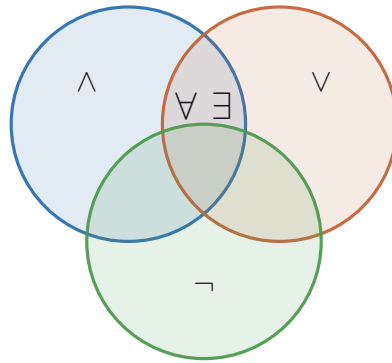




Discrete Mathematics I

A Comprehensive Reference Note

SCS 1302 · Bachelor of Science in Computer Science
University of Colombo School of Computing

Covering the eight lecture topics of the course — propositional logic, predicate logic, arguments, methods of proof, set theory, functions, relations and number theory — with definitions, theorems, proofs, diagrams, worked examples, and complete solutions to Tutorials 01–04 and Take-Home Assignments 01–02.

Aligned with K. H. Rosen, *Discrete Mathematics and Its Applications*, 7th edition, Chapters 1, 2, 4 and 9.

How this note is organised

- | | |
|-----------------|---|
| Part I | Logic and Proof (Chapters 1–4) |
| Part II | Discrete Structures (Chapters 5–8) |
| Part III | Worked Solutions and Quick-Reference Tables |

Prepared as a study reference. Every definition, theorem and worked example is traceable to the course lecture slides and problem sets.

How to Use This Note

This is a *reference* note, not a set of lecture slides transcribed. It is written so that you can read it linearly the first time and then dip into it repeatedly afterwards. Four kinds of boxes recur throughout.

Definition boxes (blue) hold the formal definitions. When an exam question says “state the definition of ...”, the wording inside these boxes is what is expected.

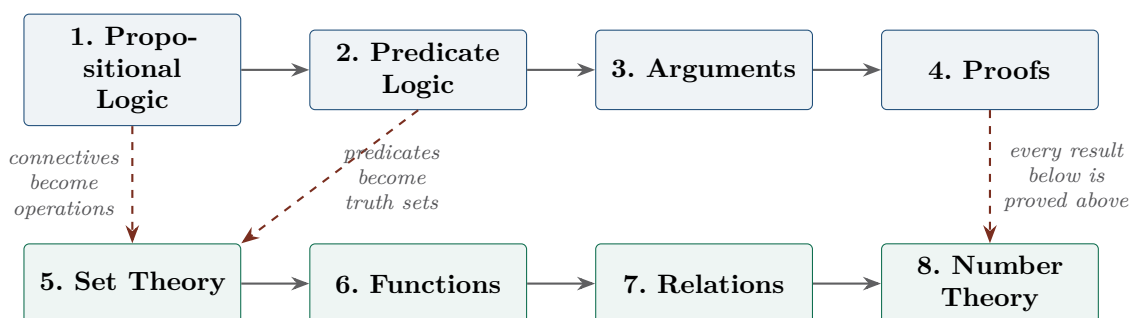
Theorem boxes (rust) hold theorems, lemmas and corollaries. Every theorem that the course proves is proved here too; theorems quoted without proof are explicitly flagged.

Example 0.1 (reading the example boxes). **Example boxes** (green) contain fully worked problems. The solution is written out at the level of detail expected in a written answer — each algebraic step named, each set inclusion argued in both directions.

Warning boxes (ochre) mark the places where marks are most often lost: the fallacies that look like valid inference rules, the “obvious” set identities that are false, the quantifier orders that are not interchangeable, the congruences you may not divide through.

The shape of the subject

The eight topics are not eight unrelated blocks. They form two chains that meet in the middle, and it helps enormously to see this early.



The dashed arrows are the ones worth internalising:

- **Chapter 1** → **Chapter 5**. Set theory is propositional logic wearing different symbols. $\cup$ is $\vee$, $\cap$ is $\wedge$, complement is $\neg$. Every set identity in Chapter 5 is a logical equivalence from Chapter 1 translated one symbol at a time. Both are examples of a *Boolean algebra*.
- **Chapter 2** → **Chapter 5**. A predicate $P(x)$ over a domain D names the subset $\{x \in D : P(x)\}$ of D — its truth set. $\forall x P(x)$ says that subset is all of D ; $\exists x P(x)$ says it is non-empty.
- **Chapter 4** → **Chapters 5–8**. Chapter 4 supplies the proof machinery; Chapters 5–8 supply the material to prove things about. Practically every proof in the second half is a

direct proof, a proof by contraposition, a proof by contradiction, a proof by cases, or a double-inclusion argument — all set up in Chapter 4.

Notation used throughout

Symbol	Meaning	Symbol	Meaning
$\neg p$	negation	$\mathbb{N}$	$\{0, 1, 2, \dots\}$
$p \wedge q$	conjunction	$\mathbb{Z}^+$	$\{1, 2, 3, \dots\}$
$p \vee q$	disjunction	$\mathbb{Z}$	all integers
$p \oplus q$	exclusive or	$\mathbb{Q}$	rationals
$p \rightarrow q$	conditional	$\mathbb{R}$	reals
$p \leftrightarrow q$	biconditional	$\mathbb{C}$	complex numbers
$p \equiv q$	logical equivalence	$\mathbb{U}$	universal set
$\forall x$	universal quantifier	$\emptyset$	empty set
$\exists x$	existential quantifier	$ A $	cardinality of A
$\exists! x$	unique existence	$\mathcal{P}(A)$	power set of A
$\mathbf{T}, \mathbf{F}$ or $1, 0$	truth values	$A \triangle B$	symmetric difference
$\models$	logical consequence	$a \mid b$	a divides b
$\therefore$	“therefore”	$a \equiv b \pmod{m}$	congruence
$\square$	empty clause	$\lfloor x \rfloor, \lceil x \rceil$	floor, ceiling

Two symbols that are constantly confused. $p \rightarrow q$ is a *compound proposition*: it has a truth value and appears inside truth tables. $p \equiv q$ is a *statement about* two propositions — it asserts they agree in every row. It is not a connective and never appears as a column heading. The bridge between them: $p \equiv q$ holds exactly when $p \leftrightarrow q$ is a tautology.

Contents

How to Use This Note	i
Part I Logic and Proof	2
1 Propositional Logic	2
1.1 Propositions	2
1.2 Logical connectives and their truth tables	3
1.2.1 Negation	3
1.2.2 Conjunction, disjunction, exclusive or	3
1.2.3 Conditional and biconditional	3
1.2.4 All five, side by side	4
1.2.5 English renderings of the conditional	4
1.2.6 Converse, contrapositive, inverse	5
1.3 Precedence and associativity	6
1.4 Constructing truth tables	6
1.5 Logical equivalence	7
1.5.1 The standard equivalence laws	8
1.5.2 Proving equivalences by a chain of laws	8
1.5.3 The principle of duality	9
1.6 Classifying propositions	10
1.6.1 Logical consequence	10
1.6.2 Consistency	11
1.7 Functional completeness	12
1.8 Normal forms	13
1.8.1 Method 1 — algebraic	13
1.8.2 Method 2 — reading normal forms off the truth table	14
1.9 Applications	15
1.9.1 Translating English into logic	15
1.9.2 Logic circuits	15
1.10 Chapter summary	16
2 Predicate Logic	17
2.1 Predicates	17
2.1.1 Truth sets	18
2.1.2 Preconditions and postconditions	18
2.2 Quantifiers	18
2.2.1 English renderings	19
2.2.2 Precedence of quantifiers	19
2.3 Binding, scope and free variables	20
2.4 Negating quantified statements	20
2.5 Equivalences involving quantifiers	21
2.6 Translating between English and predicate logic	22
2.7 Nested quantifiers	22
2.7.1 Order of quantifiers matters	23
2.7.2 Translating nested quantifiers into English	23
2.7.3 Negating nested quantifiers	24

2.8	Unique existence	24
2.9	Rewriting one quantifier as the other	24
2.10	Quantifiers and truth sets: the link to set theory	25
2.11	Chapter summary	25
3	Arguments and Rules of Inference	26
3.1	Arguments and validity	26
3.2	Rules of inference for propositional logic	27
3.2.1	Verifying resolution	27
3.3	Building formal proofs	28
3.4	Fallacies	29
3.4.1	Fallacy of affirming the consequent	29
3.4.2	Fallacy of denying the antecedent	30
3.5	Rules of inference for quantified statements	31
3.6	Showing an argument is <i>invalid</i> : countermodels	33
3.7	Resolution	34
3.7.1	Refutation	35
3.8	Chapter summary	36
4	Introduction to Proofs	38
4.1	Terminology	38
4.1.1	Formal versus informal proofs	38
4.1.2	Practical applications	38
4.2	Reading the statement of a theorem	39
4.3	Definitions you need	39
4.4	The proof methods	40
4.4.1	Vacuous proof	41
4.4.2	Trivial proof	41
4.4.3	Direct proof	41
4.4.4	Proof by contraposition	42
4.4.5	Proof by contradiction	43
4.4.6	Proofs of equivalence	43
4.4.7	Counterexamples	44
4.4.8	Exhaustive proof and proof by cases	45
4.4.9	Existence proofs	46
4.4.10	Uniqueness proofs	46
4.5	Proof strategies	47
4.5.1	Forward and backward reasoning	47
4.5.2	Conjectures	48
4.6	Chapter summary	48
Part II	Discrete Structures	51
5	Set Theory	51
5.1	Sets, elements and well-definedness	51
5.1.1	Ways of describing a set	52
5.1.2	Special sets	52
5.1.3	Cardinality	52
5.2	Subsets and equality	52
5.3	Power sets	53
5.4	Truth sets and quantifiers	54
5.5	Set operations	54

5.6	Set identities	56
5.7	Four ways to prove a set identity	56
5.7.1	Method 1: the usual (double-inclusion) method	56
5.7.2	Method 2: the set-builder method	57
5.7.3	Method 3: membership tables	58
5.7.4	Method 4: using known set identities	59
5.8	Generalized unions and intersections	60
5.9	Computer representation of sets	60
5.10	Counting: the inclusion–exclusion principle	61
5.11	Chapter summary	62
6	Functions	63
6.1	Definition and terminology	63
6.2	One-to-one (injective) functions	64
6.3	Onto (surjective) functions	65
6.4	Bijections	65
6.5	Inverse functions	67
6.6	Composition	68
6.7	The identity function	69
6.8	The graph of a function	70
6.9	Images and inverse images of subsets	70
6.9.1	Images and set operations	71
6.9.2	Inverse images and set operations	71
6.10	Floor and ceiling	72
6.11	Partial functions	73
6.12	Chapter summary	73
7	Relations	74
7.1	Cartesian products	74
7.2	Binary relations	74
7.2.1	How many relations are there?	75
7.3	Representing relations	75
7.4	Properties of relations	76
7.4.1	Worked classification: relations on a finite set	76
7.4.2	Worked classification: relations on $\mathbb{Z}$	77
7.4.3	Counting relations with a given property	78
7.5	Combining relations	79
7.6	Composition of relations	80
7.7	Powers of a relation	81
7.8	Functions as relations	82
7.9	Equivalence relations and partial orders	82
7.9.1	Hasse diagrams	83
7.10	n -ary relations	84
7.11	Chapter summary	84
8	Number Theory	86
8.1	Divisibility	86
8.2	The division algorithm	87
8.3	Congruences	88
8.3.1	Arithmetic with congruences	88
8.3.2	Fast modular exponentiation	89
8.3.3	Arithmetic on $\mathbb{Z}_m$	90
8.4	Primes	90

8.5	Greatest common divisor and least common multiple	91
8.6	The Euclidean algorithm	91
8.7	Bézout's theorem and the extended algorithm	93
8.8	Linear congruences and modular inverses	94
8.9	The Chinese remainder theorem	95
8.10	Euler's totient function	96
8.10.1	Residue systems	97
8.11	Euler's theorem and Fermat's little theorem	97
8.12	Applications	99
8.13	Chapter summary	100
Part III	Worked Solutions and Reference Tables	102
A	Worked Solutions: Tutorials 01–04	102
A.1	Tutorial 01 — Propositional Logic	102
A.2	Tutorial 02 — Predicate Logic	107
A.3	Tutorial 03 — Arguments	109
A.4	Tutorial 04 — Sets, Functions, Relations, Number Theory	112
B	Worked Solutions: Assignments 01–02	122
B.1	Assignment 01	122
B.2	Assignment 02	129
C	Quick Reference	138
C.1	Truth tables and equivalences	138
C.2	Rules of inference	139
C.3	Quantifier rules	139
C.4	Proof methods	140
C.5	Sets	140
C.6	Functions	140
C.7	Relations	141
C.8	Number theory	141
C.9	Common pitfalls	142

Part I Logic and Proof

CHAPTER 1

Propositional Logic

What this chapter is for. Propositional logic is the algebra of statements that are simply true or false. It gives us (i) a precise notation for compound English sentences, (ii) a mechanical procedure — the truth table — for deciding whether two statements say the same thing, and (iii) the classification of statements into tautologies, contradictions and contingencies that underpins every later notion of “valid argument” and “correct proof”.

1.1 Propositions

Definition 1.1 (Proposition). A *proposition* is a declarative sentence — a sentence that declares a fact — that is either true or false, but not both. The true/false value assigned to a proposition is its *truth value*, written **T** (or 1) for true and **F** (or 0) for false.

Two conditions must both hold. The sentence must be *declarative* (so questions and commands are excluded), and it must have a *determinate* truth value (so sentences containing free variables are excluded until those variables are given values).

Example 1.1 (what counts and what does not). Propositions:

- (i) “Colombo is the biggest city of Sri Lanka.” (true)
- (ii) “ $2 + 3 = 4$.” (false — but still a proposition)
- (iii) “The Moon is made of cheese.” (false)

Not propositions:

- (i) “What time is it?” (interrogative, not declarative)
- (ii) “Please be silent!” (imperative, not declarative)
- (iii) “ $x + 5 = 3$.” (truth value depends on x)

Being false does not disqualify a sentence — item (ii) in the first list is a perfectly good proposition. Only *indeterminacy* disqualifies.

Definition 1.2 (Atomic and compound propositions). A proposition that cannot be broken into smaller propositions is *atomic* (or *primitive*, or *simple*). A proposition built from two or more atomic propositions using logical connectives is *compound* (or *composite*).

Notation 1.3 (Propositional variables). Letters $p, q, r, s, \dots$ stand for atomic propositions and are called *propositional variables*. A *formula* is what you get when every atomic proposition in a compound proposition is replaced by a propositional variable — e.g. the English sentence “5 is prime and $1 = 0$ ” becomes the formula $p \wedge q$.

1.2 Logical connectives and their truth tables

Definition 1.4 (Truth table). A *truth table* for a compound proposition lists every possible combination of truth values of its propositional variables, together with the resulting truth value of the compound proposition.

There are five connectives in this course. One is unary; four are binary.

1.2.1 Negation

Definition 1.5 (Negation). Let p be a proposition. The *negation* of p , written $\neg p$, is the proposition “it is not the case that p ”. It is true exactly when p is false.

Example 1.2. Let p be “Nimal’s phone has at least 32 GB of memory.” Then $\neg p$ may be rendered as “it is not the case that Nimal’s phone has at least 32 GB of memory”, or more naturally, “Nimal’s phone has less than 32 GB of memory”. Note that the natural rendering of “ $\neg$ (at least 32)” is “*less than 32*”, not “more than 32” — negating an inequality flips it and swaps strictness.

1.2.2 Conjunction, disjunction, exclusive or

Definition 1.6 (Conjunction, disjunction, exclusive or). Let p and q be propositions.

- The *conjunction* (or *product*) $p \wedge q$, read “ p and q ”, is true when both p and q are true, and false otherwise.
- The *disjunction* (or *sum*) $p \vee q$, read “ p or q ”, is false when both p and q are false, and true otherwise. This is the *inclusive* or.
- The *exclusive or* $p \oplus q$ is true when exactly one of p, q is true, and false otherwise.

In logic the word “but” is often used in place of “and”. “The sun is shining, but it is raining” is another way of saying “the sun is shining *and* it is raining” — the contrast is rhetorical, not logical.

1.2.3 Conditional and biconditional

Definition 1.7 (Conditional statement). The *conditional* $p \rightarrow q$, read “if p then q ”, is false when p is true and q is false, and true in all three other cases. Here p is the *hypothesis* (antecedent, premise) and q is the *conclusion* (consequent).

Definition 1.8 (Biconditional). The *biconditional* $p \leftrightarrow q$, read “ p if and only if q ”, is true when p and q have the same truth value, and false otherwise.

1.2.4 All five, side by side

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \rightarrow q$	$p \leftrightarrow q$
F	F	T	F	F	F	T	T
F	T	T	F	T	T	T	F
T	F	F	F	T	T	F	F
T	T	F	T	T	F	T	T

Table 1.1: The master truth table. Everything in propositional logic is recoverable from these six columns.

