, . . . , or  $n$  elements in it. There are  $\binom{n}{0}$  subsets with zero elements,  $\binom{n}{1}$  subsets with one element,  $\binom{n}{2}$  subsets with two elements, . . . , and  $\binom{n}{n}$  subsets with  $n$  elements. Therefore,

$$\sum_{k=0}^n \binom{n}{k}$$

counts the total number of subsets of a set with  $n$  elements. By equating the two formulas we have for the number of subsets of a set with  $n$  elements, we see that

$$\sum_{k=0}^n \binom{n}{k} = 2^n.$$



# Identity

Let  $n$  be a positive integer. Then

$$\sum_{k=0}^n (-1)^k \binom{n}{k} = 0.$$

**Proof:** When we use the binomial theorem with  $x = -1$  and  $y = 1$ , we see that

$$0 = 0^n = ((-1) + 1)^n = \sum_{k=0}^n \binom{n}{k} (-1)^k 1^{n-k} = \sum_{k=0}^n \binom{n}{k} (-1)^k.$$

This proves the corollary. 

## Remark

Using the previous identity:

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots.$$

# Identity

Let  $n$  be a nonnegative integer. Then

$$\sum_{k=0}^n 2^k \binom{n}{k} = 3^n.$$

**Proof:** We recognize that the left-hand side of this formula is the expansion of  $(1 + 2)^n$  provided by the binomial theorem. Therefore, by the binomial theorem, we see that

$$(1 + 2)^n = \sum_{k=0}^n \binom{n}{k} 1^{n-k} 2^k = \sum_{k=0}^n \binom{n}{k} 2^k.$$

Hence

$$\sum_{k=0}^n 2^k \binom{n}{k} = 3^n.$$



**PASCAL'S IDENTITY** Let  $n$  and  $k$  be positive integers with  $n \geq k$ . Then

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

**Proof:** We will use a combinatorial proof. Suppose that  $T$  is a set containing  $n + 1$  elements. Let  $a$  be an element in  $T$ , and let  $S = T - \{a\}$ . Note that there are  $\binom{n+1}{k}$  subsets of  $T$  containing  $k$  elements. However, a subset of  $T$  with  $k$  elements either contains  $a$  together with  $k - 1$  elements of  $S$ , or contains  $k$  elements of  $S$  and does not contain  $a$ . Because there are  $\binom{n}{k-1}$  subsets of  $k - 1$  elements of  $S$ , there are  $\binom{n}{k-1}$  subsets of  $k$  elements of  $T$  that contain  $a$ . And there are  $\binom{n}{k}$  subsets of  $k$  elements of  $T$  that do not contain  $a$ , because there are  $\binom{n}{k}$  subsets of  $k$  elements of  $S$ . Consequently,

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$



**Remark:** It is also possible to prove this identity by algebraic manipulation from the formula for  $\binom{n}{r}$  (see Exercise 19).

(%)

1

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

1

$$\begin{pmatrix} 2 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 2 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 2 \\ 2 \end{pmatrix}$$

By Pascal's identity:

1 2 1

$$\begin{pmatrix} 3 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 3 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 3 \\ 2 \end{pmatrix} \quad \begin{pmatrix} 3 \\ 3 \end{pmatrix}$$

$$\binom{6}{4} + \binom{6}{5} = \binom{7}{5}$$

1 3 3 1

$$\begin{pmatrix} 4 \\ 0 \end{pmatrix} \begin{pmatrix} 4 \\ 1 \end{pmatrix} \begin{pmatrix} 4 \\ 2 \end{pmatrix} \begin{pmatrix} 4 \\ 3 \end{pmatrix} \begin{pmatrix} 4 \\ 4 \end{pmatrix}$$

1 4 6 4 1

$$\begin{pmatrix} 5 \\ 0 \end{pmatrix} \begin{pmatrix} 5 \\ 1 \end{pmatrix} \begin{pmatrix} 5 \\ 2 \end{pmatrix} \begin{pmatrix} 5 \\ 3 \end{pmatrix} \begin{pmatrix} 5 \\ 4 \end{pmatrix} \begin{pmatrix} 5 \\ 5 \end{pmatrix}$$

1 5 10 10 5 1

$$\begin{pmatrix} 6 \\ 0 \end{pmatrix} \begin{pmatrix} 6 \\ 1 \end{pmatrix} \begin{pmatrix} 6 \\ 2 \end{pmatrix} \begin{pmatrix} 6 \\ 3 \end{pmatrix} \begin{pmatrix} 6 \\ 4 \end{pmatrix} \begin{pmatrix} 6 \\ 5 \end{pmatrix} \begin{pmatrix} 6 \\ 6 \end{pmatrix}$$

1    6    15    20    15    6    1

$$\left(\begin{array}{c} 7 \\ 0 \end{array}\right) \left(\begin{array}{c} 7 \\ 1 \end{array}\right) \left(\begin{array}{c} 7 \\ 2 \end{array}\right) \left(\begin{array}{c} 7 \\ 3 \end{array}\right) \left(\begin{array}{c} 7 \\ 4 \end{array}\right) \left(\begin{array}{c} 7 \\ 5 \end{array}\right) \left(\begin{array}{c} 7 \\ 6 \end{array}\right) \left(\begin{array}{c} 7 \\ 7 \end{array}\right)$$

1 7 21 35 35 21 7 1

$$\left(\begin{matrix} 8 \\ 0 \end{matrix}\right) \left(\begin{matrix} 8 \\ 1 \end{matrix}\right) \left(\begin{matrix} 8 \\ 2 \end{matrix}\right) \left(\begin{matrix} 8 \\ 3 \end{matrix}\right) \left(\begin{matrix} 8 \\ 4 \end{matrix}\right) \left(\begin{matrix} 8 \\ 5 \end{matrix}\right) \left(\begin{matrix} 8 \\ 6 \end{matrix}\right) \left(\begin{matrix} 8 \\ 7 \end{matrix}\right) \left(\begin{matrix} 8 \\ 8 \end{matrix}\right)$$

1 8 28 56 70 56 28 8 1

• • •

• • •

(a)

(b)

## **FIGURE 1** Pascal's Triangle.

**VANDERMONDE'S IDENTITY** Let  $m$ ,  $n$ , and  $r$  be nonnegative integers with  $r$  not exceeding either  $m$  or  $n$ . Then

$$\binom{m+n}{r} = \sum_{k=0}^r \binom{m}{r-k} \binom{n}{k}.$$

**Remark:** This identity was discovered by mathematician Alexandre-Théophile Vandermonde in the eighteenth century.

**Proof:** Suppose that there are  $m$  items in one set and  $n$  items in a second set. Then the total number of ways to pick  $r$  elements from the union of these sets is  $\binom{m+n}{r}$ .

Another way to pick  $r$  elements from the union is to pick  $k$  elements from the second set and then  $r - k$  elements from the first set, where  $k$  is an integer with  $0 \leq k \leq r$ . Because there are  $\binom{n}{k}$  ways to choose  $k$  elements from the second set and  $\binom{m}{r-k}$  ways to choose  $r - k$  elements from the first set, the product rule tells us that this can be done in  $\binom{m}{r-k} \binom{n}{k}$  ways. Hence, the total number of ways to pick  $r$  elements from the union also equals  $\sum_{k=0}^r \binom{m}{r-k} \binom{n}{k}$ .

We have found two expressions for the number of ways to pick  $r$  elements from the union of a set with  $m$  items and a set with  $n$  items. Equating them gives us Vandermonde's identity. 

## Corollary

If  $n$  is a nonnegative integer, then

$$\binom{2n}{n} = \sum_{k=0}^n \binom{n}{k}^2.$$

**Proof:** We use Vandermonde's identity with  $m = r = n$  to obtain

$$\binom{2n}{n} = \sum_{k=0}^n \binom{n}{n-k} \binom{n}{k} = \sum_{k=0}^n \binom{n}{k}^2.$$

The last equality was obtained using the identity  $\binom{n}{k} = \binom{n}{n-k}$ . 

# Proof of this theorem left for exercise

Let  $n$  and  $r$  be nonnegative integers with  $r \leq n$ . Then

$$\binom{n+1}{r+1} = \sum_{j=r}^n \binom{j}{r}.$$

# Unit 4

**Relations - Relations, Equivalence and Partial Order Relations, Partition and Equivalence Classes, Closure of Relation, Representation and Operation on Relations, Posets, Totally Ordered Sets, Well-Ordered Sets, Least and Maximum Elements, Least Upper Bound, Greatest Lower Bound, Lattice;**

In mathematics we study relationships such as those between a positive integer and one that it divides, an integer and one that it is congruent to modulo 5, a real number and one that is larger than it, a real number  $x$  and the value  $f(x)$  where  $f$  is a function, and so on.

Relationships between elements of sets are represented using the structure called a relation, which is just a subset of the Cartesian product of the sets.

Relations can be used to solve problems such as determining which pairs of cities are linked by airline flights in a network, or producing a useful way to store information in computer databases etc.

# Unit 4

**Relations - Relations, Equivalence and Partial Order Relations, Partition and Equivalence Classes, Closure of Relation, Representation and Operation on Relations, Posets, Totally Ordered Sets, Well-Ordered Sets, Least and Maximum Elements, Least Upper Bound, Greatest Lower Bound, Lattice;**

In mathematics we study relationships such as those between a positive integer and one that it divides, an integer and one that it is congruent to modulo 5, a real number and one that is larger than it, a real number  $x$  and the value  $f(x)$  where  $f$  is a function, and so on.

Relationships between elements of sets are represented using the structure called a relation, which is just a subset of the Cartesian product of the sets.

Relations can be used to solve problems such as determining which pairs of cities are linked by airline flights in a network, or producing a useful way to store information in computer databases etc.

# Relations and Their Properties

The most direct way to express a relationship between elements of two sets is to use ordered pairs made up of two related elements. For this reason, sets of ordered pairs are called binary relations.

**Definition:** Let A and B be sets. A binary relation from A to B is a subset of  $A \times B$ .

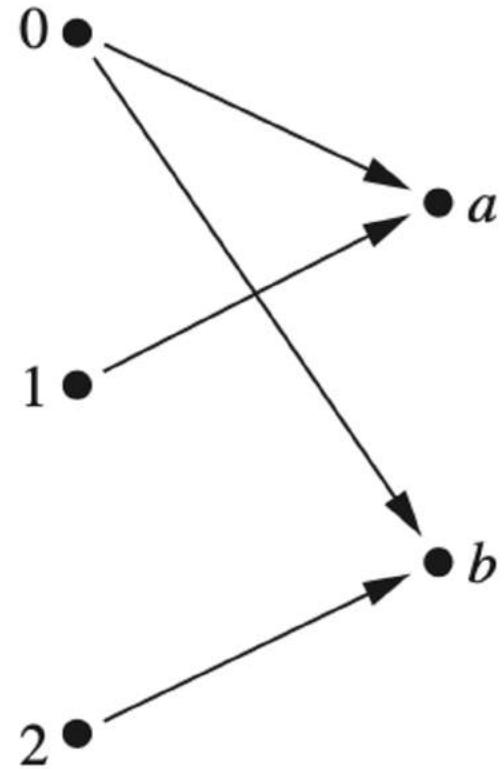
In other words, a binary relation from A to B is a set R of ordered pairs where the first element of each ordered pair comes from A and the second element comes from B.

# Notation

We use the notation  $aRb$  to denote that  $(a,b) \in R$  and  $aRb$  to denote that  $(a,b) \in R$ . Moreover, when  $(a,b)$  belongs to  $R$ ,  $a$  is said to be related to  $b$  by  $R$ .

Binary relations represent relationships between the elements of two sets. We will introduce n-ary relations, which express relationships among elements of more than two sets later.

Let  $A = \{0,1,2\}$  and  $B = \{a,b\}$ . Then  $\{(0,a),(0,b),(1,a),(2,b)\}$  is a relation from  $A$  to  $B$ . This means, for instance, that  $0 R a$ , ~~but~~ that  $1 R b$ . Relations can be represented graphically, as shown in Figure 1, using arrows to represent ordered pairs. Another way to represent this relation is to use a table, which is also done in Figure 1.



$R$	$a$	$b$
0	×	×
1	×	
2		×

**FIGURE 1** Displaying the Ordered Pairs in the Relation  $R$  from Example

See other examples from Page 573-574

# Functions as Relations

We studied functions before. Answer the following basic question.

**Question:** Functions can be defined as relations. How?

# Relations on a Set

Relations from a set A to itself are of special interest.

**Definition:** A relation on a set A is a relation from A to A.

In other words, a relation on a set A is a subset of  $A \times A$ .

**Example 1:** Let A be the set {1, 2, 3, 4}. Which ordered pairs are in the relation  $R = \{(a, b) \mid a \text{ divides } b\}$ ?

## Solution

Because  $(a, b)$  is in  $R$  if and only if  $a$  and  $b$  are positive integers not exceeding 4 such that  $a$  divides  $b$ , we see that

$$R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)\}.$$

## Example 2

Consider these relations on the set of integers:

$$R_1 = \{(a, b) \mid a \leq b\},$$

$$R_2 = \{(a, b) \mid a > b\},$$

$$R_3 = \{(a, b) \mid a = b \text{ or } a = -b\},$$

$$R_4 = \{(a, b) \mid a = b\},$$

$$R_5 = \{(a, b) \mid a = b + 1\},$$

$$R_6 = \{(a, b) \mid a + b \leq 3\}.$$

Which of these relations contain each of the pairs  $(1, 1)$ ,  $(1, 2)$ ,  $(2, 1)$ ,  $(1, -1)$ , and  $(2, 2)$ ?

## Example 2

Consider these relations on the set of integers:

$$R_1 = \{(a, b) \mid a \leq b\},$$

$$R_2 = \{(a, b) \mid a > b\},$$

$$R_3 = \{(a, b) \mid a = b \text{ or } a = -b\},$$

$$R_4 = \{(a, b) \mid a = b\},$$

$$R_5 = \{(a, b) \mid a = b + 1\},$$

$$R_6 = \{(a, b) \mid a + b \leq 3\}.$$

Which of these relations contain each of the pairs  $(1, 1)$ ,  $(1, 2)$ ,  $(2, 1)$ ,  $(1, -1)$ , and  $(2, 2)$ ?

**Solution:** The pair  $(1, 1)$  is in  $R_1$ ,  $R_3$ ,  $R_4$ , and  $R_6$ ;  $(1, 2)$  is in  $R_1$  and  $R_6$ ;  $(2, 1)$  is in  $R_2$ ,  $R_5$ , and  $R_6$ ;  $(1, -1)$  is in  $R_2$ ,  $R_3$ , and  $R_6$ ; and finally,  $(2, 2)$  is in  $R_1$ ,  $R_3$ , and  $R_4$ .

# Problem

How many relations are there on a set with  $n$  elements?

# Properties of Relations: Reflexive

There are several properties that are used to classify relations on a set. In some relations an element is always related to itself. For instance, let  $R$  be the relation on the set of all people consisting of pairs  $(x, y)$  where  $x$  and  $y$  have the same mother and the same father. Then  $xRx$  for every person  $x$ .

# Reflexive

**Definition:** A relation  $R$  on a set  $A$  is called reflexive if  $(a,a) \in R$  for every element  $a \in A$ .

**Remark:** Using quantifiers we see that the relation  $R$  on the set  $A$  is reflexive if  $\forall a((a, a) \in R)$ , where the universe of discourse is the set of all elements in  $A$ .

## Example 3

Consider the following relations on  $\{1, 2, 3, 4\}$ :

$$R_1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\},$$

$$R_2 = \{(1, 1), (1, 2), (2, 1)\},$$

$$R_3 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\},$$

$$R_4 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\},$$

$$R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\},$$

$$R_6 = \{(3, 4)\}.$$

Which of these relations are reflexive?

The relations R3 and R5 are reflexive because they both contain all pairs of the form  $(a, a)$ , namely,  $(1, 1)$ ,  $(2, 2)$ ,  $(3, 3)$ , and  $(4, 4)$ . The other relations are not reflexive because they do not contain all of these ordered pairs. In particular, R1, R2, R4, and R6 are not reflexive because  $(3, 3)$  is not in any of these relations.

# Problem

Which of the relations from Example 2 are reflexive?

**Solution:** The reflexive relations from Example 2 are  $R_1$  (because  $a \leq a$  for every integer  $a$ ),  $R_3$ , and  $R_4$ . For each of the other relations in this example it is easy to find a pair of the form  $(a, a)$  that is not in the relation. (This is left as an exercise for the reader.)

# Problem

Is the “divides” relation on the set of positive integers reflexive?

Is the “divides” relation on the set of positive integers reflexive?

**Solution:** Because  $a \mid a$  whenever  $a$  is a positive integer, the “divides” relation is reflexive. (Note that if we replace the set of positive integers with the set of all integers the relation is not reflexive because by definition 0 does not divide 0.)

# Symmetric

In some relations an element is related to a second element if and only if the second element is also related to the first element. The relation consisting of pairs  $(x,y)$ , where  $x$  and  $y$  are students at your school with at least one common class has this property.

**Definition:** A relation  $R$  on a set  $A$  is called symmetric if  $(b,a) \in R$  whenever  $(a,b) \in R$ , for all  $a,b \in A$ . A relation  $R$  on a set  $A$  such that for all  $a, b \in A$ , if  $(a, b) \in R$  and  $(b, a) \in R$ , then  $a = b$  is called antisymmetric.

**Remark:** Using quantifiers, we see that the relation  $R$  on the set  $A$  is symmetric if  $\forall a \forall b ((a, b) \in R \rightarrow (b, a) \in R)$ . Similarly, the relation  $R$  on the set  $A$  is antisymmetric if  $\forall a \forall b (((a, b) \in R \wedge (b, a) \in R) \rightarrow (a = b))$ .

That is, a relation is symmetric if and only if  $a$  is related to  $b$  implies that  $b$  is related to  $a$ . A relation is antisymmetric if and only if there are no pairs of distinct elements  $a$  and  $b$  with  $a$  related to  $b$  and  $b$  related to  $a$ . That is, the only way to have  $a$  related to  $b$  and  $b$  related to  $a$  is for  $a$  and  $b$  to be the same element.

**Note:** The terms symmetric and antisymmetric are not opposites, because a relation can have both of these properties or may lack both of them. A relation cannot be both symmetric and antisymmetric if it contains some pair of the form  $(a, b)$ , where  $a = b$ .

# Problem

Which of the relations from Example 3 are symmetric and which are antisymmetric?

# Problem

Which of the relations from Example 2 are symmetric and which are antisymmetric?

## Example

Is the “divides” relation on the set of positive integers symmetric? Is it antisymmetric?

## Example

Is the “divides” relation on the set of positive integers symmetric? Is it antisymmetric?

**Solution:** This relation is not symmetric because  $1|2$ , but  $2 \nmid 1$ . It is antisymmetric, for if  $a$  and  $b$  are positive integers with  $a | b$  and  $b | a$ , then  $a = b$ .

# Transitive

Let  $R$  be the relation consisting of all pairs  $(x, y)$  of students at your school, where  $x$  has taken more credits than  $y$ . Suppose that  $x$  is related to  $y$  and  $y$  is related to  $z$ . This means that  $x$  has taken more credits than  $y$  and  $y$  has taken more credits than  $z$ . We can conclude that  $x$  has taken more credits than  $z$ , so that  $x$  is related to  $z$ . What we have shown is that  $R$  has the transitive property, which is defined as follows.

# Definition

A relation  $R$  on a set  $A$  is called transitive if whenever  $(a,b) \in R$  and  $(b,c) \in R$ , then  $(a,c) \in R$ , for all  $a,b,c \in A$ .

**Remark:** Using quantifiers we see that the relation  $R$  on a set  $A$  is transitive if we have  $\forall a \forall b \forall c ((a, b) \in R \wedge (b, c) \in R) \rightarrow (a, c) \in R$ .

# Transitive

Let  $R$  be the relation consisting of all pairs  $(x, y)$  of students at your school, where  $x$  has taken more credits than  $y$ . Suppose that  $x$  is related to  $y$  and  $y$  is related to  $z$ . This means that  $x$  has taken more credits than  $y$  and  $y$  has taken more credits than  $z$ . We can conclude that  $x$  has taken more credits than  $z$ , so that  $x$  is related to  $z$ . What we have shown is that  $R$  has the transitive property, which is defined as follows.

# Definition

A relation  $R$  on a set  $A$  is called transitive if whenever  $(a,b) \in R$  and  $(b,c) \in R$ , then  $(a,c) \in R$ , for all  $a,b,c \in A$ .

**Remark:** Using quantifiers we see that the relation  $R$  on a set  $A$  is transitive if we have  $\forall a \forall b \forall c ((a, b) \in R \wedge (b, c) \in R) \rightarrow (a, c) \in R$ .

# Problem

Which of the relations in Example 3 are transitive?

# Problem

Which of the relations in Example 2 are transitive?

# Example

Is the “divides” relation on the set of positive integers transitive?

## Example

Is the “divides” relation on the set of positive integers transitive?

**Solution:** Suppose that  $a$  divides  $b$  and  $b$  divides  $c$ . Then there are positive integers  $k$  and  $l$  such that  $b = ak$  and  $c = bl$ . Hence,  $c = a(kl)$ , so  $a$  divides  $c$ . It follows that this relation is transitive.

Problem left for exercise

How many reflexive relations are there on a set with  $n$  elements?

# Relations

# Combining Relations: Operations

Because relations from A to B are subsets of  $A \times B$ , two relations from A to B can be combined in any way two sets can be combined.

## Example 1

Let  $A = \{1, 2, 3\}$  and  $B = \{1, 2, 3, 4\}$ . The relations  $R_1 = \{(1, 1), (2, 2), (3, 3)\}$  and  $R_2 = \{(1, 1), (1, 2), (1, 3), (1, 4)\}$  can be combined to obtain

$$R_1 \cup R_2 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (3, 3)\},$$

$$R_1 \cap R_2 = \{(1, 1)\},$$

$$R_1 - R_2 = \{(2, 2), (3, 3)\},$$

$$R_2 - R_1 = \{(1, 2), (1, 3), (1, 4)\}.$$

## Example 2

Let  $R_1$  be the “less than” relation on the set of real numbers and let  $R_2$  be the “greater than” relation on the set of real numbers, that is,  $R_1 = \{(x, y) \mid x < y\}$  and  $R_2 = \{(x, y) \mid x > y\}$ . What are  $R_1 \cup R_2$ ,  $R_1 \cap R_2$ ,  $R_1 - R_2$ ,  $R_2 - R_1$ , and  $R_1 \oplus R_2$ ?

**Solution:** We note that  $(x, y) \in R_1 \cup R_2$  if and only if  $(x, y) \in R_1$  or  $(x, y) \in R_2$ . Hence,  $(x, y) \in R_1 \cup R_2$  if and only if  $x < y$  or  $x > y$ . Because the condition  $x < y$  or  $x > y$  is the same as the condition  $x \neq y$ , it follows that  $R_1 \cup R_2 = \{(x, y) \mid x \neq y\}$ . In other words, the union of the “less than” relation and the “greater than” relation is the “not equals” relation.

Next, note that it is impossible for a pair  $(x, y)$  to belong to both  $R_1$  and  $R_2$  because it is impossible that  $x < y$  and  $x > y$ . It follows that  $R_1 \cap R_2 = \emptyset$ . We also see that  $R_1 - R_2 = R_1$ ,  $R_2 - R_1 = R_2$ , and  $R_1 \oplus R_2 = R_1 \cup R_2 - R_1 \cap R_2 = \{(x, y) \mid x \neq y\}$ . 

Go through other examples of the book.

There is another way that relations are combined that is analogous to the composition of functions.

Let  $R$  be a relation from a set  $A$  to a set  $B$  and  $S$  a relation from  $B$  to a set  $C$ . The composite of  $R$  and  $S$  is the relation consisting of ordered pairs  $(a, c)$ , where  $a \in A$ ,  $c \in C$ , and for which there exists an element  $b \in B$  such that  $(a, b) \in R$  and  $(b, c) \in S$ . We denote the composite of  $R$  and  $S$  by  $S \circ R$ .

Computing the composite of two relations requires that we find elements that are the second element of ordered pairs in the first relation and the first element of ordered pairs in the second relation.

**Example 3:** What is the composite of the relations R and S, where R is the relation from {1, 2, 3} to {1, 2, 3, 4} with  $R = \{(1,1),(1,4),(2,3),(3,1),(3,4)\}$  and S is the relation from {1,2,3,4} to {0,1,2} with  $S = \{(1, 0), (2, 0), (3, 1), (3, 2), (4, 1)\}$ ?

**Solution:**  $S \circ R$  is constructed using all ordered pairs in  $R$  and ordered pairs in  $S$ , where the second element of the ordered pair in  $R$  agrees with the first element of the ordered pair in  $S$ . For example, the ordered pairs  $(2, 3)$  in  $R$  and  $(3, 1)$  in  $S$  produce the ordered pair  $(2, 1)$  in  $S \circ R$ . Computing all the ordered pairs in the composite, we find  $S \circ R = \{(1,0),(1,1),(2,1),(2,2),(3,0),(3,1)\}$ .

Go through other examples of the book.

# Definition

Let  $R$  be a relation on the set  $A$ . The powers  $R^n$ ,  $n = 1, 2, 3, \dots$ , are defined recursively by

$$R^1 = R \quad \text{and} \quad R^{n+1} = R^n \circ R.$$

## Example 4

The definition shows that  $R^2 = R \circ R$ ,  $R^3 = R^2 \circ R = (R \circ R) \circ R$ , and so on.

Let  $R = \{(1, 1), (2, 1), (3, 2), (4, 3)\}$ . Find the powers  $R^n$ ,  $n = 2, 3, 4, \dots$ .

**Solution:** Because  $R^2 = R \circ R$ , we find that  $R^2 = \{(1, 1), (2, 1), (3, 1), (4, 2)\}$ . Furthermore, because  $R^3 = R^2 \circ R$ ,  $R^3 = \{(1, 1), (2, 1), (3, 1), (4, 1)\}$ . Additional computation shows that  $R^4$  is the same as  $R^3$ , so  $R^4 = \{(1, 1), (2, 1), (3, 1), (4, 1)\}$ . It also follows that  $R^n = R^3$  for  $n = 5, 6, 7, \dots$ . The reader should verify this. 

# Theorem

The relation  $R$  on a set  $A$  is transitive if and only if  $R^n \subseteq R$  for  $n = 1, 2, 3, \dots$ .

Proof of this theorem is left for exercise.

# Representing Relations

There are many ways to represent a relation between finite sets. As we have seen, one way is to list its ordered pairs. Another way to represent a relation is to use a table. In this section we will discuss two alternative methods for representing relations.

# Representing Relations using Matrices

A relation between finite sets can be represented using a zero–one matrix. Suppose that  $R$  is a relation from  $A = \{a_1, a_2, \dots, a_m\}$  to  $B = \{b_1, b_2, \dots, b_n\}$ . (Here the elements of the sets  $A$  and  $B$  have been listed in a particular, but arbitrary, order. Furthermore, when  $A = B$  we use the same ordering for  $A$  and  $B$ .) The relation  $R$  can be represented by the matrix  $\mathbf{M}_R = [m_{ij}]$ , where

$$m_{ij} = \begin{cases} 1 & \text{if } (a_i, b_j) \in R, \\ 0 & \text{if } (a_i, b_j) \notin R. \end{cases}$$

In other words, the zero–one matrix representing  $R$  has a 1 as its  $(i, j)$  entry when  $a_i$  is related to  $b_j$ , and a 0 in this position if  $a_i$  is not related to  $b_j$ . (Such a representation depends on the orderings used for  $A$  and  $B$ .)

## Example 5

Suppose that  $A = \{1, 2, 3\}$  and  $B = \{1, 2\}$ . Let  $R$  be the relation from  $A$  to  $B$  containing  $(a, b)$  if  $a \in A$ ,  $b \in B$ , and  $a > b$ . What is the matrix representing  $R$  if  $a_1 = 1$ ,  $a_2 = 2$ , and  $a_3 = 3$ , and  $b_1 = 1$  and  $b_2 = 2$ ?

**Solution:** Because  $R = \{(2, 1), (3, 1), (3, 2)\}$ , the matrix for  $R$  is

$$\mathbf{M}_R = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

The 1s in  $\mathbf{M}_R$  show that the pairs  $(2, 1)$ ,  $(3, 1)$ , and  $(3, 2)$  belong to  $R$ . The 0s show that no other pairs belong to  $R$ . 

# Problem

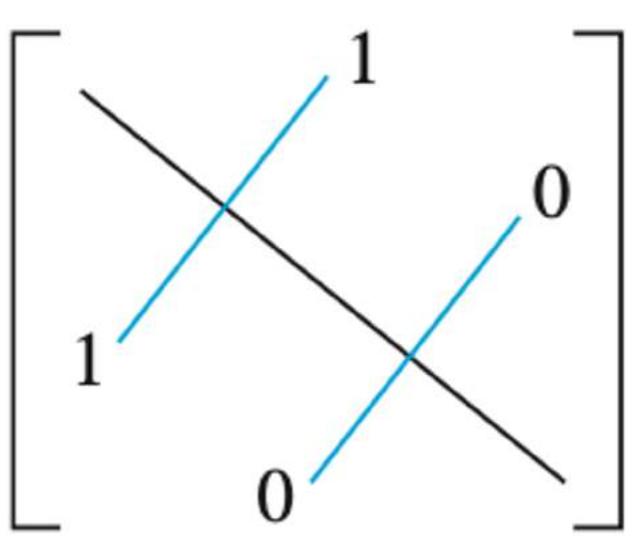
How to represent Reflexive relation using matrices?

$$\begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & \ddots & \\ & & & & & 1 & \\ & & & & & & 1 \end{bmatrix}$$

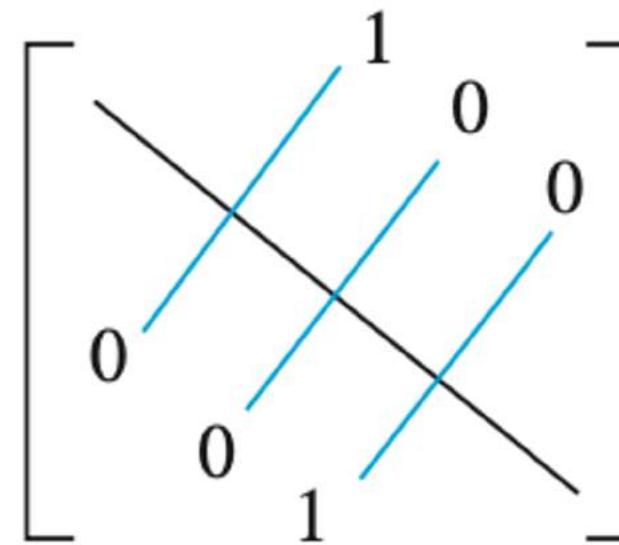
**FIGURE 1** The Zero–One Matrix for a Reflexive Relation. (Off Diagonal Elements Can Be 0 or 1.)

# Problem

How to represent Symmetric and Anti-symmetric relations using matrices?



(a) Symmetric



(b) Antisymmetric

**FIGURE 2** The Zero–One Matrices for Symmetric and Antisymmetric Relations.

## Problem

Suppose that the relation  $R$  on a set is represented by the matrix

$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

Is  $R$  reflexive, symmetric, and/or antisymmetric?

**Solution:** Because all the diagonal elements of this matrix are equal to 1,  $R$  is reflexive. Moreover, because  $\mathbf{M}_R$  is symmetric, it follows that  $R$  is symmetric. It is also easy to see that  $R$  is not antisymmetric. 

# Representing Relations using Digraphs

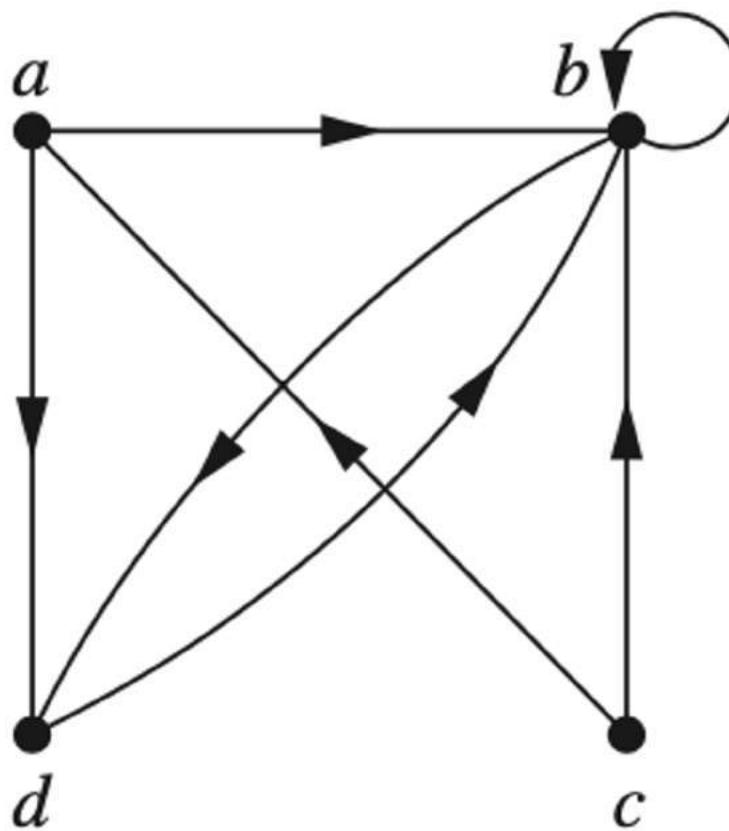
There is another important way of representing a relation using a pictorial representation. Each element of the set is represented by a point, and each ordered pair is represented using an arc with its direction indicated by an arrow. We use such pictorial representations when we think of relations on a finite set as directed graphs, or digraphs.

**Definition:** A directed graph, or digraph, consists of a set  $V$  of vertices (or nodes) together with a set  $E$  of ordered pairs of elements of  $V$  called edges (or arcs). The vertex  $a$  is called the initial vertex of the edge  $(a, b)$ , and the vertex  $b$  is called the terminal vertex of this edge.

An edge of the form  $(a, a)$  is represented using an arc from the vertex  $a$  back to itself. Such an edge is called a loop.