It pays to memorise each connective by its *single exceptional row*, rather than by all four rows:

$p \wedge q$	true in one row only: TT
$p \vee q$	false in one row only: FF
$p \rightarrow q$	false in one row only: TF
$p \leftrightarrow q$	true exactly when the two agree
$p \oplus q$	true exactly when the two differ

The conditional is the one that surprises people. $p \rightarrow q$ is *true* whenever p is false, regardless of q . “If the Moon is made of cheese, then $2 = 3$ ” is a true proposition. The conditional does not claim any causal or topical link between p and q ; it only forbids the single combination “ p true, q false”. The vacuous proof of Chapter 4 rests entirely on this.

1.2.5 English renderings of the conditional

The conditional has an unusually large number of English disguises. All of the following mean $p \rightarrow q$:

- if p , then q
- p implies q
- q if p
- p only if q
- q whenever p
- q follows from p
- p is sufficient for q
- a sufficient condition for q is p
- q is necessary for p
- a necessary condition for p is q

“only if” points the other way from “if”.

- “ p if q ” means $q \rightarrow p$.
- “ p only if q ” means $p \rightarrow q$.
- “ p if and only if q ” means $p \leftrightarrow q$.

Likewise *sufficient* conditions sit on the left of the arrow and *necessary* conditions sit on the right.

Example 1.3 (translating “only if”). Translate: “You can access the Internet from campus only if you are a computer science major or you are not a freshman.”

Solution. Let a = “you can access the Internet from campus”, c = “you are a computer science major”, f = “you are a freshman”. Since “ p only if q ” is $p \rightarrow q$, the sentence is

$$a \rightarrow (c \vee \neg f).$$

Example 1.4 (inclusive or exclusive?). Decide which “or” is meant.

- (a) “Experience with C++ or Java is required.” — **inclusive**. Knowing both is not a disqualification.
- (b) “Lunch includes soup or salad.” — **exclusive**. You get one, not both.
- (c) “To enter the country you need a passport or a voter registration card.” — **inclusive**. Having both is fine.
- (d) “Publish or perish.” — **inclusive** in form (the academic who publishes and then perishes has not falsified it), though rhetorically it is used exclusively.

1.2.6 Converse, contrapositive, inverse

Definition 1.9. From the conditional $p \rightarrow q$ we form

Name	Form	Equivalent to the original?
Conditional	$p \rightarrow q$	—
Converse	$q \rightarrow p$	No
Inverse	$\neg p \rightarrow \neg q$	No
Contrapositive	$\neg q \rightarrow \neg p$	Yes

The four-column truth table settles it at once:

p	q	$\neg p$	$\neg q$	$p \rightarrow q$ conditional	$q \rightarrow p$ converse	$\neg q \rightarrow \neg p$ contrapositive	$\neg p \rightarrow \neg q$ inverse
0	0	1	1	1	1	1	1
0	1	1	0	1	0	1	0
1	0	0	1	0	1	0	1
1	1	0	0	1	1	1	1

Table 1.2: Columns 5 and 7 agree everywhere: $p \rightarrow q \equiv \neg q \rightarrow \neg p$. Columns 6 and 8 also agree with each other (the converse and the inverse are contrapositives of one another), but neither agrees with column 5.

Example 1.5 (stating all three). “If it snows tonight, then I will stay at home.”

- **Converse:** If I stay at home tonight, then it will snow.
- **Contrapositive:** If I do not stay at home tonight, then it will not snow.
- **Inverse:** If it does not snow tonight, then I will not stay at home.

Only the contrapositive is guaranteed to have the same truth value as the original.

1.3 Precedence and associativity

Without a precedence convention, $p \vee q \rightarrow r$ is ambiguous: it could mean $(p \vee q) \rightarrow r$ or $p \vee (q \rightarrow r)$, which are different propositions.

Precedence, highest binds first

Rank	1	2	3	4	5
Operator	$\neg$	$\wedge$	$\vee$	$\rightarrow$	$\leftrightarrow$

So $p \vee q \rightarrow r$ means $(p \vee q) \rightarrow r$, and

$$\neg p \rightarrow q \vee r \rightarrow p \vee q \wedge r \quad \text{means} \quad (\neg p) \rightarrow ((q \vee r) \rightarrow (p \vee (q \wedge r))),$$

because operators of equal precedence associate to the right. A parse tree makes the grouping visible.

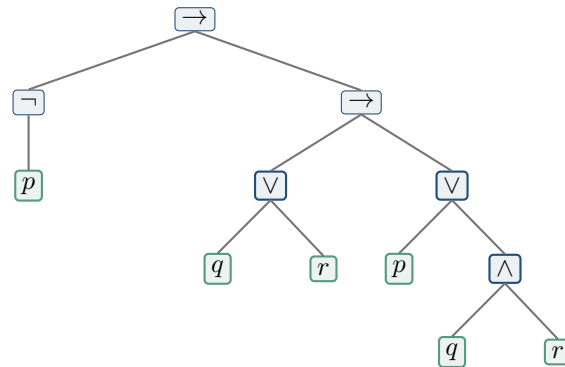


Figure 1.1: Parse tree for $\neg p \rightarrow q \vee r \rightarrow p \vee q \wedge r$. Evaluation runs bottom-up: leaves get truth values, each internal node combines its children.

1.4 Constructing truth tables

Procedure. For a compound proposition C over atomic propositions $p_1, \dots, p_n$:

1. Count the atomic propositions: n .
2. Draw a table with $m = 2^n$ rows.
3. Enumerate all 2^n combinations of truth values systematically.
4. Rank the operators of C by precedence.
5. Add one intermediate column per operator, in that order, ending with C itself.

For step 3, the standard systematic pattern is: the leftmost variable alternates in blocks of 2^{n-1} , the next in blocks of 2^{n-2} , and so on down to the rightmost, which alternates every row.

	p		q		r	
4	T	2	T	alternates every row	T	
	T		T		F	
	T	2	F		T	
	T		F		F	
4	F		T		T	
	F		T		F	
	F		F		T	
	F		F		F	

Figure 1.2: The systematic enumeration for $n = 3$: blocks of 4, 2, 1. Doing it this way guarantees you neither repeat nor omit a row.

Example 1.6 (a two-variable table). Construct the truth table of $(p \vee \neg q) \rightarrow (p \wedge q)$.

Solution. Two variables, so $2^2 = 4$ rows. Intermediate columns for $\neg q$, $p \vee \neg q$ and $p \wedge q$ come before the final column.

p	q	$\neg q$	$p \vee \neg q$	$p \wedge q$	$(p \vee \neg q) \rightarrow (p \wedge q)$
0	0	1	1	0	0
0	1	0	0	0	1
1	0	1	1	0	0
1	1	0	1	1	1

The proposition is true in exactly two rows, so it is a contingency (Section 1.6).

1.5 Logical equivalence

Definition 1.10 (Logical equivalence). Two compound propositions are *logically equivalent*, written $P \equiv Q$, when they have the same truth value for every assignment of truth values to their propositional variables.

Theorem 1.11. $P \equiv Q$ if and only if $P \leftrightarrow Q$ is a tautology.

$\equiv$ is **not a connective**. $P \equiv Q$ is a statement *about* the two propositions, made from outside the logic; it is not itself a compound proposition and never gets a truth-table column of its own. $P \leftrightarrow Q$ is a compound proposition and does get a column. Writing “ $p \equiv q$ ” inside a formula is a notation error.

The practical value of equivalence is *substitution*: if $P \equiv Q$, then replacing P by Q anywhere inside a larger proposition leaves the truth value of the whole unchanged.

1.5.1 The standard equivalence laws

Name	Law	
Identity	$p \wedge \mathbf{T} \equiv p$	$p \vee \mathbf{F} \equiv p$
Domination	$p \vee \mathbf{T} \equiv \mathbf{T}$	$p \wedge \mathbf{F} \equiv \mathbf{F}$
Idempotent	$p \vee p \equiv p$	$p \wedge p \equiv p$
Double negation	$\neg(\neg p) \equiv p$	
Commutative	$p \vee q \equiv q \vee p$	$p \wedge q \equiv q \wedge p$
Associative	$(p \vee q) \vee r \equiv p \vee (q \vee r)$	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
Distributive	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
De Morgan	$\neg(p \vee q) \equiv \neg p \wedge \neg q$	$\neg(p \wedge q) \equiv \neg p \vee \neg q$
Absorption	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Negation	$p \vee \neg p \equiv \mathbf{T}$	$p \wedge \neg p \equiv \mathbf{F}$

Table 1.3: The ten basic equivalence laws. Note that they come in dual pairs (Section 1.5.3).

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

Table 1.4: Equivalences involving conditionals and biconditionals. The first entry, $p \rightarrow q \equiv \neg p \vee q$, is the single most useful line in this chapter — it is how you get rid of arrows before applying De Morgan or distributing.

Also worth recording, since it appears in the exclusive-or exercises:

$$p \oplus q \equiv (p \wedge \neg q) \vee (\neg p \wedge q) \equiv \neg(p \wedge q) \wedge (p \vee q).$$

1.5.2 Proving equivalences by a chain of laws

Example 1.7 (chain of equivalences). Show $\neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg q$.

Solution.

$$\begin{aligned}
 \neg(p \vee (\neg p \wedge q)) &\equiv \neg p \wedge \neg(\neg p \wedge q) && \text{De Morgan} \\
 &\equiv \neg p \wedge (\neg(\neg p) \vee \neg q) && \text{De Morgan} \\
 &\equiv \neg p \wedge (p \vee \neg q) && \text{double negation} \\
 &\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) && \text{distributive} \\
 &\equiv \mathbf{F} \vee (\neg p \wedge \neg q) && \text{negation law} \\
 &\equiv \neg p \wedge \neg q && \text{identity law.}
 \end{aligned}$$

Example 1.8 (a tautology, proved algebraically). Show $(p \wedge q) \rightarrow (p \vee q) \equiv \mathbf{T}$.

Solution.

$$\begin{aligned}
 (p \wedge q) \rightarrow (p \vee q) &\equiv \neg(p \wedge q) \vee (p \vee q) && \rightarrow \text{elimination} \\
 &\equiv (\neg p \vee \neg q) \vee (p \vee q) && \text{De Morgan} \\
 &\equiv (\neg p \vee p) \vee (\neg q \vee q) && \text{commutative, associative} \\
 &\equiv \mathbf{T} \vee \mathbf{T} && \text{negation law} \\
 &\equiv \mathbf{T} && \text{domination law.}
 \end{aligned}$$

Example 1.9. Show $(p \rightarrow q) \vee (p \rightarrow r) \equiv \neg p \vee q \vee r$.

Solution.

$$\begin{aligned}
 (p \rightarrow q) \vee (p \rightarrow r) &\equiv (\neg p \vee q) \vee (\neg p \vee r) && \rightarrow \text{elimination} \\
 &\equiv (\neg p \vee \neg p) \vee q \vee r && \text{commutative, associative} \\
 &\equiv \neg p \vee q \vee r && \text{idempotent law.}
 \end{aligned}$$

1.5.3 The principle of duality

Definition 1.12 (Dual). The *dual* of a proposition built from $\wedge, \vee, \neg, \mathbf{T}, \mathbf{F}$ is obtained by interchanging $\wedge \leftrightarrow \vee$ and $\mathbf{T} \leftrightarrow \mathbf{F}$ (equivalently $1 \leftrightarrow 0$), leaving negations and variables alone.

Theorem 1.13 (Principle of duality). *If two propositions are logically equivalent, so are their duals. Consequently every law in Table 1.3 comes free with its dual — which is why the table has two columns.*

This halves what you have to memorise: learn $\neg(p \vee q) \equiv \neg p \wedge \neg q$ and the other De Morgan law follows by duality.

1.6 Classifying propositions

Definition 1.14. A compound proposition is

- a *tautology* if it is true for every assignment of truth values to its variables;
- a *contradiction* if it is false for every assignment;
- a *contingency* if it is neither.

A proposition is *satisfiable* if *some* assignment makes it true (i.e. it is a tautology or a contingency), and *unsatisfiable* otherwise. A proposition is *valid* if every entry in its truth table is true — so “valid” and “tautology” are the same thing.

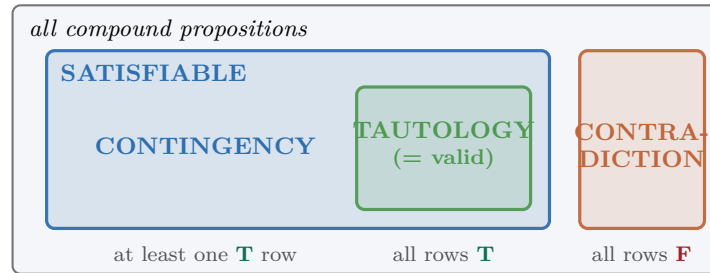


Figure 1.3: The classification. “Satisfiable” is the union of tautologies and contingencies; a contradiction is exactly an unsatisfiable proposition. Note P is a contradiction iff $\neg P$ is a tautology.

Example 1.10 (the smallest examples).

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

p itself, $\neg p$ and $p \wedge q$ are all satisfiable contingencies; $p \wedge \neg p$ is unsatisfiable.

1.6.1 Logical consequence

Definition 1.15 (Logical consequence). A proposition B is a *logical consequence* of propositions $A_1, A_2, \dots, A_n$ — written $A_1, \dots, A_n \models B$ — when

$$(A_1 \wedge A_2 \wedge \dots \wedge A_n) \rightarrow B$$

is valid (a tautology).

Example 1.11 (from p and $p \rightarrow q$, conclude q).

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

The last column is all **T**, so the implication is valid and q is a logical consequence of p and $p \rightarrow q$. This is the inference rule *modus ponens*, met again in Chapter 3.

1.6.2 Consistency

Definition 1.16 (Consistency). A set of propositions is *consistent* if there is a single assignment of truth values to all the propositional variables making *every* proposition in the set true simultaneously. Otherwise it is *inconsistent*.

Consistency of a set $\{A_1, \dots, A_n\}$ is the same as satisfiability of the single proposition $A_1 \wedge \dots \wedge A_n$.

Example 1.12 (system specifications, consistent). Are these consistent?

- “The diagnostic message is stored in the buffer or it is retransmitted.”
- “The diagnostic message is not stored in the buffer.”
- “If the diagnostic message is stored in the buffer, then it is retransmitted.”

Solution. Let p = “stored in the buffer”, q = “retransmitted”. The specifications are $p \vee q$, $\neg p$, and $p \rightarrow q$.

Method 1 (truth table).

p	q	$\neg p$	$p \vee q$	$p \rightarrow q$	$\neg p \wedge (p \vee q) \wedge (p \rightarrow q)$
0	0	1	0	1	0
0	1	1	1	1	1
1	0	0	1	0	0
1	1	0	1	1	0

Row 2 makes all three true, so the specifications are **consistent**.

Method 2 (direct reasoning — faster, and what you should do for larger systems). Suppose $\neg p$ and $p \vee q$ are true. Then p is false; since $p \vee q$ is true, q must be true; and since p is false, $p \rightarrow q$ is automatically true. So the assignment $p = \mathbf{F}$, $q = \mathbf{T}$ satisfies all three.

Example 1.13 (system specifications, inconsistent). Determine whether these are consistent.

“The system is in multiuser state if and only if it is operating normally. If the system is operating normally, then the kernel is functioning. The kernel is not functioning or the system is in interrupt mode. If the system is not in multiuser state, then it is in interrupt

mode. The system is not in interrupt mode.”

Solution. Let p = “in multiuser state”, q = “operating normally”, r = “kernel is functioning”, s = “in interrupt mode”. The specifications are

$$p \leftrightarrow q, \quad q \rightarrow r, \quad \neg r \vee s, \quad \neg p \rightarrow s, \quad \neg s.$$

A four-variable truth table has 16 rows; direct reasoning is quicker. Suppose the last four are all true. Then

- $\neg s$ true $\Rightarrow s$ is false.
- $\neg p \rightarrow s$ true with s false $\Rightarrow \neg p$ is false $\Rightarrow p$ is true.
- $\neg r \vee s$ true with s false $\Rightarrow \neg r$ is true $\Rightarrow r$ is false.
- $q \rightarrow r$ true with r false $\Rightarrow q$ is false.

Now p is true and q is false, so $p \leftrightarrow q$ is *false*. Thus whenever the last four hold, the first fails: no assignment satisfies all five. The specification set is **inconsistent**.

Why specification consistency matters. An inconsistent specification cannot be implemented by *any* system, because the requirements contradict each other. Worse, from an inconsistent set every conclusion follows, so an automated tool reasoning over the specification will happily “prove” anything.

1.7 Functional completeness

Definition 1.17 (Functionally complete). A set of connectives is *functionally complete* if every compound proposition is logically equivalent to one built using only connectives from that set.

Not all five connectives are needed. Working from Table 1.4:

$$\begin{aligned} p \rightarrow q &\equiv \neg p \vee q, & p \leftrightarrow q &\equiv (\neg p \vee q) \wedge (\neg q \vee p), \\ p \oplus q &\equiv (p \wedge \neg q) \vee (\neg p \wedge q), & p \wedge q &\equiv \neg(\neg p \vee \neg q). \end{aligned}$$

Theorem 1.18. $\{\neg, \vee\}$ is functionally complete. So is $\{\neg, \wedge\}$.

Sketch. By the displayed equivalences, $\rightarrow$, $\leftrightarrow$ and $\oplus$ are all expressible using $\neg, \wedge, \vee$; and $\wedge$ is expressible using $\neg, \vee$ by De Morgan. Hence every connective reduces to $\{\neg, \vee\}$. Dually, $\vee$ reduces to $\{\neg, \wedge\}$. ■

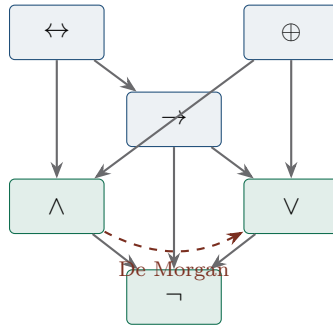


Figure 1.4: Reduction of connectives. An arrow means “is definable using”. Everything bottoms out at $\{\neg, \vee\}$ (or, by De Morgan, at $\{\neg, \wedge\}$).

1.8 Normal forms

Normal forms give every proposition a canonical shape, which is what makes automated reasoning possible.

Definition 1.19 (Literals, elementary products and sums). A *literal* is a propositional variable or its negation. An *elementary product* is a conjunction of literals, e.g. $p \wedge q \wedge \neg r$. An *elementary sum* (or *clause*) is a disjunction of literals, e.g. $p \vee \neg q \vee r$.

Definition 1.20 (DNF and CNF). A proposition is in *disjunctive normal form* (DNF) if it is a *sum of elementary products*:

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

A proposition is in *conjunctive normal form* (CNF) if it is a *product of elementary sums*:

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

Every proposition is logically equivalent to one in DNF and to one in CNF.

Mnemonic. DNF = **D**isjunction of conjunctions (“OR of ANDs”). CNF = **C**onjunction of disjunctions (“AND of ORs”). CNF is the form resolution needs (Chapter 3).

1.8.1 Method 1 — algebraic

Recipe.

1. Eliminate $\leftrightarrow$ using $P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$.
2. Eliminate $\rightarrow$ using $P \rightarrow Q \equiv \neg P \vee Q$.
3. Push $\neg$ inwards with De Morgan until it sits only on variables.
4. Distribute: $\wedge$ over $\vee$ for DNF, $\vee$ over $\wedge$ for CNF.
5. Simplify using idempotent, negation and domination laws.

Example 1.14 (DNF algebraically). Find the DNF of $(\neg p \vee \neg q) \rightarrow (p \leftrightarrow \neg q)$.

Solution.

$$\begin{aligned} (\neg p \vee \neg q) \rightarrow (p \leftrightarrow \neg q) &\equiv \neg(\neg p \vee \neg q) \vee (p \leftrightarrow \neg q) \\ &\equiv (p \wedge q) \vee [(p \wedge \neg q) \vee (\neg p \wedge \neg(\neg q))] \\ &\equiv (p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge q). \end{aligned}$$

Here the second step used De Morgan on the left disjunct and $P \leftrightarrow Q \equiv (P \wedge Q) \vee (\neg P \wedge \neg Q)$ on the right.

Example 1.15 (CNF algebraically). Find the CNF of the same proposition $x = (\neg p \vee \neg q) \rightarrow (p \leftrightarrow \neg q)$.

Solution.

$$\begin{aligned} x &\equiv \neg(\neg p \vee \neg q) \vee (p \leftrightarrow \neg q) \\ &\equiv (p \wedge q) \vee [(p \rightarrow \neg q) \wedge (\neg q \rightarrow p)] \\ &\equiv (p \wedge q) \vee [(\neg p \vee \neg q) \wedge (q \vee p)] \\ &\equiv [p \vee ((\neg p \vee \neg q) \wedge (q \vee p))] \wedge [q \vee ((\neg p \vee \neg q) \wedge (q \vee p))] \\ &\equiv (p \vee \neg p \vee \neg q) \wedge (p \vee q \vee p) \wedge (q \vee \neg p \vee \neg q) \wedge (q \vee q \vee p) \\ &\equiv \mathbf{T} \wedge (p \vee q) \wedge \mathbf{T} \wedge (p \vee q) \\ &\equiv p \vee q. \end{aligned}$$

1.8.2 Method 2 — reading normal forms off the truth table

This is faster and far less error-prone.

DNF from a truth table. For each row where the proposition is **true**, form the elementary product that “describes” that row (use p if p is true in that row, $\neg p$ if false). Take the disjunction of all such products.

CNF from a truth table. Read the DNF of $\neg x$ off the **false** rows, then negate and apply De Morgan. Equivalently: for each row where the proposition is **false**, form the elementary *sum* that is falsified by that row (use $\neg p$ if p is true in that row, p if false), and take the conjunction.

Example 1.16 (both forms from one table). Take $x = (\neg p \vee \neg q) \rightarrow (p \leftrightarrow \neg q)$ again.

p	q	$\neg p$	$\neg q$	$\neg p \vee \neg q$	$p \leftrightarrow \neg q$	x	$\neg x$
0	0	1	1	1	0	0	1
0	1	1	0	1	1	1	0
1	0	0	1	1	1	1	0
1	1	0	0	0	0	1	0

DNF: x is true in rows 2, 3, 4, described by $(\neg p \wedge q)$, $(p \wedge \neg q)$, $(p \wedge q)$. Hence

$$x \equiv (\neg p \wedge q) \vee (p \wedge \neg q) \vee (p \wedge q).$$

CNF: $\neg x$ is true only in row 1, so $\neg x \equiv \neg p \wedge \neg q$, and therefore

$$x \equiv \neg(\neg x) \equiv \neg(\neg p \wedge \neg q) \equiv p \vee q,$$

matching the algebraic answer.

1.9 Applications

1.9.1 Translating English into logic

Example 1.17 (a class of statements). Let p = “you get an A on the final exam”, q = “you do every exercise in this book”, r = “you get an A in this class”.

English	Formula
You get an A in this class, but you do not do every exercise.	$r \wedge \neg q$
You get an A on the final, you do every exercise, and you get an A in the class.	$p \wedge q \wedge r$
To get an A in this class, it is necessary for you to get an A on the final.	$r \rightarrow p$
You get an A on the final, but you do not do every exercise; nevertheless you get an A in the class.	$p \wedge \neg q \wedge r$
Getting an A on the final and doing every exercise is sufficient for getting an A in the class.	$(p \wedge q) \rightarrow r$
You get an A in this class if and only if you either do every exercise or get an A on the final.	$r \leftrightarrow (q \vee p)$

Note how “but” and “nevertheless” are just $\wedge$ with rhetorical colouring, and how “necessary” and “sufficient” place the arrow in opposite directions.

1.9.2 Logic circuits

Propositional logic is the mathematics of digital circuits: $\wedge$ is an AND gate, $\vee$ an OR gate, $\neg$ a NOT gate. Simplifying a formula with the equivalence laws means building the same circuit with fewer gates.

CHAPTER 2

Predicate Logic

Why propositional logic is not enough. Consider the argument “every integer is either even or odd; 7 is an integer; therefore 7 is even or odd.” It is obviously valid — yet in propositional logic each of the three sentences is an unrelated atom p , q , r , and $p \wedge q \rightarrow r$ is not a tautology. Propositional logic cannot see *inside* a sentence. Predicate logic supplies the missing internal structure: objects, properties of objects, and quantifiers that range over collections of objects.

2.1 Predicates

Definition 2.1 (Predicate / propositional function). A *predicate* (or *propositional function*) is an expression containing one or more variables which becomes a proposition once every variable is assigned a value. Predicates are written with capital letters and their variables in parentheses:

$$P(x) ::= “x > 3”, \quad Q(x, y, z) ::= “x + y = z”.$$

A predicate in n variables is called an n -place or n -ary predicate.

A predicate is *not* a proposition: “ $x > 3$ ” has no truth value until we know x . But $P(4)$ is the proposition “ $4 > 3$ ”, which is true, and $P(1)$ is false.

Definition 2.2 (Domain of discourse). The set of values a variable is allowed to take is the *domain of discourse* (or *universe of discourse*) of that variable.

Under this reading a predicate is literally a function into truth values. For $P(x, y) ::= “x + y = 3”$ over the reals,

$$P : \mathbb{R} \times \mathbb{R} \longrightarrow \{\text{True}, \text{False}\}, \quad P(2, 1) = \text{True}, \quad P(3, 4) = \text{False}.$$

The common sets.

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$	non-negative integers
$\mathbb{Z}^+ = \{1, 2, 3, \dots\}$	positive integers
$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$	integers
$\mathbb{Q} = \left\{ \frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{Z}^+ \right\}$	rationals
$\mathbb{R}$	reals
$\mathbb{C} = \{x + iy : x, y \in \mathbb{R}\}$	complex numbers

2.1.1 Truth sets

Definition 2.3 (Truth set). Let $P(x)$ be a predicate over a domain U . The *truth set* of P is the set of values in U making P true:

$$\{x \in U \mid P(x)\}.$$

The truth set is the bridge from this chapter to Chapter 5: *a predicate over U and a subset of U are two descriptions of the same thing.*

Example 2.1 (computing truth sets).

- (a) $P(x) ::= x + 5 > 10$ over $\mathbb{Z}^+$. $\{x \in \mathbb{Z}^+ \mid x + 5 > 10\} = \{x \in \mathbb{Z}^+ \mid x > 5\} = \{6, 7, 8, \dots\}$.
- (b) $P(x) ::= x^2 < 0$ over $\mathbb{Z}^+$. Truth set = $\emptyset$.
- (c) $P(x) ::= x^2 - 3x + 2 = 0$ over $\mathbb{R}$. Factoring, $(x - 1)(x - 2) = 0$, so the truth set is $\{1, 2\}$.
- (d) Over $\mathbb{Z}$: the truth set of $|x| = 1$ is $\{-1, 1\}$; of $x^2 = 2$ is $\emptyset$; of $|x| = x$ is $\{x \in \mathbb{Z} \mid x \geq 0\} = \mathbb{N}$.

2.1.2 Preconditions and postconditions

In program verification, predicates describing valid inputs are *preconditions* and predicates the output must satisfy are *postconditions*. “For all inputs satisfying the precondition, the output satisfies the postcondition” is exactly a quantified predicate statement — which is what makes this chapter the foundation of formal verification.

2.2 Quantifiers

Definition 2.4 (Universal quantifier). Let $P(x)$ be a predicate with domain U . The *universal quantification* of $P(x)$, written $\forall x P(x)$, is the proposition “ $P(x)$ is true for every x in U ”. An element for which P is false is a *counterexample*.

Definition 2.5 (Existential quantifier). The *existential quantification* of $P(x)$, written $\exists x P(x)$, is the proposition “there is at least one x in U for which $P(x)$ is true”.

The domain must always be stated. Without a domain, $\forall x P(x)$ and $\exists x P(x)$ are not properly defined statements. This is not pedantry: the same predicate flips truth value as the domain changes.

$$\forall x (x^2 \geq x) \text{ is } \text{false} \text{ over } \mathbb{R} \text{ (take } x = 0.2\text{), but } \text{true} \text{ over } \mathbb{Z}.$$

Similarly $\exists x (x^2 > 0)$ behaves differently on different domains, and over an empty domain it is false for every predicate.

Statement	True when	False when
$\forall x P(x)$	$P(x)$ is true for every x	there is an x with $P(x)$ false
$\exists x P(x)$	there is an x with $P(x)$ true	$P(x)$ is false for every x

Table 2.1: The meanings of the two quantifiers.

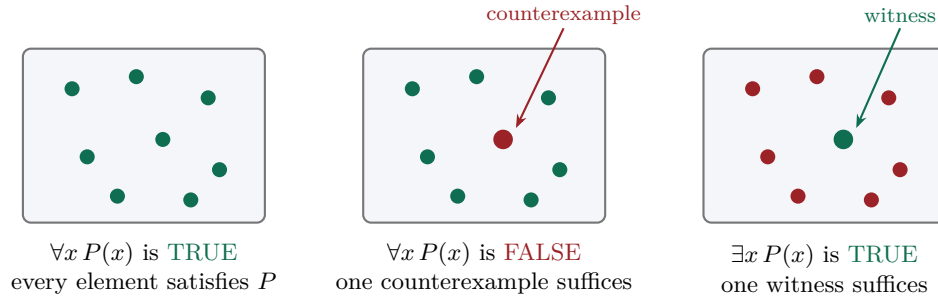


Figure 2.1: To *refute* a $\forall$ you exhibit one counterexample; to *establish* an $\exists$ you exhibit one witness. Both are cheap. Establishing a $\forall$ or refuting an $\exists$ requires an argument about all elements — both are expensive.

2.2.1 English renderings

$\forall x P(x)$	$\exists x P(x)$
for all x , $P(x)$	there exists an x such that $P(x)$
for every x , $P(x)$	there is at least one x with $P(x)$
for each x , $P(x)$	for some x , $P(x)$
given any x , $P(x)$	$P(x)$ holds for some x
for arbitrary x , $P(x)$	

Empty domains. If the domain is empty then $\forall x P(x)$ is *true* (there is no counterexample) and $\exists x P(x)$ is *false* (there is no witness) for every predicate P . Unless stated otherwise, domains in this course are assumed non-empty.

2.2.2 Precedence of quantifiers

Quantifiers bind **more tightly** than every logical connective. Therefore

$$\forall x P(x) \vee Q(x) \quad \text{means} \quad (\forall x P(x)) \vee Q(x), \quad \text{not} \quad \forall x (P(x) \vee Q(x)).$$

Always parenthesise when you mean the second. Note also that the first form has a *free* occurrence of x in $Q(x)$ and so is not even a proposition.

2.3 Binding, scope and free variables

Definition 2.6 (Bound and free). An occurrence of a variable is *bound* if it lies within the scope of a quantifier over that variable; otherwise it is *free*. The *scope* of a quantifier is the sub-formula to which it applies. A formula with no free variables is a proposition; a formula with free variables is not.

Example 2.2 (reading off the scopes). In $\exists x (x + y = 1)$, the variable x is bound by $\exists x$ but y is free. This is *not* a proposition. By contrast, $\exists x (x + 10 = 1)$ and $\forall y \exists x (x + y = 1)$ are propositions (both true over $\mathbb{R}$).

$$\forall x \left(\underbrace{\forall y (xy = x)}_{\text{scope of } y} \rightarrow x = 0 \right)$$

$\underbrace{\hspace{10em}}_{\text{scope of } x}$

Figure 2.2: Nested scopes in $\forall x (\forall y (xy = x) \rightarrow x = 0)$. The inner quantifier binds only within its own parentheses; x remains bound by the outer quantifier throughout.

Bracketing changes meaning. Compare

$$\underbrace{\forall x \forall y (xy = x \rightarrow x = 0)}_{\text{false over } \mathbb{N}} \quad \text{vs.} \quad \underbrace{\forall x (\forall y (xy = x) \rightarrow x = 0)}_{\text{true over } \mathbb{N}}.$$

In the first, y 's scope is only the equation; in the second the whole conditional. Take $x = 1, y = 1$ in the first: $1 \cdot 1 = 1$ is true but $1 = 0$ is false, so the conditional fails — a counterexample.

2.4 Negating quantified statements

Theorem 2.7 (De Morgan's laws for quantifiers).

$$\neg(\forall x P(x)) \equiv \exists x \neg P(x), \quad \neg(\exists x P(x)) \equiv \forall x \neg P(x).$$

In words: “*not all*” means “*some not*”, and “*none*” means “*all not*”. The mechanical rule is

Push the $\neg$ inwards: each quantifier it passes flips.

$\forall \longleftrightarrow \exists$, and the $\neg$ finally lands on the predicate.

Example 2.3. “Everyone likes football.” Its negation is “not everyone likes football”, i.e. “there exists someone who does not like football”: $\neg \forall x P(x) \equiv \exists x \neg P(x)$.
 “There is a plant that can fly.” Its negation is “no plant can fly”, i.e. “every plant cannot fly”: $\neg \exists x P(x) \equiv \forall x \neg P(x)$.

Example 2.4 (negation with a conditional inside). Let $Car(x)$ = “ x is a car” and $Carb(x)$ = “ x has a carburettor”. “Not all cars have carburettors” is $\neg\forall x (Car(x) \rightarrow Carb(x))$. Rewrite it with the negation pushed all the way in:

$$\begin{aligned}\neg\forall x (Car(x) \rightarrow Carb(x)) &\equiv \exists x \neg(Car(x) \rightarrow Carb(x)) \\ &\equiv \exists x \neg(\neg Car(x) \vee Carb(x)) \\ &\equiv \exists x (Car(x) \wedge \neg Carb(x)).\end{aligned}$$

Read back: “there is a car without a carburettor” — which is obviously the right negation. Notice that $\neg(A \rightarrow B) \equiv A \wedge \neg B$ did all the work.

The single commonest error in this chapter. The negation of “all cars have carburettors” is *not* “all cars lack carburettors”. Do not flip the predicate while leaving the quantifier alone. Flip *both*, and remember that the negation of a $\forall$ -with- $\rightarrow$ produces an $\exists$ -with- $\wedge$.