# Example

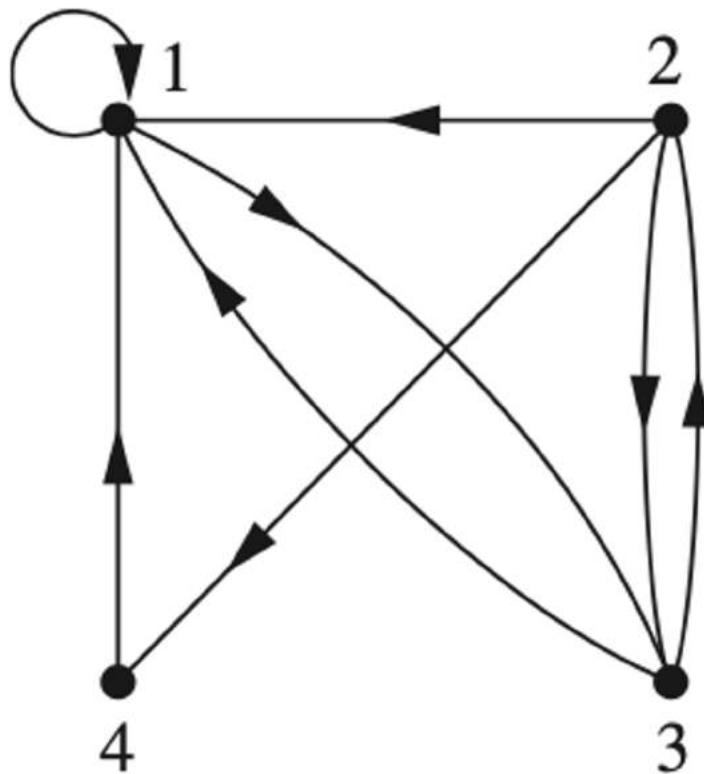
The directed graph with vertices a, b, c, and d, and edges (a, b), (a, d), (b, b), (b, d), (c, a), (c, b), and (d, b) is displayed in the Figure.



The relation  $R$  on a set  $A$  is represented by the directed graph that has the elements of  $A$  as its vertices and the ordered pairs  $(a, b)$ , where  $(a, b) \in R$ , as edges. This assignment sets up a one- to-one correspondence between the relations on a set  $A$  and the directed graphs with  $A$  as their set of vertices.

Note that relations from a set  $A$  to a set  $B$  can be represented by a directed graph where there is a vertex for each element of  $A$  and a vertex for each element of  $B$ .

The directed graph of the relation  $R = \{(1,1), (1,3), (2,1), (2,3), (2,4), (3,1), (3,2), (4,1)\}$  on the set  $\{1, 2, 3, 4\}$  is shown in Figure.



The directed graph representing a relation can be used to determine whether the relation has various properties.

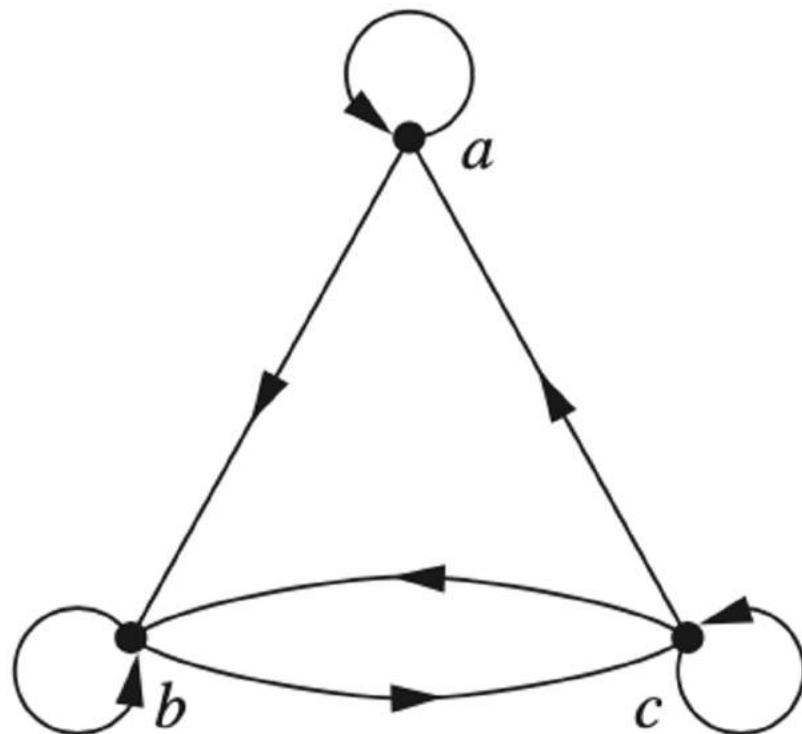
For instance, a relation is reflexive if and only if there is a loop at every vertex of the directed graph, so that every ordered pair of the form  $(x, x)$  occurs in the relation.

A relation is symmetric if and only if for every edge between distinct vertices in its digraph there is an edge in the opposite direction, so that  $(y,x)$  is in the relation whenever  $(x,y)$  is in the relation.

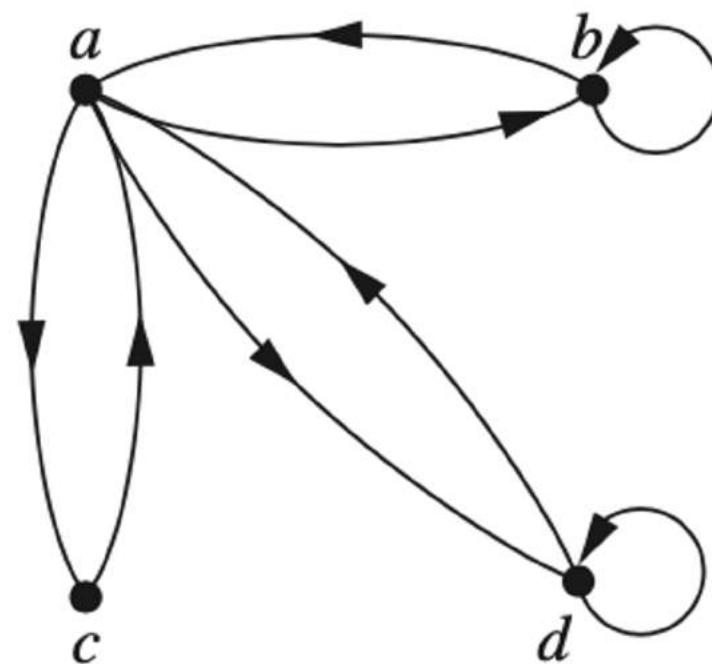
Similarly, a relation is antisymmetric if and only if there are never two edges in opposite directions between distinct vertices.

Finally, a relation is transitive if and only if whenever there is an edge from a vertex  $x$  to a vertex  $y$  and an edge from a vertex  $y$  to a vertex  $z$ , there is an edge from  $x$  to  $z$  (completing a triangle where each side is a directed edge with the correct direction).

Determine whether the relations for the directed graphs shown in Figure are reflexive, symmetric, antisymmetric, and/or transitive.



(a) Directed graph of  $R$



(b) Directed graph of  $S$

# Closures of Relations

In general, let  $R$  be a relation on a set  $A$ .  $R$  may or may not have some property  $P$ , such as reflexivity, symmetry, or transitivity. If there is a relation  $S$  with property  $P$  containing  $R$  such that  $S$  is a subset of every relation with property  $P$  containing  $R$ , then  $S$  is called the closure of  $R$  with respect to  $P$ .

(Note that the closure of a relation with respect to a property may not exist; see Exercises 15 and 35.) We will see how reflexive, symmetric, and transitive closures of relations can be found.

# Reflexive Closure

The relation  $R = \{(1, 1), (1, 2), (2, 1), (3, 2)\}$  on the set  $A = \{1, 2, 3\}$  is not reflexive. How can we produce a reflexive relation containing  $R$  that is as small as possible?

The relation  $R = \{(1, 1), (1, 2), (2, 1), (3, 2)\}$  on the set  $A = \{1, 2, 3\}$  is not reflexive. How can we produce a reflexive relation containing  $R$  that is as small as possible? This can be done by adding  $(2, 2)$  and  $(3, 3)$  to  $R$ , because these are the only pairs of the form  $(a, a)$  that are not in  $R$ . Clearly, this new relation contains  $R$ .

Furthermore, any reflexive relation that contains  $R$  must also contain  $(2, 2)$  and  $(3, 3)$ . Because this relation contains  $R$ , is reflexive, and is contained within every reflexive relation that contains  $R$ , it is called the **reflexive closure** of  $R$ .

As this example illustrates, given a relation  $R$  on a set  $A$ , the reflexive closure of  $R$  can be formed by adding to  $R$  all pairs of the form  $(a, a)$  with  $a \in A$ , not already in  $R$ . The addition of these pairs produces a new relation that is reflexive, contains  $R$ , and is contained within any reflexive relation containing  $R$ . We see that the reflexive closure of  $R$  equals  $R \cup \Delta$ , where  $\Delta = \{(a, a) \mid a \in A\}$  is the **diagonal relation** on  $A$ . (The reader should verify this.)

## Example 1

What is the reflexive closure of the relation  $R = \{(a, b) \mid a < b\}$  on the set of integers?

## Example 1

What is the reflexive closure of the relation  $R = \{(a, b) \mid a < b\}$  on the set of integers?

**Solution:** The reflexive closure of  $R$  is

$$R \cup \Delta = \{(a, b) \mid a < b\} \cup \{(a, a) \mid a \in \mathbf{Z}\} = \{(a, b) \mid a \leq b\}.$$

# Symmetric Closure

The relation  $\{(1, 1), (1, 2), (2, 2), (2, 3), (3, 1), (3, 2)\}$  on  $\{1, 2, 3\}$  is not symmetric. How can we produce a symmetric relation that is as small as possible and contains R?

# Symmetric Closure

The relation  $\{(1, 1), (1, 2), (2, 2), (2, 3), (3, 1), (3, 2)\}$  on  $\{1, 2, 3\}$  is not symmetric. How can we produce a symmetric relation that is as small as possible and contains  $R$ ?

To do this, we need only add  $(2, 1)$  and  $(1, 3)$ , because these are the only pairs of the form  $(b,a)$  with  $(a, b) \in R$  that are not in  $R$ . This new relation is symmetric and contains  $R$ . Furthermore, any symmetric relation that contains  $R$  must contain this new relation, because a symmetric relation that contains  $R$  must contain  $(2, 1)$  and  $(1, 3)$ . Consequently, this new relation is called the **symmetric closure** of  $R$ .

# Symmetric Closure

As this example illustrates, the symmetric closure of a relation  $R$  can be constructed by adding all ordered pairs of the form  $(b,a)$ , where  $(a,b)$  is in the relation, that are not already present in  $R$ . Adding these pairs produces a relation that is symmetric, that contains  $R$ , and that is contained in any symmetric relation that contains  $R$ . The symmetric closure of a relation can be constructed by taking the union of a relation with its inverse; that is,  $R \cup R^{-1}$  is the symmetric closure of  $R$ , where  $R^{-1} = \{(b, a) \mid (a, b) \in R\}$ .

## Example 2

What is the symmetric closure of the relation  $R = \{(a, b) \mid a > b\}$  on the set of positive integers?

## Example 2

What is the symmetric closure of the relation  $R = \{(a, b) \mid a > b\}$  on the set of positive integers?

Solution: The symmetric closure of  $R$  is the relation  $R \cup R^{-1} = \{(a,b) \mid a > b\} \cup \{(b,a) \mid a > b\} = \{(a,b) \mid a \neq b\}$ .

# Transitive closure

Consider the relation  $R = \{(1, 3), (1, 4), (2, 1), (3, 2)\}$  on the set  $\{1, 2, 3, 4\}$ . This relation is not transitive because it does not contain all pairs of the form  $(a,c)$  where  $(a,b)$  and  $(b,c)$  are in  $R$ . The pairs of this form not in  $R$  are  $(1, 2)$ ,  $(2, 3)$ ,  $(2, 4)$ , and  $(3, 1)$ . Adding these pairs does not produce a transitive relation, because the resulting relation contains  $(3, 1)$  and  $(1, 4)$  but does not contain  $(3, 4)$ . This shows that constructing the transitive closure of a relation is more complicated than constructing either the reflexive or symmetric closure.

Read pages 599-603 to understand the algorithm to find Transitive Closure. We are here showing only the algorithm. The proof is left for the reader to explore.

## Theorem

Let  $\mathbf{M}_R$  be the zero–one matrix of the relation  $R$  on a set with  $n$  elements. Then the zero–one matrix of the transitive closure  $R^*$  is

$$\mathbf{M}_{R^*} = \mathbf{M}_R \vee \mathbf{M}_R^{[2]} \vee \mathbf{M}_R^{[3]} \vee \dots \vee \mathbf{M}_R^{[n]}.$$

Read page 593 to understand the notations, join, boolean product and power of matrices.

## Example 3

Find the zero–one matrix of the transitive closure of the relation  $R$  where

$$\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

*Solution:* By Theorem 3, it follows that the zero–one matrix of  $R^*$  is

$$\mathbf{M}_{R^*} = \mathbf{M}_R \vee \mathbf{M}_R^{[2]} \vee \mathbf{M}_R^{[3]}.$$

Because

$$\mathbf{M}_R^{[2]} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad \mathbf{M}_R^{[3]} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix},$$

$$\mathbf{M}_{R^*} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} \vee \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \vee \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

# Equivalence Relations

Consider this relation. The integers  $a$  and  $b$  are related by the “congruence modulo 4” relation when 4 divides  $a - b$ .

Is this relation reflexive?

Consider this relation. The integers  $a$  and  $b$  are related by the “congruence modulo 4” relation when 4 divides  $a - b$ .

Is this relation symmetric?

Consider this relation. The integers  $a$  and  $b$  are related by the “congruence modulo 4” relation when 4 divides  $a - b$ .

Is this relation transitive?

Consider this relation. The integers  $a$  and  $b$  are related by the “congruence modulo 4” relation when 4 divides  $a - b$ .

This relation is reflexive, symmetric, and transitive. It is not hard to see that  $a$  is related to  $b$  if and only if  $a$  and  $b$  have the same remainder when divided by 4. It follows that this relation splits the set of integers into four different classes. When we care only what remainder an integer leaves when it is divided by 4, we need only know which class it is in, not its particular value.

This is an example of equivalence relation, namely, relations that are reflexive, symmetric, and transitive.

In this section we will study relations with a particular combination of properties that allows them to be used to relate objects that are similar in some way.

Definition: A relation on a set  $A$  is called an equivalence relation if it is reflexive, symmetric, and transitive.

In an equivalence relation, when two elements are related it makes sense to say they are equivalent.

**Definition:** Two elements  $a$  and  $b$  that are related by an equivalence relation are called equivalent. The notation  $a \sim b$  is often used to denote that  $a$  and  $b$  are equivalent elements with respect to a particular equivalence relation.

For the notion of equivalent elements to make sense, every element should be equivalent to itself, as the reflexive property guarantees for an equivalence relation. It makes sense to say that a and b are related (not just that a is related to b) by an equivalence relation, because when a is related to b, by the symmetric property, b is related to a. Furthermore, because an equivalence relation is transitive, if a and b are equivalent and b and c are equivalent, it follows that a and c are equivalent.

## Example 1

Let  $R$  be the relation on the set of integers such that  $aRb$  if and only if  $a=b$  or  $a=-b$ .

Is it an equivalence relation?

## Example 2

Let  $R$  be the relation on the set of real numbers such that  $aRb$  if and only if  $a - b$  is an integer.

Is it an equivalence relation?

One of the most widely used equivalence relations is congruence modulo  $m$ , where  $m$  is an integer greater than 1.

**Congruence Modulo  $m$**  Let  $m$  be an integer with  $m > 1$ . Show that the relation

$$R = \{(a, b) \mid a \equiv b \pmod{m}\}$$

is an equivalence relation on the set of integers.

**Solution:** Recall from Section 4.1 that  $a \equiv b \pmod{m}$  if and only if  $m$  divides  $a - b$ . Note that  $a - a = 0$  is divisible by  $m$ , because  $0 = 0 \cdot m$ . Hence,  $a \equiv a \pmod{m}$ , so congruence modulo  $m$  is reflexive. Now suppose that  $a \equiv b \pmod{m}$ . Then  $a - b$  is divisible by  $m$ , so  $a - b = km$ , where  $k$  is an integer. It follows that  $b - a = (-k)m$ , so  $b \equiv a \pmod{m}$ . Hence, congruence modulo  $m$  is symmetric. Next, suppose that  $a \equiv b \pmod{m}$  and  $b \equiv c \pmod{m}$ . Then  $m$  divides both  $a - b$  and  $b - c$ . Therefore, there are integers  $k$  and  $l$  with  $a - b = km$  and  $b - c = lm$ . Adding these two equations shows that  $a - c = (a - b) + (b - c) = km + lm = (k + l)m$ . Thus,  $a \equiv c \pmod{m}$ . Therefore, congruence modulo  $m$  is transitive. It follows that congruence modulo  $m$  is an equivalence relation. 

# Examples

1. Suppose that  $R$  is the relation on the set of strings of English letters such that  $aRb$  if and only if  $l(a) = l(b)$ , where  $l(x)$  is the length of the string  $x$ . Is  $R$  an equivalence relation?
2. Is the “divides” relation on the set of positive integers an equivalence relation?
3. Let  $R$  be the relation on the set of real numbers such that  $xRy$  if and only if  $x$  and  $y$  are real numbers that differ by less than 1, that is  $|x - y| < 1$ .

# Equivalence Classes

Let  $A$  be the set of all students in your school who graduated from high school. Consider the relation  $R$  on  $A$  that consists of all pairs  $(x, y)$ , where  $x$  and  $y$  graduated from the same high school.

Is it equivalence relation?

# Equivalence Classes

Let  $A$  be the set of all students in your school who graduated from high school. Consider the relation  $R$  on  $A$  that consists of all pairs  $(x, y)$ , where  $x$  and  $y$  graduated from the same high school.

Is it equivalence relation?

Yes.

Given a student  $x$ , we can form the set of all students equivalent to  $x$  with respect to  $R$ . This set consists of all students who graduated from the same high school as  $x$  did. This subset of  $A$  is called an equivalence class of the relation.

# Definition

Let  $R$  be an equivalence relation on a set  $A$ . The set of all elements that are related to an element  $a$  of  $A$  is called the equivalence class of  $a$ . The equivalence class of  $a$  with respect to  $R$  is denoted by  $[a]_R$ . When only one relation is under consideration, we can delete the subscript  $R$  and write  $[a]$  for this equivalence class.

In other words, if  $R$  is an equivalence relation on a set  $A$ , the equivalence class of the element  $a$  is

$$[a]_R = \{s \mid (a,s) \in R\}$$

If  $b \in [a]_R$ , then  $b$  is called a representative of this equivalence class. Any element of a class can be used as a representative of this class. That is, there is nothing special about the particular element chosen as the representative of the class.

## Example 3

What is the equivalence class of an integer for the equivalence relation of Example 1?

**Solution:** Because an integer is equivalent to itself and its negative in this equivalence relation, it follows that  $[a] = \{-a, a\}$ . This set contains two distinct integers unless  $a = 0$ . For instance,  $[7] = \{-7, 7\}$ ,  $[-5] = \{-5, 5\}$ , and  $[0] = \{0\}$ .

## Example 3

What is the equivalence class of an integer for the equivalence relation of Example 1?

**Solution:** Because an integer is equivalent to itself and its negative in this equivalence relation, it follows that  $[a] = \{-a, a\}$ . This set contains two distinct integers unless  $a = 0$ . For instance,  $[7] = \{-7, 7\}$ ,  $[-5] = \{-5, 5\}$ , and  $[0] = \{0\}$ .

# Problem

What are the equivalence classes of 0 and 1 for congruence modulo 4?

## Problem

What are the equivalence classes of 0 and 1 for congruence modulo 4?

**Solution:** The equivalence class of 0 contains all integers  $a$  such that  $a \equiv 0 \pmod{4}$ . The integers in this class are those divisible by 4. Hence, the equivalence class of 0 for this relation is

$$[0] = \{\dots, -8, -4, 0, 4, 8, \dots\}.$$

The equivalence class of 1 contains all the integers  $a$  such that  $a \equiv 1 \pmod{4}$ . The integers in this class are those that have a remainder of 1 when divided by 4. Hence, the equivalence class of 1 for this relation is

$$[1] = \{\dots, -7, -3, 1, 5, 9, \dots\}.$$



This problem can easily be generalized, replacing 4 with any positive integer  $m$ . The equivalence classes of the relation congruence modulo  $m$  are called the congruence classes modulo  $m$ . The congruence class of an integer  $a$  modulo  $m$  is denoted by  $[a]_m$ , so

$$[a]_m = \{ \dots, a-2m, a-m, a, a+m, a+2m, \dots \}.$$

For instance, it follows that

$$[0]_4 = \{ \dots, -8, -4, 0, 4, 8, \dots \} \text{ and } [1]_4 = \{ \dots, -7, -3, 1, 5, 9, \dots \}.$$

# Equivalence Classes and Partitions

Let  $R$  be a relation on the set  $A$ . Theorem 1 shows that the equivalence classes of two elements of  $A$  are either identical or disjoint.

## Theorem 1

Let  $R$  be an equivalence relation on a set  $A$ . These statements for elements  $a$  and  $b$  of  $A$  are equivalent:

- (i)  $aRb$
- (ii)  $[a] = [b]$
- (iii)  $[a] \cap [b] \neq \emptyset$

**Proof:** We first show that (i) implies (ii). Assume that  $aRb$ . We will prove that  $[a] = [b]$  by showing  $[a] \subseteq [b]$  and  $[b] \subseteq [a]$ . Suppose  $c \in [a]$ . Then  $aRc$ . Because  $aRb$  and  $R$  is symmetric, we know that  $bRa$ . Furthermore, because  $R$  is transitive and  $bRa$  and  $aRc$ , it follows that  $bRc$ . Hence,  $c \in [b]$ . This shows that  $[a] \subseteq [b]$ . The proof that  $[b] \subseteq [a]$  is similar; it is left as an exercise for the reader.

Second, we will show that (ii) implies (iii). Assume that  $[a] = [b]$ . It follows that  $[a] \cap [b] \neq \emptyset$  because  $[a]$  is nonempty (because  $a \in [a]$  because  $R$  is reflexive).

Next, we will show that (iii) implies (i). Suppose that  $[a] \cap [b] \neq \emptyset$ . Then there is an element  $c$  with  $c \in [a]$  and  $c \in [b]$ . In other words,  $aRc$  and  $bRc$ . By the symmetric property,  $cRb$ . Then by transitivity, because  $aRc$  and  $cRb$ , we have  $aRb$ .

Because (i) implies (ii), (ii) implies (iii), and (iii) implies (i), the three statements, (i), (ii), and (iii), are equivalent. 

We are now in a position to show how an equivalence relation *partitions* a set. Let  $R$  be an equivalence relation on a set  $A$ . The union of the equivalence classes of  $R$  is all of  $A$ , because an element  $a$  of  $A$  is in its own equivalence class, namely,  $[a]_R$ . In other words,

$$\bigcup_{a \in A} [a]_R = A.$$

In addition, from Theorem 1, it follows that these equivalence classes are either equal or disjoint, so

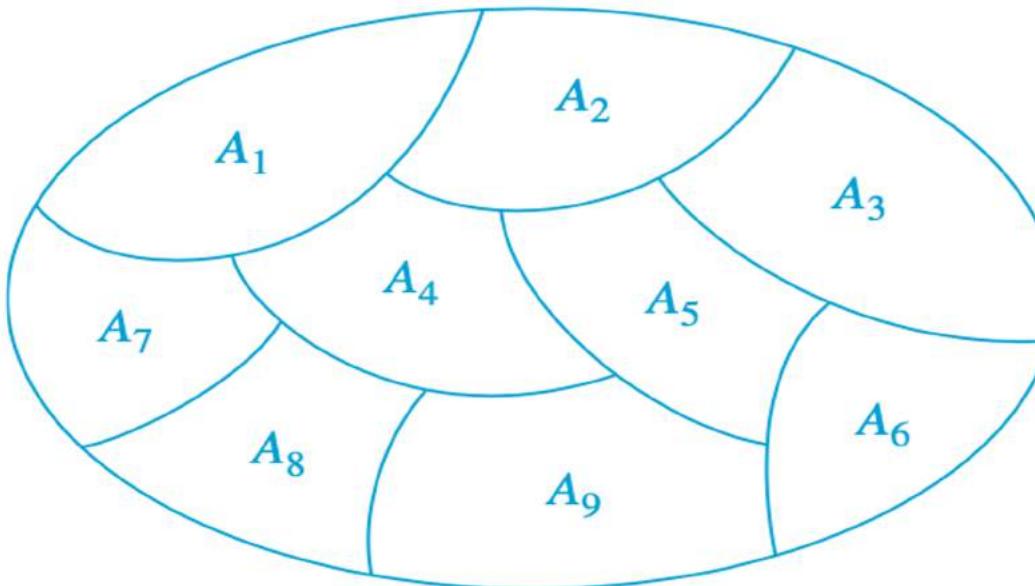
$$[a]_R \cap [b]_R = \emptyset,$$

when  $[a]_R \neq [b]_R$ .

These two observations show that the equivalence classes form a partition of  $A$ , because they split  $A$  into disjoint subsets. More precisely, a **partition** of a set  $S$  is a collection of disjoint nonempty subsets of  $S$  that have  $S$  as their union. In other words, the collection of subsets  $A_i$ ,  $i \in I$  (where  $I$  is an index set) forms a partition of  $S$  if and only if

$$A_i \neq \emptyset \text{ for } i \in I,$$

$$A_i \cap A_j = \emptyset \text{ when } i \neq j,$$



**FIGURE 1 A Partition of a Set.**

and

$$\bigcup_{i \in I} A_i = S.$$

Suppose that  $S = \{1, 2, 3, 4, 5, 6\}$ . The collection of sets  $A_1 = \{1, 2, 3\}$ ,  $A_2 = \{4, 5\}$ , and  $A_3 = \{6\}$  forms a partition of  $S$ , because these sets are disjoint and their union is  $S$ .

We have seen that the equivalence classes of an equivalence relation on a set form a partition of the set. The subsets in this partition are the equivalence classes. Conversely, every partition of a set can be used to form an equivalence relation. Two elements are equivalent with respect to this relation if and only if they are in the same subset of the partition.

To see this, assume that  $\{A_i \mid i \in I\}$  is a partition on  $S$ . Let  $R$  be the relation on  $S$  consisting of the pairs  $(x, y)$ , where  $x$  and  $y$  belong to the same subset  $A_i$  in the partition. To show that  $R$  is an equivalence relation we must show that  $R$  is reflexive, symmetric, and transitive.

We see that  $(a, a) \in R$  for every  $a \in S$ , because  $a$  is in the same subset as itself. Hence,  $R$  is reflexive. If  $(a, b) \in R$ , then  $b$  and  $a$  are in the same subset of the partition, so that  $(b, a) \in R$  as well. Hence,  $R$  is symmetric. If  $(a, b) \in R$  and  $(b, c) \in R$ , then  $a$  and  $b$  are in the same subset  $X$  in the partition, and  $b$  and  $c$  are in the same subset  $Y$  of the partition. Because the subsets of the partition are disjoint and  $b$  belongs to  $X$  and  $Y$ , it follows that  $X = Y$ . Consequently,  $a$  and  $c$  belong to the same subset of the partition, so  $(a, c) \in R$ . Thus,  $R$  is transitive.

It follows that  $R$  is an equivalence relation. The equivalence classes of  $R$  consist of subsets of  $S$  containing related elements, and by the definition of  $R$ , these are the subsets of the partition.

## Theorem 2

Let  $R$  be an equivalence relation on a set  $S$ . Then the equivalence classes of  $R$  form a partition of  $S$ . Conversely, given a partition  $\{A_i \mid i \in I\}$  of the set  $S$ , there is an equivalence relation  $R$  that has the sets  $A_i, i \in I$ , as its equivalence classes.

List the ordered pairs in the equivalence relation  $R$  produced by the partition  $A_1 = \{1, 2, 3\}$ ,  $A_2 = \{4, 5\}$ , and  $A_3 = \{6\}$  of  $S = \{1, 2, 3, 4, 5, 6\}$ .

**Solution:** The subsets in the partition are the equivalence classes of R. The pair  $(a, b) \in R$  if and only if a and b are in the same subset of the partition. The pairs  $(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2)$ , and  $(3, 3)$  belong to R because  $A_1 = \{1, 2, 3\}$  is an equivalence class; the pairs  $(4, 4), (4, 5), (5, 4)$ , and  $(5, 5)$  belong to R because  $A_2 = \{4, 5\}$  is an equivalence class; and finally the pair  $(6, 6)$  belongs to R because  $\{6\}$  is an equivalence class. No pair other than those listed belongs to R.

The congruence classes modulo  $m$  provide a useful illustration of Theorem 2. There are  $m$  different congruence classes modulo  $m$ , corresponding to the  $m$  different remainders possible when an integer is divided by  $m$ . They form a partition of the set of integers.

**Example:** What are the sets in the partition of the integers arising from congruence modulo 4?

**Solution:** There are four congruence classes, corresponding to  $[0]_4$ ,  $[1]_4$ ,  $[2]_4$ , and  $[3]_4$ . They are the sets

$$[0]_4 = \{\dots, -8, -4, 0, 4, 8, \dots\},$$

$$[1]_4 = \{\dots, -7, -3, 1, 5, 9, \dots\},$$

$$[2]_4 = \{\dots, -6, -2, 2, 6, 10, \dots\},$$

$$[3]_4 = \{\dots, -5, -1, 3, 7, 11, \dots\}.$$

These congruence classes are disjoint, and every integer is in exactly one of them. In other words, as Theorem 2 says, these congruence classes form a partition. 

# Partial Orderings

We often use relations to order some or all of the elements of sets. For instance, we order words using the relation containing pairs of words  $(x, y)$ , where  $x$  comes before  $y$  in the dictionary. We schedule projects using the relation consisting of pairs  $(x,y)$ , where  $x$  and  $y$  are tasks in a project such that  $x$  must be completed before  $y$  begins. We order the set of integers using the relation containing the pairs  $(x,y)$ , where  $x$  is less than  $y$ . When we add all of the pairs of the form  $(x, x)$  to these relations, we obtain a relation that is reflexive, antisymmetric, and transitive.

# Definition

A relation  $R$  on a set  $S$  is called a partial ordering or partial order if it is reflexive, antisymmetric, and transitive. A set  $S$  together with a partial ordering  $R$  is called a partially ordered set, or poset, and is denoted by  $(S, R)$ . Members of  $S$  are called elements of the poset.

Give an example of Poset.

## Example

The “greater than or equal” relation ( $\geq$ ) is a partial ordering on the set of integers.

Because  $a \geq a$  for every integer  $a$ ,  $\geq$  is reflexive. If  $a \geq b$  and  $b \geq a$ , then  $a = b$ . Hence,  $\geq$  is antisymmetric. Finally,  $\geq$  is transitive because  $a \geq b$  and  $b \geq c$  imply that  $a \geq c$ . It follows that  $\geq$  is a partial ordering on the set of integers and  $(\mathbb{Z}, \geq)$  is a poset.

# Other Examples of Posets

1. The divisibility relation  $|$  is a partial ordering on the set of positive integers, because it is reflexive, antisymmetric, and transitive, as was shown in Section 9.1. We see that  $(\mathbb{Z}^+, |)$  is a poset.
2. The inclusion relation  $\subseteq$  is a partial ordering on the power set of a set  $S$ .
3. Let  $R$  be the relation on the set of people such that  $xRy$  if  $x$  and  $y$  are people and  $x$  is older than  $y$ . Is  $R$  a partial ordering?

In different posets different symbols such as  $\leq$ ,  $\subseteq$ , and  $|$ , are used for a partial ordering. However, we need a symbol that we can use when we discuss the ordering relation in an arbitrary poset. Customarily, the notation  $a \preceq b$  is used to denote that  $(a, b) \in R$  in an arbitrary poset  $(S, R)$ . This notation is used because the “less than or equal to” relation on the set of real numbers is the most familiar example of a partial ordering and the symbol  $\preceq$  is similar to the  $\leq$  symbol. (Note that the symbol  $\preceq$  is used to denote the relation in *any* poset, not just the “less than or equals” relation.) The notation  $a \prec b$  denotes that  $a \preceq b$ , but  $a \neq b$ . Also, we say “ $a$  is less than  $b$ ” or “ $b$  is greater than  $a$ ” if  $a \prec b$ .

When  $a$  and  $b$  are elements of the poset  $(S, \preceq)$ , it is not necessary that either  $a \preceq b$  or  $b \preceq a$ . For instance, in  $(P(\mathbf{Z}), \subseteq)$ ,  $\{1, 2\}$  is not related to  $\{1, 3\}$ , and vice versa, because neither set is contained within the other. Similarly, in  $(\mathbf{Z}^+, |)$ , 2 is not related to 3 and 3 is not related to 2, because  $2 \nmid 3$  and  $3 \nmid 2$ . This leads to Definition 2.

### **Definition 2:**

The elements  $a$  and  $b$  of a poset  $(S, \preceq)$  are called *comparable* if either  $a \preceq b$  or  $b \preceq a$ . When  $a$  and  $b$  are elements of  $S$  such that neither  $a \preceq b$  nor  $b \preceq a$ ,  $a$  and  $b$  are called *incomparable*.

In the poset  $(\mathbb{Z}^+, |)$ , are the integers 3 and 9 comparable? Are 5 and 7 comparable?

**Solution:** The integers 3 and 9 are comparable, because  $3 \mid 9$ . The integers 5 and 7 are incomparable, because  $5 \nmid 7$  and  $7 \nmid 5$ .

The adjective “partial” is used to describe partial orderings because pairs of elements may be incomparable. When every two elements in the set are comparable, the relation is called a total ordering.

## Definition 3

If  $(S, \preceq)$  is a poset and every two elements of  $S$  are comparable,  $S$  is called a *totally ordered* or *linearly ordered set*, and  $\preceq$  is called a *total order* or a *linear order*. A totally ordered set is also called a *chain*.

The poset  $(\mathbb{Z}, \leq)$  is totally ordered, because  $a \leq b$  or  $b \leq a$  whenever  $a$  and  $b$  are integers.

The poset  $(\mathbb{Z}^+, | )$  is not totally ordered because it contains elements that are incomparable, such as 5 and 7.

# Well Ordering

$(S, \preccurlyeq)$  is a *well-ordered set* if it is a poset such that  $\preccurlyeq$  is a total ordering and every nonempty subset of  $S$  has a least element.

$(\mathbb{Z}^+, \leq)$  is well-ordered, where  $\leq$  is the usual “less than or equal to” relation.

The set of ordered pairs of positive integers,  $\mathbf{Z}^+ \times \mathbf{Z}^+$ , with  $(a_1, a_2) \preccurlyeq (b_1, b_2)$  if  $a_1 < b_1$ , or if  $a_1 = b_1$  and  $a_2 \leq b_2$  (the lexicographic ordering), is a well-ordered set. The verification of this is left as Exercise 53. The set  $\mathbf{Z}$ , with the usual  $\leq$  ordering, is not well-ordered because the set of negative integers, which is a subset of  $\mathbf{Z}$ , has no least element. 

# Lexicographic Order

The words in a dictionary are listed in alphabetic, or lexicographic, order, which is based on the ordering of the letters in the alphabet. This is a special case of an ordering of strings on a set constructed from a partial ordering on the set. We will show how this construction works in any poset.

First, we will show how to construct a partial ordering on the Cartesian product of two posets,  $(A_1, \preceq_1)$  and  $(A_2, \preceq_2)$ . The **lexicographic ordering**  $\prec$  on  $A_1 \times A_2$  is defined by specifying that one pair is less than a second pair if the first entry of the first pair is less than (in  $A_1$ ) the first entry of the second pair, or if the first entries are equal, but the second entry of this pair is less than (in  $A_2$ ) the second entry of the second pair. In other words,  $(a_1, a_2)$  is less than  $(b_1, b_2)$ , that is,

$$(a_1, a_2) \prec (b_1, b_2),$$

either if  $a_1 \prec_1 b_1$  or if both  $a_1 = b_1$  and  $a_2 \prec_2 b_2$ .

We obtain a partial ordering  $\preceq$  by adding equality to the ordering  $\prec$  on  $A_1 \times A_2$ . The verification of this is left as an exercise.

Determine whether  $(3, 5) \prec (4, 8)$ , whether  $(3, 8) \prec (4, 5)$ , and whether  $(4, 9) \prec (4, 11)$  in the poset  $(\mathbf{Z} \times \mathbf{Z}, \preccurlyeq)$ , where  $\preccurlyeq$  is the lexicographic ordering constructed from the usual  $\leq$  relation on  $\mathbf{Z}$ .

**Solution:** Because  $3 < 4$ , it follows that  $(3, 5) \prec (4, 8)$  and that  $(3, 8) \prec (4, 5)$ . We have  $(4, 9) \prec (4, 11)$ , because the first entries of  $(4, 9)$  and  $(4, 11)$  are the same but  $9 < 11$ . 

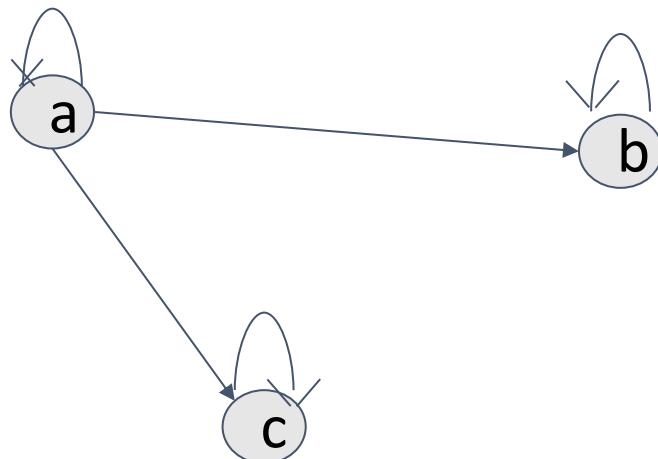
# Hasse Diagrams

- A graphical representation of Partial Ordering
- Since partial ordering is a binary relation, it can be represented by a directed graph
- However, many edges can be omitted, because such an ordering must be reflexive and transitive
- Also, we may order the vertices in the graph in a ‘vertical’ manner, such that all edges are pointing from low to high
- Directions on an edge can be omitted

The resulting diagram contains sufficient information to find the partial ordering, as we will explain later. The resulting diagram is called the Hasse diagram of poset.

# Example

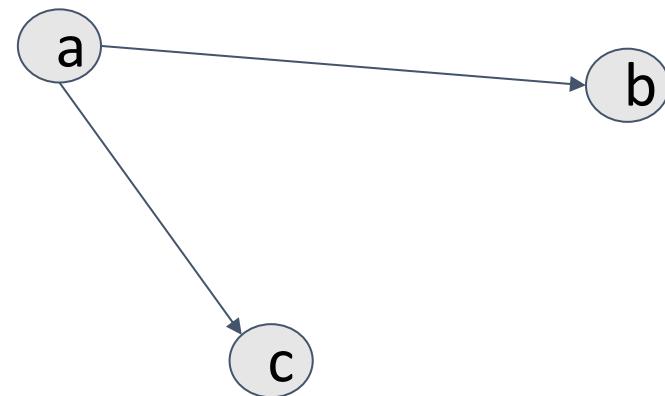
Let a partial ordering  $R$  is defined on a set  $\{a,b,c\}$  such that  $R = \{(a,b), (a,c), (a,a), (b,b), (c,c)\}$ . Let's draw it's digraph.



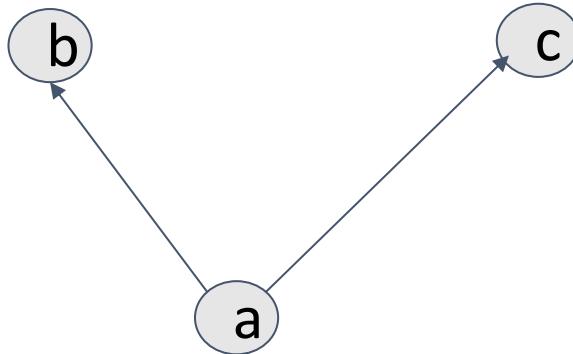
This is a digraph. Let us first remove self loop, because if it is a partial ordering then it is of course reflexive.

# Example

Let a partial ordering  $R$  is defined on a set  $\{a,b,c\}$  such that  $R = \{(a,b),(a,c),(a,a),(b,b),(c,c)\}$ . Let's draw it's digraph.



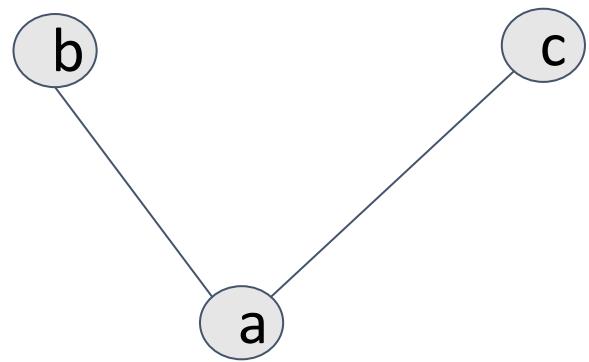
We may order the vertices in the graph in a ‘vertical’ manner, such that all edges are pointing from low to high. Note that  $a < b$  and  $a < c$  but  $b$  is not related to  $c$ . So you know that  $a$  is at the lower level but  $b$  and  $c$  are at the same level. This is due to covering relation.

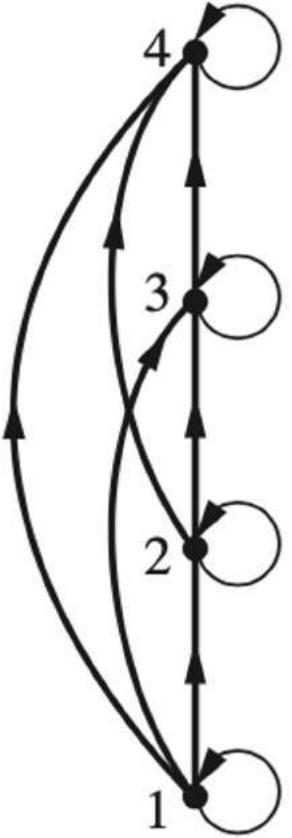


Let  $(S, \preceq)$  be a poset. We say that an element  $y \in S$  **covers** an element  $x \in S$  if  $x \prec y$  and there is no element  $z \in S$  such that  $x \prec z \prec y$ . The set of pairs  $(x, y)$  such that  $y$  covers  $x$  is called the **covering relation** of  $(S, \preceq)$ . From the description of the Hasse diagram of a poset, we see that the edges in the Hasse diagram of  $(S, \preceq)$  are upwardly pointing edges corresponding to the pairs in the covering relation of  $(S, \preceq)$ .

You can also delete the direction of the edges because in Hasse Diagram all edges are pointed “upward”.

# Hasse Diagram





(a)

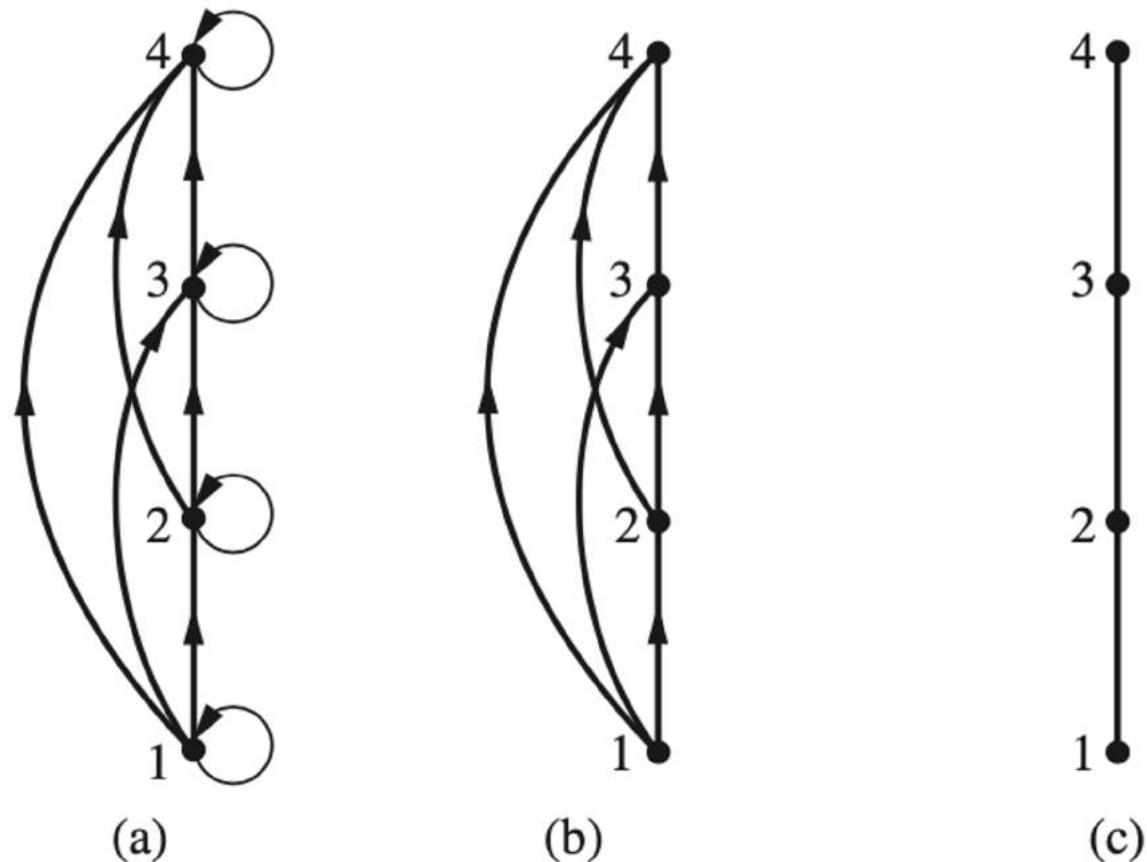


(b)



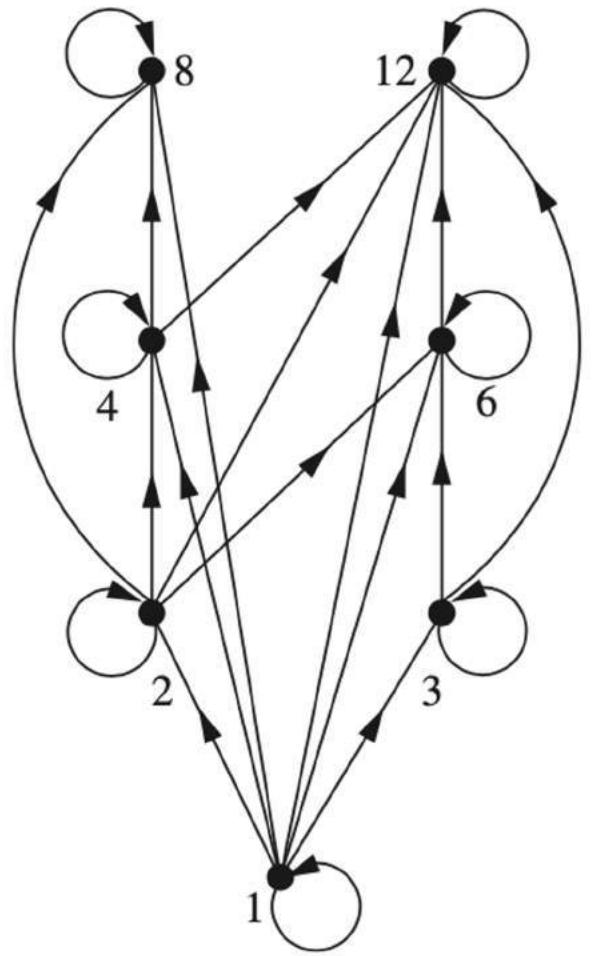
(c)

**FIGURE 2** Constructing the Hasse Diagram  
for  $(\{1, 2, 3, 4\}, \leq)$ .

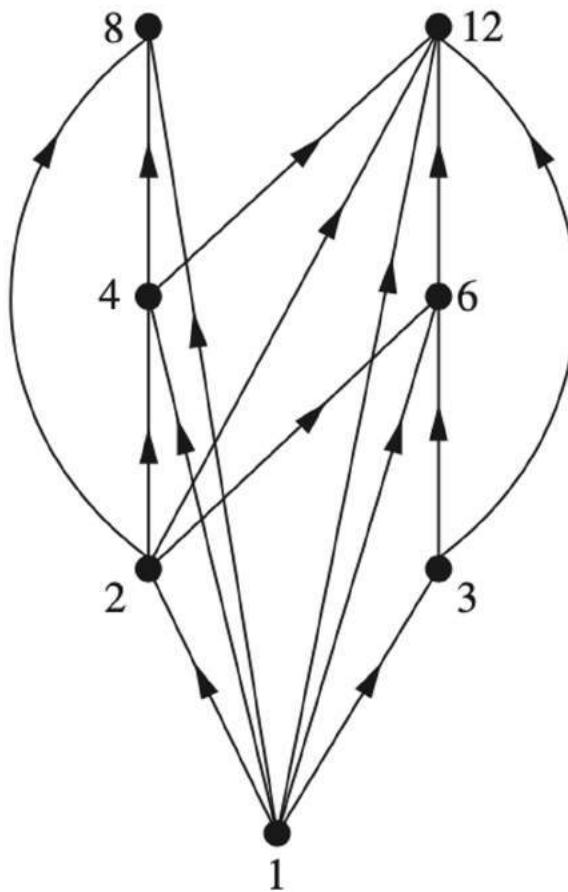


**FIGURE 2** Constructing the Hasse Diagram  
for  $(\{1, 2, 3, 4\}, \leq)$ .

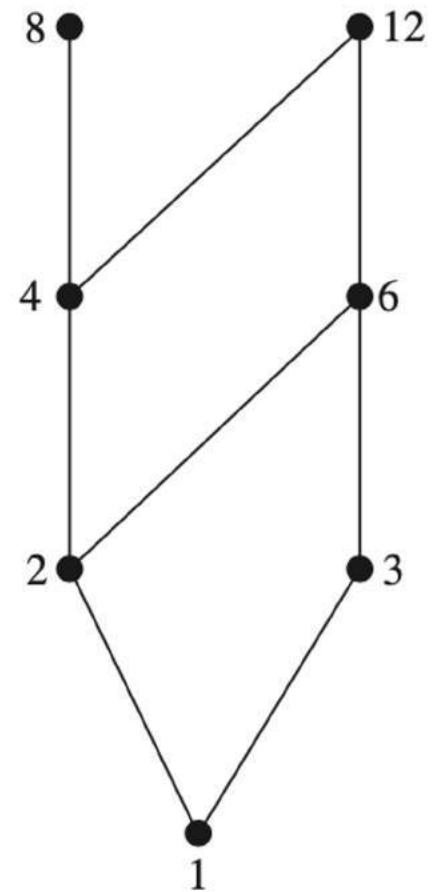
This relation is called a total order or a linear order. It is also called a chain. Why?



(a)

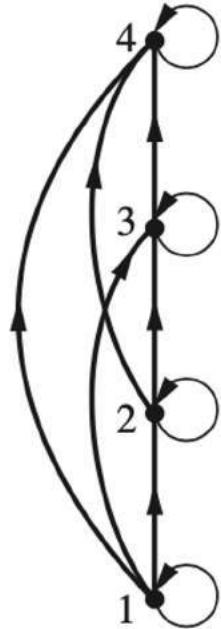


(b)



(c)

**FIGURE 3** Constructing the Hasse Diagram of  $(\{1, 2, 3, 4, 6, 8, 12\}, |)$ .



(a)

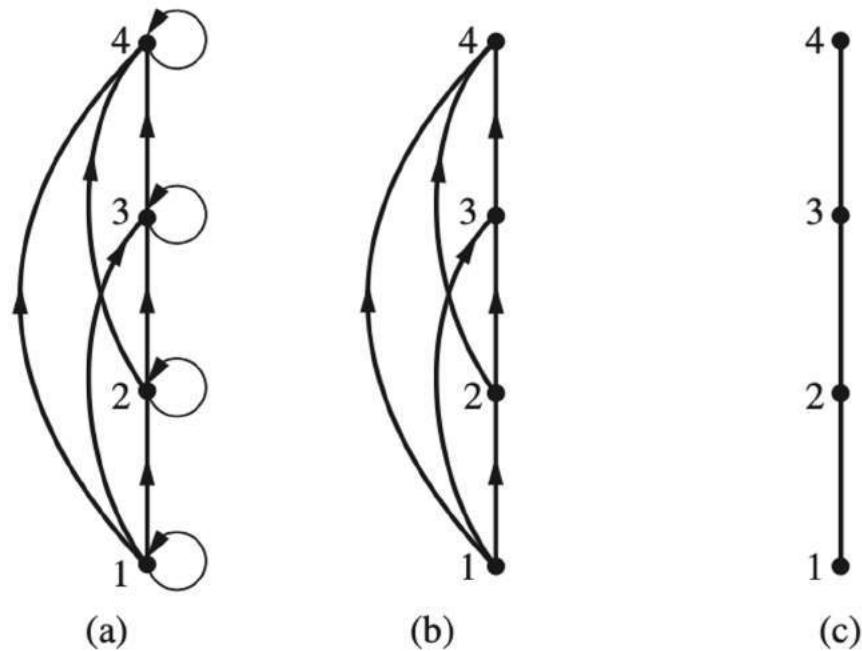


(b)



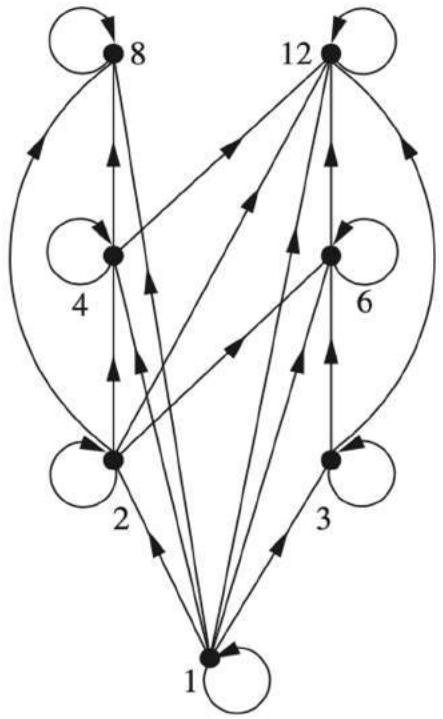
(c)

**FIGURE 2** Constructing the Hasse Diagram  
for  $(\{1, 2, 3, 4\}, \leq)$ .

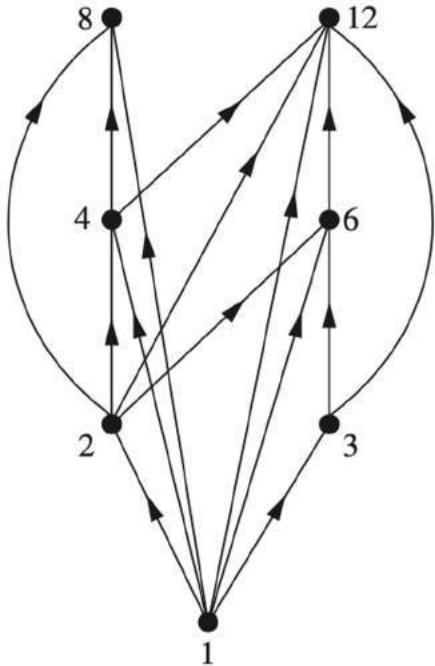


**FIGURE 2** Constructing the Hasse Diagram  
for  $(\{1, 2, 3, 4\}, \leq)$ .

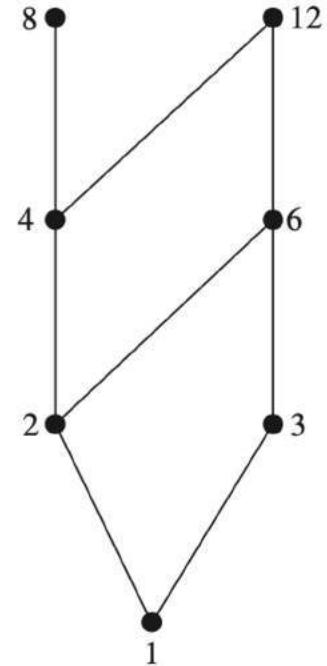
This relation is called a total order or a linear order. It is also called a chain. Why?



(a)



(b)



(c)

**FIGURE 3** Constructing the Hasse Diagram of  $(\{1, 2, 3, 4, 6, 8, 12\}, |)$ .

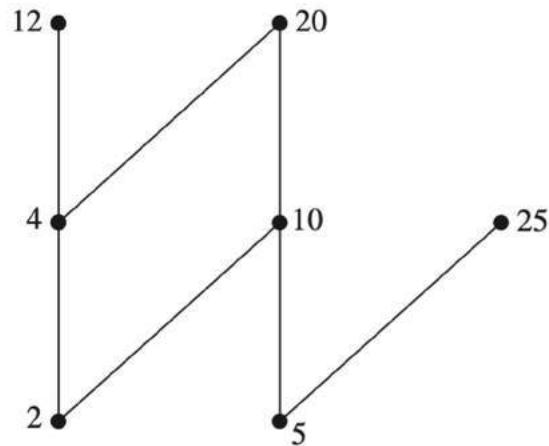
# Problem

Draw Hasse Diagram of ( $\{3, 6, 18, 24, 72\}$ ,  $|$ ).

# Maximal and Minimal Elements

Elements of posets that have certain extremal properties are important for many applications. An element of a poset is called maximal if it is not less than any element of the poset. That is,  $a$  is **maximal** in the poset  $(S, \preccurlyeq)$  if there is no  $b \in S$  such that  $a \prec b$ . Similarly, an element of a poset is called minimal if it is not greater than any element of the poset. That is,  $a$  is **minimal** if there is no element  $b \in S$  such that  $b \prec a$ . Maximal and minimal elements are easy to spot using a Hasse diagram. They are the “top” and “bottom” elements in the diagram.

Which elements of the poset  $(\{2, 4, 5, 10, 12, 20, 25\}, |)$  are maximal, and which are minimal?



**FIGURE 5** The Hasse  
Diagram of a Poset.

Which elements of the poset  $(\{2, 4, 5, 10, 12, 20, 25\}, |)$  are maximal, and which are minimal?

**Solution:** The Hasse diagram in Figure 5 for this poset shows that the maximal elements are 12, 20, and 25, and the minimal elements are 2 and 5. As this example shows, a poset can have more than one maximal element and more than one minimal element.

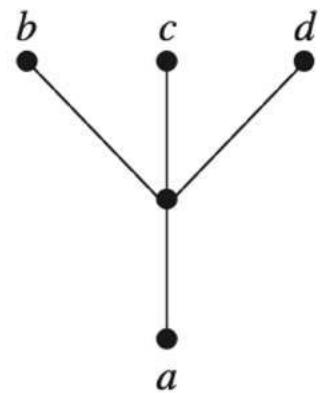
# Greatest and Least Element

Sometimes there is an element in a poset that is greater than every other element. Such an element is called the greatest element. That is,  $a$  is the **greatest element** of the poset  $(S, \preceq)$  if  $b \preceq a$  for all  $b \in S$ . The greatest element is unique when it exists [see Exercise 40(a)]. Likewise, an element is called the least element if it is less than all the other elements in the poset. That is,  $a$  is the **least element** of  $(S, \preceq)$  if  $a \preceq b$  for all  $b \in S$ . The least element is unique when it exists [see Exercise 40(b)].

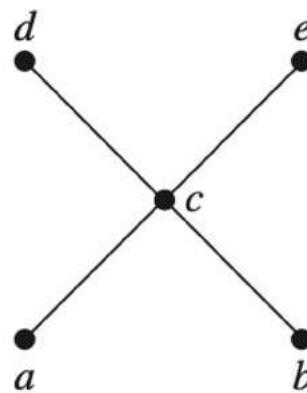
---

## Example

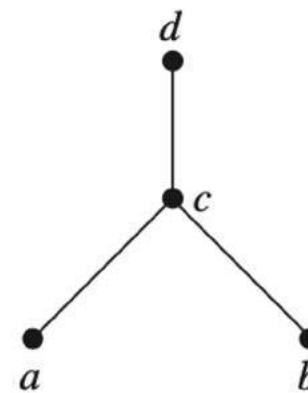
Determine whether the posets represented by each of the Hasse diagrams in Figure 6 have a greatest element and a least element.



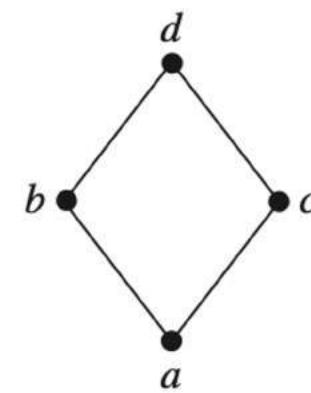
(a)



(b)



(c)



(d)

**FIGURE 6** Hasse Diagrams of Four Posets.

**Solution:** The least element of the poset with Hasse diagram (a) is a. This poset has no greatest element. The poset with Hasse diagram (b) has neither a least nor a greatest element. The poset with Hasse diagram (c) has no least element. Its greatest element is d. The poset with Hasse diagram (d) has least element a and greatest element d.

# Example

Is there a greatest element and a least element in the poset  $(\mathbb{Z}^+, |)$ ?

## Example

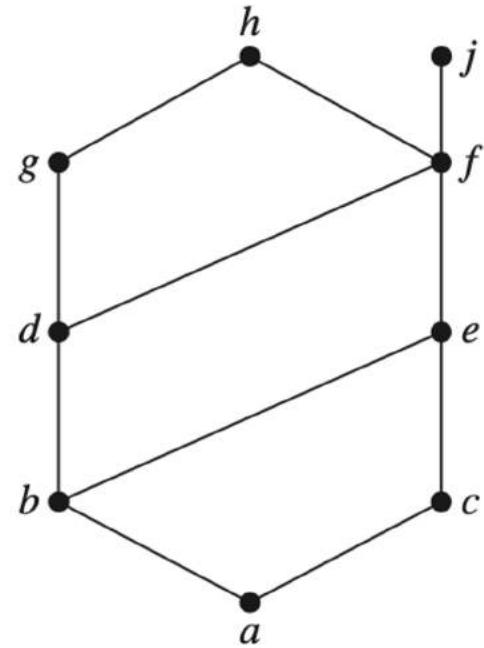
Is there a greatest element and a least element in the poset  $(\mathbb{Z}^+, |)$ ?

**Solution:** The integer 1 is the least element because  $1|n$  whenever  $n$  is a positive integer. Because there is no integer that is divisible by all positive integers, there is no greatest element.

# Upper and Lower Bound

Sometimes it is possible to find an element that is greater than or equal to all the elements in a subset  $A$  of a poset  $(S, \preccurlyeq)$ . If  $u$  is an element of  $S$  such that  $a \preccurlyeq u$  for all elements  $a \in A$ , then  $u$  is called an **upper bound** of  $A$ . Likewise, there may be an element less than or equal to all the elements in  $A$ . If  $l$  is an element of  $S$  such that  $l \preccurlyeq a$  for all elements  $a \in A$ , then  $l$  is called a **lower bound** of  $A$ .

Find the lower and upper bounds of the subsets  $\{a, b, c\}$ ,  $\{j, h\}$ , and  $\{a, c, d, f\}$  in the poset with the Hasse diagram shown in Figure 7.



**FIGURE 7** The Hasse Diagram of a Poset.

## LUB and GLB

The element  $x$  is called the **least upper bound** of the subset  $A$  if  $x$  is an upper bound that is less than every other upper bound of  $A$ . Because there is only one such element, if it exists, it makes sense to call this element *the* least upper bound [see Exercise 42(a)]. That is,  $x$  is the least upper bound of  $A$  if  $a \preceq x$  whenever  $a \in A$ , and  $x \preceq z$  whenever  $z$  is an upper bound of  $A$ . Similarly, the element  $y$  is called the **greatest lower bound** of  $A$  if  $y$  is a lower bound of  $A$  and  $z \preceq y$  whenever  $z$  is a lower bound of  $A$ . The greatest lower bound of  $A$  is unique if it exists [see Exercise 42(b)]. The greatest lower bound and least upper bound of a subset  $A$  are denoted by  $\text{glb}(A)$  and  $\text{lub}(A)$ , respectively.

## Example

Find the greatest lower bound and the least upper bound of  $\{b, d, g\}$ , if they exist, in the poset shown in Figure 7.

**Solution:** The upper bounds of  $\{b, d, g\}$  are  $g$  and  $h$ . Because  $g \prec h$ ,  $g$  is the least upper bound. The lower bounds of  $\{b, d, g\}$  are  $a$  and  $b$ . Because  $a \prec b$ ,  $b$  is the greatest lower bound. 

## Example

Find the greatest lower bound and the least upper bound of the sets  $\{3, 9, 12\}$  and  $\{1, 2, 4, 5, 10\}$ , if they exist, in the poset  $(\mathbf{Z}^+, |)$ .

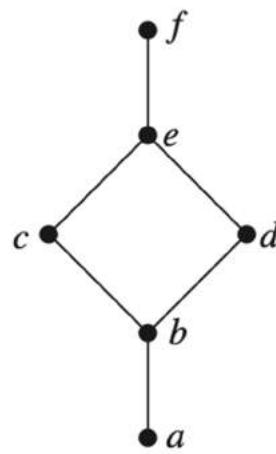
**Solution:** An integer is a lower bound of  $\{3, 9, 12\}$  if 3, 9, and 12 are divisible by this integer. The only such integers are 1 and 3. Because  $1 \mid 3$ , 3 is the greatest lower bound of  $\{3, 9, 12\}$ . The only lower bound for the set  $\{1, 2, 4, 5, 10\}$  with respect to  $|$  is the element 1. Hence, 1 is the greatest lower bound for  $\{1, 2, 4, 5, 10\}$ .

An integer is an upper bound for  $\{3, 9, 12\}$  if and only if it is divisible by 3, 9, and 12. The integers with this property are those divisible by the least common multiple of 3, 9, and 12, which is 36. Hence, 36 is the least upper bound of  $\{3, 9, 12\}$ . A positive integer is an upper bound for the set  $\{1, 2, 4, 5, 10\}$  if and only if it is divisible by 1, 2, 4, 5, and 10. The integers with this property are those integers divisible by the least common multiple of these integers, which is 20. Hence, 20 is the least upper bound of  $\{1, 2, 4, 5, 10\}$ . 

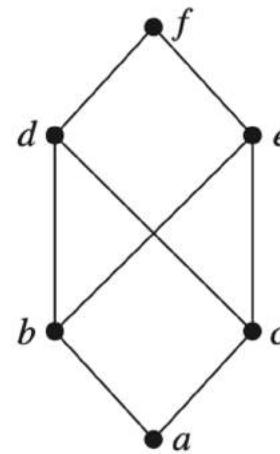
# Lattices

A partially ordered set in which every pair of elements has both a least upper bound and a greatest lower bound is called a lattice. Lattices have many special properties.

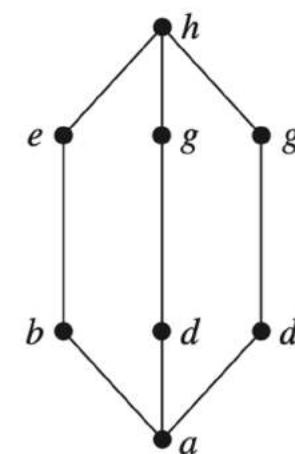
Determine whether the posets represented by each of the Hasse diagrams in Figure 8 are lattices.



(a)



(b)



(c)

**FIGURE 8** Hasse Diagrams of Three Posets.

**Solution:** The posets represented by the Hasse diagrams in (a) and (c) are both lattices because in each poset every pair of elements has both a least upper bound and a greatest lower bound, as the reader should verify. On the other hand, the poset with the Hasse diagram shown in (b) is not a lattice, because the elements b and c have no least upper bound. To see this, note that each of the elements d, e, and f is an upper bound, but none of these three elements precedes the other two with respect to the ordering of this poset.

See the examples in page 627.

**End of Unit 4**

# UNIT V

# Syllabus

**Unit – 5 [9 Hours]:** Solving Linear Equations Solving  $Ax = b$ , Elimination with Matrices, Multiplication and Inverse Matrices, Factorization into  $A = LU$ , Transposes and Permutations; Vector Spaces and Subspaces - Spaces of Vectors, Column Space, Null Space, Row Space, Left Null Space, Independence, Basis, and Dimension, Rank and Row Reduced Form, Invertible Matrices;

# Text book

- Gilbert Strang, Introduction to linear algebra,  
3<sup>rd</sup> edition

# Introduction

- Linear algebra is a branch of mathematics that studies systems of linear equations, matrices, vectors, and vector spaces.

- The heart of linear algebra is in two operations-both with vectors.
- We add vectors to get  $v+w$
- We multiply numbers to get  $cv$  and  $dw$ . combining those two operations gives linear combination  $cv+dw$ .

# Vectors and Linear combinations

“You can’t add apples and oranges.” In a strange way, this is the reason for vectors! If we keep the number of apples separate from the number of oranges, we have a pair of numbers. That pair is a *two-dimensional vector*  $v$ , with “components”  $v_1$  and  $v_2$ :

$$v = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \quad \begin{array}{l} v_1 = \text{number of apples} \\ v_2 = \text{number of oranges.} \end{array}$$

---

1

We write  $v$  as a *column vector*. The main point so far is to have a single letter  $v$  (in *boldface italic*) for this pair of numbers  $v_1$  and  $v_2$  (in *lightface italic*).