2.5 Equivalences involving quantifiers

Theorem 2.8 (Distribution that works). *For predicates P, Q over the same domain,*

$$\forall x (P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x), \quad \exists x (P(x) \vee Q(x)) \equiv \exists x P(x) \vee \exists x Q(x).$$

Proof. Let U be the common domain.

($\Rightarrow$) Suppose $\forall x (P(x) \wedge Q(x))$ is true. Then $P(a) \wedge Q(a)$ is true for every $a \in U$; hence $P(a)$ is true for every $a \in U$ and $Q(a)$ is true for every $a \in U$; that is, $\forall x P(x) \wedge \forall x Q(x)$ is true.

($\Leftarrow$) Suppose $\forall x P(x) \wedge \forall x Q(x)$ is true. Then $\forall x P(x)$ is true and $\forall x Q(x)$ is true, so for each $a \in U$ both $P(a)$ and $Q(a)$ are true, hence $P(a) \wedge Q(a)$ is true for all $a \in U$, i.e. $\forall x (P(x) \wedge Q(x))$ is true.

The second equivalence is the dual and is proved the same way, replacing “for all a ” by “for some a ” throughout. ■

Distribution that fails. In general

$$\forall x (P(x) \vee Q(x)) \not\equiv \forall x P(x) \vee \forall x Q(x), \quad \exists x (P(x) \wedge Q(x)) \not\equiv \exists x P(x) \wedge \exists x Q(x).$$

Counterexample 1. Over $\mathbb{Z}$, let $P(x)$ = “ x is even” and $Q(x)$ = “ x is odd”. Then $\forall x (P(x) \vee Q(x))$ is **true** (every integer is even or odd), but $\forall x P(x) \vee \forall x Q(x)$ is **false** (neither disjunct holds).

Counterexample 2. Over $\mathbb{Z}^+$, let $P(x)$ = “ x is prime” and $Q(x)$ = “ x is composite”. Then $\exists x P(x) \wedge \exists x Q(x)$ is **true** (2 and 4 respectively), but $\exists x (P(x) \wedge Q(x))$ is **false** — no integer is both.

Mnemonic. $\forall$ distributes over $\wedge$; $\exists$ distributes over $\vee$. The mismatched pairs do not.

Similarly $\forall x (P(x) \rightarrow Q(x))$ and $\forall x P(x) \rightarrow \forall x Q(x)$ are *not* equivalent: the second is implied by the first but not conversely. Over $\mathbb{Z}$ with $P(x)$ = “ x is even” and $Q(x)$ = “ x is odd”, the second is vacuously true (its hypothesis $\forall x P(x)$ is false) while the first is false (take $x = 2$).

2.6 Translating between English and predicate logic

Example 2.5 (a systematic translation exercise). Let the universe be $\mathbb{Z}$ and let $N(x)$ = “ x is a non-negative integer”, $E(x)$ = “ x is even”, $O(x)$ = “ x is odd”, $P(x)$ = “ x is prime”.

English	Formula
There exists an even integer.	$\exists x E(x)$
All prime integers are non-negative.	$\forall x (P(x) \rightarrow N(x))$
Every integer is even or odd.	$\forall x (E(x) \vee O(x))$
Not all integers are odd.	$\neg[\forall x O(x)]$
Not all primes are odd.	$\neg[\forall x (P(x) \rightarrow O(x))]$
If an integer is not odd, then it is even.	$\forall x (\neg O(x) \rightarrow E(x))$
The only even prime is 2.	$\forall x (P(x) \wedge E(x) \rightarrow x = 2)$
There exists an odd prime.	$\exists x (P(x) \wedge O(x))$

The two default patterns. Almost every “all A s are B s” and “some A is a B ” translates using one of these two shapes, and they use *different* connectives:

“All A s are B s” $\rightsquigarrow \forall x (A(x) \rightarrow B(x))$, “Some A is a B ” $\rightsquigarrow \exists x (A(x) \wedge B(x))$.

Using $\wedge$ with $\forall$ would assert that *everything* is an A ; using $\rightarrow$ with $\exists$ is trivially satisfied by any non- A . Both are classic errors.

2.7 Nested quantifiers

Example 2.6 (familiar algebra, formally). With domain $\mathbb{R}$ throughout:

$\forall x \forall y (x + y = y + x)$	commutativity of addition
$\forall x \forall y \forall z ((x + y) + z = x + (y + z))$	associativity of addition
$\forall x \exists y (x + y = 0)$	existence of additive inverses
$\exists x \forall y (x + y = y)$	existence of an additive identity
$\forall x (x \neq 0 \rightarrow \exists y (xy = 1))$	multiplicative inverses
$\forall x \forall y \forall z (x(y + z) = xy + xz)$	distributivity

Note the shape of the identity axiom: $\exists$ comes *first*, because a single number (0) works for every y . The inverse axiom has $\forall$ first, because the inverse depends on x .

2.7.1 Order of quantifiers matters

$\exists x \forall y$ and $\forall y \exists x$ mean **different** things, and confusing them is the deepest error in this chapter.

Example 2.7 (antivirus programs). Let $K(P, V)$ = “antivirus program P kills computer virus V ”.

$\exists P \forall V K(P, V)$ There is *one* antivirus program that kills *every* virus.

$\forall V \exists P K(P, V)$ For every virus there is *some* program that kills it.

The first is a far stronger claim: it demands a single universal program. The second allows a different program for each virus.

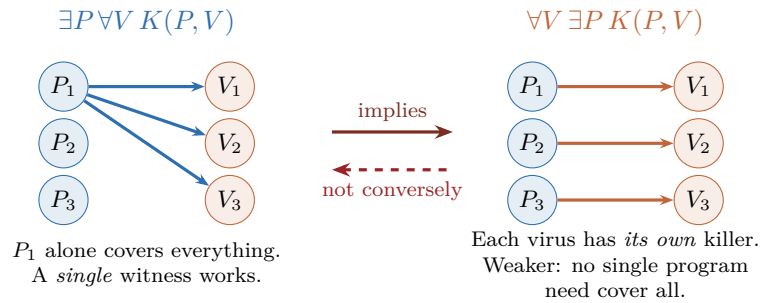


Figure 2.3: $\exists P \forall V$ implies $\forall V \exists P$, never the reverse. The left situation is a special case of the right one.

Theorem 2.9 (Quantifier-swap implication). $\exists x \forall y P(x, y) \rightarrow \forall y \exists x P(x, y)$ is valid. The converse is not.

Reordering rules.

- Two adjacent *like* quantifiers may always be swapped: $\forall x \forall y \equiv \forall y \forall x$ and $\exists x \exists y \equiv \exists y \exists x$.
- Two adjacent *unlike* quantifiers may **not** be swapped.

2.7.2 Translating nested quantifiers into English

Example 2.8. Let $C(x)$ = “ x has a computer” and $F(x, y)$ = “ x and y are friends”, both domains being the students in this class. Translate

$$\forall x (C(x) \vee \exists y (C(y) \wedge F(x, y))).$$

Solution. Literally: “For every student x in this class, either x has a computer, or there is a student y such that y has a computer and x and y are friends.”

Idiomatically: “Every student in this class either has a computer or has a friend who has a computer.”

2.7.3 Negating nested quantifiers

Apply the de Morgan rule repeatedly, flipping each quantifier as the negation passes it.

Example 2.9. Express the negation of $\forall x \exists y (xy = 1)$ with no negation preceding a quantifier (domain $\mathbb{R}$).

Solution.

$$\begin{aligned}\neg[\forall x \exists y (xy = 1)] &\equiv \exists x \neg[\exists y (xy = 1)] \\ &\equiv \exists x \forall y [\neg(xy = 1)] \\ &\equiv \exists x \forall y (xy \neq 1).\end{aligned}$$

(The negation is in fact *true*: take $x = 0$.)

Example 2.10 (three nested quantifiers). Negate $\forall x \exists y \forall z (P(x, y) \rightarrow Q(y, z))$.

Solution.

$$\begin{aligned}\neg\forall x \exists y \forall z (P(x, y) \rightarrow Q(y, z)) \\ \equiv \exists x \forall y \exists z \neg(P(x, y) \rightarrow Q(y, z)) \\ \equiv \exists x \forall y \exists z (P(x, y) \wedge \neg Q(y, z)).\end{aligned}$$

All three quantifiers flipped; the conditional became a conjunction.

2.8 Unique existence

Definition 2.10 (Unique existential quantifier). $\exists! x P(x)$ asserts that exactly one element of the domain satisfies P . It abbreviates

$$\exists! x P(x) \equiv \exists x (P(x) \wedge \forall y (y \neq x \rightarrow \neg P(y))) \equiv \exists x (P(x) \wedge \forall y (P(y) \rightarrow y = x)).$$

The two-part shape of the definition dictates the two-part shape of a uniqueness proof (Chapter 4): first *existence*, then *uniqueness*.

2.9 Rewriting one quantifier as the other

Because $\neg\neg P \equiv P$, any statement can be written with only $\forall$ or only $\exists$.

Example 2.11 (each statement two ways).

- (a) **Not all cars have carburettors.** With $\forall$ only: $\neg\forall x (Car(x) \rightarrow Carb(x))$. With $\exists$ only: $\exists x (Car(x) \wedge \neg Carb(x))$.
- (b) **No dogs are intelligent.** With $\forall$: $\forall x (D(x) \rightarrow \neg I(x))$. With $\exists$: $\neg\exists x (D(x) \wedge I(x))$.
- (c) **Some numbers are not real.** With $\exists$: $\exists x (N(x) \wedge \neg R(x))$. With $\forall$: $\neg\forall x (N(x) \rightarrow R(x))$.

2.10 Quantifiers and truth sets: the link to set theory

Theorem 2.11. Let P be a predicate over a domain U with truth set $T = \{x \in U \mid P(x)\}$. Then

$$\forall x P(x) \text{ is true} \iff T = U, \quad \exists x P(x) \text{ is true} \iff T \neq \emptyset.$$

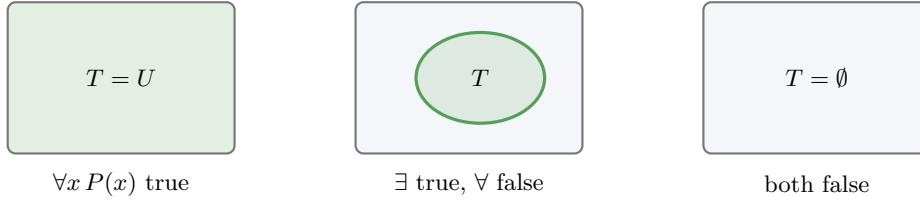


Figure 2.4: Quantifiers read as statements about the size of the truth set. This is the picture to keep in mind when Chapter 5 defines $A \subseteq B \iff \forall x (x \in A \rightarrow x \in B)$.

2.11 Chapter summary

- A predicate becomes a proposition only when all its variables are instantiated or quantified. A domain of discourse must always be specified.
- The truth set $\{x \in U \mid P(x)\}$ turns a predicate into a subset of the domain; $\forall$ says the truth set is everything, $\exists$ says it is non-empty.
- Quantifiers bind more tightly than any connective.
- $\neg \forall x P(x) \equiv \exists x \neg P(x)$ and $\neg \exists x P(x) \equiv \forall x \neg P(x)$: push the negation in and flip every quantifier it passes.
- $\forall$ distributes over $\wedge$; $\exists$ distributes over $\vee$. The other two directions are *false* — learn the even/odd and prime/composite counterexamples.
- “All A s are B s” is $\forall x (A(x) \rightarrow B(x))$; “some A is a B ” is $\exists x (A(x) \wedge B(x))$.
- Like quantifiers commute; unlike quantifiers do not. $\exists x \forall y \rightarrow \forall y \exists x$, never the converse.
- $\exists! x P(x)$ unpacks into existence plus uniqueness — and so does its proof.

CHAPTER 3

Arguments and Rules of Inference

What this chapter is for. Chapters 1 and 2 gave us a language. This chapter gives us the *rules of the game*: which steps are legitimate when moving from what you are given to what you want. A formal proof is nothing more than a finite list of such steps, each one justified by a named rule. Everything in Chapter 4 and beyond is an informal, compressed version of what happens here.

3.1 Arguments and validity

Definition 3.1 (Argument). An *argument* in propositional logic is a finite sequence of propositions. All but the last are the *premises*; the last is the *conclusion*.

Definition 3.2 (Valid argument). An argument is *valid* if the truth of all its premises forces the conclusion to be true. Equivalently, with premises $P_1, \dots, P_n$ and conclusion C , the argument is valid iff

$$(P_1 \wedge P_2 \wedge \dots \wedge P_n) \rightarrow C$$

is a tautology.

An *argument form* is the same thing with propositional variables in place of specific propositions. An argument form is valid if the conclusion is true whenever all premises are true, no matter which propositions are substituted.

Validity is not truth. A valid argument can have a false conclusion — if one of its premises is false. Validity is a property of the *form*, not of the content. Conversely an argument with a true conclusion may be invalid.

Arguments are conventionally displayed vertically, with a rule under the premises and $\therefore$ before the conclusion:

$$\frac{p \rightarrow q \quad p}{\therefore q}$$

Example 3.1 (a valid argument). “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.” With p = “you have a current password”, q = “you can log onto the network”, the form is $p \rightarrow q$, $p \therefore q$. Look at the truth table of $p \rightarrow q$: in the only row where both p and $p \rightarrow q$ are true (row **TT**), q is true as well. The argument is valid.

3.2 Rules of inference for propositional logic

Each rule below is a valid argument form; a formal proof strings them together.

Rule	Name	Rule	Name
$\frac{p \quad p \rightarrow q}{\therefore q}$	Modus ponens	$\frac{p}{\therefore p \vee q}$	Addition
$\frac{\neg q \quad p \rightarrow q}{\therefore \neg p}$	Modus tollens	$\frac{p \wedge q}{\therefore p}$	Simplification
$\frac{p \rightarrow q \quad q \rightarrow r}{\therefore p \rightarrow r}$	Hypothetical syllogism	$\frac{p \quad q}{\therefore p \wedge q}$	Conjunction
$\frac{p \vee q \quad \neg p}{\therefore q}$	Disjunctive syllogism	$\frac{p \vee q}{\therefore p \vee q}$	Resolution

Table 3.1: The eight rules of inference for propositional logic.

How to remember them.

- *Modus ponens* (“the way that affirms”): affirm the antecedent, conclude the consequent.
- *Modus tollens* (“the way that denies”): deny the consequent, conclude the denial of the antecedent. It is modus ponens applied to the contrapositive.
- *Hypothetical syllogism* is transitivity of $\rightarrow$.
- *Disjunctive syllogism* is elimination of a disjunct.
- *Addition* weakens; *simplification* drops a conjunct; *conjunction* joins.
- *Resolution* generalises both modus ponens and disjunctive syllogism, and is the engine of automated theorem proving.

3.2.1 Verifying resolution

Example 3.2 (resolution is valid). Show that $p \vee q, \neg p \vee r \therefore q \vee r$ is valid.

Solution.

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

Both premises are true only in rows 1, 3, 5, 6 — and in every one of those rows the conclusion $q \vee r$ is true. The argument is valid. (Rows 4 and 8, where the conclusion fails, both have a false premise.)

3.3 Building formal proofs

Format. Number every line. In one column write the proposition; in the other write its justification — either “Premise”, or a rule name together with the line numbers it was applied to, or an equivalence law.

Example 3.3 (chaining conditionals). Show that the premises

- “If you send me an e-mail message, then I will finish writing the program,”
- “If you do not send me an e-mail message, then I will go to sleep early,”
- “If I go to sleep early, then I will wake up feeling refreshed”

lead to “If I do not finish writing the program, then I will wake up feeling refreshed.”

Solution. Let p = “you send me an e-mail message”, q = “I will finish writing the program”, r = “I will go to sleep early”, s = “I will wake up feeling refreshed”. The argument form is

$$p \rightarrow q, \quad \neg p \rightarrow r, \quad r \rightarrow s \quad \therefore \quad \neg q \rightarrow s.$$

Step	Proposition	Reason
1	$p \rightarrow q$	Premise
2	$\neg q \rightarrow \neg p$	Contrapositive of (1)
3	$\neg p \rightarrow r$	Premise
4	$\neg q \rightarrow r$	Hypothetical syllogism, (2) and (3)
5	$r \rightarrow s$	Premise
6	$\neg q \rightarrow s$	Hypothetical syllogism, (4) and (5)

Example 3.4 (mixing several rules). Show that this argument is valid: “If today is a Friday, then I have a test in CS or a test in Mathematics. If my Mathematics lecturer is sick, then I will not have a test in Mathematics. Today is Friday and my Mathematics lecturer is sick. Therefore, I have a test in CS.”

Solution. Let p = “today is Friday”, q = “I have a test in CS”, r = “I have a test in Mathematics”, s = “my Mathematics lecturer is sick”. The form is

$$p \rightarrow (q \vee r), \quad s \rightarrow \neg r, \quad p \wedge s \quad \therefore \quad q.$$

Step	Proposition	Reason
1	$p \wedge s$	Premise
2	s	Simplification from (1)
3	p	Simplification from (1)
4	$s \rightarrow \neg r$	Premise
5	$\neg r$	Modus ponens, (2) and (4)
6	$p \rightarrow (q \vee r)$	Premise
7	$q \vee r$	Modus ponens, (3) and (6)
8	q	Disjunctive syllogism, (5) and (7)

Hence the argument is valid.