# Definition of vector

- ▶ a *vector* is an ordered list of numbers
- ▶ written as

$$\begin{bmatrix} -1.1 \\ 0.0 \\ 3.6 \\ -7.2 \end{bmatrix} \quad \text{or} \quad \begin{pmatrix} -1.1 \\ 0.0 \\ 3.6 \\ -7.2 \end{pmatrix}$$

or  $(-1.1, 0, 3.6, -7.2)$

- ▶ numbers in the list are the *elements* (*entries*, *coefficients*, *components*)
- ▶ number of elements is the *size* (*dimension*, *length*) of the vector
- ▶ vector above has dimension 4; its third entry is 3.6
- ▶ vector of size  $n$  is called an  $n$ -*vector*
- ▶ numbers are called *scalars*

# Vector Addition

Even if we don't add  $v_1$  to  $v_2$ , we do *add vectors*. The first components of  $v$  and  $w$  stay separate from the second components:

$$v = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \quad \text{and} \quad w = \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} \quad \text{add to} \quad v + w = \begin{bmatrix} v_1 + w_1 \\ v_2 + w_2 \end{bmatrix}.$$

Subtraction also follows same idea

# Properties of Vector Addition

- ▶ *commutative*:  $a + b = b + a$
- ▶ *associative*:  $(a + b) + c = a + (b + c)$   
(so we can write both as  $a + b + c$ )
- ▶  $a + 0 = 0 + a = a$
- ▶  $a - a = 0$

# Scalar Multiplication

The other basic operation is *scalar multiplication*. Vectors can be multiplied by 2 or by  $-1$  or by any number  $c$ . There are two ways to double a vector. One way is to add  $\mathbf{v} + \mathbf{v}$ . The other way (the usual way) is to multiply each component by 2:

$$2\mathbf{v} = \begin{bmatrix} 2v_1 \\ 2v_2 \end{bmatrix} \quad \text{and} \quad -\mathbf{v} = \begin{bmatrix} -v_1 \\ -v_2 \end{bmatrix}.$$

The components of  $c\mathbf{v}$  are  $cv_1$  and  $cv_2$ . The number  $c$  is called a “scalar”.

- Notice that the sum of  $v$  and  $-v$  is a zero vector.
- This  $0$  is not same as number  $0$ . The vector zero has the components  $0$  and  $0$ .

# Properties of Scalar Multiplication

- ▶ associative:  $(\beta\gamma)a = \beta(\gamma a)$
- ▶ left distributive:  $(\beta + \gamma)a = \beta a + \gamma a$
- ▶ right distributive:  $\beta(a + b) = \beta a + \beta b$

# Linear Combination

- Linear algebra is built on these operations  $v+w$  and  $cv$  ( adding vectors and multiplying by scalars).
- By combining these operations we form linear combinations of  $v$  and  $w$ .
- Multiplying  $v$  by  $c$  and  $w$  by  $d$  and then add:  
 $cv+dw$ .

# Definition

- The sum of  $c\mathbf{v}$  and  $d\mathbf{w}$  is a linear combination of  $\mathbf{v}$  and  $\mathbf{w}$ .

Four special linear combinations are: sum, difference, zero, and a scalar multiple  $c\mathbf{v}$ :

$1\mathbf{v} + 1\mathbf{w}$  = sum of vectors in Figure 1.1

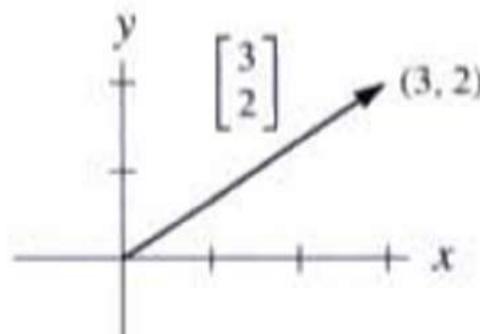
$1\mathbf{v} - 1\mathbf{w}$  = difference of vectors in Figure 1.1

$0\mathbf{v} + 0\mathbf{w}$  = *zero vector*

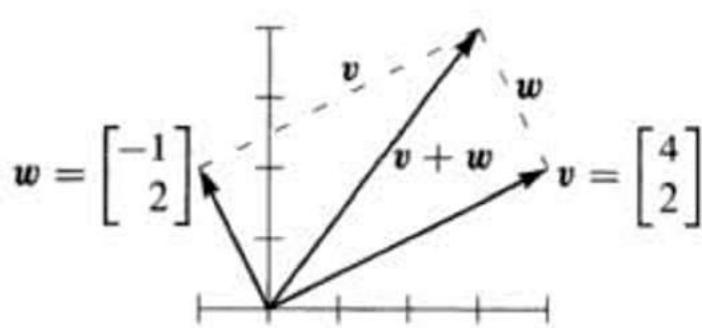
$c\mathbf{v} + 0\mathbf{w}$  = vector  $c\mathbf{v}$  in the direction of  $\mathbf{v}$

# Representation Of a vector

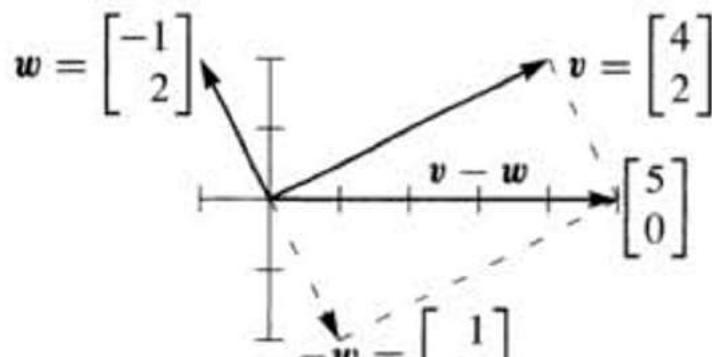
- For algebra we just need components 3 and 2
- In the plane, that vector  $v$  is represented by an arrow. The arrow goes  $v_1 = 3$  units to the right and  $v_2 = 2$  units up. It ends at a point whose x and y coordinates are (3,2).
- So we have 3 ways to describe a vector  $v$  by an arrow or a point or a pair of numbers.



# vector addition/subtraction representation



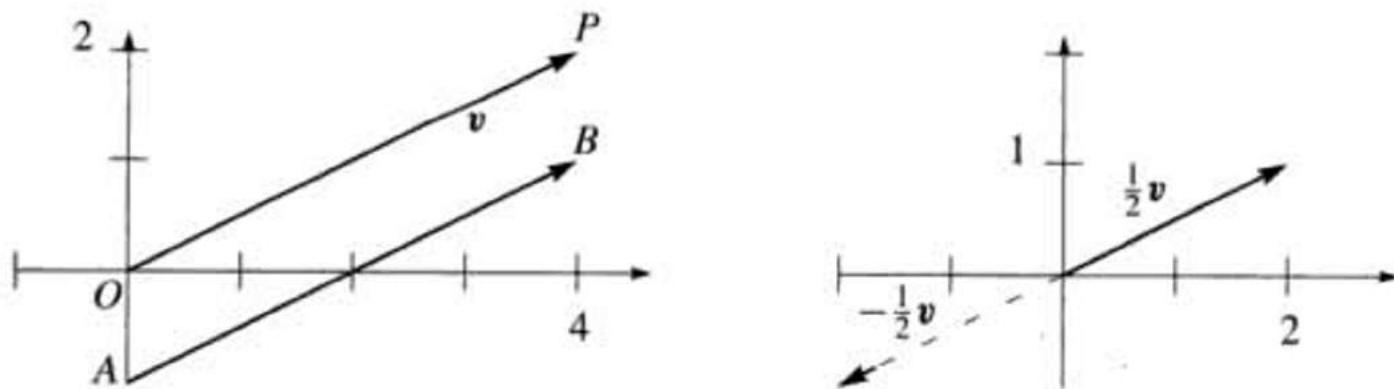
$$v + w = \begin{bmatrix} 4 \\ 2 \end{bmatrix} + \begin{bmatrix} -1 \\ 2 \end{bmatrix} = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$$



$$v - w = \begin{bmatrix} 4 \\ 2 \end{bmatrix} - \begin{bmatrix} -1 \\ 2 \end{bmatrix} = \begin{bmatrix} 5 \\ 0 \end{bmatrix}$$

**Figure 1.1** Vector addition  $v + w$  produces the diagonal of a parallelogram. The linear combination on the right is  $v - w$ .

The zero vector has  $v_1 = 0$  and  $v_2 = 0$ . It is too short to draw a decent arrow, but you know that  $\mathbf{v} + \mathbf{0} = \mathbf{v}$ . For  $2\mathbf{v}$  we double the length of the arrow. We reverse its direction for  $-\mathbf{v}$ . This reversing gives the subtraction on the right side of Figure 1.1.



**Figure 1.2** The arrow usually starts at the origin  $(0, 0)$ ;  $c\mathbf{v}$  is always parallel to  $\mathbf{v}$ .

# Vectors in 3 Dimension

A vector with two components corresponds to a point in the  $xy$  plane. The components of  $\mathbf{v}$  are the coordinates of the point:  $x = v_1$  and  $y = v_2$ . The arrow ends at this point  $(v_1, v_2)$ , when it starts from  $(0, 0)$ . Now we allow vectors to have three components  $(v_1, v_2, v_3)$ . The  $xy$  plane is replaced by three-dimensional space.

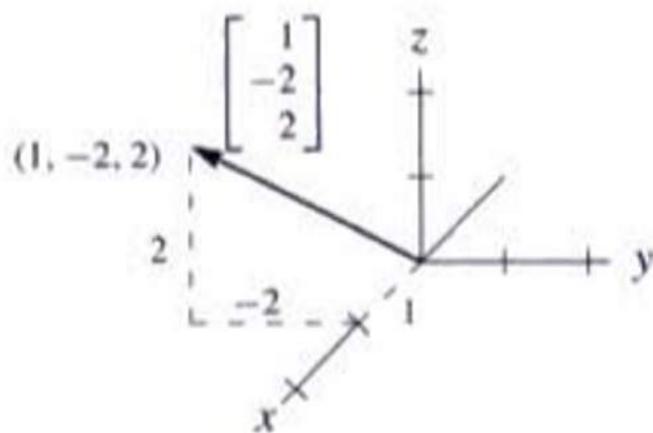
Here are typical vectors (still column vectors but with three components):

$$\mathbf{v} = \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} \quad \text{and} \quad \mathbf{w} = \begin{bmatrix} 2 \\ 3 \\ -1 \end{bmatrix} \quad \text{and} \quad \mathbf{v} + \mathbf{w} = \begin{bmatrix} 3 \\ 5 \\ 1 \end{bmatrix} .$$

# Vector representation in 3-Dimensional space

Here vector  $v = \begin{bmatrix} 1 \\ -2 \\ 2 \end{bmatrix}$  corresponds to an arrow in 3-space

From now on  $v = \begin{bmatrix} 1 \\ -2 \\ 2 \end{bmatrix}$  / is also written as  $v=(1,-2,2)$



# Linear combination of vectors in 3 dimension

A typical linear combination of three vectors in three dimensions is  $\mathbf{u} + 4\mathbf{v} - 2\mathbf{w}$ :

**Linear combination** 
$$\begin{bmatrix} 1 \\ 0 \\ 3 \end{bmatrix} + 4 \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} - 2 \begin{bmatrix} 2 \\ 3 \\ -1 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 9 \end{bmatrix}.$$

# Dot product or inner product

- Definition: The dot product or inner product of  $v = (v_1, v_2)$  and  $w = (w_1, w_2)$  is the number
- $v \cdot w = v_1 w_1 + v_2 w_2$
- Ex- The vectors  $v = (4, 2)$  and  $w = (-1, 2)$  have a *zero* dot product:

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix} \cdot \begin{bmatrix} -1 \\ 2 \end{bmatrix} = -4 + 4 = 0.$$

Here the dot product is zero it means that the two vectors are perpendicular

## Note:

- The dot product  $w \cdot v$  equals  $v \cdot w$ .
- The order of  $v$  and  $w$  makes no difference
- What is the dot product of the vector with it self?

# Definition

- The length or norm of a vector  $v$  is the square root of  $v \cdot v$ .

$$\text{length} = \|v\| = \sqrt{v \cdot v}.$$

In two dimensions the length is  $\sqrt{v_1^2 + v_2^2}$ . In three dimensions it is  $\sqrt{v_1^2 + v_2^2 + v_3^2}$ .

# Definition

- A unit vector  $u$  is a vector whose length equals to one. Then  $u \cdot u = 1$

**Example 4** The standard unit vectors along the  $x$  and  $y$  axes are written  $i$  and  $j$ . In the  $xy$  plane, the unit vector that makes an angle “theta” with the  $x$  axis is  $(\cos \theta, \sin \theta)$ :

**Unit vectors**  $i = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$  and  $j = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$  and  $u = \begin{bmatrix} \cos \theta \\ \sin \theta \end{bmatrix}$ .

When  $\theta = 0$ , the horizontal vector  $u$  is  $i$ . When  $\theta = 90^\circ$  (or  $\frac{\pi}{2}$  radians), the vertical vector is  $j$ . At any angle, the components  $\cos \theta$  and  $\sin \theta$  produce  $u \cdot u = 1$  because  $\cos^2 \theta + \sin^2 \theta = 1$ .

# Some more key points about vectors

**1A Unit vectors** Divide any nonzero vector  $v$  by its length. Then  $u = v/\|v\|$  is a unit vector in the same direction as  $v$ .

**1B Right angles** The dot product is  $v \cdot w = 0$  when  $v$  is perpendicular to  $w$ .

**1C** If  $u$  and  $U$  are unit vectors then  $u \cdot U = \cos \theta$ . Certainly  $|u \cdot U| \leq 1$ .

**1D (a) COSINE FORMULA** If  $v$  and  $w$  are nonzero vectors then

$$\frac{v \cdot w}{\|v\| \|w\|} = \cos \theta.$$

**(b) SCHWARZ INEQUALITY** If  $v$  and  $w$  are any vectors then  $|v \cdot w| \leq \|v\| \|w\|$ .

# SOLVING LINEAR EQUATIONS

# VECTORS AND LINEAR EQUATIONS

- The central problem of linear algebra is to solve a system of equations which are linear(Equations are called linear when the unknowns are only multiplied by numbers.  
we never see  $x$  times  $y$ )

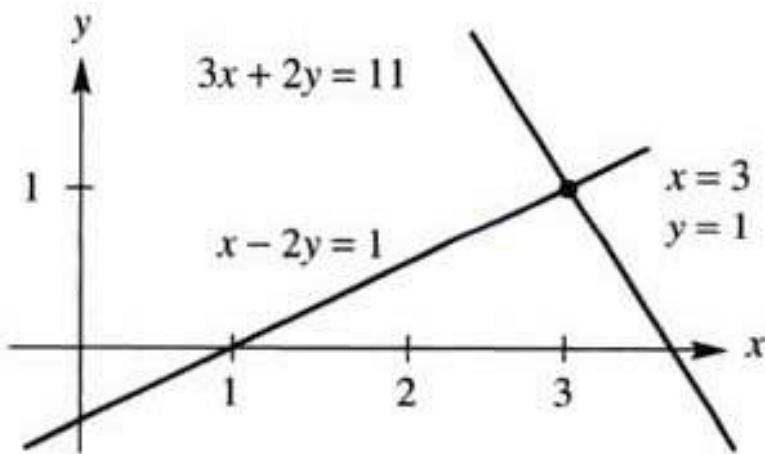
- Two equations in two unknowns
- Example 1: Let us consider the following example. which has 2 equations in two unknowns.
  - $x - 2y = 1$
  - $3x + 2y = 11$

These system of equations can be graphically represented as

- 1) Row picture
- 2) Column Picture

# Row Picture

- The row picture shows two lines meeting at a single point



**Figure 2.1** *Row picture:* The point  $(3, 1)$  where the lines meet is the solution.

Figure 2.1 shows that line  $x - 2y = 1$ . The second line in this “row picture” comes from the second equation  $3x + 2y = 11$ .

# Column Picture

Turn now to the column picture. I want to recognize the linear system as a “vector equation”. Instead of numbers we need to see *vectors*. If you separate the original system into its columns instead of its rows, you get

$$x \begin{bmatrix} 1 \\ 3 \end{bmatrix} + y \begin{bmatrix} -2 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 \\ 11 \end{bmatrix} = b. \quad (2)$$

This has two column vectors on the left side. The problem is *to find the combination of those vectors that equals the vector on the right*. We are multiplying the first column by  $x$  and the second column by  $y$ , and adding. With the right choices  $x = 3$  and  $y = 1$ , this produces  $3(\text{column 1}) + 1(\text{column 2}) = b$ .

The basic vector operations involved here are

**Scalar multiplication**       $3 \begin{bmatrix} 1 \\ 3 \end{bmatrix} = \begin{bmatrix} 3 \\ 9 \end{bmatrix}$

**Vector addition**       $\begin{bmatrix} 3 \\ 9 \end{bmatrix} + \begin{bmatrix} -2 \\ 2 \end{bmatrix} = \begin{bmatrix} 3-2 \\ 9+2 \end{bmatrix} = \begin{bmatrix} 1 \\ 11 \end{bmatrix}$

$$v = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}, \quad (v_1, v_2)$$

$$\vec{0} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Ex. Find unit vector in the direction  $\begin{bmatrix} 3 \\ 2 \end{bmatrix}$ .

$$v = \begin{bmatrix} 3 \\ 2 \end{bmatrix}, \quad \|v\| = \sqrt{9+4} = \sqrt{13}$$

$$u = \frac{v}{\|v\|} = \frac{1}{\sqrt{13}} \begin{bmatrix} 3 \\ 2 \end{bmatrix}$$

1  
1  
1  
1

(1, 1, 1)

(1, 1, 1)

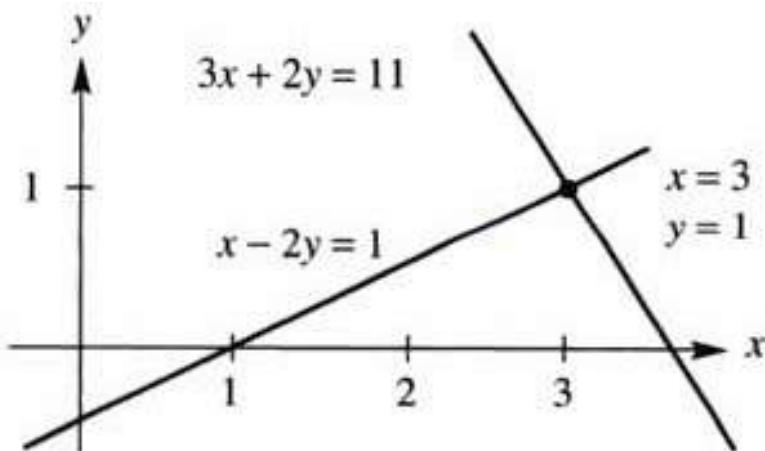
- Two equations in two unknowns
- Example 1: Let us consider the following example. which has 2 equations in two unknowns.
  - $x - 2y = 1$
  - $3x + 2y = 11$

These system of equations can be graphically represented as

- 1) Row picture
- 2) Column Picture

# Row Picture

- The row picture shows two lines meeting at a single point



**Figure 2.1** *Row picture:* The point  $(3, 1)$  where the lines meet is the solution.

Figure 2.1 shows that line  $x - 2y = 1$ . The second line in this “row picture” comes from the second equation  $3x + 2y = 11$ .

# Column Picture

Turn now to the column picture. I want to recognize the linear system as a “vector equation”. Instead of numbers we need to see *vectors*. If you separate the original system into its columns instead of its rows, you get

$$x \begin{bmatrix} 1 \\ 3 \end{bmatrix} + y \begin{bmatrix} -2 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 \\ 11 \end{bmatrix} = b. \quad (2)$$

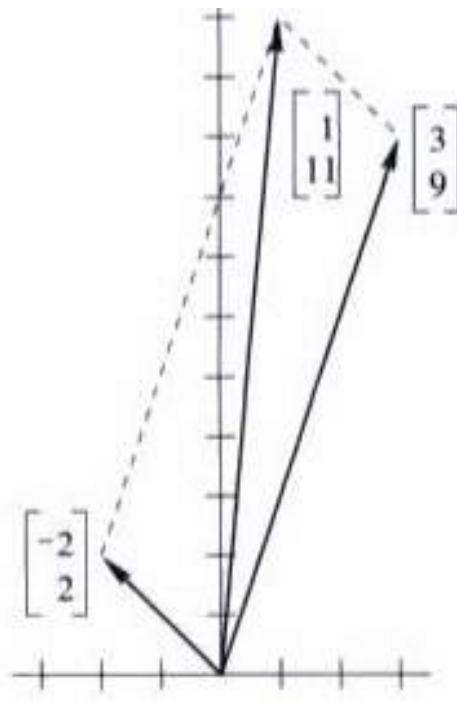
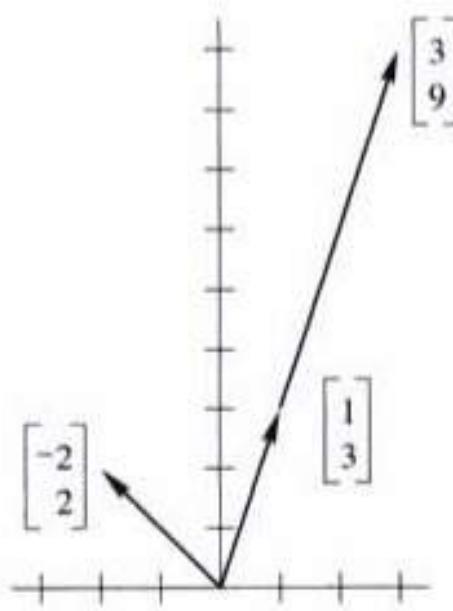
This has two column vectors on the left side. The problem is *to find the combination of those vectors that equals the vector on the right*. We are multiplying the first column by  $x$  and the second column by  $y$ , and adding. With the right choices  $x = 3$  and  $y = 1$ , this produces  $3(\text{column 1}) + 1(\text{column 2}) = b$ .

The basic vector operations involved here are

**Scalar multiplication**       $3 \begin{bmatrix} 1 \\ 3 \end{bmatrix} = \begin{bmatrix} 3 \\ 9 \end{bmatrix}$

**Vector addition**       $\begin{bmatrix} 3 \\ 9 \end{bmatrix} + \begin{bmatrix} -2 \\ 2 \end{bmatrix} = \begin{bmatrix} 3-2 \\ 9+2 \end{bmatrix} = \begin{bmatrix} 1 \\ 11 \end{bmatrix}$

- The column picture combines the column vectors on the left side to produce the vector  $b$  on the right side



*Column picture:* A combination of columns produces the right side (1,11).

# Coefficient Matrix

- For Example:

$$x - 2y = 1$$

$$3x + 2y = 11$$

The coefficient matrix on the left side of the equation is the 2 by 2 matrix A

Coefficient matrix A=  $\begin{bmatrix} 1 & -2 \\ 3 & 2 \end{bmatrix}$

Look at the matrix by rows and by columns.

Its rows give row picture and its columns give column picture.

# Matrix Equation

- Now using coefficient matrix we can represent the example equations as a matrix problem

$$AX=b$$

- Matrix equation is given by

$$\begin{bmatrix} 1 & -2 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 11 \end{bmatrix}$$

In the below matrix equation

Matrix equation

$$\begin{bmatrix} 1 & -2 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 11 \end{bmatrix}.$$

The row picture deals with the two rows of  $A$ . The column picture combines the columns.  
The numbers  $x = 3$  and  $y = 1$  go into the solution vector  $\mathbf{x}$ . Then

$$A\mathbf{x} = \mathbf{b} \quad \text{is} \quad \begin{bmatrix} 1 & -2 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 11 \end{bmatrix}.$$

# Three equations in three unknowns

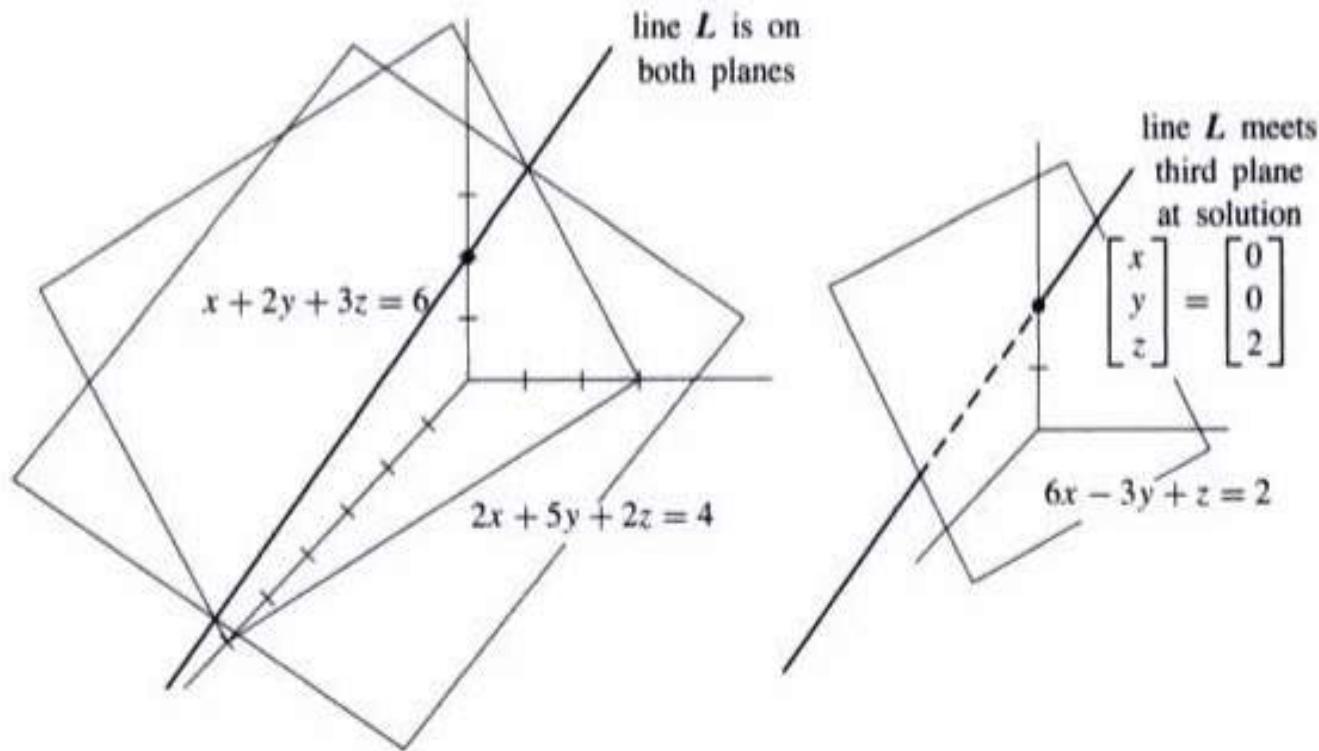
The three unknowns are  $x, y, z$ . The linear equations  $Ax = b$  are

$$\begin{array}{rcl} x + 2y + 3z & = & 6 \\ 2x + 5y + 2z & = & 4 \\ 6x - 3y + z & = & 2 \end{array} \tag{3}$$

We look for numbers  $x, y, z$  that solve all three equations at once. Those desired numbers might or might not exist. For this system, they do exist. When the number of unknowns matches the number of equations, there is *usually* one solution. Before solving the problem, we visualize it both ways:

# Row Picture

**The row picture shows three planes meeting at a single point.**



**Row picture of three equations: Three planes meet at a point.**

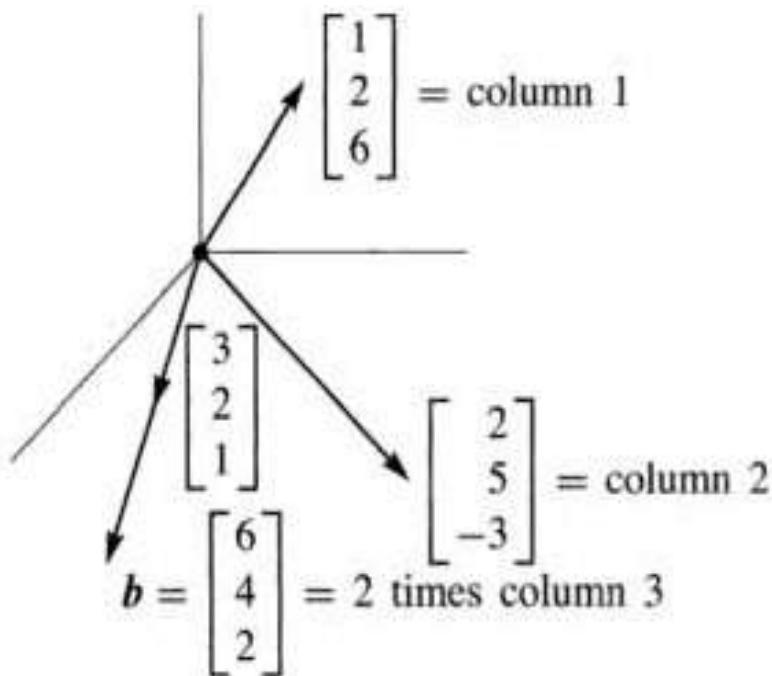
# Column Picture

**The column picture combines three columns to produce the vector  $(6, 4, 2)$ .**

**The column picture starts with the vector form of the equations:**

$$x \begin{bmatrix} 1 \\ 2 \\ 6 \end{bmatrix} + y \begin{bmatrix} 2 \\ 5 \\ -3 \end{bmatrix} + z \begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 6 \\ 4 \\ 2 \end{bmatrix}. \quad (4)$$

The unknown numbers  $x, y, z$  are the coefficients in this linear combination. We want to multiply the three column vectors by the correct numbers  $x, y, z$  to produce  $\mathbf{b} = (6, 4, 2)$ .



**Figure 2.4** Column picture:  $(x, y, z) = (0, 0, 2)$  because  $2(3, 2, 1) = (6, 4, 2) = b$ .

Figure 2.4 shows this column picture. Linear combinations of those columns can produce any vector  $b$ ! The combination that produces  $b = (6, 4, 2)$  is just 2 times the third column. *The coefficients we need are  $x = 0$ ,  $y = 0$ , and  $z = 2$ .* This is also the intersection point of the three planes in the row picture. It solves the system:

# Coefficient Matrix

The coefficient matrix for the system of equations in example 2 is given by

Example 2

$$\begin{array}{l} x + 2y + 3z = 6 \\ 2x + 5y + 2z = 4 \\ 6x - 3y + z = 2 \end{array}$$

*The coefficient matrix is  $A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 2 \\ 6 & -3 & 1 \end{bmatrix}$ .*

# Matrix equation

- Representing Example 2 as a matrix problem

$$AX = b$$

*Matrix equation*

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 2 \\ 6 & -3 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 6 \\ 4 \\ 2 \end{bmatrix}.$$

# ELIMINATION USING MATRICES

- Let us consider the following example

$$\begin{aligned}x - 2y &= 1 \\3x + 2y &= 11\end{aligned}$$

As you know , We can solve these linear equation with two unknowns by the method of elimination

<b>Before</b>	$x - 2y = 1$	<b>After</b>	$x - 2y = 1$	<i>(multiply by 3 and subtract)</i>
	$3x + 2y = 11$		$8y = 8$	<i>(x has been eliminated)</i>

The last equation  $8y = 8$  instantly gives  $y = 1$ . Substituting for  $y$  in the first equation leaves  $x - 2 = 1$ . Therefore  $x = 3$  and the solution  $(x, y) = (3, 1)$  is complete.

Elimination produces an **upper triangular system**—this is the goal. The nonzero coefficients 1,  $-2$ , 8 form a triangle. The last equation  $8y = 8$  reveals  $y = 1$ , and we go up the triangle to  $x$ . This quick process is called **back substitution**. It is used for upper triangular systems of any size, after forward elimination is complete.

# We now combine two ideas elimination and matrices

- The goal is to express all the steps of elimination in the clearest possible way .
- You will see how to subtract a multiple of one row from another row using matrices

# Let us consider an example with three unknowns

$$\begin{aligned} 2x_1 + 4x_2 - 2x_3 &= 2 \\ 4x_1 + 9x_2 - 3x_3 &= 8 \quad \text{is the same as} \\ -2x_1 - 3x_2 + 7x_3 &= 10 \end{aligned} \qquad \left[ \begin{array}{ccc|c} 2 & 4 & -2 & 2 \\ 4 & 9 & -3 & 8 \\ -2 & -3 & 7 & 10 \end{array} \right] \left[ \begin{array}{c} x_1 \\ x_2 \\ x_3 \end{array} \right] = \left[ \begin{array}{c} 2 \\ 8 \\ 10 \end{array} \right].$$

Here system of linear equations are expressed in  $AX=b$  form

*The unknown is  $x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$  and the solution is  $x = \begin{bmatrix} -1 \\ 2 \\ 2 \end{bmatrix}$ .*

Key point:  $Ax = b$  represents the row form and also the column form of the equations.  
We can multiply by taking a column of  $A$  at a time:

$$Ax = (-1) \begin{bmatrix} 2 \\ 4 \\ -2 \end{bmatrix} + 2 \begin{bmatrix} 4 \\ 9 \\ -3 \end{bmatrix} + 2 \begin{bmatrix} -2 \\ -3 \\ 7 \end{bmatrix} = \begin{bmatrix} 2 \\ 8 \\ 10 \end{bmatrix}.$$

**2A** The product  $Ax$  is a combination of the columns of  $A$ . Components of  $x$  multiply columns:  $Ax = x_1$  times (column 1) +  $\cdots$  +  $x_n$  times (column  $n$ ).