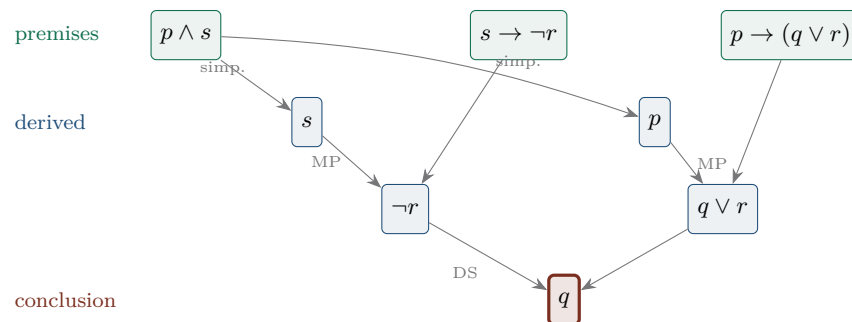


Figure 3.1: The same proof drawn as a derivation graph. Premises at the top, the conclusion at the bottom; each arrow is one application of a rule of inference.

3.4 Fallacies

Two invalid forms look deceptively like modus ponens and modus tollens. Learn to recognise them.

3.4.1 Fallacy of affirming the consequent

$$\frac{p \rightarrow q \quad q}{\therefore p} \quad \text{INVALID}$$

Example 3.5. “If you do every problem in this book, then you will learn discrete mathematics. You learned discrete mathematics. Therefore you did every problem in this book.”

Solution.

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

In the highlighted row both premises $p \rightarrow q$ and q are true while the conclusion p is false. Invalid. (Concretely: you might have learnt discrete mathematics some other way.)

3.4.2 Fallacy of denying the antecedent

$$\frac{p \rightarrow q \quad \neg p}{\therefore \neg q} \quad \text{INVALID}$$

Example 3.6.

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

Again the highlighted row has true premises and a false conclusion.

	Valid	Fallacy
Work forwards	modus ponens: $p \rightarrow q, p \therefore q$	affirming the consequent: $p \rightarrow q, q \therefore p$
Work backwards	modus tollens: $p \rightarrow q, \neg q \therefore \neg p$	denying the antecedent: $p \rightarrow q, \neg p \therefore \neg q$
The valid rules use the <i>antecedent positively</i> or the <i>consequent negatively</i> . Both fallacies do the opposite.		

3.5 Rules of inference for quantified statements

Rule	Name
$\frac{\forall x P(x)}{\therefore P(c) \text{ for any particular } c}$	Universal instantiation (UI)
$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$	Universal generalisation (UG)
$\frac{\exists x P(x)}{\therefore P(c) \text{ for some (new) } c}$	Existential instantiation (EI)
$\frac{P(c) \text{ for some particular } c}{\therefore \exists x P(x)}$	Existential generalisation (EG)

Table 3.2: The four quantifier rules.

Two side conditions that mark the difference between a correct and an incorrect proof.

1. **UG requires c to be arbitrary.** You may conclude $\forall x P(x)$ from $P(c)$ only if nothing whatever was assumed about c . If c arrived via existential instantiation, it is *not* arbitrary and UG is illegal.
2. **EI must introduce a fresh name, used consistently.** From $\exists x P(x)$ you may write $P(a)$ for a *new* symbol a . If you later instantiate a second existential statement, you must use a *different* symbol — the two witnesses need not be the same object. Conversely, once you have named a witness a , every subsequent step about that witness must use the same a .

Good practice: do all existential instantiations *first*, then universal instantiations at the names you have introduced.

Example 3.7 (a full quantified proof). Show that the premises “A student in this class has not read the book” and “Everyone in this class passed the first exam” imply “Someone who passed the exam has not read the book.”

Solution. Let $C(x)$ = “ x is in this class”, $B(x)$ = “ x has read the book”, $P(x)$ = “ x passed the first exam”. The form is

$$\exists x (C(x) \wedge \neg B(x)), \quad \forall x (C(x) \rightarrow P(x)) \quad \therefore \quad \exists x (P(x) \wedge \neg B(x)).$$

Step	Proposition	Reason
1	$\exists x (C(x) \wedge \neg B(x))$	Premise
2	$C(a) \wedge \neg B(a)$	Existential instantiation, (1)
3	$C(a)$	Simplification, (2)
4	$\forall x (C(x) \rightarrow P(x))$	Premise
5	$C(a) \rightarrow P(a)$	Universal instantiation, (4)
6	$P(a)$	Modus ponens, (3) and (5)
7	$\neg B(a)$	Simplification, (2)
8	$P(a) \wedge \neg B(a)$	Conjunction, (6) and (7)
9	$\exists x (P(x) \wedge \neg B(x))$	Existential generalisation, (8)

Notice the pattern: EI first (step 2, introducing the witness a), then UI *at that same* a (step 5), propositional work in the middle, EG at the end.

Example 3.8 (ending with universal generalisation). Premises: $\forall x (B(x) \rightarrow I(x))$, $\forall x (I(x) \rightarrow D(x))$, $\neg \exists x (M(x) \wedge D(x))$. Conclusion: $\forall x (B(x) \rightarrow \neg M(x))$.

Solution. Let a be an arbitrary element of the universe.

Step	Proposition	Reason
1	$\neg \exists x (M(x) \wedge D(x))$	Premise
2	$\forall x \neg (M(x) \wedge D(x))$	Negation of quantifier, (1)
3	$\forall x (\neg M(x) \vee \neg D(x))$	De Morgan, (2)
4	$\forall x (D(x) \rightarrow \neg M(x))$	$\rightarrow$ elimination, (3)
5	$B(a) \rightarrow I(a)$	UI of premise 1
6	$I(a) \rightarrow D(a)$	UI of premise 2
7	$D(a) \rightarrow \neg M(a)$	UI of (4)
8	$B(a) \rightarrow D(a)$	Hypothetical syllogism, (5) and (6)
9	$B(a) \rightarrow \neg M(a)$	Hypothetical syllogism, (8) and (7)
10	$\forall x (B(x) \rightarrow \neg M(x))$	Universal generalisation, (9)

Step 10 is legitimate precisely because a was chosen arbitrarily at the start and nothing was ever assumed about it.

Example 3.9 (a longer mixed proof). “Anyone who performs well is either intelligent or a good actor. If someone is intelligent, then he/she can count from 1 to 10. Gary performs well. Gary can only count from 1 to 3. Therefore, not everyone is both intelligent and a good actor.”

Solution. Let $P(x)$ = “ x performs well”, $I(x)$ = “ x is intelligent”, $A(x)$ = “ x is a good actor”, $C(x)$ = “ x can count from 1 to 10”, and write G for Gary. The form is

$$\forall x (P(x) \rightarrow (I(x) \vee A(x))), \quad \forall x (I(x) \rightarrow C(x)), \quad P(G), \quad \neg C(G) \quad \therefore \quad \neg \forall x (I(x) \wedge A(x)).$$

Step	Proposition	Reason
1	$\forall x (P(x) \rightarrow (I(x) \vee A(x)))$	Premise
2	$P(G) \rightarrow (I(G) \vee A(G))$	Universal instantiation, (1)
3	$P(G)$	Premise
4	$I(G) \vee A(G)$	Modus ponens, (2) and (3)
5	$\forall x (I(x) \rightarrow C(x))$	Premise
6	$I(G) \rightarrow C(G)$	Universal instantiation, (5)
7	$\neg C(G)$	Premise
8	$\neg I(G)$	Modus tollens, (6) and (7)
9	$\neg I(G) \vee \neg A(G)$	Addition, (8)
10	$\neg(I(G) \wedge A(G))$	De Morgan, (9)
11	$\exists x \neg(I(x) \wedge A(x))$	Existential generalisation, (10)
12	$\neg \forall x (I(x) \wedge A(x))$	Negation of quantifier, (11)

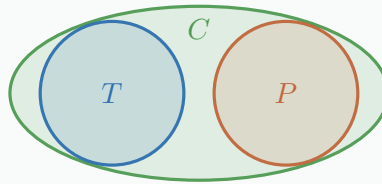
3.6 Showing an argument is *invalid*: countermodels

To show an argument *is* valid you give a proof. To show it is *not* valid you exhibit a single interpretation — a *countermodel* — in which every premise is true but the conclusion is false. For quantified arguments a Venn diagram is usually the fastest way to construct one.

Example 3.10 (the “some–some” fallacy). Test: “Some trigonometric functions are continuous. Some continuous functions are periodic. Therefore some trigonometric functions are periodic.”

Solution. With T, C, P the obvious predicates the form is

$$\exists x (T(x) \wedge C(x)), \quad \exists x (C(x) \wedge P(x)) \quad \therefore \quad \exists x (T(x) \wedge P(x)).$$



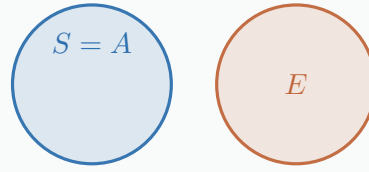
$$T \cap C \neq \emptyset \quad \checkmark \quad C \cap P \neq \emptyset \quad \checkmark \quad \text{but } T \cap P = \emptyset$$

In this interpretation both premises hold and the conclusion fails. The argument is **invalid**.

Example 3.11 (two negative premises). Test: “Some scientists are not engineers. Some astronauts are not engineers. Hence some scientists are not astronauts.”

Solution. Form: $\exists x (S(x) \wedge \neg E(x)), \exists x (A(x) \wedge \neg E(x)) \therefore \exists x (S(x) \wedge \neg A(x))$.

Countermodel: let $S = A$ be one and the same set, disjoint from E .

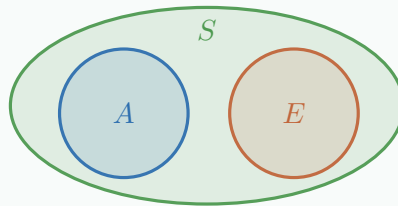


Both premises true (nothing in $S = A$ is in E),
but no scientist is a non-astronaut: conclusion false.

Invalid.

Example 3.12 (all + some-not). Test: “All astronauts are scientists. Some astronauts are not engineers. Hence some engineers are not scientists.”

Solution. Form: $\forall x (A(x) \rightarrow S(x)), \exists x (A(x) \wedge \neg E(x)) \therefore \exists x (E(x) \wedge \neg S(x))$.



Put E inside S . Both premises hold,
but there is no engineer outside S .

Invalid.

Building a countermodel systematically. Draw the circles so that (i) every universal premise $\forall x(A \rightarrow B)$ has A inside B , (ii) every existential premise $\exists x(A \wedge B)$ has A and B overlapping with a dot in the overlap, and (iii) the region required by the conclusion is empty. If you can draw such a picture, the argument is invalid, and the picture *is* your countermodel — you may also describe it as a finite domain, e.g. “let the universe be $\{1\}$ with $A(1), S(1), E(1)$ true and ...”.

3.7 Resolution

Resolution is a single rule of inference that is *refutation complete* for propositional logic: it needs only clauses (CNF), and it proves things by deriving a contradiction. It is the basis of PROLOG and of most automated reasoning systems.

Definition 3.3 (Literal, clause, resolvent). A *literal* is a variable or its negation. A *clause* is a disjunction of literals. Given clauses C_1 and C_2 , if C_1 contains a literal ℓ and C_2 contains the complementary literal $\neg\ell$, then deleting ℓ from C_1 and $\neg\ell$ from C_2 and taking the disjunction of what remains produces the *resolvent* of C_1 and C_2 .

Example 3.13. $C_1 = p \vee q \vee \neg s$ and $C_2 = \neg p \vee u$ resolve on p to give the resolvent $q \vee \neg s \vee u$.

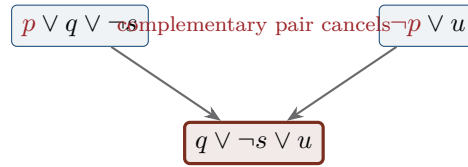


Figure 3.2: One resolution step. The complementary literals disappear; everything else survives.

Theorem 3.4. A resolvent C of clauses C_1 and C_2 is a logical consequence of C_1 and C_2 :

$$\begin{array}{l} C_1 = p \vee C'_1 \\ C_2 = \neg p \vee C'_2 \\ \hline \therefore C'_1 \vee C'_2 \end{array}$$

Proof. Suppose both premises are true. If p is true then $\neg p$ is false, so C'_2 must be true; if p is false then C'_1 must be true. Either way $C'_1 \vee C'_2$ holds. ■

Resolution subsumes the familiar rules.

$$\begin{array}{ccc} \text{Modus ponens: } \frac{p}{p \rightarrow q} \equiv \frac{p}{\neg p \vee q} & \text{Modus tollens: } \frac{\neg q}{\neg p \vee q} \\ \hline \therefore q & \hline \therefore \neg p \end{array}$$

Both are single resolution steps.

3.7.1 Refutation

Definition 3.5 (Deduction, refutation). Given a set S of clauses, a *deduction* of C from S is a finite sequence $C_1, C_2, \dots, C_k$ of clauses in which each C_i is either a member of S or a resolvent of two earlier clauses, with $C_k = C$. A deduction of the *empty clause* $\square$ from S is a *refutation* (or proof) of S : it shows S is unsatisfiable.

How to use resolution to prove an argument valid.

1. Convert every premise to CNF and list the clauses.
2. **Negate the conclusion**, convert it to CNF, and add those clauses too.
3. Resolve repeatedly. If you derive $\square$, the enlarged set is unsatisfiable — meaning the premises cannot hold with the conclusion false. The argument is valid.
4. If no further resolvents are possible and $\square$ has not appeared, the set is satisfiable and the argument is invalid; a satisfying assignment is a countermodel.

Example 3.14 (modus tollens by refutation). Prove $\neg q, p \rightarrow q \therefore \neg p$.

Solution. Clauses: $\neg q$; $\neg p \vee q$; and the negated conclusion p .

$$\begin{array}{l} \neg q \\ \neg p \vee q \\ \hline p \\ \therefore \square \end{array}$$

Resolving $\neg q$ with $\neg p \vee q$ gives $\neg p$; resolving $\neg p$ with p gives $\square$. Hence the argument is

valid.

Example 3.15 (the Friday-test argument again, by resolution). Premises $p \rightarrow (q \vee r)$, $s \rightarrow \neg r$, $p \wedge s$; conclusion q .

Solution. In clausal form: $\neg p \vee q \vee r$; $\neg s \vee \neg r$; p ; s .

Step	Clause	Reason
1	$\neg p \vee q \vee r$	Premise
2	p	Premise
3	$q \vee r$	Resolution, (1) and (2)
4	$\neg s \vee \neg r$	Premise
5	$\neg s \vee q$	Resolution, (3) and (4)
6	s	Premise
7	q	Resolution, (5) and (6)

The conclusion is derived directly (no refutation needed here). Compare with the eight-line proof using four different rules earlier: resolution used one rule throughout.

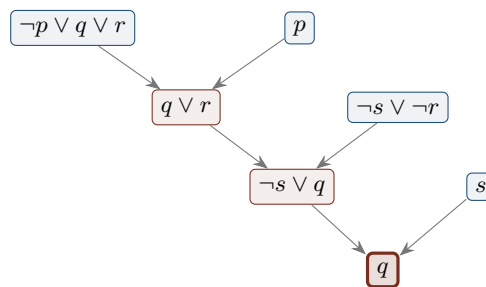


Figure 3.3: The resolution derivation as a tree. Leaves are premises, internal nodes are resolvents, the root is the conclusion.

Applications. Resolution is the inference engine of the logic programming language PROLOG, and is used throughout artificial intelligence for automated reasoning, planning and verification. Its appeal is that it needs *one* rule and a normal form, rather than a catalogue of eight rules plus judgement about which to apply.

3.8 Chapter summary

- An argument is valid iff (conjunction of premises) $\rightarrow$ (conclusion) is a tautology. Validity concerns form, not truth.
- Eight propositional rules: modus ponens, modus tollens, hypothetical syllogism, disjunctive syllogism, addition, simplification, conjunction, resolution.
- Two fallacies to avoid: affirming the consequent ($p \rightarrow q$, $q \therefore p$) and denying the antecedent ($p \rightarrow q$, $\neg p \therefore \neg q$).

- Four quantifier rules: UI, UG, EI, EG. UG needs an *arbitrary* constant; EI needs a *fresh* one, used consistently. Do EI before UI.
- To prove invalidity, build a countermodel — a Venn diagram or small finite domain making the premises true and the conclusion false.
- Resolution: put everything in CNF, negate the conclusion, resolve to $\square$. One rule, mechanically applicable, and the basis of PROLOG.

CHAPTER 4

Introduction to Proofs

What this chapter is for. A proof is a valid argument (Chapter 3) that establishes a mathematical statement. This chapter catalogues the standard *strategies* — direct, contrapositive, contradiction, cases, existence, uniqueness — and, more importantly, tells you *which to reach for* given the shape of the statement. Every proof in Chapters 5–8 is one of these.

4.1 Terminology

Definition 4.1. • A *theorem* is a statement that has been shown to be true.

- A *proof* is a valid argument establishing the truth of a statement, built from axioms (statements assumed true), definitions, previously proved theorems, and rules of inference.
- A *lemma* is a simple theorem used as an intermediate result in the proof of another theorem.
- A *corollary* is a proposition that follows directly from a theorem already proved.
- A *conjecture* is a statement whose truth value is unknown. Once proved it becomes a theorem.
- An instance of incorrect reasoning is a *fallacy*.

4.1.1 Formal versus informal proofs

A fully formal proof lists every rule of inference used, as in Chapter 3. Such proofs are extremely long and are what machines check. Proofs written for human readers are *informal*:

- more than one rule of inference may be used in a single step;
- routine steps may be skipped;
- the axioms assumed and the rules used are not stated explicitly.

Informal does not mean vague. An informal proof must still be *reconstructible* into a formal one by a competent reader. Skipping a step is fine; skipping the *idea* is not.

4.1.2 Practical applications

Proof is not an academic ritual. It is used to verify that computer programs are correct, to establish that operating systems are secure, to make inferences in artificial intelligence, and to show that system specifications are consistent (Chapter 1).

4.2 Reading the statement of a theorem

Most theorems are conditional statements or quantified conditional statements, even when they do not look like it.

Example 4.1 (unpacking an informal statement). “The sum of two odd integers is even.” Formally:

$$\forall m, n \in \mathbb{Z} \ (m \text{ and } n \text{ are odd} \rightarrow m + n \text{ is even}),$$

or with $O(n) = “n \text{ is odd}”$,

$$\forall m, n \in \mathbb{Z} \ (O(m) \wedge O(n) \rightarrow \neg O(m + n)).$$

The shape of the statement dictates the shape of the proof.

Statement shape	How the proof starts
$\forall x P(x)$	“Let x be arbitrary. ...”
$\exists x P(x)$	“Take $x = \dots$ ” (constructive) or an indirect argument
$p \rightarrow q$	“Suppose p therefore q .”
$p \leftrightarrow q$	Two proofs: $p \rightarrow q$ and $q \rightarrow p$
$\exists! x P(x)$	Two parts: existence, then uniqueness
$p_1 \vee \dots \vee p_n \rightarrow q$	One case per p_i

4.3 Definitions you need

Every proof about parity or rationality below turns on one of these.

Definition 4.2. • An integer n is *even* if there exists $k \in \mathbb{Z}$ with $n = 2k$.

- An integer n is *odd* if there exists $k \in \mathbb{Z}$ with $n = 2k + 1$.
- A real number r is *rational* if there exist $a \in \mathbb{Z}$, $b \in \mathbb{Z}^+$ with $r = a/b$; otherwise it is *irrational*.

The rhythm of an elementary number proof. *Unfold* the definition of the hypothesis into an equation with a witness k ; do *algebra*; *re-fold* the result into the definition of the conclusion by exhibiting a new witness k' . Three moves, every time.

4.4 The proof methods

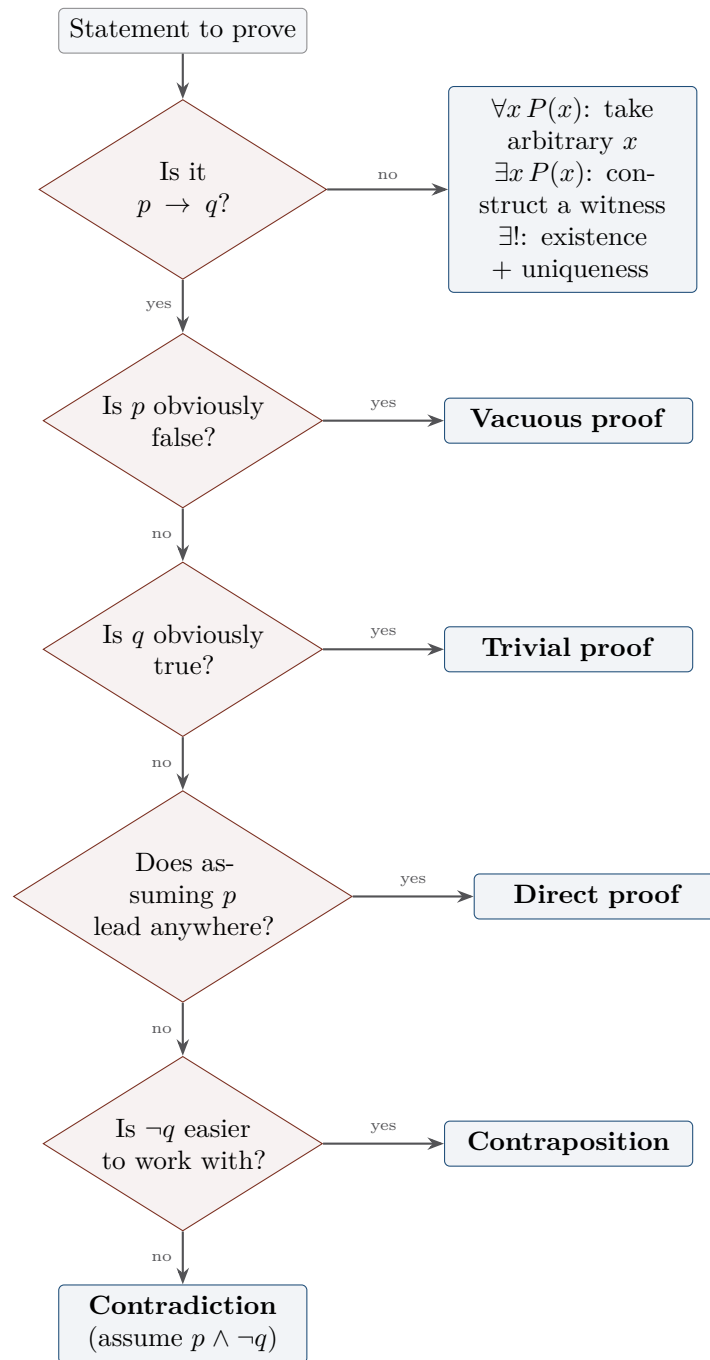


Figure 4.1: A decision tree for choosing a proof strategy. In practice you try direct first; if the algebra stalls, look at the contrapositive; if that also stalls, assume the negation and hunt for a contradiction. If the hypothesis naturally splits, add proof by cases on top of whichever method you chose.

4.4.1 Vacuous proof

Definition 4.3. To prove $p \rightarrow q$ by a *vacuous proof*, show that p is false. Then $p \rightarrow q$ is true regardless of q .

Example 4.2. Prove $\forall x \in \mathbb{R} (x^2 < -1 \rightarrow x^2 + 1 < 0)$.

Solution. For every real x we have $x^2 \geq 0 > -1$, so the hypothesis $x^2 < -1$ is false for every x . Hence the conditional is true for every x , and the universally quantified statement holds.

4.4.2 Trivial proof

Definition 4.4. To prove $p \rightarrow q$ by a *trivial proof*, show that q is true. Then $p \rightarrow q$ is true regardless of p .

Example 4.3. Prove $\forall x \in \mathbb{R} (x \geq 0 \rightarrow x^2 + 2x + 1 \geq 0)$.

Solution. For every real x , $x^2 + 2x + 1 = (x + 1)^2 \geq 0$. The conclusion holds for all x , so the conditional is true whatever the hypothesis does.

4.4.3 Direct proof

Definition 4.5. In a *direct proof* of $p \rightarrow q$, assume p is true and use definitions, axioms, previously proved results and rules of inference to show that q must be true.

Example 4.4 (sum of two odd integers is even).

Solution. Let $m, n \in \mathbb{Z}$ be arbitrary and suppose both are odd.

By definition there exist $k_1, k_2 \in \mathbb{Z}$ with $n = 2k_1 + 1$ and $m = 2k_2 + 1$. Then

$$n + m = (2k_1 + 1) + (2k_2 + 1) = 2k_1 + 2k_2 + 2 = 2(k_1 + k_2 + 1) = 2k',$$

where $k' = k_1 + k_2 + 1 \in \mathbb{Z}$. So $n + m$ is even by definition.

Since m and n were arbitrary, the sum of any two odd integers is even.

Example 4.5 (sum of two rationals is rational).

Solution. Let p, q be arbitrary rational numbers. Then $p = \frac{a}{b}$ and $q = \frac{c}{d}$ for some $a, c \in \mathbb{Z}$ and $b, d \in \mathbb{Z}^+$. Hence

$$p + q = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

where $ad + bc \in \mathbb{Z}$ and $bd \in \mathbb{Z}^+$. So $p + q$ is rational.

Example 4.6 (if n is odd then n^2 is odd).

Solution. The statement is $\forall n \in \mathbb{Z} (O(n) \rightarrow O(n^2))$.

Let $n \in \mathbb{Z}$ be arbitrary and suppose n is odd, so $n = 2k + 1$ for some $k \in \mathbb{Z}$. Then

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2k_1 + 1,$$

where $k_1 = 2k^2 + 2k \in \mathbb{Z}$. Hence n^2 is odd.

4.4.4 Proof by contraposition

Definition 4.6. Since $p \rightarrow q \equiv \neg q \rightarrow \neg p$, a *proof by contraposition* of $p \rightarrow q$ assumes $\neg q$ and derives $\neg p$.

When to reach for it. When the conclusion is a negative or “hard-to-start-from” statement and its negation is a positive, constructive one. “ n^2 is odd $\rightarrow n$ is odd” is hopeless directly (what do you do with “ $n^2 = 2k + 1$?”), but its contrapositive “ n is even $\rightarrow n^2$ is even” is one line.

Example 4.7 (if n^2 is odd then n is odd).

Solution. The statement is $\forall n \in \mathbb{Z} (O(n^2) \rightarrow O(n))$, whose contrapositive is $\forall n \in \mathbb{Z} (\neg O(n) \rightarrow \neg O(n^2))$.

Let $n \in \mathbb{Z}$ be arbitrary and suppose n is even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2) = 2k_1,$$

where $k_1 = 2k^2 \in \mathbb{Z}$. Hence n^2 is even. This proves the contrapositive, and therefore the original statement.

Example 4.8 (a factor is at most the square root). Prove: if $n = ab$ where $a, b \in \mathbb{Z}^+$, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Solution. Contrapositive: if $\neg(a \leq \sqrt{n} \text{ or } b \leq \sqrt{n})$ then $n \neq ab$.

Suppose $\neg(a \leq \sqrt{n} \text{ or } b \leq \sqrt{n})$. By De Morgan, $a > \sqrt{n}$ and $b > \sqrt{n}$. Since both are positive,

$$ab > \sqrt{n} \cdot \sqrt{n} = n,$$

so $ab \neq n$. This establishes the contrapositive, hence the original statement.

Do not confuse proof by contraposition with proof by contradiction. In contraposition you assume *only* $\neg q$ and derive $\neg p$ — there is no contradiction anywhere, and the proof is direct in form. In contradiction you assume $p \wedge \neg q$ and derive an absurdity.

4.4.5 Proof by contradiction

Definition 4.7. To prove a statement p by *contradiction*, assume $\neg p$ and derive a contradiction $r \wedge \neg r$. Since $\neg p \rightarrow (r \wedge \neg r)$ is true while $r \wedge \neg r$ is false, $\neg p$ must be false, so p is true.

To prove $p \rightarrow q$ by contradiction, assume $p \wedge \neg q$ and derive a contradiction.

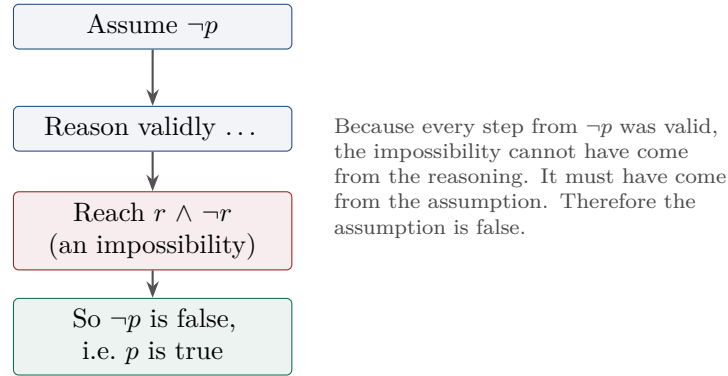


Figure 4.2: The logic of proof by contradiction.

Example 4.9 ($\sqrt{2}$ is irrational).

Solution. Let p be the proposition “ $\sqrt{2}$ is irrational”. Suppose $\neg p$ is true, i.e. $\sqrt{2}$ is rational. Then

$$\sqrt{2} = \frac{a}{b}, \quad b \neq 0, \quad \gcd(a, b) = 1$$

(any fraction can be reduced to lowest terms). Squaring,

$$a^2 = 2b^2,$$

so a^2 is even, hence a is even (this uses the contraposition result above: if a were odd, a^2 would be odd). Write $a = 2k$ for some $k \in \mathbb{Z}$. Substituting,

$$2b^2 = a^2 = (2k)^2 = 4k^2 \implies b^2 = 2k^2,$$

so b^2 is even, hence b is even. But then $2 \mid a$ and $2 \mid b$, so $\gcd(a, b) \geq 2$, contradicting $\gcd(a, b) = 1$.

We have derived $\gcd(a, b) = 1$ and $\gcd(a, b) \neq 1$ — a contradiction. Hence $\neg p$ is false and $\sqrt{2}$ is irrational.

4.4.6 Proofs of equivalence

To prove $p \leftrightarrow q$ you must prove *both* $p \rightarrow q$ and $q \rightarrow p$, because $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$.

For several statements $p_1, p_2, \dots, p_n$ claimed to be equivalent, proving all $n(n-1)$ implications $p_i \rightarrow p_j$ is wasteful. Instead use the identity

$$p_1 \leftrightarrow p_2 \leftrightarrow \dots \leftrightarrow p_n \equiv (p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \dots \wedge (p_n \rightarrow p_1),$$

i.e. prove a *cycle* of n implications.

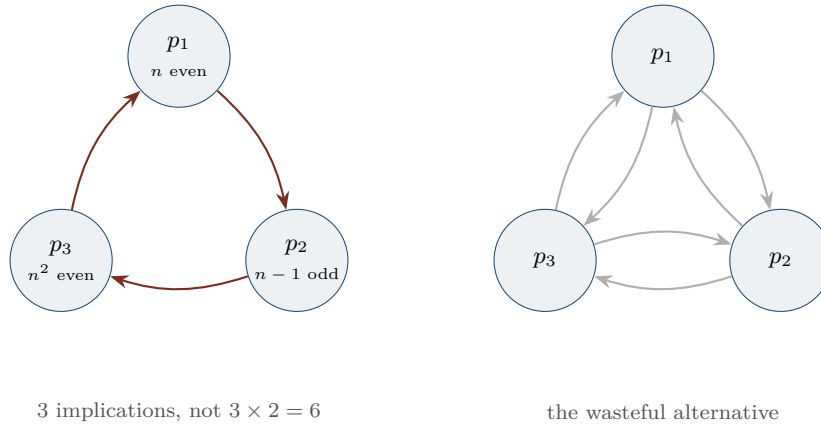


Figure 4.3: Proving equivalence of several statements by a cycle. Any two statements are connected by following the cycle round, so all implications follow by hypothetical syllogism.

Example 4.10 (three equivalent statements). Show that for an integer n the following are equivalent: p_1 : n is even; p_2 : $n - 1$ is odd; p_3 : n^2 is even.

Solution. We prove the cycle $p_1 \rightarrow p_2 \rightarrow p_3 \rightarrow p_1$.

$p_1 \Rightarrow p_2$. Suppose n is even, $n = 2k$ for some $k \in \mathbb{Z}$. Then

$$n - 1 = 2k - 1 = 2(k - 1) + 1 = 2k_1 + 1, \quad k_1 = k - 1 \in \mathbb{Z},$$

so $n - 1$ is odd.

$p_2 \Rightarrow p_3$. Suppose $n - 1$ is odd, so $n - 1 = 2k + 1$ for some $k \in \mathbb{Z}$, giving $n = 2k + 2$. Then

$$n^2 = (2k + 2)^2 = 4k^2 + 8k + 4 = 2(2k^2 + 4k + 2) = 2k_1,$$

with $k_1 = 2k^2 + 4k + 2 \in \mathbb{Z}$, so n^2 is even.

$p_3 \Rightarrow p_1$, by contraposition ($\neg p_1 \Rightarrow \neg p_3$). Suppose n is odd, $n = 2k + 1$. Then

$$n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2k_1 + 1,$$

so n^2 is odd, i.e. not even.

The cycle is complete, so all three are equivalent.

4.4.7 Counterexamples

To *disprove* $\forall x P(x)$ it suffices to exhibit one x with $P(x)$ false.

Example 4.11. Prove or disprove: for any integer n , if n^2 is positive then n is positive.