One point to repeat about matrix notation: The entry in row 1, column 1 (the top left corner) is called  $a_{11}$ . The entry in row 1, column 3 is  $a_{13}$ . The entry in row 3, column 1 is  $a_{31}$ . (Row number comes before column number.) The word “entry” for a matrix corresponds to the word “component” for a vector. General rule: *The entry in row  $i$ , column  $j$  of the matrix  $A$  is  $a_{ij}$ .*

**Example 1** This matrix has  $a_{ij} = 2i + j$ . Then  $a_{11} = 3$ . Also  $a_{12} = 4$  and  $a_{21} = 5$ . Here is  $Ax$  with numbers and letters:

$$\begin{bmatrix} 3 & 4 \\ 5 & 6 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \cdot 2 + 4 \cdot 1 \\ 5 \cdot 2 + 6 \cdot 1 \end{bmatrix} \quad \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} a_{11}x_1 + a_{12}x_2 \\ a_{21}x_1 + a_{22}x_2 \end{bmatrix}.$$

The first component of  $Ax$  is  $6 + 4 = 10$ . That is the product of the row  $[3 \ 4]$  with the column  $(2, 1)$ . *A row times a column gives a dot product!*

The  $i$ th component of  $Ax$  involves row  $i$ , which is  $[a_{i1} \ a_{i2} \ \cdots \ a_{in}]$ . The short formula for its dot product with  $x$  uses “sigma notation”:

**2B** The  $i$ th component of  $Ax$  is  $a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n$ . This is

$$\sum_{j=1}^n a_{ij}x_j$$

The sigma symbol  $\sum$  is an instruction to add. Start with  $j = 1$  and stop with  $j = n$ . Start the sum with  $a_{i1}x_1$  and stop with  $a_{in}x_n$ .<sup>1</sup>

# Matrix form of one elimination step

- Here we want to change  $\mathbf{b}$  to  $\mathbf{b}_{\text{new}}$ .

$$\mathbf{b} = \begin{bmatrix} 2 \\ 8 \\ 10 \end{bmatrix} \quad \text{changes to} \quad \mathbf{b}_{\text{new}} = \begin{bmatrix} 2 \\ 4 \\ 10 \end{bmatrix}.$$

We want to do that subtraction with a matrix! The same result  $\mathbf{b}_{\text{new}} = E\mathbf{b}$  is achieved when we multiply an “elimination matrix”  $E$  times  $\mathbf{b}$ . It subtracts  $2b_1$  from  $b_2$ :

*The elimination matrix is*  $E = \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$

**Multiplication by  $E$  subtracts 2 times row 1 from row 2.** Rows 1 and 3 stay the same:

$$\begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 8 \\ 10 \end{bmatrix} = \begin{bmatrix} 2 \\ 4 \\ 10 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 - 2b_1 \\ b_3 \end{bmatrix}$$

Notice how  $b_1 = 2$  and  $b_3 = 10$  stay the same. The first and third rows of  $E$  are the first and third rows of the identity matrix  $I$ . The new second component is the number 4 that appeared after the elimination step. This is  $b_2 - 2b_1$ .

# Definition of elimination matrix

It is easy to describe the “elementary matrices” or “elimination matrices” like  $E$ . Start with the identity matrix  $I$ . *Change one of its zeros to the multiplier  $-\ell$ :*

**2C** The *identity matrix* has 1’s on the diagonal and otherwise 0’s. Then  $Ib = b$ . The *elementary matrix or elimination matrix*  $E_{ij}$  that subtracts a multiple  $\ell$  of row  $j$  from row  $i$  has the extra nonzero entry  $-\ell$  in the  $i, j$  position.

Example:

$$\text{Identity } I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{Elimination } E_{31} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -4 & 0 & 1 \end{bmatrix}.$$

When you multiply  $I$  times  $b$ , you get  $b$ . But  $E_{31}$  subtracts  $\ell$  times the first component from the third component. With  $\ell = 4$  we get  $9 - 4 = 5$ :

$$Ib = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \\ 9 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \\ 9 \end{bmatrix} \quad \text{and} \quad Eb = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -4 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \\ 9 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \\ 5 \end{bmatrix}.$$

$$v = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}_{3 \times 1}$$

$$\omega = \begin{bmatrix} 1 & 2 & 3 \end{bmatrix}_{1 \times 3}$$

$$A = B$$

$$v = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} \quad \omega = \begin{bmatrix} 10 \\ 5 \\ 6 \end{bmatrix}$$

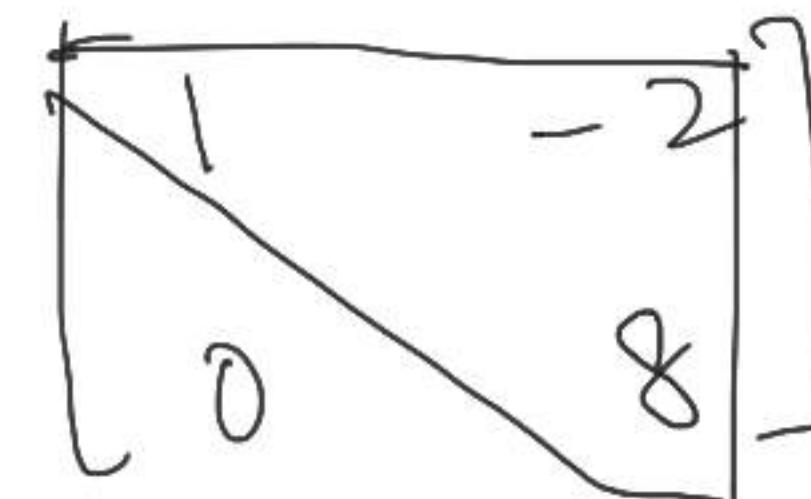
$$v \cdot \omega = [1 \ 2 \ 3] \begin{bmatrix} 10 \\ 5 \\ 6 \end{bmatrix} = 1 \times 10 + 2 \times 5 + 3 \times 6$$

$$2x - 3y = -2$$

$$x + 5y = 6$$

$$\begin{array}{l} x - 2y = 1 \\ 3x + 2y = 11 \end{array}$$

$$\begin{array}{l} x - 2y = 1 \\ 8y = 8 \end{array}$$

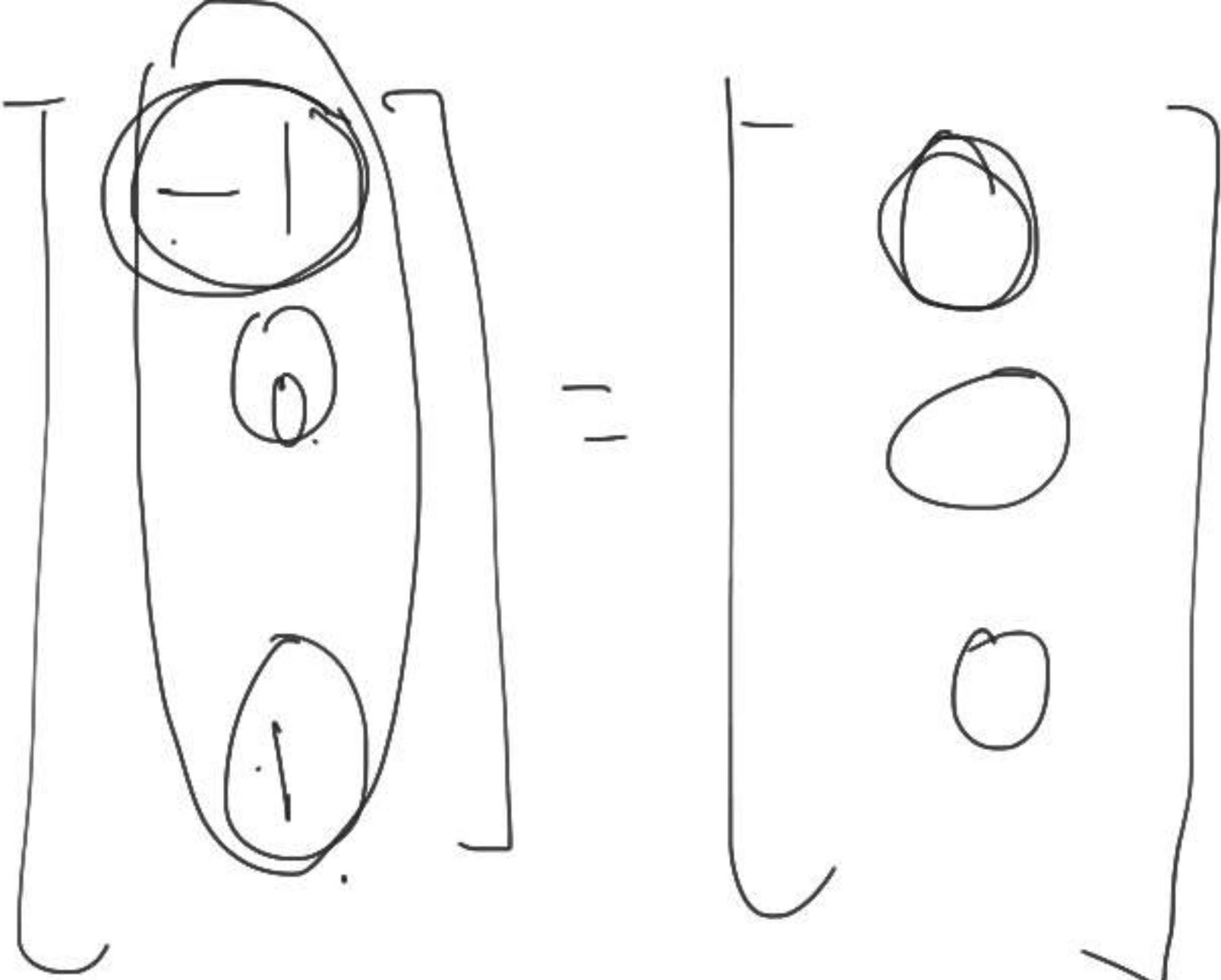
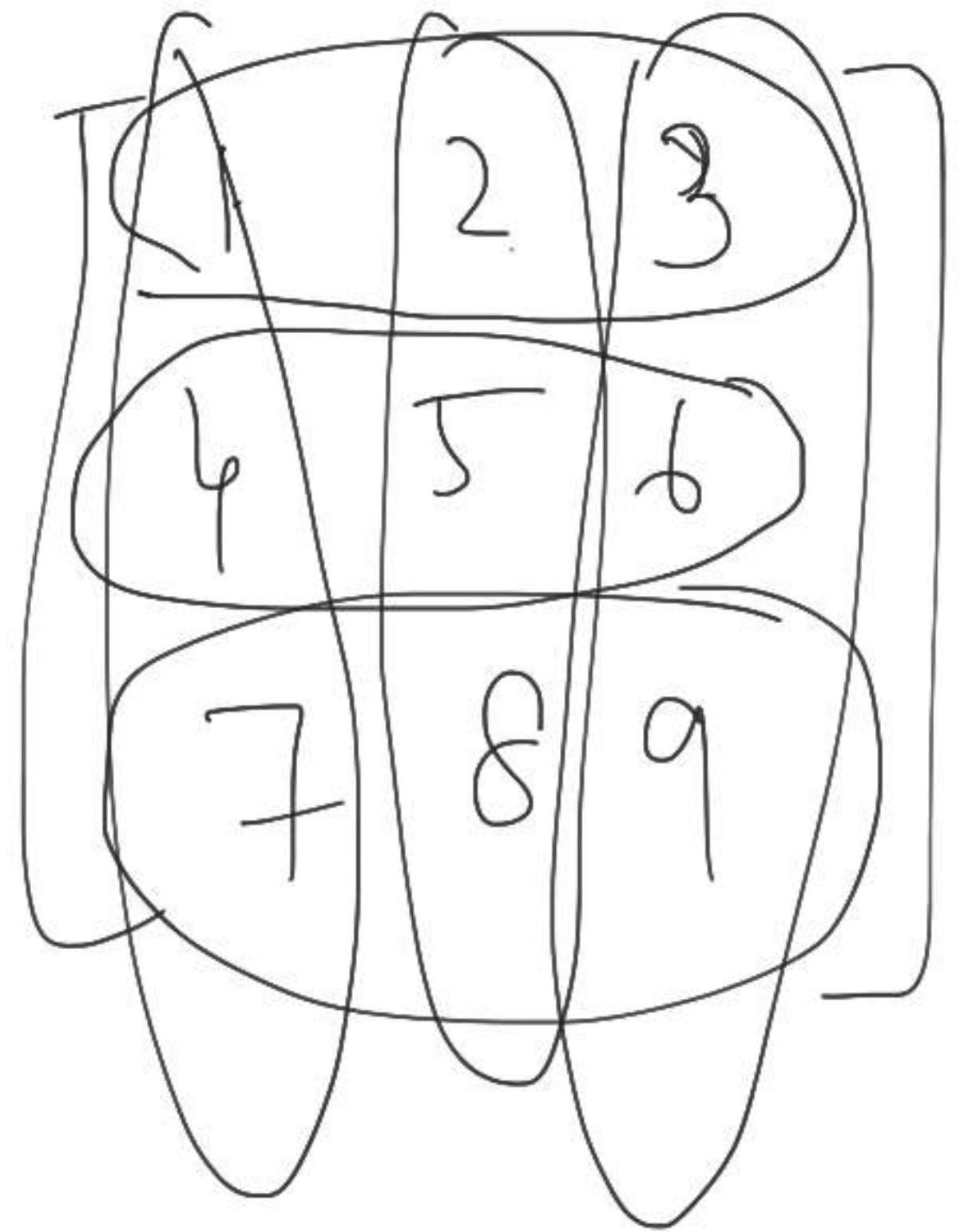


$$x - 3y + 2z = 0$$

$$x + y + z = 3$$

$$x - 5y + 6z = 2$$

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = b$$



$$\begin{bmatrix}
 1 & 0 & 0 \\
 -2 & 1 & 0 \\
 0 & 0 & 1
 \end{bmatrix}
 \begin{bmatrix}
 2 \\
 8 \\
 10
 \end{bmatrix}
 =
 \begin{bmatrix}
 2 \\
 4 \\
 10
 \end{bmatrix}$$

$A$        $b$        $=$        $b_{\text{new}}$

$R_2 = R_2 - 2 \times R_1$

E



# Matrix form of one elimination step

- Here we want to change  $\mathbf{b}$  to  $\mathbf{b}_{\text{new}}$ .

$$\mathbf{b} = \begin{bmatrix} 2 \\ 8 \\ 10 \end{bmatrix} \quad \text{changes to} \quad \mathbf{b}_{\text{new}} = \begin{bmatrix} 2 \\ 4 \\ 10 \end{bmatrix}.$$

We want to do that subtraction with a matrix! The same result  $\mathbf{b}_{\text{new}} = E\mathbf{b}$  is achieved when we multiply an “elimination matrix”  $E$  times  $\mathbf{b}$ . It subtracts  $2b_1$  from  $b_2$ :

*The elimination matrix is*  $E = \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$

**Multiplication by  $E$  subtracts 2 times row 1 from row 2.** Rows 1 and 3 stay the same:

$$\begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 8 \\ 10 \end{bmatrix} = \begin{bmatrix} 2 \\ 4 \\ 10 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 - 2b_1 \\ b_3 \end{bmatrix}$$

Notice how  $b_1 = 2$  and  $b_3 = 10$  stay the same. The first and third rows of  $E$  are the first and third rows of the identity matrix  $I$ . The new second component is the number 4 that appeared after the elimination step. This is  $b_2 - 2b_1$ .

# Definition of elimination matrix

It is easy to describe the “elementary matrices” or “elimination matrices” like  $E$ . Start with the identity matrix  $I$ . Change one of its zeros to the multiplier  $-\ell$ :

**2C** The *identity matrix* has 1’s on the diagonal and otherwise 0’s. Then  $I\mathbf{b} = \mathbf{b}$ .  
The *elementary matrix or elimination matrix*  $E_{ij}$  that subtracts a multiple  $\ell$  of row  $j$  from row  $i$  has the extra nonzero entry  $-\ell$  in the  $i, j$  position.

Example:

$$\text{Identity } I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{Elimination } E_{31} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -4 & 0 & 1 \end{bmatrix}.$$

When you multiply  $I$  times  $\mathbf{b}$ , you get  $\mathbf{b}$ . But  $E_{31}$  subtracts  $\ell$  times the first component from the third component. With  $\ell = 4$  we get  $9 - 4 = 5$ :

$$I\mathbf{b} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \\ 9 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \\ 9 \end{bmatrix} \quad \text{and} \quad E\mathbf{b} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -4 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \\ 9 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \\ 5 \end{bmatrix}.$$

# Matrix multiplication

- Here E is the elimination matrix multiplied with Matrix A

- $EA = \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 4 & -2 \\ 4 & 9 & -3 \\ -2 & -3 & 7 \end{bmatrix} = \begin{bmatrix} 2 & 4 & -2 \\ 0 & 1 & 1 \\ -2 & -3 & 7 \end{bmatrix}$  (with the zero).

---

This step does not change rows 1 and 3 of A. Those rows are unchanged in  $EA$ —only row 2 is different. *Twice the first row has been subtracted from the second row.*

- Matrix multiplication agrees with elimination

Consider,       $Ax=b$

Multiplying Elimination matrix E on both sides

$$E(Ax)=Eb$$

$(EA)x=Eb$  ( by associative law  $A(BC)=(AB)C$  )

often  $AB \neq BA$ )

It can be represented as  $EAx=Eb$  ( parentheses not need)

Note  $EA \neq AE$  ( not commutative)

# Row Exchange Matrix

**2E Row Exchange Matrix**  $P_{ij}$  is the identity matrix with rows  $i$  and  $j$  reversed.  
When  $P_{ij}$  multiplies a matrix  $A$ , it exchanges rows  $i$  and  $j$  of  $A$ .

To exchange rows 2 and 3 . Use the following permutation matrix

**Permutation matrix**  $P_{23} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$

This is a **row exchange matrix**. Multiplying by  $P_{23}$  exchanges components 2 and 3 of any column vector. Therefore it also exchanges rows 2 and 3 of any matrix:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \\ 5 \end{bmatrix} = \begin{bmatrix} 1 \\ 5 \\ 3 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 4 & 1 \\ 0 & 0 & 3 \\ 0 & 6 & 5 \end{bmatrix} = \begin{bmatrix} 2 & 4 & 1 \\ 0 & 6 & 5 \\ 0 & 0 & 3 \end{bmatrix}.$$

# The Augmented Matrix

Key idea: Elimination does the same row operations to  $A$  and to  $b$ . We can include  $b$  as an extra column and follow it through elimination. The matrix  $A$  is enlarged or “augmented” by the extra column  $b$ :

Augmented matrix  $[A \ b] = \begin{bmatrix} 2 & 4 & -2 & 2 \\ 4 & 9 & -3 & 8 \\ -2 & -3 & 7 & 10 \end{bmatrix}$ .

Elimination acts on whole rows of this matrix. The left side and right side are both multiplied by  $E$ , to subtract 2 times equation 1 from equation 2. With  $[A \ b]$  those steps happen together:

$$\begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 4 & -2 & 2 \\ 4 & 9 & -3 & 8 \\ -2 & -3 & 7 & 10 \end{bmatrix} = \begin{bmatrix} 2 & 4 & -2 & 2 \\ 0 & 1 & 1 & 4 \\ -2 & -3 & 7 & 10 \end{bmatrix}.$$

The new second row contains 0, 1, 1, 4. The new second equation is  $x_2 + x_3 = 4$ . Matrix multiplication works by rows and at the same time by columns:

**R** (by rows): Each row of  $E$  acts on  $[A \ b]$  to give a row of  $[EA \ Eb]$ .

**C** (by columns):  $E$  acts on each column of  $[A \ b]$  to give a column of  $[EA \ Eb]$ .

# Gaussian Elimination

- Gaussian elimination is a method for solving matrix equations of the form  $\mathbf{Ax}=\mathbf{b}$

To perform Gaussian elimination starting with the system of equations

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kk} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{bmatrix},$$

compose the "augmented matrix equation"

$$\left[ \begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1k} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2k} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kk} & b_k \end{array} \right] \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix}.$$

The whole process of elimination is a sequence of row operations alias matrix multiplication

## Procedure to

For a 4 by 4 problem, or an  $n$  by  $n$  problem, elimination proceeds the same way. Here is the whole idea of forward elimination, column by column:

**Column 1.** Use the first equation to create zeros below the first pivot.

**Column 2.** Use the new equation 2 to create zeros below the second pivot.

**Columns 3 to  $n$ .** Keep going to find the other pivots and the triangular  $U$ .

The result of forward elimination is an upper triangular system.

Copyrighted

After column 2 we have

$$\begin{bmatrix} x & x & x & x \\ 0 & x & x & x \\ 0 & 0 & x & x \\ 0 & 0 & x & x \end{bmatrix}$$

We want

$$\begin{bmatrix} x & x & x & x \\ x & x & x & x \\ x & x & x & x \\ x & x & x & x \end{bmatrix}$$

A linear system becomes upper triangular after elimination.

The upper triangular system is solved by back substitution (starting at the bottom).

Elimination subtracts  $\ell_{ij}$  times equation  $j$  from equation  $i$ , to make the  $(i, j)$  entry zero.

Pivots are on the diagonal of the triangle after elimination

$$\rho_{i \leftarrow j} \left[ \begin{array}{cccc} x & x & x & x \\ 0 & x & x & x \\ 0 & 0 & x & x \\ 0 & 0 & x & x \end{array} \right]$$

The multiplier is  $\ell_{ij} = \frac{\text{entry to eliminate in row } i}{\text{pivot in row } j}$ . Pivots can not be zero!

A zero in the pivot position can be repaired if there is a nonzero below it.

If there is full set of pivots. It is nonsingular. Then the linear system has exactly one solution

If there is no full set of pivots. It is singular. Then the linear equations have infinitely many solutions or no solution

## example

- Solve using Gaussian elimination

$$2x + 4y - 2z = 2$$

$$4x + 9y - 3z = 8$$

$$-2x - 3y + 7z = 10$$

# Inverse matrices

**DEFINITION** The matrix  $A$  is *invertible* if there exists a matrix  $A^{-1}$  such that

$$A^{-1}A = I \quad \text{and} \quad AA^{-1} = I. \quad (1)$$

***Not all matrices have inverses.*** This is the first question we ask about a square matrix: Is  $A$  invertible? We don't mean that we immediately calculate  $A^{-1}$ . In most problems we never compute it! Here are six "notes" about  $A^{-1}$ .

**Note 1** ***The inverse exists if and only if elimination produces n pivots*** (row exchanges allowed). Elimination solves  $Ax = b$  without explicitly using  $A^{-1}$ .

$$A = \begin{bmatrix} 1 & -4 & 2 & 3 & 5 \\ -1 & 0 & 2 & 3 & 1 \\ 1 & 0 & 0 & 3 & 1 \end{bmatrix}$$

$$R_2 = R_2 - 4 \times R_1$$

$$E_{21} = \begin{bmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$EA_{21} = \begin{bmatrix} 1 & 3 & 5 \\ 0 & -10 & -19 \\ 1 & 0 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 3 & 5 \\ 4 & 2 & 1 \\ 1 & 0 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 3 & 5 \\ 1 & 0 & 3 \\ 4 & 2 & 1 \end{bmatrix}$$

P

A

$$\begin{bmatrix} 1 & 3 & 5 \\ 4 & 2 & 1 \\ 1 & 0 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 3 & 5 \\ 4 & 2 & 1 \\ 1 & 0 & 3 \end{bmatrix}$$

$$1x - 2y = 1$$

$$3x + 2y = 11$$

$$\begin{aligned} Ax &= b \\ Ux &= c \end{aligned}$$

multiplizier =  $\frac{1}{2}$

$$\begin{bmatrix} 1 & -2 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 11 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -2 \\ 0 & 8 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 8 \end{bmatrix}$$

pivot = first non-zero in the row  
that does the elimination

multiplier = (entry to eliminate) divided  
by (pivot)

$$\boxed{4}x - 8 = 4$$

$$l_{21} = \frac{3}{4}$$

$$3x + 2y = 1$$

# Breakdown of elimination

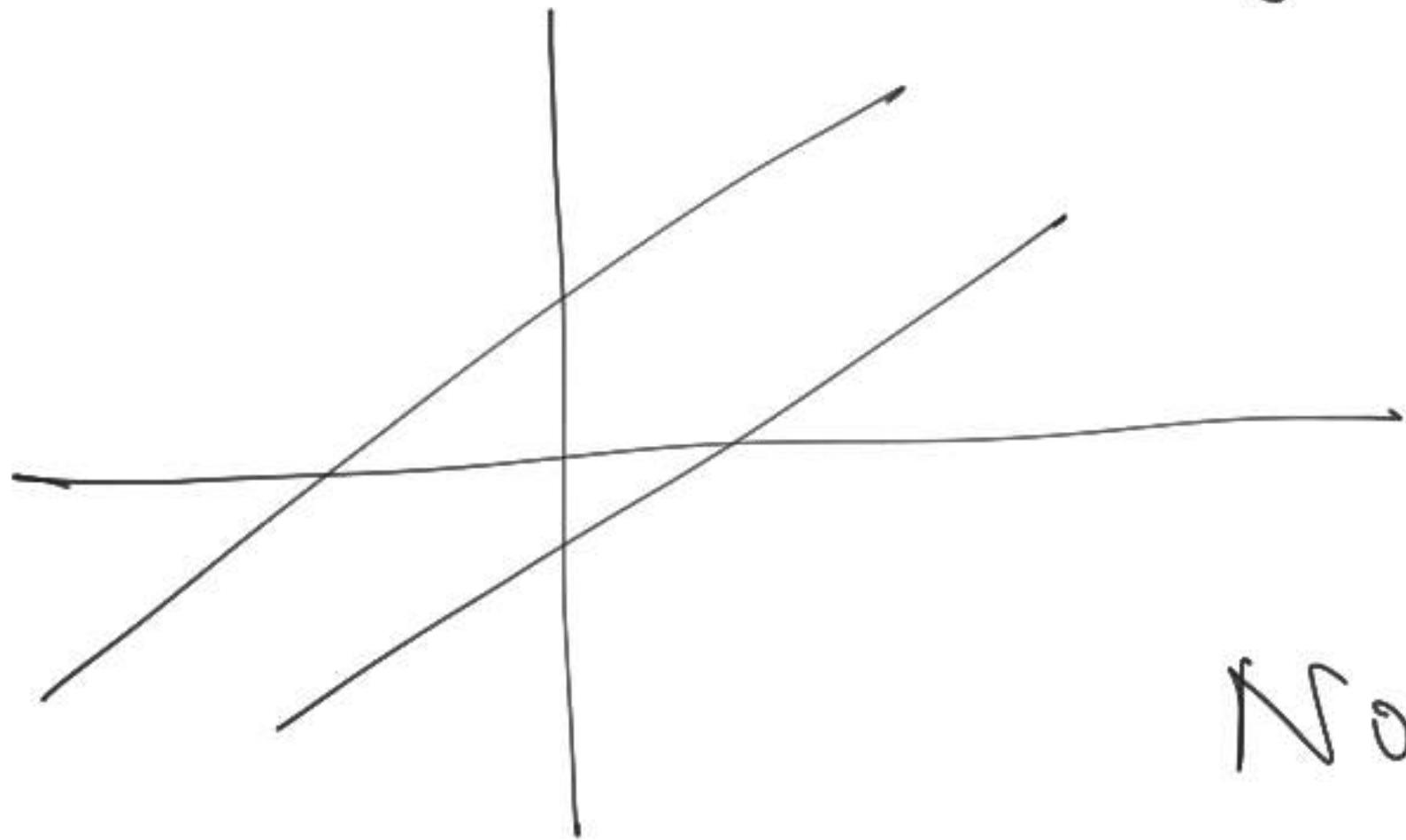
(1)

$$x - 2y = 1$$

$$x - 2y = 1$$

$$3x - 6y = 11$$

$$0y = 8$$



No sol<sup>n</sup>

$$\begin{array}{r} 1 \\ -2 \end{array}$$



②

$$x - 2y = 1$$

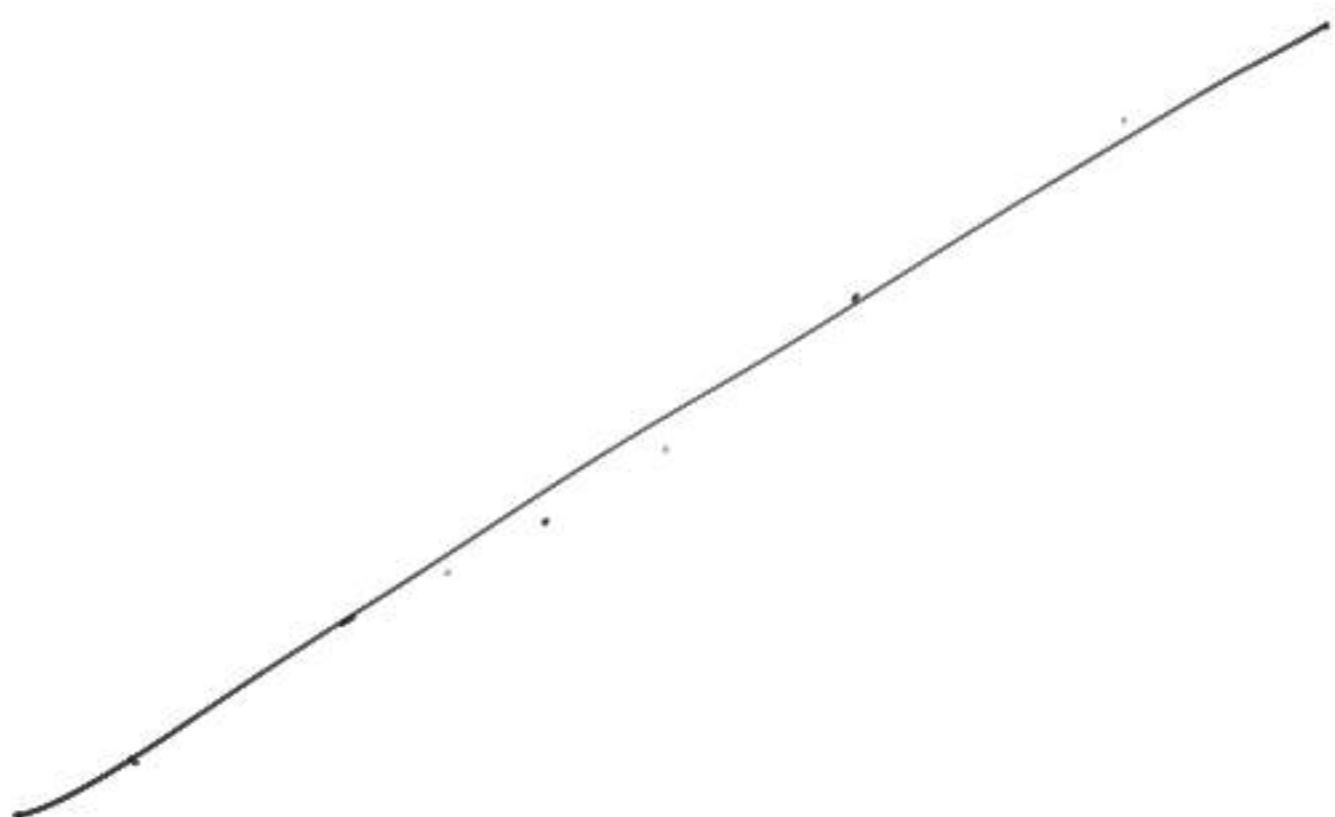
$$3x - 6y = 3$$

$$\boxed{x - 2y = 1}$$

$$0y = 0$$

Infinitely

many  
sol's.



3

Temporary failure

$$8x + 2y = 4$$

$$3x - 2y = 5$$

$$\boxed{3}x - 2y = 5$$

$$2y = 4$$

$$\left[ \begin{array}{ccc|c} 1 & -1 & 2 \\ 0 & \cancel{2} & \cancel{-3} & 4 \\ 0 & \cancel{2} & 2 & 1 \end{array} \right]$$

$$x - 2y = 1$$

$$R_g = R_2 - 3 \times R_1$$

$$3x + 2y = 1$$

$$\begin{bmatrix} 1 & -2 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -2 & 1 \\ 3 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -2 & 1 \\ 0 & 8 & 8 \end{bmatrix}$$

$$\left| \begin{array}{l} 2x + 4y - 2z = 2 \\ 4x + 9y - 3z = 8 \\ -2x - 3y + 7z = 10 \end{array} \right| \quad \left| \begin{array}{ccc|c} 2 & 4 & -2 & 2 \\ 0 & 1 & 1 & 4 \\ 0 & 1 & 5 & 12 \end{array} \right|$$

$$A = \left| \begin{array}{ccc|c} 2 & 4 & -2 & 2 \\ 4 & 9 & -3 & 8 \\ -2 & -3 & 7 & 10 \end{array} \right| \quad \xrightarrow{R_2 = R_2 - 2 \times R_1} \left| \begin{array}{ccc|c} 2 & 4 & -2 & 2 \\ 0 & 1 & 1 & 4 \\ -2 & -3 & 7 & 10 \end{array} \right|$$

$|A| = 8$

$\xrightarrow{u_x=0} \left| \begin{array}{ccc|c} 2 & 4 & -2 & 2 \\ 0 & 1 & 1 & 4 \\ 0 & 0 & 1 & 8 \end{array} \right|$

$$2x + 4y - 2z = 2 \quad x = -1$$

$$y + z = 4 \quad y = 2$$

$$4z = 8 \rightarrow z = 2$$





$$[A] \quad [M] = [AN]$$

$$[A^{-1}] \quad [AM] = [N]$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 2 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix} = \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix} \begin{bmatrix} R_3 - 2R_1 \\ R_3 - 2R_1 \\ R_3 - 2R_1 \end{bmatrix}$$

$$E_{31}^{-1} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix} \begin{bmatrix} F_{31} \\ F_{31} \\ F_{31} \end{bmatrix}$$

# Inverse matrices

**DEFINITION** The matrix  $A$  is *invertible* if there exists a matrix  $A^{-1}$  such that

$$A^{-1}A = I \quad \text{and} \quad AA^{-1} = I. \quad (1)$$

***Not all matrices have inverses.*** This is the first question we ask about a square matrix: Is  $A$  invertible? We don't mean that we immediately calculate  $A^{-1}$ . In most problems we never compute it! Here are six "notes" about  $A^{-1}$ .

---

**Note 1** *The inverse exists if and only if elimination produces  $n$  pivots* (row exchanges allowed). Elimination solves  $Ax = b$  without explicitly using  $A^{-1}$ .

**Note 2** The matrix  $A$  cannot have two different inverses. Suppose  $BA = I$  and also  $AC = I$ . Then  $B = C$ , according to this “proof by parentheses”:

$$B(AC) = (BA)C \quad \text{gives} \quad BI = IC \quad \text{or} \quad B = C. \quad (2)$$

This shows that a *left-inverse*  $B$  (multiplying from the left) and a *right-inverse*  $C$  (multiplying  $A$  from the right to give  $AC = I$ ) must be the *same matrix*.

**Note 3** If  $A$  is invertible, the one and only solution to  $Ax = b$  is  $x = A^{-1}b$ :

**Multiply**  $Ax = b$  **by**  $A^{-1}$ . **Then**  $x = A^{-1}Ax = A^{-1}b$ .

**Note 4** (Important) *Suppose there is a nonzero vector  $x$  such that  $Ax = \mathbf{0}$ . Then  $A$  cannot have an inverse.* No matrix can bring  $\mathbf{0}$  back to  $x$ .

If  $A$  is invertible, then  $Ax = \mathbf{0}$  can only have the zero solution  $x = \mathbf{0}$ .

**Note 5** A 2 by 2 matrix is invertible if and only if  $ad - bc$  is not zero:

**2 by 2 Inverse:** 
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}. \quad (3)$$

This number  $ad - bc$  is the *determinant* of  $A$ . A matrix is invertible if its determinant is not zero (Chapter 5). The test for  $n$  pivots is usually decided before the determinant appears.

**Note 6** A diagonal matrix has an inverse provided no diagonal entries are zero:

$$\text{If } A = \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{bmatrix} \text{ then } A^{-1} = \begin{bmatrix} 1/d_1 & & \\ & \ddots & \\ & & 1/d_n \end{bmatrix}.$$

**Example 1** The 2 by 2 matrix  $A = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}$  is not invertible. It fails the test in Note 5, because  $ad - bc$  equals  $2 - 2 = 0$ . It fails the test in Note 3, because  $Ax = 0$  when  $x = (2, -1)$ . It fails to have two pivots as required by Note 1. Elimination turns the second row of  $A$  into a zero row.

# Finding $A^{-1}$ by Gauss Jordan method

The Gauss-Jordan method solves  $AA^{-1} = I$  to find the  $n$  columns of  $A^{-1}$ . The augmented matrix  $[A \ I]$  is row-reduced to  $[I \ A^{-1}]$ .

**Example 4** Find  $A^{-1}$  by Gauss-Jordan elimination starting from  $A = \begin{bmatrix} 2 & 3 \\ 4 & 7 \end{bmatrix}$ . There are two row operations and then a division to put 1's in the pivots:

$$\begin{aligned}[A \ I] &= \begin{bmatrix} 2 & 3 & 1 & 0 \\ 4 & 7 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 2 & 3 & 1 & 0 \\ 0 & 1 & -2 & 1 \end{bmatrix} \\ &\rightarrow \begin{bmatrix} 2 & 0 & 7 & -3 \\ 0 & 1 & -2 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & \frac{7}{2} & -\frac{3}{2} \\ 0 & 1 & -2 & 1 \end{bmatrix} = [I \ A^{-1}].\end{aligned}$$

The reduced echelon form of  $[A \ I]$  is  $[I \ A^{-1}]$ . This  $A^{-1}$  involves division by the determinant  $2 \cdot 7 - 3 \cdot 4 = 2$ . The code for  $X = \text{inverse}(A)$  has three important lines!

# Example

- If  $A = \begin{bmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{bmatrix}$  Find  $A^{-1}$

# Factorization into A=LU

The Matrix A is represented as the product of 2 or 3 special matrices. The key idea is the factorization of matrix A into triangular matrices

$$A = LU$$

where U is upper triangular matrix with pivots on its diagonals

L is the lower triangular matrix with 1's as its diagonal elements

- The factorization that comes from the elimination is  $A = LU$  without row exchanges.

- We already know  $U$ , the upper triangular matrix with the pivots on its diagonal. The elimination steps take  $A$  to  $U$ . We will show how reversing those steps (taking  $U$  back to  $A$ ) is achieved by a lower triangular  $L$ . ***The entries of  $L$  are exactly the multipliers  $\ell_{ij}$*** —which multiplied row  $j$  when it was subtracted from row  $i$ .

Start with a 2 by 2 example. The matrix  $A$  contains 2, 1, 6, 8. The number to eliminate is 6. ***Subtract 3 times row 1 from row 2.*** That step is  $E_{21}$  in the forward direction. The return step from  $U$  to  $A$  is  $L = E_{21}^{-1}$  (an addition using +3):

$$\text{Forward from } A \text{ to } U : \quad E_{21}A = \begin{bmatrix} 1 & 0 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 6 & 8 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 0 & 5 \end{bmatrix} = U$$

$$\text{Back from } U \text{ to } A : \quad E_{21}^{-1}U = \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 0 & 5 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 6 & 8 \end{bmatrix} = A.$$

The second line is our factorization. Instead of  $E_{21}^{-1}U = A$  we write  $LU = A$ . Move now to larger matrices with many  $E$ 's. ***Then  $L$  will include all their inverses.***

Each step from  $A$  to  $U$  multiplies by a matrix  $E_{ij}$  to produce zero in the  $(i, j)$  position. To keep this clear, we stay with the most frequent case—***when no row exchanges are involved***. If  $A$  is 3 by 3, we multiply by  $E_{21}$  and  $E_{31}$  and  $E_{32}$ . The multipliers  $\ell_{ij}$  produce zeros in the  $(2, 1)$  and  $(3, 1)$  and  $(3, 2)$  positions—all below the diagonal. Elimination ends with the upper triangular  $U$ .

Now move those  $E$ 's onto the other side, *where their inverses multiply  $U$* :

$$(E_{32}E_{31}E_{21})A = U \quad \text{becomes} \quad A = (E_{21}^{-1}E_{31}^{-1}E_{32}^{-1})U \quad \text{which is} \quad A = LU. \quad (1)$$

$$E = \begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$E^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 5 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$E^{-1} E A = A$$

$$\begin{bmatrix} L \\ A \end{bmatrix} \begin{bmatrix} x \\ a \end{bmatrix} = \begin{bmatrix} b \end{bmatrix}$$

n pivots

$$x = A^{-1} b$$

$$U x = c$$

$$x = \begin{bmatrix} \end{bmatrix}$$

$$\begin{bmatrix} 1 & -2 \\ 5 & -10 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$A$        $\sqrt{x}$

$$Ax = b$$
$$x = A^{-1}b$$

$A$        $\circled{A} x = 0$

$x$

$$Ax = b$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

✓

$$x_1 + 2x_2 = 0$$

$$x_1 = 0$$

$$3x_1 + 4x_2 = 0$$

$$x_2 = 0$$

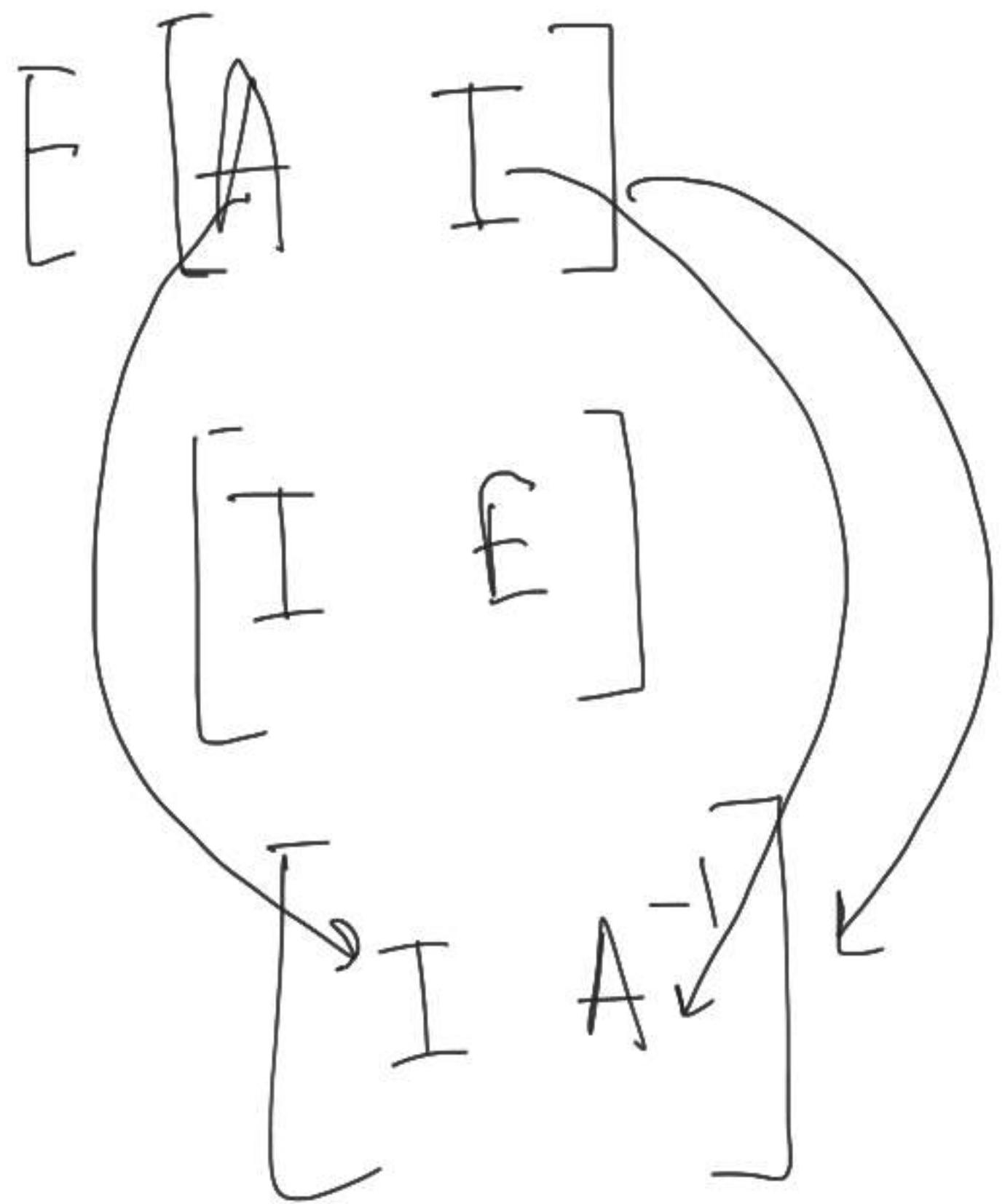
$$\begin{bmatrix} 1 & -2 \\ 5 & -10 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \end{bmatrix}$$

$$x - 2y = 3$$

$$\checkmark 5x - 10y = 1$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

✓



$$I = E \xrightarrow{A} A^{-1}$$

$$[A \quad I] = \begin{bmatrix} 2 & -1 & 0 & 1 & 0 & 0 \\ -1 & 2 & -1 & 0 & 1 & 0 \\ 0 & -1 & 2 & 0 & 0 & 1 \end{bmatrix}$$

$$A \quad I$$

$$\frac{2}{3} \quad \frac{2}{3} \quad 0$$

$$\frac{4}{3}$$

$$= \begin{bmatrix} 2 & -1 & 0 & 1 & 0 & 0 \\ 0 & \frac{3}{2} & -1 & \frac{1}{2} & 1 & 0 \\ 0 & -1 & 2 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 2 & -1 & 0 & 1 & 0 & 0 \\ 0 & \frac{3}{2} & -1 & \frac{1}{2} & 1 & 0 \\ 0 & 0 & \frac{4}{3} & \frac{1}{3} & \frac{2}{3} & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 2 & -1 & 0 & 1 & 0 & 0 \\ 0 & \frac{3}{2} & 0 & \frac{3}{4} & \frac{3}{2} & \frac{3}{4} \\ 0 & 0 & \frac{4}{3} & \frac{1}{3} & \frac{2}{3} & 1 \end{bmatrix}$$

$$R_1 = R_1 - \frac{2}{3} \times R_2$$

$$\therefore \begin{bmatrix} 2 & 0 & 0 & \frac{3}{2} & 1 & \frac{1}{2} \\ 0 & \frac{3}{2} & 0 & \frac{3}{4} & \frac{3}{2} & \frac{3}{4} \\ 0 & 0 & \frac{4}{3} & \frac{1}{3} & \frac{2}{3} & 1 \end{bmatrix}$$

$$\therefore \begin{bmatrix} 1 & 0 & 0 & \frac{3}{4} & \frac{1}{2} & \frac{1}{4} \\ 0 & 1 & 0 & \frac{1}{2} & 1 & \frac{1}{2} \\ 0 & 0 & 1 & \frac{1}{4} & \frac{1}{2} & \frac{3}{4} \end{bmatrix} \rightarrow A^{-1}$$

$E_{32} \quad E_{31} \quad E_{21}$ 

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} = \mathcal{U}$$

$A$

$$\frac{E_{-1}^{-1} \quad E_{-1}^{-1} \quad E_{-1}^{-1} \quad \mathcal{U}}{L \quad \mathcal{U} = A} = A$$

**Remark** The  $LU$  factorization is “unsymmetric” because  $U$  has the pivots on its diagonal where  $L$  has 1's. This is easy to change. **Divide  $U$  by a diagonal matrix  $D$  that contains the pivots.** That leaves a new matrix with 1's on the diagonal:

$$\text{Split } U \text{ into} \begin{bmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_n \end{bmatrix} \begin{bmatrix} 1 & u_{12}/d_1 & u_{13}/d_1 & \cdot \\ & 1 & u_{23}/d_2 & \cdot \\ & & \ddots & \vdots \\ & & & 1 \end{bmatrix}.$$

It is convenient (but a little confusing) to keep the same letter  $U$  for this new upper triangular matrix. It has 1's on the diagonal (like  $L$ ). Instead of the normal  $LU$ , the new form has  $D$  in the middle: **Lower triangular  $L$  times diagonal  $D$  times upper triangular  $U$ .**

- Factorize  $A = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 4 & 2 \\ 6 & 3 & 5 \end{bmatrix}$  into LU and LDU

# Transpose of a matrix

We need one more matrix, and fortunately it is much simpler than the inverse. It is the “*transpose*” of  $A$ , which is denoted by  $A^T$ . *The columns of  $A^T$  are the rows of  $A$ .*

When  $A$  is an  $m$  by  $n$  matrix, the transpose is  $n$  by  $m$ :

$$\text{If } A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 0 & 4 \end{bmatrix} \text{ then } A^T = \begin{bmatrix} 1 & 0 \\ 2 & 0 \\ 3 & 4 \end{bmatrix}.$$

You can write the rows of  $A$  into the columns of  $A^T$ . Or you can write the columns of  $A$  into the rows of  $A^T$ . The matrix “flips over” its main diagonal. The entry in row  $i$ , column  $j$  of  $A^T$  comes from row  $j$ , column  $i$  of the original  $A$ :

$$(A^T)_{ij} = A_{ji}.$$

The transpose of a lower triangular matrix is upper triangular. (But the inverse is still lower triangular.) The transpose of  $A^T$  is  $A$ .

# Properties of Transpose of matrices

- Transpose of  $A+B$  is  $A^T + B^T$
- The Transpose of  $AB$  is  $B^T A^T$
- The Transpose of  $A^{-1}$  is  $(A^{-1})^T = (A^T)^{-1}$

**Example 1** The inverse of  $A = \begin{bmatrix} 1 & 0 \\ 6 & 1 \end{bmatrix}$  is  $A^{-1} = \begin{bmatrix} 1 & 0 \\ -6 & 1 \end{bmatrix}$ . The transpose is  $A^T = \begin{bmatrix} 1 & 6 \\ 0 & 1 \end{bmatrix}$ .

$(A^{-1})^T$  and  $(A^T)^{-1}$  are both equal to  $\begin{bmatrix} 1 & -6 \\ 0 & 1 \end{bmatrix}$ .

# Symmetric Matrix

**DEFINITION** A *symmetric matrix* has  $A^T = A$ . This means that  $a_{ji} = a_{ij}$ .

**Example 2**  $A = \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix} = A^T$  and  $D = \begin{bmatrix} 1 & 0 \\ 0 & 10 \end{bmatrix} = D^T$ .

$A$  is symmetric because of the 2's on opposite sides of the diagonal. The rows agree with the columns. In  $D$  those 2's are zeros. Every diagonal matrix is symmetric.

**The inverse of a symmetric matrix is also symmetric.** (We have to add: "If  $A$  is invertible.") The transpose of  $A^{-1}$  is  $(A^{-1})^T = (A^T)^{-1} = A^{-1}$ , so  $A^{-1}$  is symmetric:

$$A^{-1} = \begin{bmatrix} 5 & -2 \\ -2 & 1 \end{bmatrix} \quad \text{and} \quad D^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 0.1 \end{bmatrix}.$$

Now we show that *multiplying any matrix  $R$  by  $R^T$  gives a symmetric matrix*.

2K If  $A = A^T$  can be factored into  $LDU$  with no row exchanges, then  $U = L^T$ .  
The symmetric factorization of a symmetric matrix is  $A = LDL^T$ .

- Example factorize the matrix  $A = \begin{bmatrix} 1 & 2 \\ 2 & 7 \end{bmatrix}$
- Here  $A = A^T$

$$\begin{bmatrix} 1 & 2 \\ 2 & 7 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

# Permutation Matrices

**DEFINITION** A *permutation matrix*  $P$  has the rows of  $I$  in any order.

The transpose plays a special role for a *permutation matrix*. This matrix  $P$  has a single “1” in every row and every column. Then  $P^T$  is also a permutation matrix—maybe the same or maybe different. Any product  $P_1 P_2$  is again a permutation matrix. We now create every  $P$  from the identity matrix, by reordering the rows of  $I$ .

The simplest permutation matrix is  $P = I$  (*no exchanges*). The next simplest are the row exchanges  $P_{ij}$ . Those are constructed by exchanging two rows  $i$  and  $j$  of  $I$ . Other permutations reorder more rows. By doing all possible row exchanges to  $I$ , we get all possible permutation matrices:

**Example 4** There are six 3 by 3 permutation matrices. Here they are without the zeros:

$$I = \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix} \quad P_{21} = \begin{bmatrix} 1 & 1 & \\ 1 & & 1 \end{bmatrix} \quad P_{32}P_{21} = \begin{bmatrix} 1 & 1 & \\ 1 & & 1 \end{bmatrix}$$
$$P_{31} = \begin{bmatrix} & 1 & \\ 1 & & \\ & 1 & \end{bmatrix} \quad P_{32} = \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix} \quad P_{21}P_{32} = \begin{bmatrix} 1 & 1 & \\ 1 & & 1 \end{bmatrix}.$$

More important:  $P^{-1}$  is always the same as  $P^T$ . The two matrices on the right are transposes—and inverses—of each other. When we multiply  $PP^T$ , the “1” in the first row of  $P$  hits the “1” in the first column of  $P^T$  (since the first row of  $P$  is the first column of  $P^T$ ). It misses the ones in all the other columns. So  $PP^T = I$ .

Another proof of  $P^T = P^{-1}$  looks at  $P$  as a product of row exchanges. A row exchange is its own transpose and its own inverse.  $P^T$  and  $P^{-1}$  both come from the product of row exchanges in the opposite order. So  $P^T$  and  $P^{-1}$  are the same.

**Symmetric matrices lead to  $A = LDL^T$ . Now permutations lead to  $PA = LU$ .**

## Definition

2L If  $A$  is invertible, a permutation  $P$  will put its rows in the right order to factor  $PA = LU$ . There must be a full set of pivots, after row exchanges.

### Example

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 2 & 1 \\ 2 & 7 & 9 \end{bmatrix} \xrightarrow{A} \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 2 & 7 & 9 \end{bmatrix} \xrightarrow{PA} \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 3 & 7 \end{bmatrix} \xrightarrow{\ell_{31}=2} \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 4 \end{bmatrix} \xrightarrow{\ell_{32}=3}$$

The matrix  $PA$  is in good order, and it factors as usual into  $L U$ :

$$PA = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 4 \end{bmatrix} = LU. \quad (8)$$

We started with  $A$  and ended with  $U$ . *The only requirement is invertibility of  $A$ .*

# VECTOR SPACES AND SUBSPACES

- Previously we have studied that

The columns of  $Ax$  and  $AB$  are linear combinations of  $n$  vectors—the columns of  $A$ . This chapter moves from numbers and vectors to a third level of understanding (the highest level). Instead of individual columns, we look at “spaces” of vectors. Without seeing *vector spaces* and especially their *subspaces*, you haven’t understood everything about  $Ax = b$ .

We begin with the most important vector spaces. They are denoted by  $\mathbf{R}^1$ ,  $\mathbf{R}^2$ ,  $\mathbf{R}^3$ ,  $\mathbf{R}^4$ , . . . . Each space  $\mathbf{R}^n$  consists of a whole collection of vectors.  $\mathbf{R}^5$  contains all column vectors with five components. This is called “5-dimensional space.”

# Definition

**DEFINITION** *The space  $\mathbf{R}^n$  consists of all column vectors  $v$  with  $n$  components.*

The components of  $v$  are real numbers, which is the reason for the letter  $\mathbf{R}$ . A vector whose  $n$  components are complex numbers lies in the space  $\mathbf{C}^n$ .

The vector space  $\mathbf{R}^2$  is represented by the usual  $xy$  plane. Each vector  $v$  in  $\mathbf{R}^2$  has two components. The word “space”, asks us to think of all those vectors—the whole plane. Each vector gives the  $x$  and  $y$  coordinates of a point in the plane.

Similarly the vectors in  $\mathbf{R}^3$  correspond to points  $(x, y, z)$  in three-dimensional space. The one-dimensional space  $\mathbf{R}^1$  is a line (like the  $x$  axis). As before, we print vectors as a column between brackets, or along a line using commas and parentheses:

$$\begin{bmatrix} 4 \\ 0 \\ 1 \end{bmatrix} \text{ is in } \mathbf{R}^3, \quad (1, 1, 0, 1, 1) \text{ is in } \mathbf{R}^5, \quad \begin{bmatrix} 1+i \\ 1-i \end{bmatrix} \text{ is in } \mathbf{C}^2.$$

$$A \rightarrow U$$

$$A = L U$$

$$A = \begin{bmatrix} 1 & 2 & 3 \\ * & 5 & 6 \\ * & * & 9 \end{bmatrix}$$

$$E_{32} E_{31} E_{21} A = U$$

$$A = \underbrace{E_{21}^{-1} E_{31}^{-1} E_{32}^{-1}}_L U$$

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 3 & 5 \\ 4 & 6 & 8 \end{bmatrix}$$

Factorize  $A = LU$

$$\begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -4 & 0 & 1 \end{bmatrix}$$

$$A =$$

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 3 \\ 0 & 2 & 4 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{bmatrix}$$

$$\begin{bmatrix} E_{31} & E_{21} \\ E_{31} & E_{21} \end{bmatrix}$$

$$A =$$

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 3 \\ 0 & 0 & -2 \end{bmatrix}$$

$$L = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 2 & 1 \end{bmatrix} = E_{21}^{-1} E_{31}^{-1} E_{32}^{-1}$$

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 2 & 1 \end{bmatrix} \xrightarrow{L} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{bmatrix} \xrightarrow{U}$$

$$F = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -y & 1 \end{bmatrix}$$

$$F^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & y & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 2 & 8 \\ 0 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 5 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}$$

L                  U                  ✓  
 ✓                  D                  ✓  
 ✓                  ✓

$A = LDU$

$RR^T$  is symmetric

$$(RR^T)^T = (R^T)^T R^T = RR^T$$

$$A = L D W \quad A^T = W^T D L^T$$

$$A^T = A$$

|

$$= L D W$$

$$\boxed{L^T = W}$$

$$\begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix} - 2 \begin{bmatrix} 2 \\ -1 \\ 3 \end{bmatrix} = 2 \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} - 1 \begin{bmatrix} 4 \\ 5 \\ 6 \end{bmatrix} + 3 \begin{bmatrix} 7 \\ 8 \\ 9 \end{bmatrix}$$

$A$

# VECTOR SPACES AND SUBSPACES

- Previously we have studied that

The columns of  $Ax$  and  $AB$  are linear combinations of  $n$  vectors—the columns of  $A$ . This chapter moves from numbers and vectors to a third level of understanding (the highest level). Instead of individual columns, we look at “spaces” of vectors. Without seeing *vector spaces* and especially their *subspaces*, you haven’t understood everything about  $Ax = b$ .

We begin with the most important vector spaces. They are denoted by  $\mathbf{R}^1$ ,  $\mathbf{R}^2$ ,  $\mathbf{R}^3$ ,  $\mathbf{R}^4$ , . . . . Each space  $\mathbf{R}^n$  consists of a whole collection of vectors.  $\mathbf{R}^5$  contains all column vectors with five components. This is called “5-dimensional space.”

# Definition

**DEFINITION** *The space  $\mathbf{R}^n$  consists of all column vectors  $v$  with  $n$  components.*

The components of  $v$  are real numbers, which is the reason for the letter  $\mathbf{R}$ . A vector whose  $n$  components are complex numbers lies in the space  $\mathbf{C}^n$ .

The vector space  $\mathbf{R}^2$  is represented by the usual  $xy$  plane. Each vector  $v$  in  $\mathbf{R}^2$  has two components. The word “space”, asks us to think of all those vectors—the whole plane. Each vector gives the  $x$  and  $y$  coordinates of a point in the plane.

Similarly the vectors in  $\mathbf{R}^3$  correspond to points  $(x, y, z)$  in three-dimensional space. The one-dimensional space  $\mathbf{R}^1$  is a line (like the  $x$  axis). As before, we print vectors as a column between brackets, or along a line using commas and parentheses:

$$\begin{bmatrix} 4 \\ 0 \\ 1 \end{bmatrix} \text{ is in } \mathbf{R}^3, \quad (1, 1, 0, 1, 1) \text{ is in } \mathbf{R}^5, \quad \begin{bmatrix} 1+i \\ 1-i \end{bmatrix} \text{ is in } \mathbf{C}^2.$$

- The two essential vector operations go on inside the vector space

*We can add any vectors in  $\mathbb{R}^n$ , and we can multiply any vector by any scalar.*

- Inside the vector space means the result stays in the space
- A whole series of properties can be verified in  $\mathbb{R}^n$
- Commutative law  $v+w=w+v$
- Distributive law  $c(v+w)=cv+cw$
- There is unique zero vector satisfying  $0+v=0$
- These are the 3 of the 8 conditions listed at the starting
- These 8 conditions are required of every vector space

A real vector space is a set of “vectors” together with rules for vector addition and for multiplication by real numbers. The addition and the multiplication must produce vectors that are in the space. And the eight conditions must be satisfied (which is usually no problem). Here are three vector spaces other than  $\mathbf{R}^n$ :

- M The vector space of *all real 2 by 2 matrices*.
- F The vector space of *all real functions*  $f(x)$ .
- Z The vector space that consists only of a *zero vector*.

# Subspaces

**DEFINITION** A *subspace* of a vector space is a set of vectors (including  $\mathbf{0}$ ) that satisfies two requirements: *If  $v$  and  $w$  are vectors in the subspace and  $c$  is any scalar, then* (i)  $v + w$  is in the subspace and (ii)  $cv$  is in the subspace.

In other words, the set of vectors is “closed” under addition  $v + w$  and multiplication  $cv$  (and  $cw$ ). Those operations leave us in the subspace. We can also subtract, because  $-w$  is in the subspace and its sum with  $v$  is  $v - w$ . In short, *all linear combinations stay in the subspace*.

First fact: *Every subspace contains the zero vector.* The plane in  $\mathbf{R}^3$  has to go through  $(0, 0, 0)$ . We mention this separately, for extra emphasis, but it follows directly from rule (ii). Choose  $c = 0$ , and the rule requires  $0\mathbf{v}$  to be in the subspace.

Planes that don't contain the origin fail those tests. When  $\mathbf{v}$  is on such a plane,  $-\mathbf{v}$  and  $0\mathbf{v}$  are *not* on the plane. A plane that misses the origin is not a subspace.

*Lines through the origin are also subspaces.* When we multiply by 5, or add two vectors on the line, we stay on the line. But the line must go through  $(0, 0, 0)$ .

Another subspace is all of  $\mathbf{R}^3$ . The whole space is a subspace (*of itself*). Here is a list of all the possible subspaces of  $\mathbf{R}^3$ :

- |                                   |                                    |
|-----------------------------------|------------------------------------|
| (L) Any line through $(0, 0, 0)$  | ( $\mathbf{R}^3$ ) The whole space |
| (P) Any plane through $(0, 0, 0)$ | (Z) The single vector $(0, 0, 0)$  |

**Example 1** Keep only the vectors  $(x, y)$  whose components are positive or zero (this is a quarter-plane). The vector  $(2, 3)$  is included but  $(-2, -3)$  is not. So rule (ii) is violated when we try to multiply by  $c = -1$ . *The quarter-plane is not a subspace.*

**Example 2** Include also the vectors whose components are both negative. Now we have two quarter-planes. Requirement (ii) is satisfied; we can multiply by any  $c$ . But rule (i) now fails. The sum of  $v = (2, 3)$  and  $w = (-3, -2)$  is  $(-1, 1)$ , which is outside the quarter-planes. *Two quarter-planes don't make a subspace.*

Rules (i) and (ii) involve vector addition  $v + w$  and multiplication by scalars like  $c$  and  $d$ . The rules can be combined into a single requirement—the rule for subspaces:

**A subspace containing  $v$  and  $w$  must contain all linear combinations  $cv + dw$ .**

**Example 3** Inside the vector space  $\mathbf{M}$  of all 2 by 2 matrices, here are two subspaces:

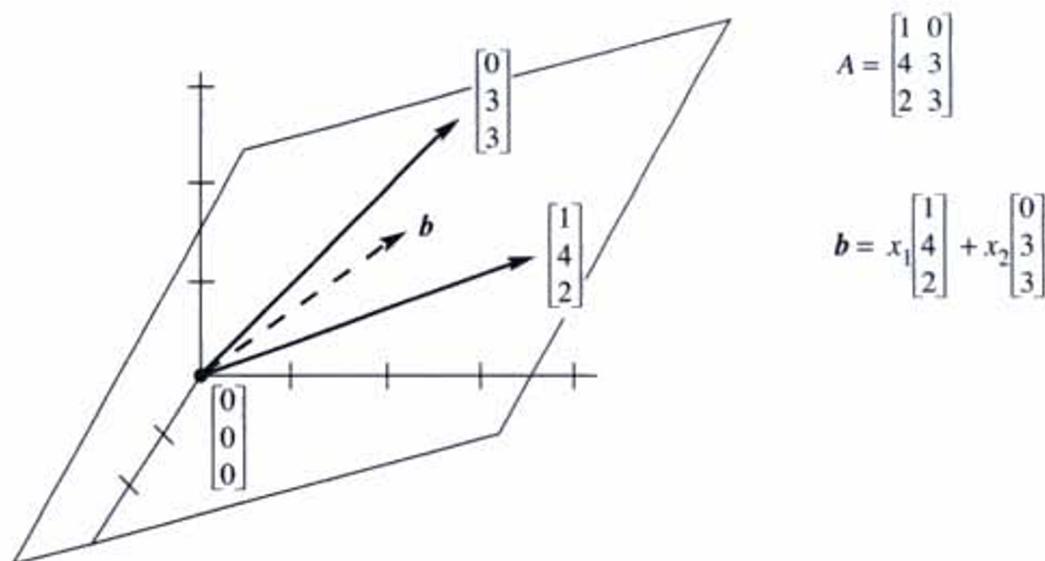
- (U) All upper triangular matrices  $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$     (D) All diagonal matrices  $\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}$ .

Add any two matrices in **U**, and the sum is in **U**. Add diagonal matrices, and the sum is diagonal. In this case **D** is also a subspace of **U**! Of course the zero matrix is in these subspaces, when  $a$ ,  $b$ , and  $d$  all equal zero.

To find a smaller subspace of diagonal matrices, we could require  $a = d$ . The matrices are multiples of the identity matrix  $I$ . The sum  $2I + 3I$  is in this subspace, and so is 3 times  $4I$ . It is a “line of matrices” inside  $\mathbf{M}$  and **U** and **D**.

# COLUMN SPACE

**DEFINITION** The *column space* consists of *all linear combinations of the columns*. The combinations are all possible vectors  $Ax$ . They fill the column space  $C(A)$ .



**Figure 3.2** The column space  $C(A)$  is a plane containing the two columns.  $Ax = b$  is solvable when  $b$  is on that plane. Then  $b$  is a combination of the columns.

- Note:

3A The system  $Ax = b$  is solvable if and only if  $b$  is in the column space of  $A$ .

When  $b$  is in the column space, it is a combination of the columns. The coefficients in that combination give us a solution  $x$  to the system  $Ax = b$ .

Suppose  $A$  is an  $m$  by  $n$  matrix. Its columns have  $m$  components (not  $n$ ). So the columns belong to  $\mathbf{R}^m$ . **The column space of  $A$  is a subspace of  $\mathbf{R}^m$  (not  $\mathbf{R}^n$ )**. The set of all column combinations  $Ax$  satisfies rules (i) and (ii) for a subspace: When we add linear combinations or multiply by scalars, we still produce combinations of the columns. The word “subspace” is justified by *taking all linear combinations*.

Here is a 3 by 2 matrix  $A$ , whose column space is a subspace of  $\mathbf{R}^3$ . It is a plane.

#### Example 4

$$A\mathbf{x} \text{ is } \begin{bmatrix} 1 & 0 \\ 4 & 3 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \text{ which is } x_1 \begin{bmatrix} 1 \\ 4 \\ 2 \end{bmatrix} + x_2 \begin{bmatrix} 0 \\ 3 \\ 3 \end{bmatrix}:$$

The column space consists of all combinations of the two columns—any  $x_1$  times the first column plus any  $x_2$  times the second column. *Those combinations fill up a plane in  $\mathbb{R}^3$*  (Figure 3.2). If the right side  $\mathbf{b}$  lies on that plane, then it is one of the combinations and  $(x_1, x_2)$  is a solution to  $A\mathbf{x} = \mathbf{b}$ . The plane has zero thickness, so it is more likely that  $\mathbf{b}$  is not in the column space. Then there is no solution to our 3 equations in 2 unknowns.