Solution. With $P(n)$ = “ n is positive” and $Q(n)$ = “ n^2 is positive”, the statement is $\forall n \in \mathbb{Z} (Q(n) \rightarrow P(n))$. It is **false**: take $n = -1$. Then $n^2 = 1 > 0$ but $n = -1$ is not positive. One counterexample is a complete disproof.

4.4.8 Exhaustive proof and proof by cases

Definition 4.8. A theorem of the form $(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$ is proved *by cases* by proving each $p_i \rightarrow q$ separately. If the cases are finitely many concrete possibilities checked one by one, the proof is *exhaustive*.

The method is justified by the equivalence

$$\begin{aligned} (p_1 \vee \cdots \vee p_n) \rightarrow q &\equiv \neg(p_1 \vee \cdots \vee p_n) \vee q \\ &\equiv (\neg p_1 \wedge \cdots \wedge \neg p_n) \vee q \\ &\equiv (\neg p_1 \vee q) \wedge \cdots \wedge (\neg p_n \vee q) \\ &\equiv (p_1 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q). \end{aligned}$$

The cases must be **exhaustive** — their disjunction must cover every possibility. They need not be mutually exclusive, but if you leave a gap the proof is worthless. State explicitly why your cases cover everything.

Example 4.12 (associativity of min). Let $a \sqcup b = \min(a, b)$ for $a, b \in \mathbb{Z}$. Show $(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)$ for all $a, b, c \in \mathbb{Z}$.

Solution. Let $a, b, c \in \mathbb{Z}$ be arbitrary. Since $\leq$ is a total order there are $3! = 6$ orderings to consider:

$$a \leq b \leq c, \quad a \leq c \leq b, \quad b \leq a \leq c, \quad b \leq c \leq a, \quad c \leq a \leq b, \quad c \leq b \leq a.$$

Case 1: $a \leq b \leq c$. LHS = $(a \sqcup b) \sqcup c = a \sqcup c = a$; RHS = $a \sqcup (b \sqcup c) = a \sqcup b = a$. Equal. The remaining five cases are checked identically; in each, both sides equal the smallest of the three. Since the six cases exhaust all possibilities, the identity holds for all integers.

Example 4.13 (no integer solutions). Show there are no integers x, y with $x^2 + 3y^2 = 8$.

Solution. If $|x| \geq 3$ then $x^2 \geq 9 > 8$; if $|y| \geq 2$ then $3y^2 \geq 12 > 8$. So it is enough to consider $x \in \{-2, -1, 0, 1, 2\}$ and $y \in \{-1, 0, 1\}$.

The possible values of x^2 are 0, 1, 4; the possible values of $3y^2$ are 0, 3. The largest attainable sum is $4 + 3 = 7 < 8$. Hence $x^2 + 3y^2 = 8$ is impossible over $\mathbb{Z}$.

Example 4.14 (absolute values, by cases). Prove that for all $x \in \mathbb{R}$, $-5 \leq |x + 2| - |x - 3| \leq 5$.

Solution. By definition

$$|x + 2| = \begin{cases} x + 2 & x \geq -2 \\ -(x + 2) & x < -2 \end{cases} \quad |x - 3| = \begin{cases} x - 3 & x \geq 3 \\ -(x - 3) & x < 3. \end{cases}$$

The breakpoints are -2 and 3 , giving three exhaustive cases.

Case 1: $x < -2$. Both absolute values use their negative branch:

$$|x + 2| - |x - 3| = -(x + 2) - (-(x - 3)) = -x - 2 + x - 3 = -5,$$

so $-5 \leq -5 \leq 5$. ✓

Case 2: $-2 \leq x < 3$.

$$|x + 2| - |x - 3| = (x + 2) - (-(x - 3)) = 2x - 1.$$

From $-2 \leq x < 3$ we get $-4 \leq 2x < 6$, hence $-5 \leq 2x - 1 < 5$. ✓

Case 3: $x \geq 3$.

$$|x + 2| - |x - 3| = (x + 2) - (x - 3) = 5,$$

so $-5 \leq 5 \leq 5$. ✓

The three cases cover all of $\mathbb{R}$, so the inequality holds for every real x .

4.4.9 Existence proofs

Definition 4.9. A theorem of the form $\exists x P(x)$ is proved by an *existence proof*. It is *constructive* if it exhibits an explicit a with $P(a)$ true, and *non-constructive* if it establishes existence without producing such an a .

Example 4.15 (constructive). Show that there is a positive integer expressible as the sum of cubes of positive integers in two different ways.

Solution. Take 1729:

$$1729 = 10^3 + 9^3 = 12^3 + 1^3.$$

Example 4.16 (non-constructive). Show that there exist irrational numbers x and y such that x^y is rational.

Solution. We know $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$. Either it is rational or it is not.

Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational. Then take $x = y = \sqrt{2}$; both are irrational and x^y is rational.

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational. Then take $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$; both are irrational, and

$$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2,$$

which is rational.

In either case such x, y exist. The proof is **non-constructive** because it never settles which case actually holds — we finish without knowing a specific pair.

4.4.10 Uniqueness proofs

Definition 4.10. To prove $\exists! x P(x)$, prove two things:

1. **Existence:** exhibit an x with $P(x)$ true.
2. **Uniqueness:** show that if $P(y)$ holds then $y = x$ (equivalently, if $y \neq x$ then $\neg P(y)$).

This mirrors the definition $\exists! x P(x) \equiv \exists x (P(x) \wedge \forall y (P(y) \rightarrow y = x))$.

Example 4.17. Show that if $a, b \in \mathbb{R}$ with $a \neq 0$, then there is a unique real r with $ar + b = 0$.

Solution. Existence. Since $a \neq 0$, the number $r = -b/a$ is a real number, and

$$a \cdot \left(\frac{-b}{a}\right) + b = -b + b = 0.$$

Uniqueness. Suppose $y \in \mathbb{R}$ also satisfies $ay + b = 0$. Then $ay = -b$, and since $a \neq 0$ we may divide to get $y = -b/a = r$. So the solution is unique.

4.5 Proof strategies

4.5.1 Forward and backward reasoning

Most proofs are found by working *backwards* from the goal (what would suffice to prove it?) until you reach something you can establish *forwards* from the hypotheses. The written proof, however, is always presented forwards.

Example 4.18 (AM–GM for two numbers). Prove that $\frac{x+y}{2} > \sqrt{xy}$ when x, y are distinct positive reals.

Solution. Search (backwards).

$$\begin{aligned} \frac{x+y}{2} > \sqrt{xy} &\iff \frac{(x+y)^2}{4} > xy && \text{(both sides positive; square)} \\ &\iff (x+y)^2 > 4xy \\ &\iff x^2 + 2xy + y^2 > 4xy \\ &\iff x^2 - 2xy + y^2 > 0 \\ &\iff (x-y)^2 > 0, \end{aligned}$$

and the last line is true because $x \neq y$. Now reverse it.

Proof (forwards). Suppose x and y are distinct positive reals. Since $x \neq y$, $(x-y)^2 > 0$, i.e. $x^2 - 2xy + y^2 > 0$. Adding $4xy$ to both sides,

$$x^2 + 2xy + y^2 > 4xy \implies (x+y)^2 > 4xy \implies x+y > 2\sqrt{xy}$$

(taking positive square roots, legitimate since $x+y > 0$), and therefore $\frac{x+y}{2} > \sqrt{xy}$.

Never present the backward search as the proof unless every step is a genuine “if and only if”. Writing “ $\frac{x+y}{2} > \sqrt{xy} \Rightarrow \dots \Rightarrow (x-y)^2 > 0$, which is true, QED” assumes what you are trying to prove. Do the search on scrap paper; write the forward chain.

4.5.2 Conjectures

Definition 4.11. A *conjecture* is a statement believed true but not proved.

Example 4.19 (the $3x + 1$ conjecture). Define $T : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ by

$$T(x) = \begin{cases} x/2 & \text{if } x \text{ is even,} \\ 3x + 1 & \text{if } x \text{ is odd.} \end{cases}$$

The $3x + 1$ (Collatz) conjecture states $\forall n \exists m (T^m(n) = 1)$: repeatedly applying T always eventually reaches 1.

Starting from 5:

$$5 \xrightarrow{3x+1} 16 \xrightarrow{/2} 8 \xrightarrow{/2} 4 \xrightarrow{/2} 2 \xrightarrow{/2} 1,$$

so $T^5(5) = 1$.

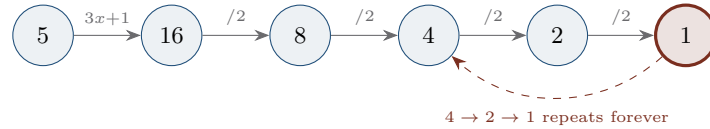


Figure 4.4: The trajectory of 5 under T . The conjecture has been verified by computer for all x up to roughly 5.6×10^{13} , but it remains unproved — verification is not proof.

No amount of checking proves a $\forall$ statement over an infinite domain. A single counterexample would disprove Collatz; 5.6×10^{13} confirmations prove nothing. This asymmetry is exactly the one in Chapter 2.

4.6 Chapter summary

Method	Assume	Derive
Vacuous	—	p is false
Trivial	—	q is true
Direct	p	q
Contraposition	$\neg q$	$\neg p$
Contradiction	$p \wedge \neg q$ (or $\neg p$)	$r \wedge \neg r$
Cases	each p_i in turn	q each time
Counterexample	—	one x with $\neg P(x)$
Constructive existence	—	an explicit witness
Non-constructive existence	—	existence without a witness
Uniqueness	$P(y)$	$y = x$, plus existence

Additional habits worth forming: unfold definitions immediately; search backwards but write forwards; state why your cases are exhaustive; and remember that verifying instances never proves a universal statement.

Part II Discrete Structures

CHAPTER 5

Set Theory

What this chapter is for. Sets are the fundamental discrete structure: functions, relations and number-theoretic objects are all defined in terms of them. The deeper point is that set theory *is* propositional logic in different clothing — both are instances of a *Boolean algebra*. Every set identity in this chapter is a logical equivalence from Chapter 1 with $\cup$ for $\vee$, $\cap$ for $\wedge$, and complement for $\neg$.

5.1 Sets, elements and well-definedness

Definition 5.1 (Set). A *set* is any well-defined collection of distinct objects. The objects are its *elements* or *members*. Order is irrelevant and repetition is not recorded.

Example 5.1. $A = \{\text{Amal, Bimal, Dias, Ganesh}\}$ is a set of names; $B = \{1, 3, 5, 7, 9\}$ is the set of odd natural numbers between 1 and 10; $C = \{2, 4, 6, 8, 10\}$ is the corresponding even set.

“Well-defined” is a real requirement. Given any object, there must be no ambiguity about whether it belongs.

- “The positive integers less than 10” is **well-defined**: exactly $1, \dots, 9$.
- “The interesting books” is **not** well-defined: different people would include different books.

Repetition is not recorded. The collection $\{\text{Amal, Bimal, Amal, Dias, Ganesh}\}$ lists “Amal” twice. As a *set* it is $\{\text{Amal, Bimal, Dias, Ganesh}\}$, with cardinality 4, not 5. Elements are distinct by definition.

Notation 5.2. Sets are usually written with upper-case letters, elements with lower-case.

$$x \in A \quad \text{“}x \text{ is a member of } A\text{”}, \quad x \notin A \quad \text{“}x \text{ is not a member of } A\text{”}.$$

The number of members of A is its *cardinality*, written $|A|$.

5.1.1 Ways of describing a set

Method	Example
Roster (list between braces)	$S = \{a, b, c, d\}$
Braces with ellipses	$A = \{1, 2, \dots, 100\}$, $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
Verbal description	“ A is the set of all integers from 1 to 100 inclusive”
Set-builder notation	$A = \{x \mid x \in \mathbb{Z}, 1 \leq x \leq 100\}$

For example

$$\mathbb{Q}^+ = \left\{x \in \mathbb{R} \mid x = \frac{p}{q} \text{ for some } p, q \in \mathbb{Z}^+\right\}.$$

5.1.2 Special sets

Definition 5.3. • The *null set* (or *empty set*) $\emptyset = \{ \}$ has no elements.

- The *universal set* $\mathbb{U}$ is the set of all elements under consideration in a given discussion.
- A *singleton* is a set with exactly one element.

$\{0\}$ is **not** the empty set — it is a singleton whose one element happens to be the number 0, so $|\{0\}| = 1$. Likewise $\{\emptyset\}$ is a singleton whose only element is the empty set, so $|\{\emptyset\}| = 1$ while $|\emptyset| = 0$.

5.1.3 Cardinality

Definition 5.4. If S has n elements for some $n \in \mathbb{N}$, then S is *finite* and n is its *cardinality*, written $|S|$. A set that is not finite is *infinite*.

$|\{a, b, c, d\}| = 4$ and $|\emptyset| = 0$; $\mathbb{N}$ is infinite.

5.2 Subsets and equality

Definition 5.5 (Subset). A is a *subset* of B , written $A \subseteq B$, if every element of A is an element of B :

$$A \subseteq B \iff \forall x (x \in A \rightarrow x \in B).$$

If $A \subseteq B$ and $A \neq B$ then A is a *proper subset*, written $A \subsetneq B$:

$$A \subsetneq B \iff \forall x (x \in A \rightarrow x \in B) \wedge \exists x (x \in B \wedge x \notin A).$$

Theorem 5.6. For every set A : (i) $\emptyset \subseteq A$, and (ii) $A \subseteq A$.

Proof. (i) $\emptyset \subseteq A$ means $\forall x (x \in \emptyset \rightarrow x \in A)$. The assertion $x \in \emptyset$ is false for every x , so each conditional is *vacuously* true (Chapter 4). Hence $\emptyset \subseteq A$.

(ii) $\forall x (x \in A \rightarrow x \in A)$ holds trivially. ■

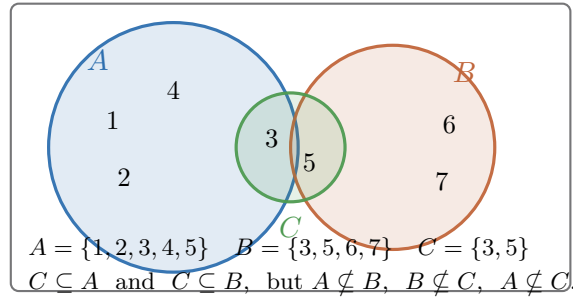
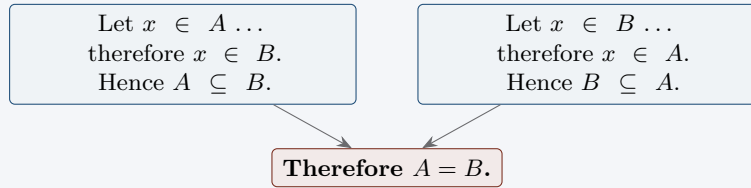


Figure 5.1: Subsets in a Venn diagram. C sits inside both A and B ; neither of A , B contains the other.

Definition 5.7 (Equality of sets). $A = B$ means A and B have exactly the same elements. Equivalently

$$A = B \iff A \subseteq B \text{ and } B \subseteq A \iff \forall x (x \in A \leftrightarrow x \in B).$$

This is the single most important proof template in the chapter. To prove two sets equal, prove *two* inclusions. Every “usual method” proof below has this shape:



5.3 Power sets

Definition 5.8 (Power set). The *power set* of A , written $\mathcal{P}(A)$ or 2^A , is the set of all subsets of A :

$$\mathcal{P}(A) = \{S \mid S \subseteq A\}.$$

Example 5.2.

$$\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Also $\mathcal{P}(\emptyset) = \{\emptyset\}$ (one element) and $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$ (two elements).

Theorem 5.9. If $|A| = n$ then $|\mathcal{P}(A)| = 2^n$.

Proof. To build a subset of A , decide independently for each of the n elements whether to include it: 2 choices per element, n elements, hence $2 \times 2 \times \dots \times 2 = 2^n$ subsets. ■

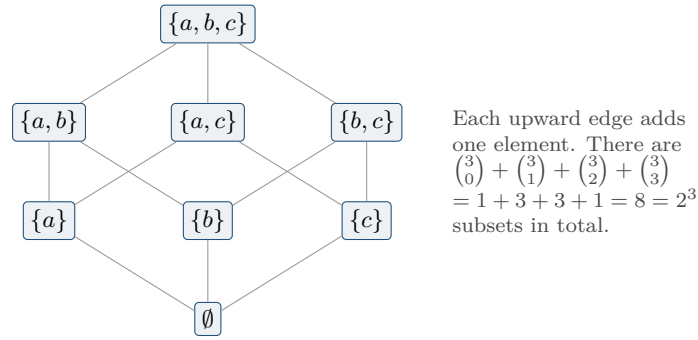


Figure 5.2: The power set of $\{a, b, c\}$ drawn as a lattice ordered by $\subseteq$. This is a *Hasse diagram* — see Chapter 7.

5.4 Truth sets and quantifiers

Definition 5.10. Given a predicate P and a domain D , the *truth set* of P is $\{x \in D \mid P(x)\}$.