**Example 5** Describe the column spaces (they are subspaces of  $\mathbf{R}^2$ ) for

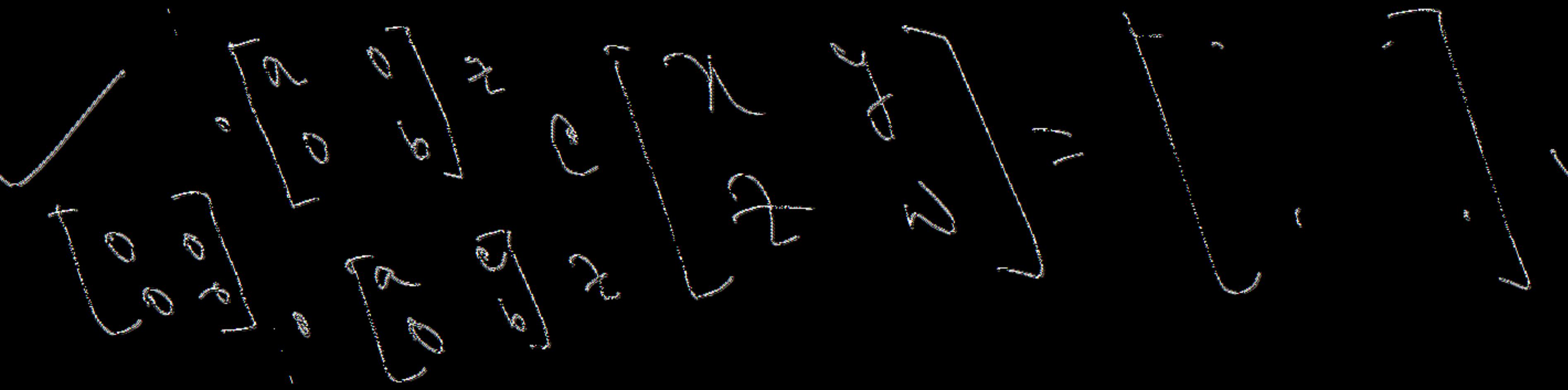
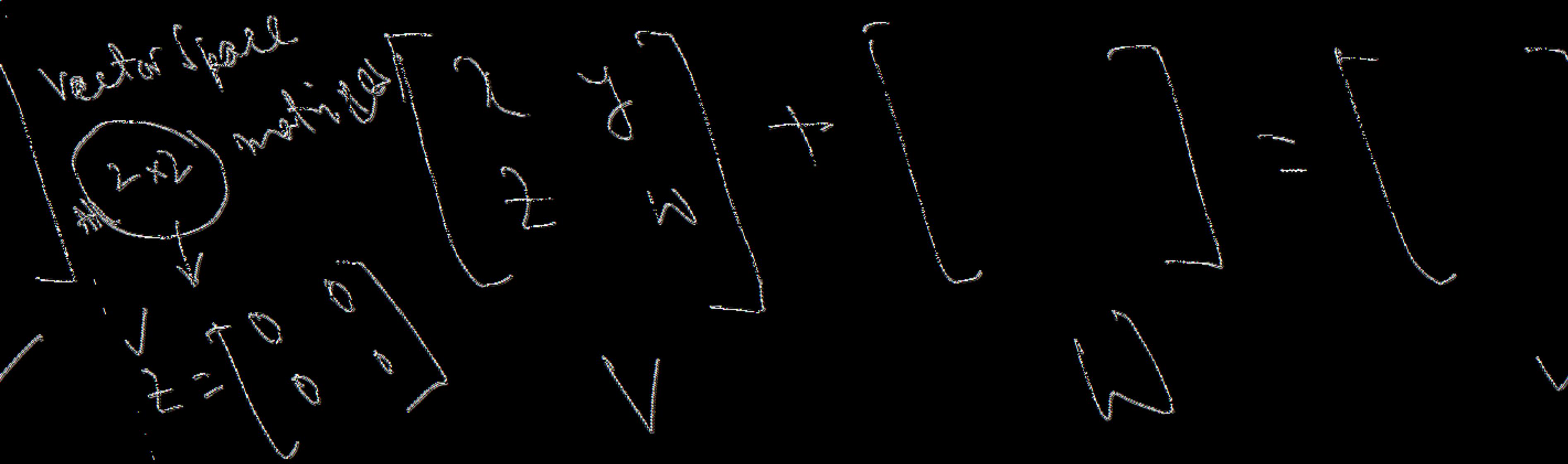
$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad A = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 0 & 4 \end{bmatrix}.$$

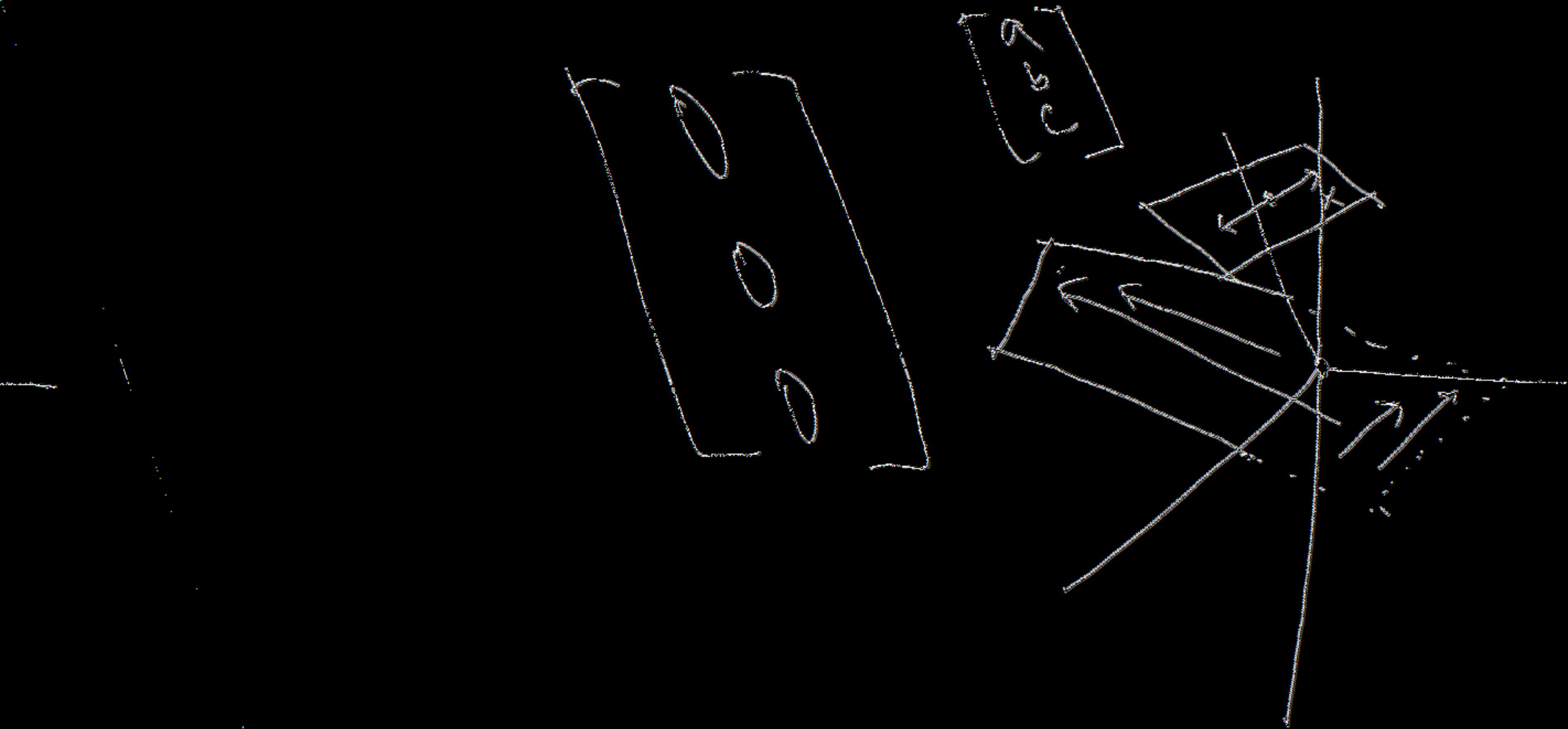
**Solution** The column space of  $I$  is the *whole space*  $\mathbf{R}^2$ . Every vector is a combination of the columns of  $I$ . In vector space language,  $C(I)$  is  $\mathbf{R}^2$ .

The column space of  $A$  is only a line. The second column  $(2, 4)$  is a multiple of the first column  $(1, 2)$ . Those vectors are different, but our eye is on vector *spaces*. The column space contains  $(1, 2)$  and  $(2, 4)$  and all other vectors  $(c, 2c)$  along that line. The equation  $Ax = b$  is only solvable when  $b$  is on the line.

The third matrix (with three columns) places no restriction on  $b$ . The column space  $C(B)$  is all of  $\mathbf{R}^2$ . Every  $b$  is attainable. The vector  $b = (5, 4)$  is column 2 plus column 3, so  $x$  can be  $(0, 1, 1)$ . The same vector  $(5, 4)$  is also 2(column 1) + column 3, so another possible  $x$  is  $(2, 0, 1)$ . This matrix has the same column space as  $I$ —any  $b$  is allowed. But now  $x$  has extra components and there are more solutions.

The next section creates another vector space, to describe all the solutions of  $Ax = \mathbf{0}$ . This section created the column space, to describe all the attainable right sides  $b$ .







C6H6

Ammon

$C(A)$  is a subgraph  
 $2^m$  nodes

$x_2 + x_3$

$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

$x_3$

$C(A)$  or  $\sigma^2$

$$V = \sqrt{V_0^2 + V_1^2}$$

$$t_1 - t_2$$

$$W = \sqrt{W_0^2 + W_1^2}$$

$$+ \dots$$

+ ... Hardy

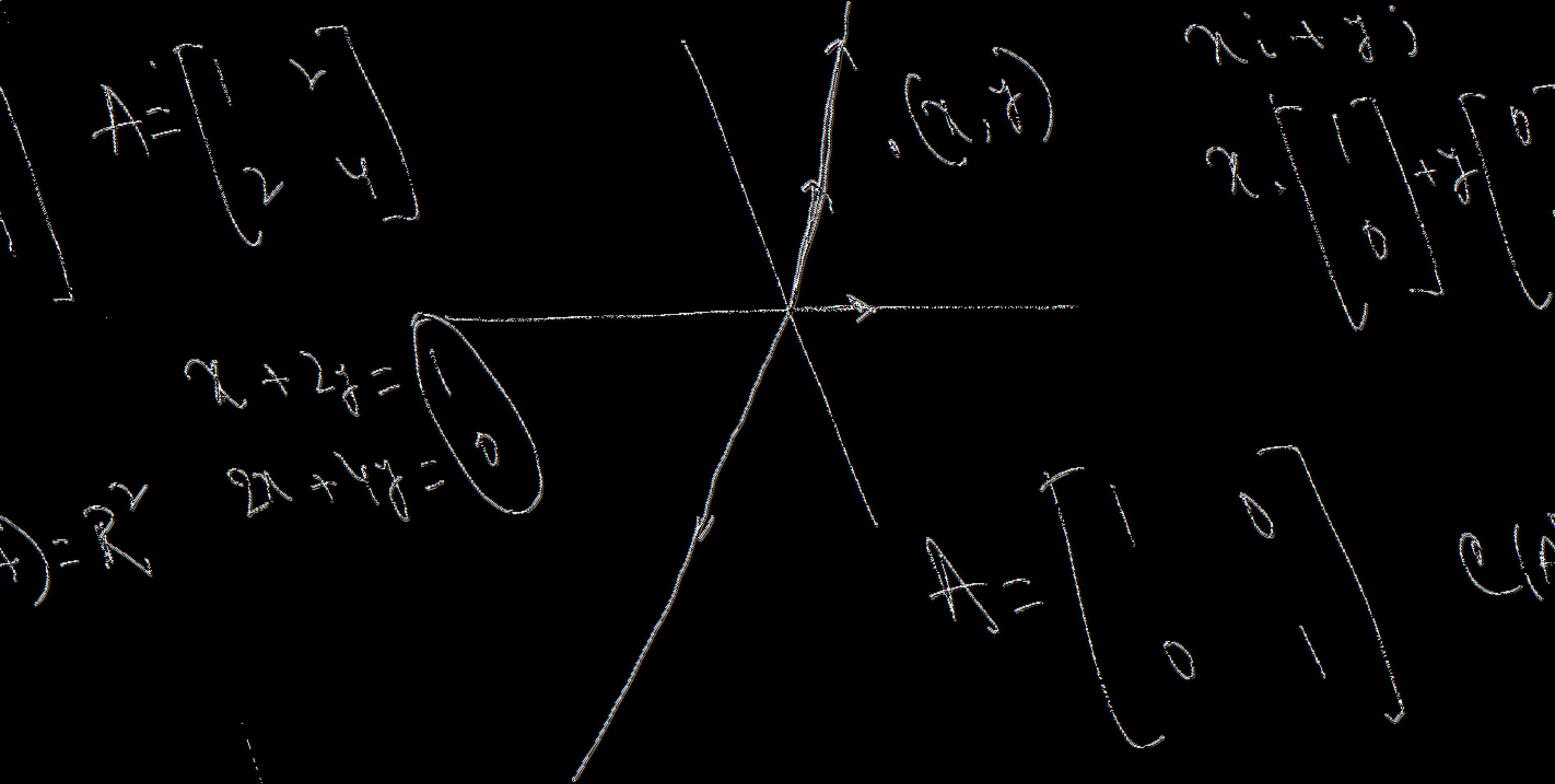
$$CV + CW \in CA$$

$$2(CV + CW) \in CA$$

$$+ (CV + CW)$$

$$+ (CV + CW)$$





$$Ax_1 + x_2 = 0 \quad | -x_2$$

$$Ax_1 = 0$$

$$Ax_2 = 0$$

$$A(cx_1 + dx_2) = cAx_1 + dAx_2 =$$

$\in N(A)$

$N(A)$  is a  
subspace of  $P$

$$AX = b \quad , \quad b \neq 0$$

$$0$$

$$AX = 0$$

A matrix is invertible

$N(A)$ : zero vector

# NULL Space of A

- Definition: The null space of A consists of all the solutions to  $AX=0$ . These solution vectors  $x$  are in  $R^n$ . The null space containing all solutions is denoted by  $N(A)$

Check that the solution vectors form a subspace. Suppose  $\mathbf{x}$  and  $\mathbf{y}$  are in the nullspace (this means  $A\mathbf{x} = \mathbf{0}$  and  $A\mathbf{y} = \mathbf{0}$ ). The rules of matrix multiplication give  $A(\mathbf{x} + \mathbf{y}) = \mathbf{0} + \mathbf{0}$ . The rules also give  $A(c\mathbf{x}) = c\mathbf{0}$ . The right sides are still zero. Therefore  $\mathbf{x} + \mathbf{y}$  and  $c\mathbf{x}$  are also in the nullspace  $N(A)$ . Since we can add and multiply without leaving the nullspace, it is a subspace.

To repeat: The solution vectors  $\mathbf{x}$  have  $n$  components. They are vectors in  $\mathbf{R}^n$ , so *the nullspace is a subspace of  $\mathbf{R}^n$* . The column space  $C(A)$  is a subspace of  $\mathbf{R}^m$ .

If the right side  $\mathbf{b}$  is not zero, the solutions of  $A\mathbf{x} = \mathbf{b}$  do *not* form a subspace. The vector  $\mathbf{x} = \mathbf{0}$  is only a solution if  $\mathbf{b} = \mathbf{0}$ . When the set of solutions does not include  $\mathbf{x} = \mathbf{0}$ , it cannot be a subspace. Section 3.4 will show how the solutions to  $A\mathbf{x} = \mathbf{b}$  (if there are any solutions) are shifted away from the origin by one particular

**Example 1** The equation  $x + 2y + 3z = 0$  comes from the 1 by 3 matrix  $A = [1 \ 2 \ 3]$ . This equation produces a plane through the origin. The plane is a subspace of  $\mathbf{R}^3$ . *It is the nullspace of A.*

The solutions to  $x + 2y + 3z = 6$  also form a plane, but not a subspace.

**Example 2** Describe the nullspace of  $A = \begin{bmatrix} 1 & 2 \\ 3 & 6 \end{bmatrix}$ .

**Solution** Apply elimination to the linear equations  $A\mathbf{x} = \mathbf{0}$ :

$$\begin{bmatrix} x_1 + 2x_2 = 0 \\ 3x_1 + 6x_2 = 0 \end{bmatrix} \rightarrow \begin{bmatrix} x_1 + 2x_2 = 0 \\ 0 = 0 \end{bmatrix}$$

There is really only one equation. The second equation is the first equation multiplied by 3. In the row picture, the line  $x_1 + 2x_2 = 0$  is the same as the line  $3x_1 + 6x_2 = 0$ . That line is the nullspace  $N(A)$ .

To describe this line of solutions, here is an efficient way. Choose one point on the line (one “*special solution*”). Then all points on the line are multiples of this one. We choose the second component to be  $x_2 = 1$  (a special choice). From the equation  $x_1 + 2x_2 = 0$ , the first component must be  $x_1 = -2$ . The special solution is  $(-2, 1)$ :

The nullspace  $N(A)$  contains all multiples of  $s = \begin{bmatrix} -2 \\ 1 \end{bmatrix}$ .

*The nullspace consists of all combinations of those special solutions.*

**Example 3** Describe the nullspaces of these three matrices  $A$ ,  $B$ ,  $C$ :

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 8 \end{bmatrix} \quad B = \begin{bmatrix} A \\ 2A \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 8 \\ 2 & 4 \\ 6 & 16 \end{bmatrix} \quad C = [A \ 2A] = \begin{bmatrix} 1 & 2 & 2 & 4 \\ 3 & 8 & 6 & 16 \end{bmatrix}.$$

**Solution** The equation  $Ax = \mathbf{0}$  has only the zero solution  $x = \mathbf{0}$ . The nullspace is  $\mathbf{Z}$ . It contains only the single point  $x = \mathbf{0}$  in  $\mathbf{R}^2$ . This comes from elimination:

$$\begin{bmatrix} 1 & 2 \\ 3 & 8 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \text{ yields } \begin{bmatrix} 1 & 2 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \text{ and } \begin{bmatrix} x_1 = 0 \\ x_2 = 0 \end{bmatrix}.$$

$A$  is invertible. There are no special solutions. All columns have pivots.

The rectangular matrix  $B$  has the same nullspace  $\mathbf{Z}$ . The first two equations in  $Bx = \mathbf{0}$  again require  $x = \mathbf{0}$ . The last two equations would also force  $x = \mathbf{0}$ . When we add extra equations, the nullspace certainly cannot become larger. The extra rows impose more conditions on the vectors  $x$  in the nullspace.

The rectangular matrix  $C$  is different. It has extra columns instead of extra rows. The solution vector  $x$  has *four* components. Elimination will produce pivots in the first two columns of  $C$ , but the last two columns are “free”. They don’t have pivots:

$$C = \begin{bmatrix} 1 & 2 & 2 & 4 \\ 3 & 8 & 6 & 16 \end{bmatrix} \text{ becomes } U = \begin{bmatrix} 1 & 2 & 2 & 4 \\ 0 & 2 & 0 & 4 \end{bmatrix}$$

$\uparrow \uparrow \uparrow \uparrow$

pivot columns      free columns

For the free variables  $x_3$  and  $x_4$ , we make special choices of ones and zeros. First  $x_3 = 1$ ,  $x_4 = 0$  and second  $x_3 = 0$ ,  $x_4 = 1$ . The pivot variables  $x_1$  and  $x_2$  are

determined by the equation  $Ux = \mathbf{0}$ . We get two special solutions in the nullspace of  $C$  (and also the nullspace of  $U$ ). The special solutions are:

$$s_1 = \begin{bmatrix} -2 \\ 0 \\ 1 \\ 0 \end{bmatrix} \text{ and } s_2 = \begin{bmatrix} 0 \\ -2 \\ 0 \\ 1 \end{bmatrix}$$

← pivot  
← variables  
← free  
← variables

- The upper triangular matrix is further simplified in two ways

1. *Produce zeros above the pivots*, by eliminating upward.
2. *Produce ones in the pivots*, by dividing the whole row by its pivot.

- By following these steps the null space remains same. This null space becomes easiest to see when we reach reduced row echelon form of R.

- Refer to example 3

$$C = \begin{bmatrix} 1 & 2 & 2 & 4 \\ 3 & 8 & 6 & 16 \end{bmatrix} \text{ becomes } U = \begin{bmatrix} 1 & 2 & 2 & 4 \\ 0 & 2 & 0 & 4 \end{bmatrix}$$

↑      ↑      ↑      ↑  
**pivot columns      free columns**

$U$  is further simplified reduced row echelon form

$$U = \begin{bmatrix} 1 & 2 & 2 & 4 \\ 0 & 2 & 0 & 4 \end{bmatrix} \text{ becomes } R = \begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \end{bmatrix}.$$

↑      ↑  
**pivot columns contain 1**

# Solving $AX=0$ by elimination where A is rectangular Matrix

- A is a rectangular Matrix we still use elimination. we solve m equations in n unknowns . We follow the below two steps

1. Forward elimination from  $A$  to a triangular  $U$  (or its reduced form  $R$ ).
2. Back substitution in  $Ux = \mathbf{0}$  or  $Rx = \mathbf{0}$  to find  $x$ .

You will notice difference in back substitution when A and U have fewer than n pivots

# We will consider the following example

Let  $A = \begin{bmatrix} 1 & 1 & 2 & 3 \\ 2 & 2 & 8 & 10 \\ 3 & 3 & 10 & 13 \end{bmatrix}$ . Solving  $AX=0$  by elimination

$$A = \begin{bmatrix} 1 & 1 & 2 & 3 \\ 2 & 2 & 8 & 10 \\ 3 & 3 & 10 & 13 \end{bmatrix}.$$

Certainly  $a_{11} = 1$  is the first pivot. Clear out the 2 and 3 below that pivot:

$$A \rightarrow \begin{bmatrix} 1 & 1 & 2 & 3 \\ 0 & 0 & 4 & 4 \\ 0 & 0 & 4 & 4 \end{bmatrix} \quad \begin{array}{l} (\text{subtract } 2 \times \text{ row 1}) \\ (\text{subtract } 3 \times \text{ row 1}) \end{array}$$

- Here second pivot is zero. The entry below that position is also zero so row exchange is not possible.
- We move on to third column and consider our second pivot to be 4 .Using that pivot may make elements below pivot to be zero by elimination

The resulting Upper Triangle matrix is

**Triangular  $U$  :** 
$$U = \begin{bmatrix} 1 & 1 & 2 & 3 \\ 0 & 0 & 4 & 4 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$
 (only two pivots)  
(the last equation became  $0 = 0$ )

P The *pivot* variables are  $x_1$  and  $x_3$ , since columns 1 and 3 contain pivots.

F The *free* variables are  $x_2$  and  $x_4$ , because columns 2 and 4 have no pivots.

**Special Solutions** to  $x_1 + x_2 + 2x_3 + 3x_4 = 0$  and  $4x_3 + 4x_4 = 0$

- Set  $x_2 = 1$  and  $x_4 = 0$ . By back substitution  $x_3 = 0$ . Then  $x_1 = -1$ .
- Set  $x_2 = 0$  and  $x_4 = 1$ . By back substitution  $x_3 = -1$ . Then  $x_1 = -1$ .

These special solutions solve  $U\mathbf{x} = \mathbf{0}$  and therefore  $A\mathbf{x} = \mathbf{0}$ . They are in the nullspace. The good thing is that *every solution is a combination of the special solutions*.

*Complete Solution*  $\mathbf{x} = x_2 \begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$  special  $+ x_4 \begin{bmatrix} -1 \\ 0 \\ -1 \\ 1 \end{bmatrix}$  special  $= \begin{bmatrix} -x_2 - x_4 \\ x_2 \\ -x_4 \\ x_4 \end{bmatrix}$  complete (1)

**Example 4** Find the nullspace of  $U = \begin{bmatrix} 1 & 5 & 7 \\ 0 & 0 & 9 \end{bmatrix}$ .

The second column of  $U$  has no pivot. So  $x_2$  is free. The special solution has  $x_2 = 1$ . Back substitution into  $9x_3 = 0$  gives  $x_3 = 0$ . Then  $x_1 + 5x_2 = 0$  or  $x_1 = -5$ . The solutions to  $U\mathbf{x} = \mathbf{0}$  are multiples of one special solution:

$$\mathbf{x} = x_2 \begin{bmatrix} -5 \\ 1 \\ 0 \end{bmatrix}$$

The nullspace of  $U$  is a line in  $\mathbf{R}^3$ .

# Rank of a matrix

- The matrix  $m$  by  $n$  give the size of a matrix but not necessarily the true size of a linear system.
- The true size of  $A$  is given by its Rank.
- Definition: The rank of  $A$  is the number of pivots. This number is  $r$ .

- *A has full row rank if every row has a pivot:  $r = m$ . No zero rows in  $R$ .*
- *A has full column rank if every column has a pivot:  $r = n$ . No free variables.*

**Example 1** When all rows are multiples of one pivot row, the rank is  $r = 1$ :

$$\begin{bmatrix} 1 & 3 & 4 \\ 2 & 6 & 8 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 3 \\ 0 & 5 \end{bmatrix} \text{ and } \begin{bmatrix} 5 \\ 2 \end{bmatrix} \text{ and } [6] \text{ all have rank 1.}$$

The reduced row echelon forms  $R = \text{rref}(A)$  can be checked by eye:

$$R = \begin{bmatrix} 1 & 3 & 4 \\ 0 & 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } [1] \text{ have only one pivot.}$$

Our second definition of rank is coming at a higher level. It deals with entire rows and entire columns—vectors and not just numbers. The matrices  $A$  and  $U$  and  $R$

have  $r$  independent rows (the pivot rows). They also have  $r$  independent columns (the pivot columns). Section 3.5 says what it means for rows or columns to be independent.

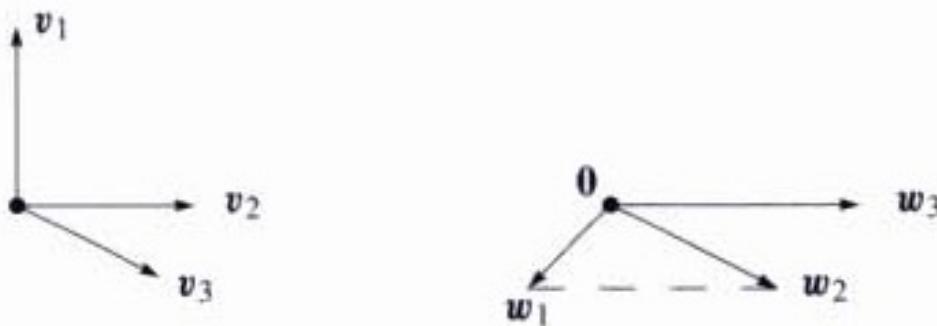
A third definition of rank, at the top level of linear algebra, will deal with *spaces* of vectors. The rank  $r$  is the “dimension” of the column space. It is also the dimension of the row space. The great thing is that  $r$  also reveals the dimension of the nullspace.

# Linear Independence

**DEFINITION** The columns of  $A$  are *linearly independent* when the only solution to  $Ax = 0$  is  $x = 0$ . *No other combination Ax of the columns gives the zero vector.*

With linearly independent columns, the nullspace  $N(A)$  contains only the zero vector. Let me illustrate linear independence (and linear dependence) with three vectors in  $\mathbb{R}^3$ :

1. If three vectors are *not* in the same plane, they are independent. No combination of  $v_1, v_2, v_3$  in Figure 3.4 gives zero except  $0v_1 + 0v_2 + 0v_3$ .
2. If three vectors  $w_1, w_2, w_3$  are *in the same plane*, they are dependent.



**Figure 3.4** Independent vectors  $v_1, v_2, v_3$ . Dependent vectors  $w_1, w_2, w_3$ . The combination  $w_1 - w_2 + w_3$  is  $(0, 0, 0)$ .

# Definition

- The sequence of vectors  $v_1, v_2, v_3, \dots, v_n$  is linearly independent if and only if the combination that gives the zero vector is  $0v_1 + 0v_2 + 0v_3 + \dots + 0v_n$ . Thus linear independence means that

$x_1v_1 + x_2v_2 + \dots + x_nv_n = 0$  only happens when all x's are zeros.

**Example 1** The columns of  $A$  are dependent.  $Ax = \mathbf{0}$  has a nonzero solution:

$$Ax = \begin{bmatrix} 1 & 0 & 3 \\ 2 & 1 & 5 \\ 1 & 0 & 3 \end{bmatrix} \begin{bmatrix} -3 \\ 1 \\ 1 \end{bmatrix} \quad \text{is} \quad -3 \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} + 1 \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + 1 \begin{bmatrix} 3 \\ 5 \\ 3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

The rank of  $A$  is only  $r = 2$ . *Independent columns would give full column rank  $r = n = 3$ .*

In that matrix the rows are also dependent. Row 1 minus row 3 is the zero row. For a *square matrix*, we will show that dependent columns imply dependent rows (and vice versa).

# Note

**3H** The columns of  $A$  are independent exactly when the rank is  $r = n$ . There are  $n$  pivots and no free variables. Only  $x = \mathbf{0}$  is in the nullspace.

**3I** Any set of  $n$  vectors in  $\mathbf{R}^m$  must be linearly dependent if  $n > m$ .

One case is of special importance because it is clear from the start. Suppose seven columns have five components each ( $m = 5$  is less than  $n = 7$ ). Then the columns *must be dependent*. Any seven vectors from  $\mathbf{R}^5$  are dependent. The rank of  $A$  cannot be larger than 5. There cannot be more than five pivots in five rows. The system  $Ax = \mathbf{0}$  has at least  $7 - 5 = 2$  free variables, so it has nonzero solutions—which means that the columns are dependent.

# Row Space

**DEFINITION** The *row space* of a matrix is the subspace of  $\mathbf{R}^n$  spanned by the rows.

The rows on m by n matrix have n components. They are vectors in  $R^n$

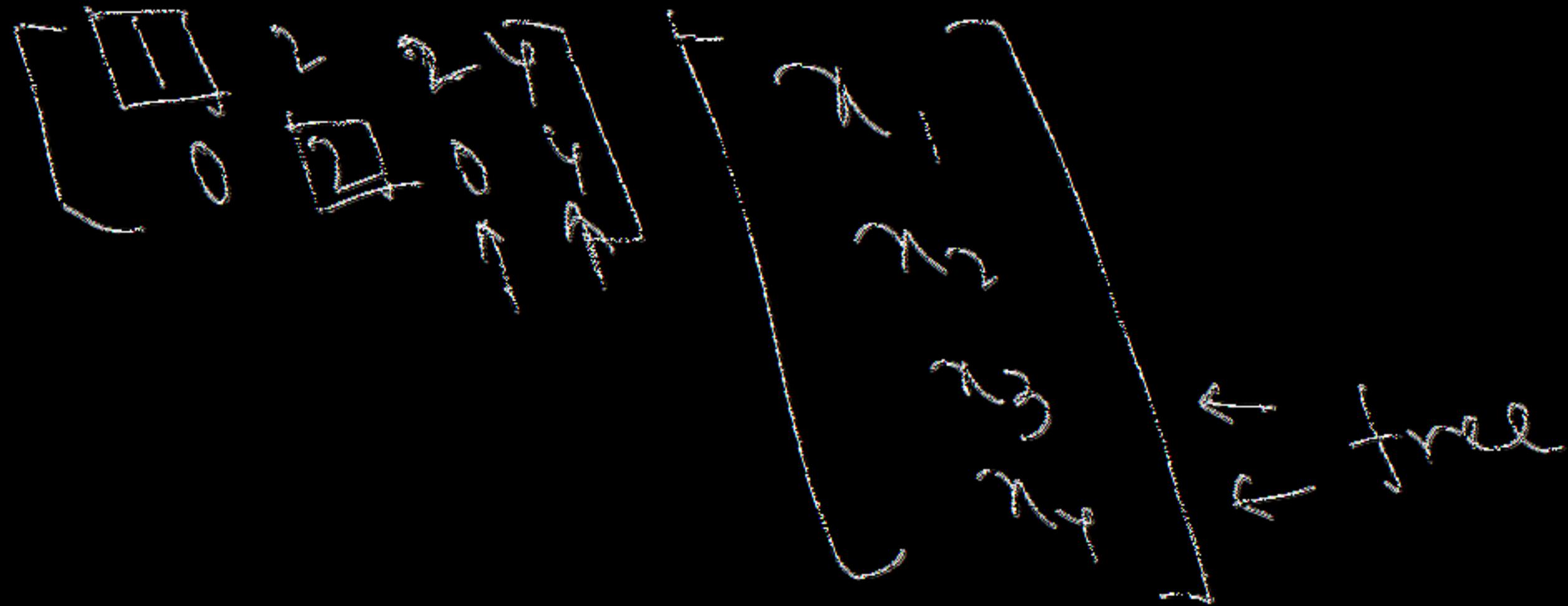
As we know rows of A are the columns of  $A^T$

The row space of A is  $C(A^T)$ . It is the column space of  $A^T$ . It is the sub space of  $R^n$ .

### Example 5

$$A = \begin{bmatrix} 1 & 4 \\ 2 & 7 \\ 3 & 5 \end{bmatrix} \text{ and } A^T = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 7 & 5 \end{bmatrix}. \text{ Here } m = 3 \text{ and } n = 2.$$

The column space of  $A$  is spanned by the two columns of  $A$ . It is a plane in  $\mathbf{R}^3$ . *The row space of  $A$  is spanned by the three rows of  $A$*  (which are columns of  $A^T$ ). This row space is all of  $\mathbf{R}^2$ . Remember: The rows are in  $\mathbf{R}^n$ . The columns are in  $\mathbf{R}^m$ . Same numbers, different vectors, different spaces.



$$x_3=1, x_4=0, x_1=x_2, x_1=0$$

$$x_3=0, x_4=1, x_1=0, x_2=0$$

$$v = \begin{pmatrix} 1 & 2 & 1 & 5 \\ 0 & 2 & 0 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 2 & 0 & 4 \end{pmatrix}$$

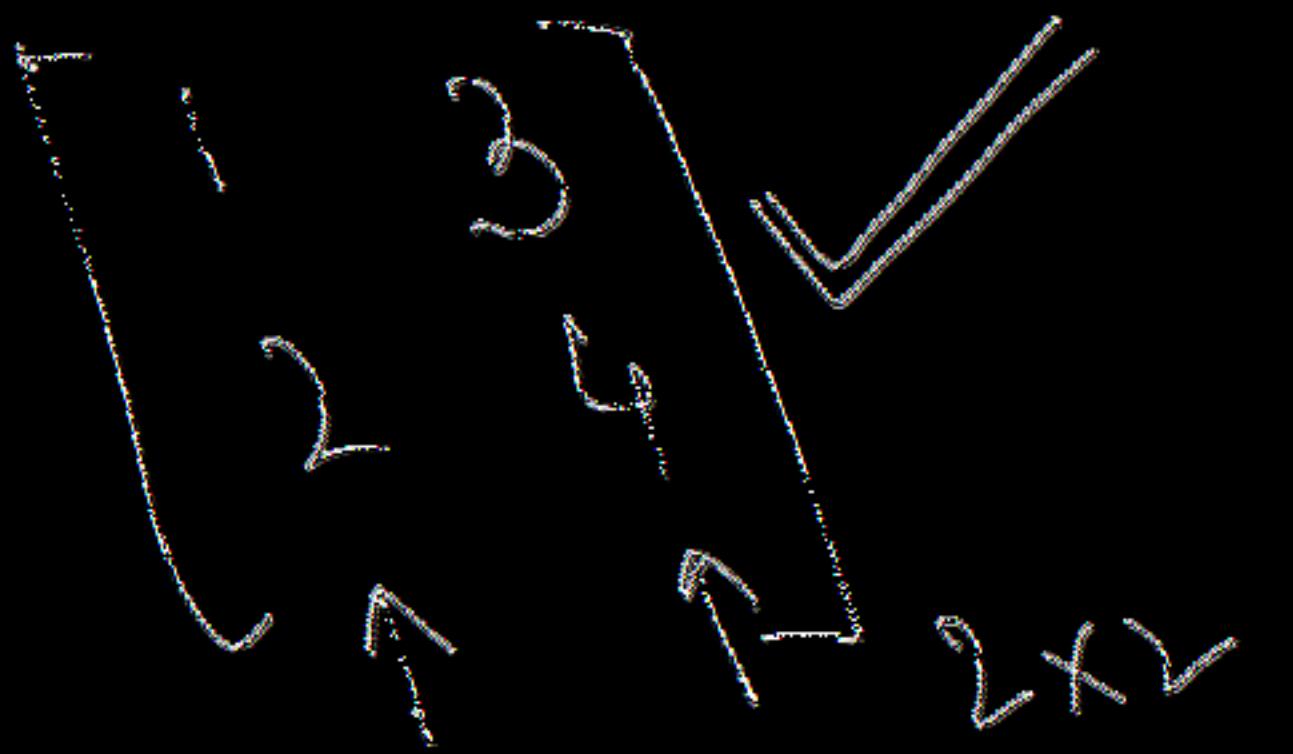
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} -2 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

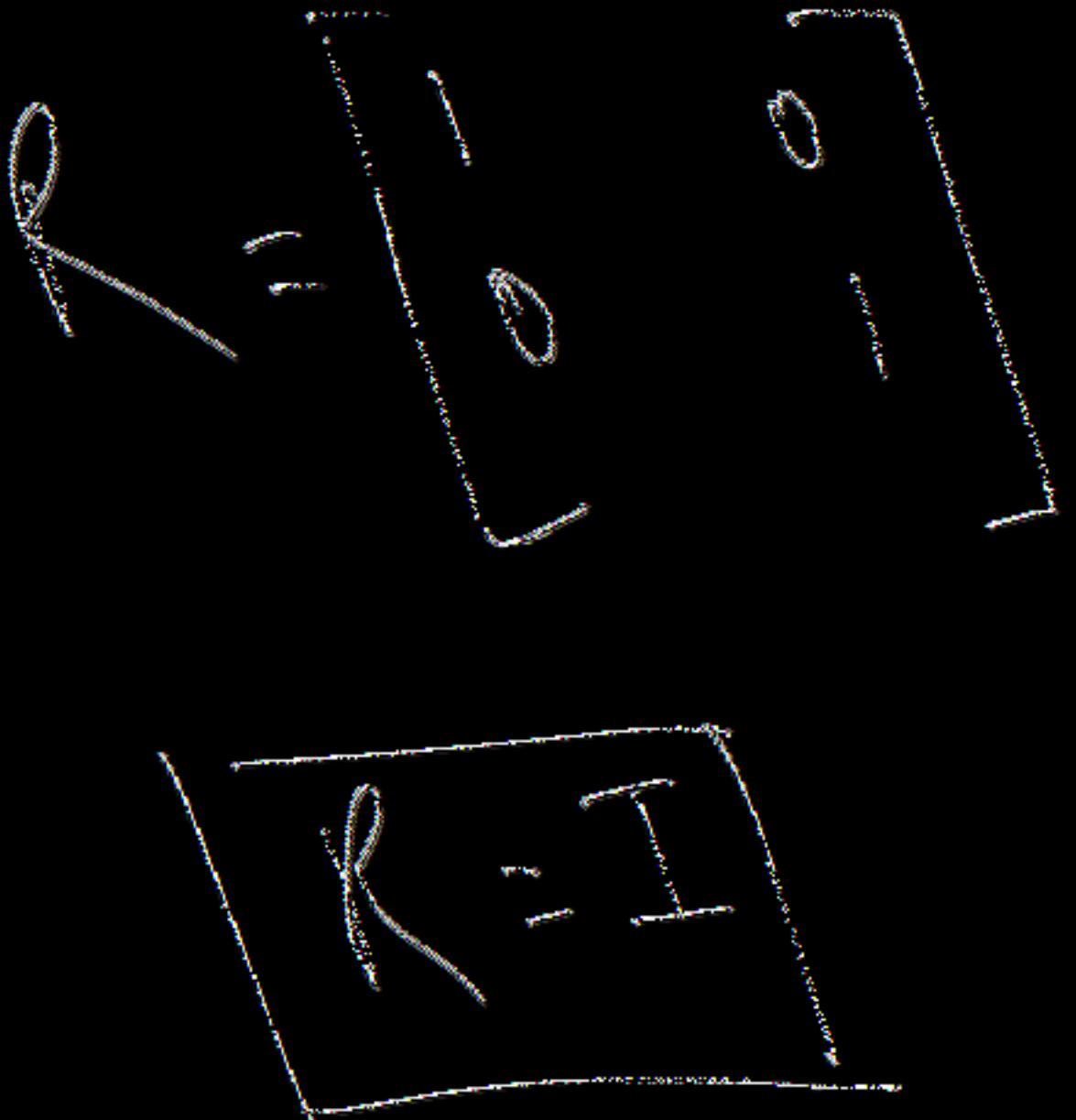
non zero

less reduced ech

$y = \langle 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 \rangle$

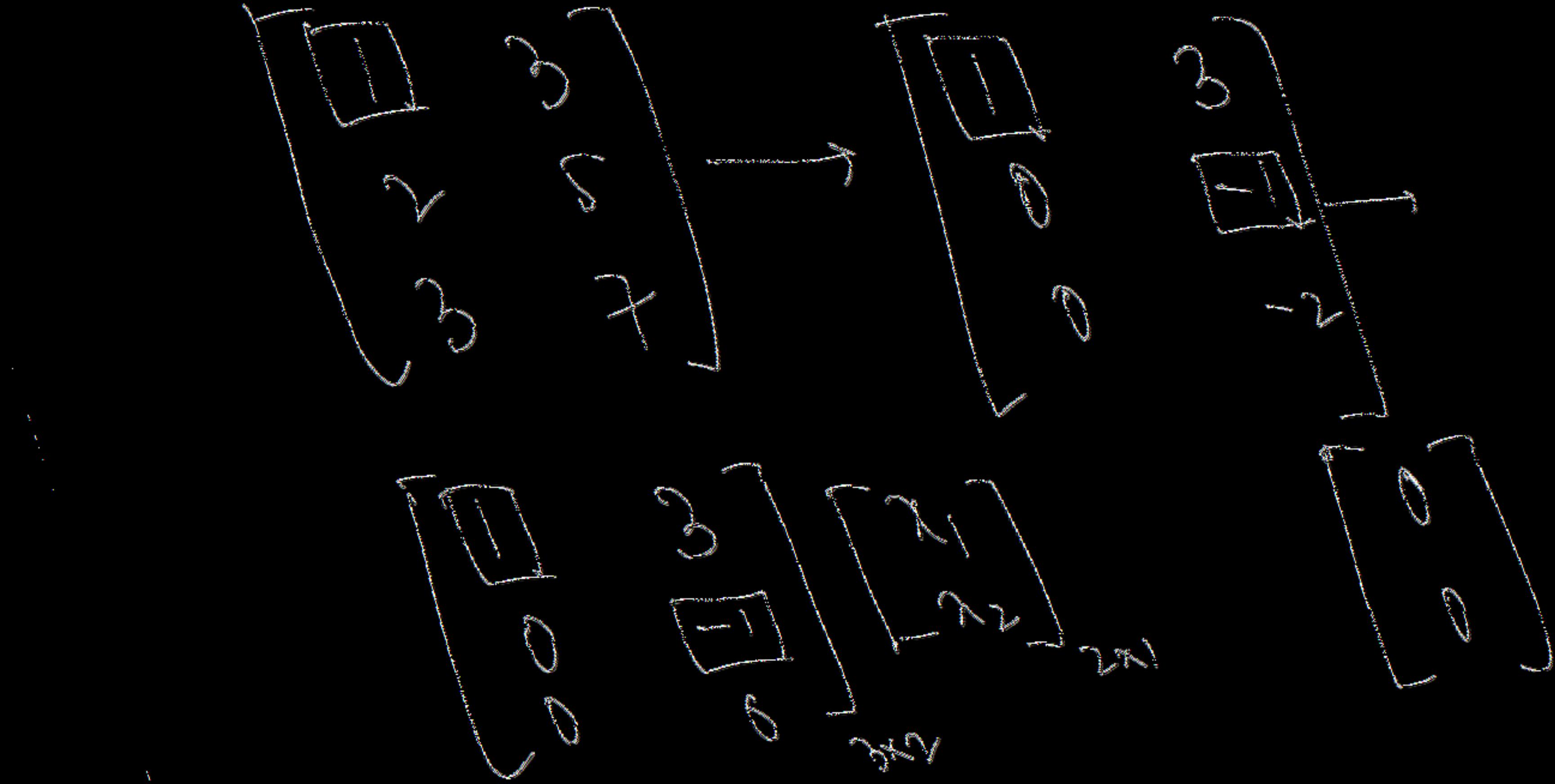


$\mu_{-2}$



$x^2$   $\sqrt{3}$   $+x^2$   $\sqrt{3}$   $5$   $9$   $-10$

$$x^2 - x = 1$$



$$x_1 + 3x_2 = 0$$

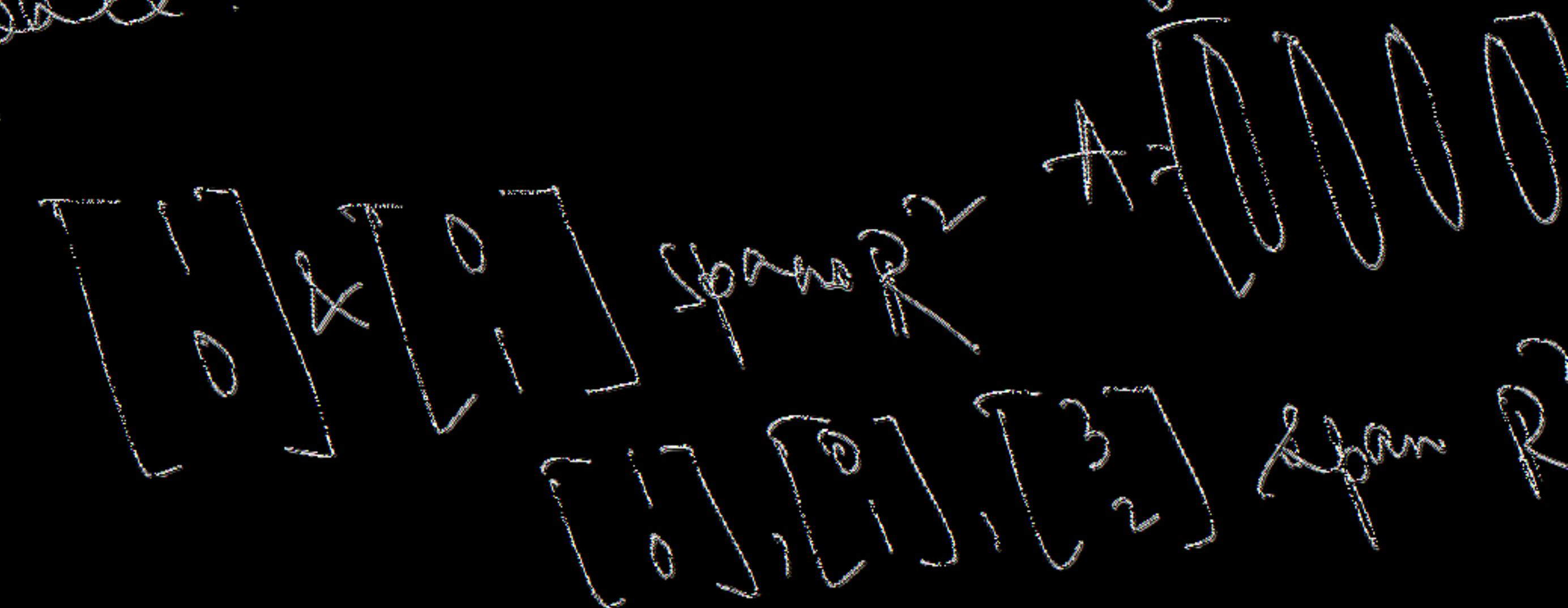
$$-x_2 > 0$$

$$\boxed{x_2 > 0, x_1 = 0}$$

1  
2  
3  
4

5  
 $2+3$   
6  
7  
8

A set of vectors spans a space if  
their linear combinations fill the  
space.



# Row Space

**DEFINITION** The *row space* of a matrix is the subspace of  $\mathbf{R}^n$  spanned by the rows.

The rows on m by n matrix have n components. They are vectors in  $R^n$

As we know rows of A are the columns of  $A^T$

The row space of A is  $C(A^T)$ . It is the column space of  $A^T$ . It is the sub space of  $R^n$ .

### Example 5

$$A = \begin{bmatrix} 1 & 4 \\ 2 & 7 \\ 3 & 5 \end{bmatrix} \text{ and } A^T = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 7 & 5 \end{bmatrix}. \text{ Here } m = 3 \text{ and } n = 2.$$

The column space of  $A$  is spanned by the two columns of  $A$ . It is a plane in  $\mathbf{R}^3$ . *The row space of  $A$  is spanned by the three rows of  $A$*  (which are columns of  $A^T$ ). This row space is all of  $\mathbf{R}^2$ . Remember: The rows are in  $\mathbf{R}^n$ . The columns are in  $\mathbf{R}^m$ . Same numbers, different vectors, different spaces.

- Basis:

**DEFINITION** A *basis* for a vector space is a sequence of vectors that has two properties at once:

1. The vectors are *linearly independent*.
2. The vectors *span the space*.

**There is one and only one way to write  $v$  as a combination of the basis vectors.**

**Reason:** Suppose  $v = a_1v_1 + \cdots + a_nv_n$  and also  $v = b_1v_1 + \cdots + b_nv_n$ . By subtraction  $(a_1 - b_1)v_1 + \cdots + (a_n - b_n)v_n$  is the zero vector. From the independence of the  $v$ 's, each  $a_i - b_i = 0$ . Hence  $a_i = b_i$ .

**Example 6** The columns of  $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$  produce the “standard basis” for  $\mathbf{R}^2$ .

The basis vectors  $i = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$  and  $j = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$  are independent. They span  $\mathbf{R}^2$ .

Everybody thinks of this basis first. The vector  $i$  goes across and  $j$  goes straight up. The columns of the 3 by 3 identity matrix are the standard basis  $i, j, k$ . The columns of the  $n$  by  $n$  identity matrix give the “standard basis” for  $\mathbf{R}^n$ . Now we find other bases.

**Example 7** (Important) The columns of *any invertible n by n matrix* give a basis for  $\mathbf{R}^n$ :

$$A = \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix} \quad \text{and} \quad A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{but not} \quad A = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}.$$

When  $A$  is invertible, its columns are independent. The only solution to  $Ax = \mathbf{0}$  is  $x = \mathbf{0}$ . The columns span the whole space  $\mathbf{R}^n$ —because every vector  $b$  is a combination of the columns.  $Ax = b$  can always be solved by  $x = A^{-1}b$ . Do you see how everything comes together for invertible matrices? Here it is in one sentence:

# Note

3J The vectors  $v_1, \dots, v_n$  are a *basis for  $\mathbb{R}^n$*  exactly when they are *the columns of an  $n$  by  $n$  invertible matrix*. Thus  $\mathbb{R}^n$  has infinitely many different bases.

3K *The pivot columns of  $A$  are a basis for its column space.* The pivot rows of  $A$  are a basis for its row space. So are the pivot rows of its echelon form  $R$ .

**Example 8** This matrix is not invertible. Its columns are not a basis for anything!

$$A = \begin{bmatrix} 2 & 4 \\ 3 & 6 \end{bmatrix} \text{ which reduces to } R = \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}.$$

Column 1 of  $A$  is the pivot column. That column alone is a basis for its column space. The second column of  $A$  would be a different basis. So would any nonzero multiple of that column. There is no shortage of bases! So we often make a definite choice: the pivot columns.

Notice that the pivot column of this  $R$  ends in zero. That column is a basis for the column space of  $R$ , but it is not even a member of the column space of  $A$ . The column spaces of  $A$  and  $R$  are different. Their bases are different.

The row space of  $A$  is the *same* as the row space of  $R$ . It contains  $(2, 4)$  and  $(1, 2)$  and all other multiples of those vectors. As always, there are infinitely many bases to choose from. I think the most natural choice is to pick the nonzero rows of  $R$  (rows with a pivot). So this matrix  $A$  with rank one has only one vector in the basis:

Basis for the column space:  $\begin{bmatrix} 2 \\ 3 \end{bmatrix}$ . Basis for the row space:  $\begin{bmatrix} 1 \\ 2 \end{bmatrix}$ .

# Dimension of vector space

**DEFINITION** The *dimension of a space* is the number of vectors in every basis.

This matches our intuition. The line through  $\mathbf{v} = (1, 5, 2)$  has dimension one. It is a subspace with one vector  $\mathbf{v}$  in its basis. Perpendicular to that line is the plane  $x + 5y + 2z = 0$ . This plane has dimension 2. To prove it, we find a basis  $(-5, 1, 0)$  and  $(-2, 0, 1)$ . The dimension is 2 because the basis contains two vectors.

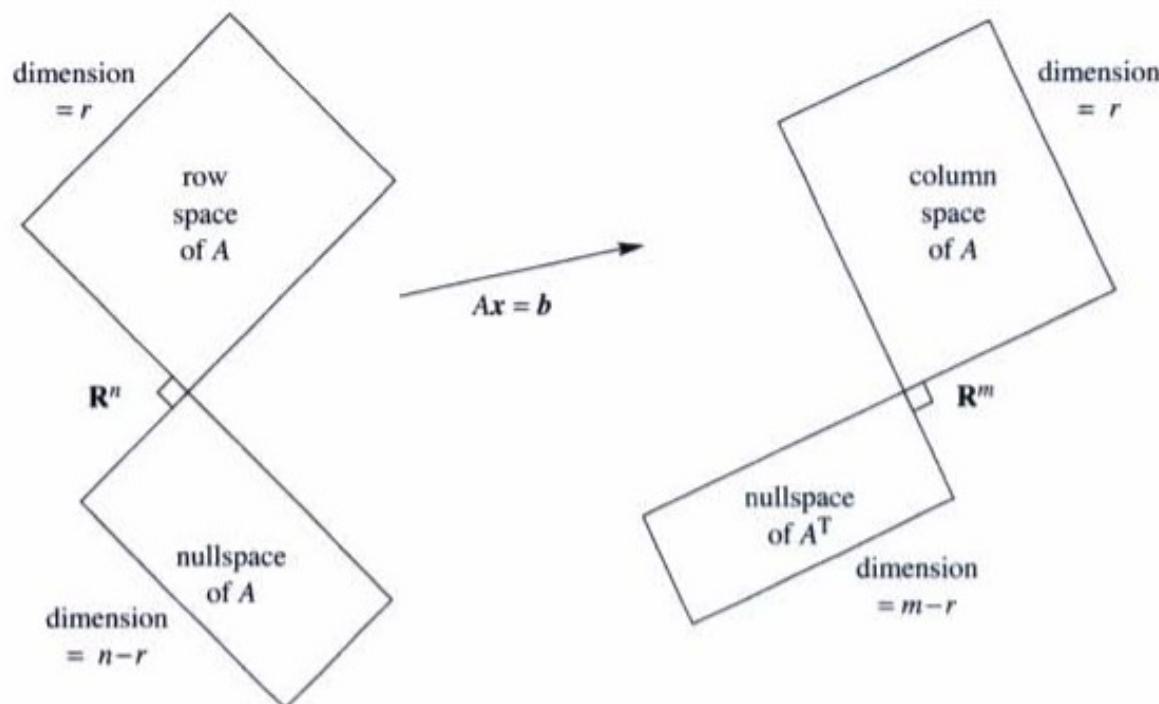
**End of UNIT 5**

# UNIT 6

ORTHOGONALITY

**DEFINITION** Two subspaces  $V$  and  $W$  of a vector space are *orthogonal* if every vector  $v$  in  $V$  is perpendicular to every vector  $w$  in  $W$ :

$$v \cdot w = 0 \quad \text{or} \quad v^T w = 0 \quad \text{for all } v \text{ in } V \text{ and all } w \text{ in } W.$$



**Figure 4.1** Two pairs of orthogonal subspaces. Dimensions add to  $n$  and add to  $m$ .

**Example 1** The floor of your room (extended to infinity) is a subspace  $V$ . The line where two walls meet is a subspace  $W$  (one-dimensional). Those subspaces are orthogonal. Every vector up the meeting line is perpendicular to every vector in the floor. The origin  $(0, 0, 0)$  is in the corner. We assume you don't live in a tent.

**Example 2** Suppose  $V$  is still the floor but  $W$  is a wall (a two-dimensional space). The wall and floor look like orthogonal subspaces but they are not! You can find vectors in  $V$  and  $W$  that are not perpendicular. In fact a vector running along the bottom of the wall is also in the floor. This vector is in both  $V$  and  $W$ —and it is not perpendicular to itself.

When a vector is in two orthogonal subspaces, it *must* be zero. It is perpendicular to itself. It is  $v$  and it is  $w$ , so  $v^T v = 0$ . This has to be the zero vector.

# Note 1

**4A** Every vector  $x$  in the nullspace of  $A$  is perpendicular to every row of  $A$ , because  $Ax = \mathbf{0}$ . *The nullspace and row space are orthogonal subspaces.*

**Example 3** The rows of  $A$  are perpendicular to  $x = (1, 1, -1)$  in the nullspace:

$$Ax = \begin{bmatrix} 1 & 3 & 4 \\ 5 & 2 & 7 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \quad \text{gives the dot products} \quad \begin{aligned} 1 + 3 - 4 &= 0 \\ 5 + 2 - 7 &= 0 \end{aligned}$$

Now we turn to the other two subspaces. In this example, the column space is all of  $\mathbf{R}^2$ . The nullspace of  $A^T$  is only the zero vector. Those two subspaces are also orthogonal.

## Note 2

**4B** Every vector  $y$  in the nullspace of  $A^T$  is perpendicular to every column of  $A$ .  
*The left nullspace and the column space are orthogonal in  $\mathbb{R}^m$ .*

$$A^T y = \begin{bmatrix} (\text{column 1})^T \\ \dots \\ (\text{column } n)^T \end{bmatrix} \begin{bmatrix} y \end{bmatrix} = \begin{bmatrix} 0 \\ \dots \\ 0 \end{bmatrix}. \quad (3)$$

The dot product of  $y$  with every column of  $A$  is zero. Then  $y$  in the left nullspace is perpendicular to each column—and to the whole column space.

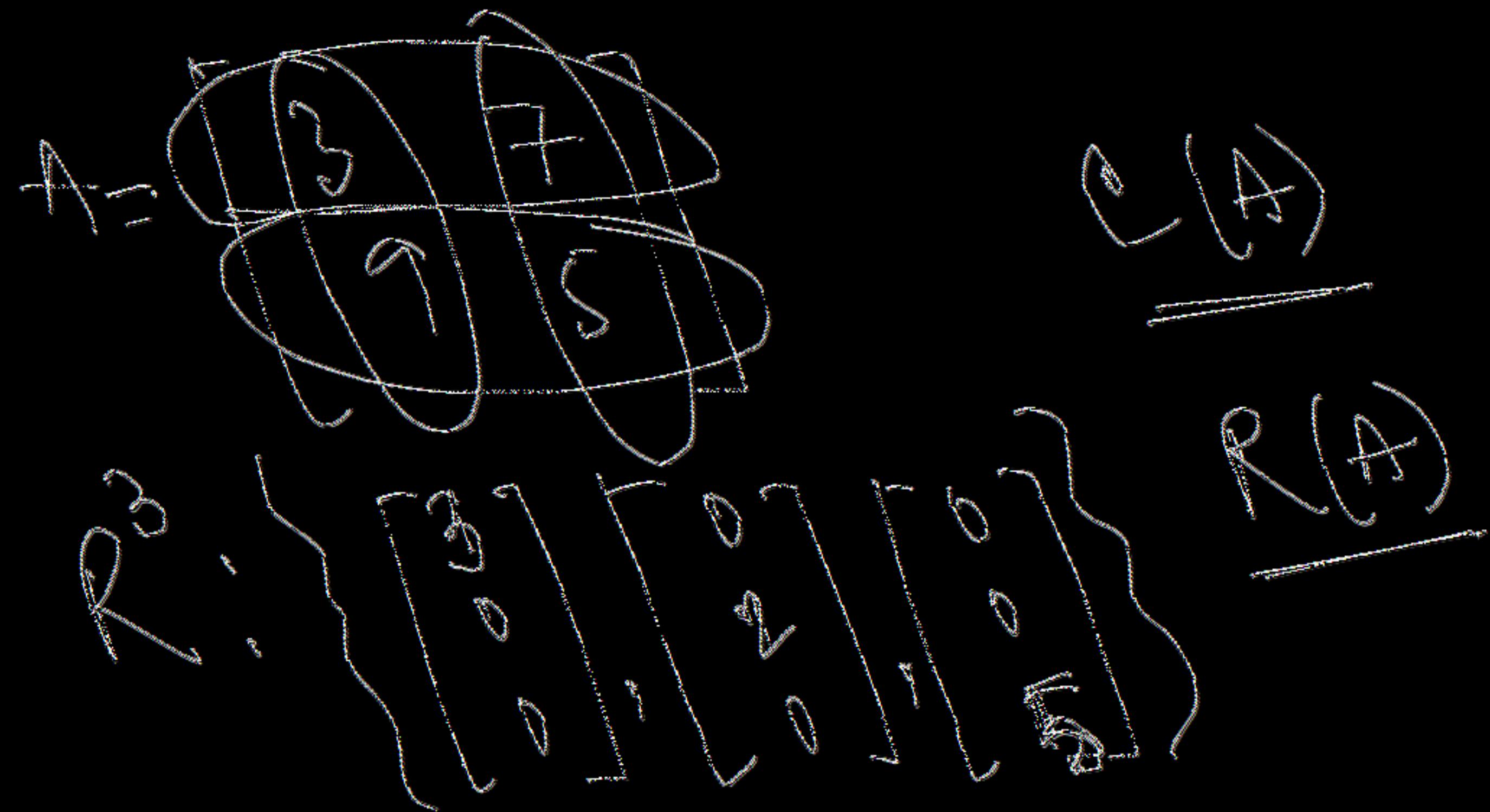
$$2x + x = 0$$

$$4_1 \quad 4_2$$

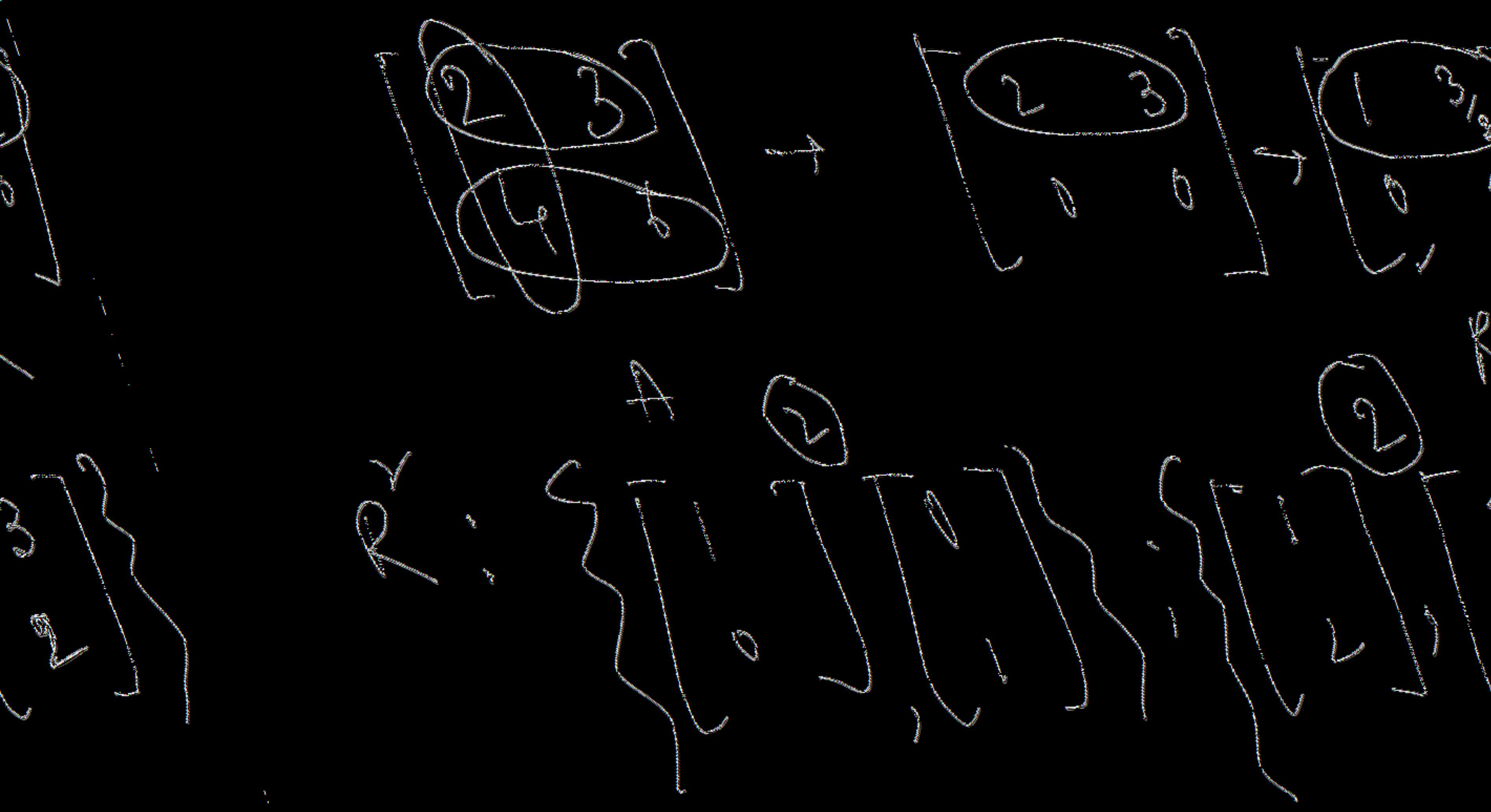
$$A = \{1, 2, 3, 4, 5, 6, 7\}$$

$$C(A) \subset R^2$$

6, 8, 1, 1, 6, 2



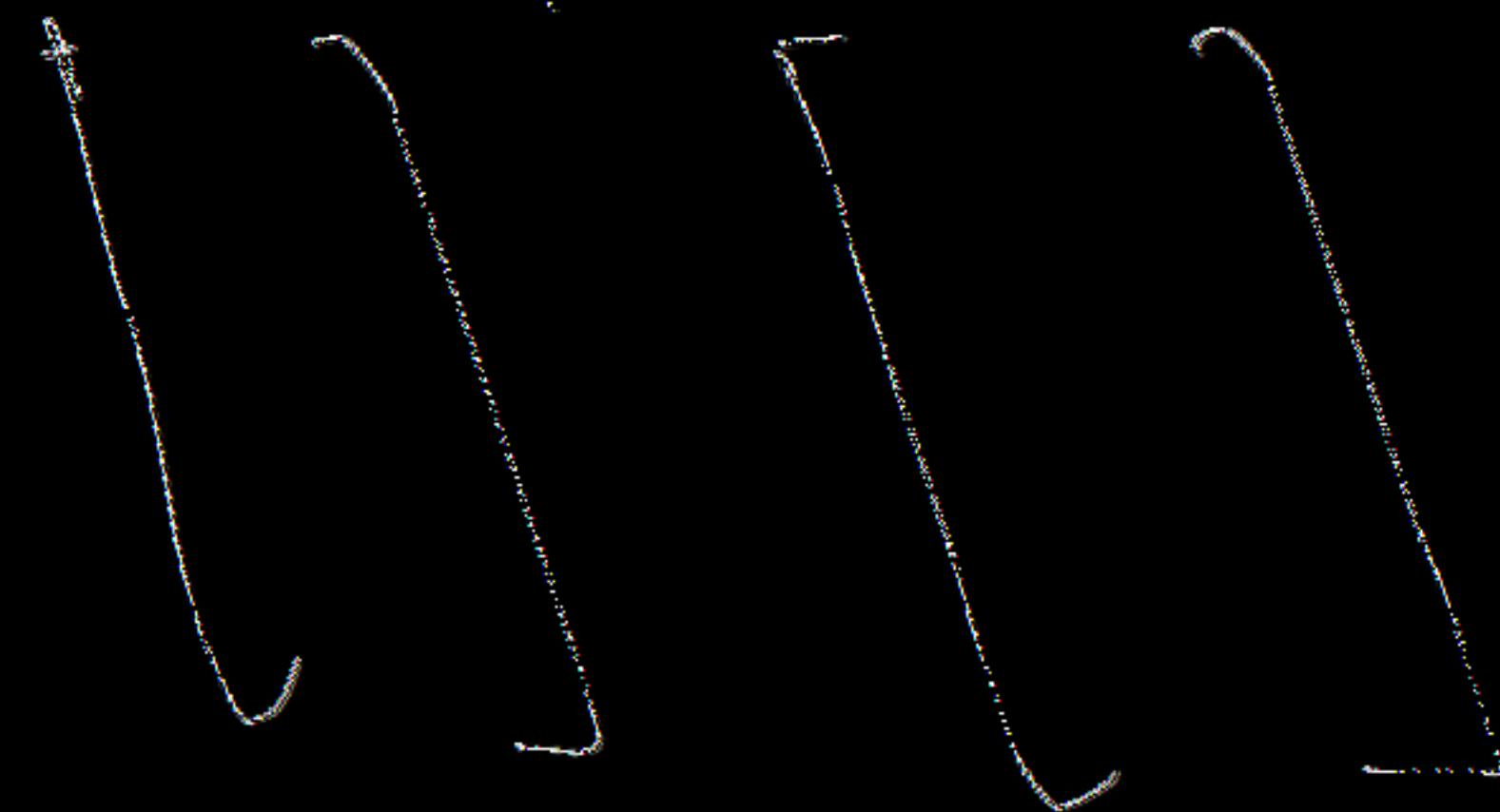
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20



$\nabla A \neq 0$

This is for  $N(A)$

$$x + 5y + 2t = 0$$



$$AX = 0$$

$$\boxed{AX = B}$$

$$\begin{bmatrix} 1 & 3 & 0 & 2 & 1 \\ 0 & 3 & 1 & 4 & 2 \\ -1 & 3 & 1 & 8 & 4 \end{bmatrix} \xrightarrow{\text{Row operations}}$$

$$\begin{bmatrix} A & B \end{bmatrix} \xrightarrow{\text{Row operations}}$$

$$\begin{bmatrix} I & A^{-1}B \end{bmatrix}$$

$$\begin{bmatrix} 1 & 3 & 0 & 2 & 1 \\ 0 & 3 & 1 & 4 & 2 \\ -1 & 3 & 1 & 8 & 4 \end{bmatrix} \xrightarrow{\text{Row operations}} \begin{bmatrix} 1 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 2 & 1 \end{bmatrix}$$

Partition left  $A$

$$x_2 - x_3 = 0$$

$$x_1 = 1, x_3 = b$$

$$x_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad x_n = \begin{pmatrix} -3 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Complete Sol =  $x_0 + t x_n$ .

$$\lambda_2 = 0$$

left null space

$$A^T y = 0 \quad N(A)$$

$$R(A) = C(A^T)$$

A man  
has



pxn