Theorem 5.11. Over domain $\mathbb{U}$,

$$\forall x P(x) \text{ is true} \iff \text{truth set of } P = \mathbb{U}, \quad \exists x P(x) \text{ is true} \iff \text{truth set of } P \neq \emptyset.$$

Example 5.3. Domain $\mathbb{Z}$. Let $P(x)$ be $|x| = 1$, $Q(x)$ be $x^2 = 2$, $R(x)$ be $|x| = x$.

$$\text{truth set of } P = \{x \in \mathbb{Z} \mid |x| = 1\} = \{-1, 1\},$$

$$\text{truth set of } Q = \{x \in \mathbb{Z} \mid x^2 = 2\} = \emptyset,$$

$$\text{truth set of } R = \{x \in \mathbb{Z} \mid |x| = x\} = \{x \in \mathbb{Z} \mid x \geq 0\} = \mathbb{N}.$$

5.5 Set operations

All sets are assumed to be subsets of a universal set $\mathbb{U}$. Each operation is *defined* by the corresponding logical connective.

Definition 5.12.

$$A \cup B = \{x \mid x \in A \vee x \in B\} \quad \text{union}$$

$$A \cap B = \{x \mid x \in A \wedge x \in B\} \quad \text{intersection}$$

$$A - B = \{x \mid x \in A \wedge x \notin B\} \quad \text{difference (complement of } B \text{ relative to } A)$$

$$\bar{A} = \mathbb{U} - A = \{x \in \mathbb{U} \mid x \notin A\} \quad \text{complement}$$

$$A \triangle B = (A - B) \cup (B - A) \quad \text{symmetric difference}$$

A and B are *disjoint* if $A \cap B = \emptyset$.

Note that

$$A \triangle B = \{x \mid (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\},$$

which is exactly $\oplus$ applied to the membership predicates.

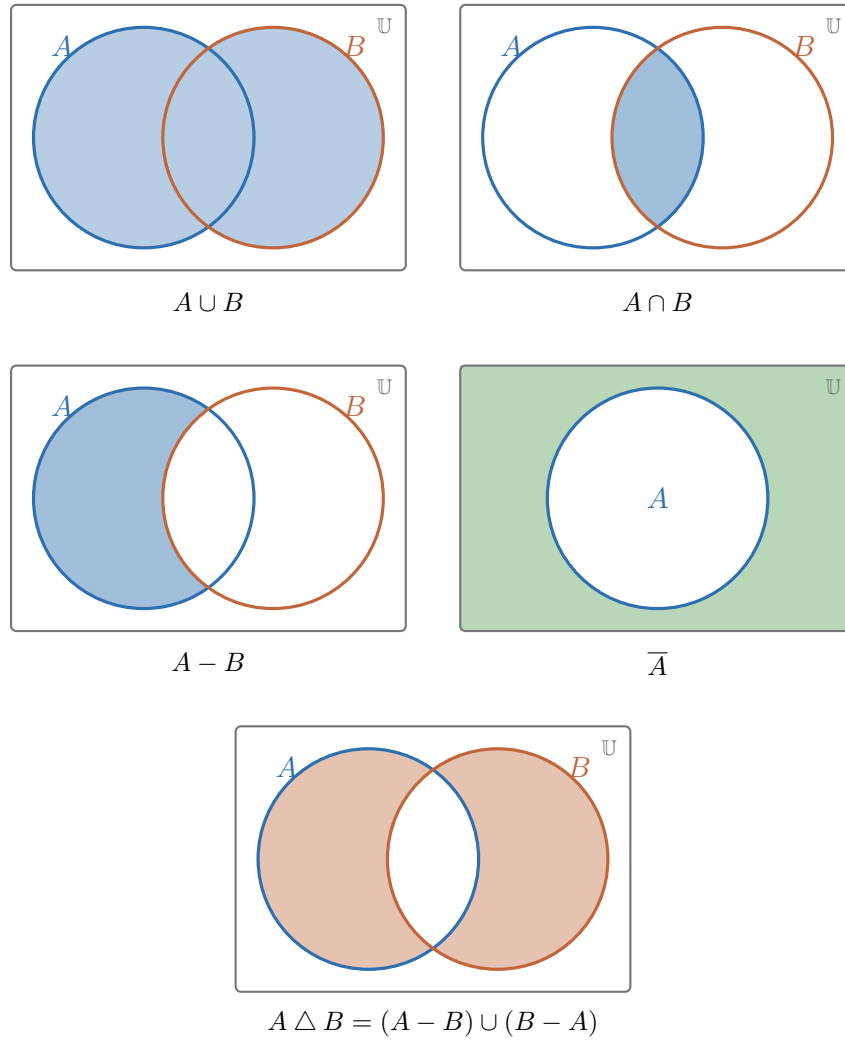
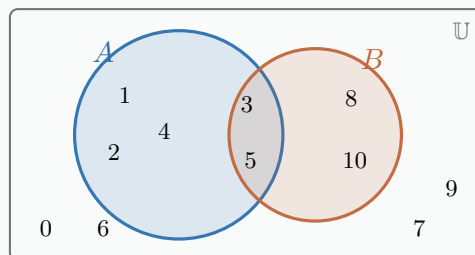


Figure 5.3: The five set operations. Shading marks the resulting set. Note how each picture matches a truth table: $\cup$ shades where “ A or B ” holds, $\cap$ where “ A and B ” holds, $\triangle$ where exactly one holds.

Example 5.4 (computing with a concrete universe). Let $\mathbb{U} = \{0, 1, \dots, 10\}$, $A = \{1, 2, 3, 4, 5\}$, $B = \{3, 5, 8, 10\}$.

$$\begin{aligned} A \cap B &= \{3, 5\}, & A \cup B &= \{1, 2, 3, 4, 5, 8, 10\}, \\ A - B &= \{1, 2, 4\}, & B - A &= \{8, 10\}, \\ \overline{A} &= \{0, 6, 7, 8, 9, 10\}, & A \triangle B &= \{1, 2, 4, 8, 10\}. \end{aligned}$$



Everything outside both circles — namely 0, 6, 7, 9 — lies in $\overline{A} \cap \overline{B} = \overline{A \cup B}$.

Venn diagrams are for *intuition and counterexamples*, not for proof. A two-set diagram has 4 regions and a three-set diagram has 8; for four or more sets the standard circles cannot show all 2^n regions, so a diagram can silently omit a case. Use the element method, set-builder method, membership table, or set identities for proofs.

5.6 Set identities

Name	Identity	
Identity	$A \cap \mathbb{U} = A$	$A \cup \emptyset = A$
Domination	$A \cup \mathbb{U} = \mathbb{U}$	$A \cap \emptyset = \emptyset$
Idempotent	$A \cup A = A$	$A \cap A = A$
Complementation	$\overline{(\overline{A})} = A$	
Commutative	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Associative	$A \cup (B \cup C) = (A \cup B) \cup C$	$A \cap (B \cap C) = (A \cap B) \cap C$
Distributive	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
De Morgan	$\overline{A \cap B} = \overline{A} \cup \overline{B}$	$\overline{A \cup B} = \overline{A} \cap \overline{B}$
Absorption	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
Complement	$A \cup \overline{A} = \mathbb{U}$	$A \cap \overline{A} = \emptyset$
Difference	$A - B = A \cap \overline{B}$	

Table 5.1: The set identities. Compare with Table 1.3: the tables are the same table.

The translation dictionary.

Logic	$\vee$	$\wedge$	$\neg$	T	F
Sets	$\cup$	$\cap$	$\neg$	$\mathbb{U}$	$\emptyset$

Anything proved in one column is automatically true in the other. The last identity, $A - B = A \cap \overline{B}$, corresponds to $p \wedge \neg q$, and is the standard first move when simplifying expressions with differences.

5.7 Four ways to prove a set identity

5.7.1 Method 1: the usual (double-inclusion) method

Example 5.5 (De Morgan by double inclusion). Prove $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Solution. ($\subseteq$) Let $x \in \overline{A \cap B}$. Then

$$\begin{aligned} x \notin A \cap B &\implies \neg(x \in A \cap B) \\ &\implies \neg(x \in A \wedge x \in B) \\ &\implies \neg(x \in A) \vee \neg(x \in B) \quad (\text{De Morgan, logic}) \\ &\implies x \notin A \vee x \notin B \\ &\implies x \in \overline{A} \vee x \in \overline{B} \\ &\implies x \in \overline{A} \cup \overline{B}. \end{aligned}$$

Hence $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$.

($\supseteq$) Let $x \in \overline{A} \cup \overline{B}$. Then

$$\begin{aligned} x \in \overline{A} \vee x \in \overline{B} &\implies x \notin A \vee x \notin B \\ &\implies \neg(x \in A) \vee \neg(x \in B) \\ &\implies \neg(x \in A \wedge x \in B) \\ &\implies \neg(x \in A \cap B) \implies x \notin A \cap B \implies x \in \overline{A \cap B}. \end{aligned}$$

Hence $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$.

Both inclusions hold, therefore $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

5.7.2 Method 2: the set-builder method

If every step is an “if and only if”, the two inclusions can be done at once as a chain of set equalities.

Example 5.6 (the other De Morgan law). Prove $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Solution.

$$\begin{aligned} \overline{A \cup B} &= \{x \mid x \notin A \cup B\} \\ &= \{x \mid \neg(x \in A \cup B)\} \\ &= \{x \mid \neg(x \in A \vee x \in B)\} \\ &= \{x \mid \neg(x \in A) \wedge \neg(x \in B)\} \quad (\text{De Morgan, logic}) \\ &= \{x \mid x \notin A \wedge x \notin B\} \\ &= \{x \mid x \in \overline{A} \wedge x \in \overline{B}\} \\ &= \{x \mid x \in \overline{A} \cap \overline{B}\} \\ &= \overline{A} \cap \overline{B}. \end{aligned}$$

Example 5.7 (distributive law by biconditional chain). Show $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Solution. For arbitrary x ,

$$\begin{aligned}
 x \in A \cup (B \cap C) &\iff (x \in A) \vee (x \in B \cap C) \\
 &\iff (x \in A) \vee (x \in B \wedge x \in C) \\
 &\iff (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \quad (\text{distributive, logic}) \\
 &\iff x \in (A \cup B) \wedge x \in (A \cup C) \\
 &\iff x \in (A \cup B) \cap (A \cup C).
 \end{aligned}$$

Since $\forall x (x \in A \cup (B \cap C) \iff x \in (A \cup B) \cap (A \cup C))$, the two sets are equal.

5.7.3 Method 3: membership tables

A membership table is a truth table in which 1 means “ x is in this set” and 0 means it is not. Two sets are equal iff their columns agree.

Example 5.8 (De Morgan by membership table).

A	B	$A \cap B$	$\overline{A \cap B}$	$\overline{A}$	$\overline{B}$	$\overline{A \cup B}$
0	0	0	1	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	1	1
1	1	1	0	0	0	0

Columns 4 and 7 agree in every row, so $\overline{A \cap B} = \overline{A \cup B}$.

Example 5.9 (three-set distributive law by membership table). Show $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

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

Columns 5 and 8 agree throughout.

5.7.4 Method 4: using known set identities

Once Table 5.1 is available, most identities are proved by algebra alone. **Name the identity used at every step** — this is routinely required for marks.

Example 5.10. Show $\overline{A \cup (B \cap C)} = (\overline{C} \cup \overline{B}) \cap \overline{A}$.

Solution.

$$\begin{aligned} \overline{A \cup (B \cap C)} &= \overline{A} \cap \overline{B \cap C} && \text{De Morgan} \\ &= \overline{A} \cap (\overline{B} \cup \overline{C}) && \text{De Morgan} \\ &= \overline{A} \cap (\overline{C} \cup \overline{B}) && \text{commutative} \\ &= (\overline{C} \cup \overline{B}) \cap \overline{A} && \text{commutative.} \end{aligned}$$

Example 5.11. Show $(P - Q) \cap (R - Q) = (P \cap R) - Q$.

Solution. For arbitrary x ,

$$\begin{aligned} x \in (P - Q) \cap (R - Q) &\iff x \in P - Q \wedge x \in R - Q \\ &\iff (x \in P \wedge x \notin Q) \wedge (x \in R \wedge x \notin Q) \\ &\iff x \in P \wedge x \in R \wedge x \notin Q && (\text{idempotent, commutative}) \\ &\iff (x \in P \cap R) \wedge x \notin Q \\ &\iff x \in (P \cap R) - Q. \end{aligned}$$

Therefore $(P - Q) \cap (R - Q) = (P \cap R) - Q$.

Example 5.12 (a longer identity chain). Using set identities, show $(A - B) - (B - C) = A - B$.

Solution.

$$\begin{aligned} (A - B) - (B - C) &= (A - B) \cap \overline{B - C} && (X - Y = X \cap \overline{Y}) \\ &= (A \cap \overline{B}) \cap \overline{B \cap C} && (X - Y = X \cap \overline{Y}) \\ &= (A \cap \overline{B}) \cap (\overline{B} \cup \overline{C}) && \text{De Morgan} \\ &= [(A \cap \overline{B}) \cap \overline{B}] \cup [(A \cap \overline{B}) \cap \overline{C}] && \text{distributive} \\ &= [A \cap (\overline{B} \cap \overline{B})] \cup [(A \cap \overline{B}) \cap \overline{C}] && \text{associative} \\ &= (A \cap \overline{B}) \cup [(A \cap \overline{B}) \cap \overline{C}] && \text{idempotent} \\ &= A \cap \overline{B} && \text{absorption} \\ &= A - B && (X \cap \overline{Y} = X - Y). \end{aligned}$$

Example 5.13 (two short ones). For subsets A, B, C of $\mathbb{U}$, show (1) $A - B = A \cap \overline{B}$ and (2) $\overline{A \cap B \cap C} = \overline{A} \cup \overline{B} \cup \overline{C}$.

Solution. (1) For arbitrary x : $x \in A - B \iff x \in A \wedge x \notin B \iff x \in A \wedge x \in \overline{B} \iff x \in A \cap \overline{B}$.

(2)

$$\begin{aligned}
\overline{A \cap B \cap C} &= \overline{(A \cap B) \cap C} && \text{associativity of } \cap \\
&= \overline{A \cap B} \cup \overline{C} && \text{De Morgan} \\
&= (\overline{A} \cup \overline{B}) \cup \overline{C} && \text{De Morgan} \\
&= \overline{A} \cup \overline{B} \cup \overline{C} && \text{associativity of } \cup.
\end{aligned}$$

5.8 Generalized unions and intersections

Definition 5.13. For sets $A_1, A_2, \dots, A_n$,

$$\bigcup_{i=1}^n A_i = \{x \mid x \in A_i \text{ for some } i\}, \quad \bigcap_{i=1}^n A_i = \{x \mid x \in A_i \text{ for all } i\}.$$

The same definitions apply to infinite families, with n replaced by ∞ .

Example 5.14 (a decreasing family). For $i = 1, 2, 3, \dots$ let $A_i = \{i, i+1, i+2, \dots\}$. Then

$$A_1 = \mathbb{Z}^+, \quad A_2 = \mathbb{Z}^+ - \{1\}, \quad \dots, \quad A_n = \mathbb{Z}^+ - \{1, 2, \dots, n-1\},$$

so the family is *nested downwards*: $A_1 \supseteq A_2 \supseteq \dots$. Hence

$$\bigcup_{i=1}^n A_i = A_1 = \mathbb{Z}^+, \quad \bigcap_{i=1}^n A_i = A_n = \{n, n+1, \dots\}.$$

Taking $n \rightarrow \infty$: $\bigcup_{i=1}^{\infty} A_i = \mathbb{Z}^+$ and $\bigcap_{i=1}^{\infty} A_i = \emptyset$ (no positive integer exceeds every i).

Example 5.15 (an increasing family). For $i = 1, 2, 3, \dots$ let $A_i = \{1, 2, \dots, i\}$. Then $A_1 \subseteq A_2 \subseteq \dots$, so

$$\bigcup_{i=1}^{\infty} A_i = \mathbb{Z}^+, \quad \bigcap_{i=1}^{\infty} A_i = A_1 = \{1\}.$$

Rule of thumb for nested families. If the family is increasing, the union is the “limit” and the intersection is the first set. If it is decreasing, the union is the first set and the intersection is the “limit”.

5.9 Computer representation of sets

Storing a set as an unordered list makes union, intersection and difference slow. If the universe is finite we can do far better.

Definition 5.14 (Bit-string representation). Fix an ordering $a_1, a_2, \dots, a_n$ of the universal set $\mathbb{U}$. A subset $A \subseteq \mathbb{U}$ is represented by the bit string of length n whose i th bit is 1 if $a_i \in A$ and 0 otherwise.

Theorem 5.15. Under this representation, with $\vee, \wedge, \neg$ applied bitwise,

$$\text{bits}(A \cup B) = \text{bits}(A) \vee \text{bits}(B), \quad \text{bits}(A \cap B) = \text{bits}(A) \wedge \text{bits}(B), \quad \text{bits}(\overline{A}) = \neg \text{bits}(A).$$

Example 5.16. Let $\mathbb{U} = \{1, 2, \dots, 10\}$ in increasing order, $A = \{1, 2, 3, 4, 5\}$, $B = \{1, 3, 5, 7, 9\}$.

$$\text{bits}(A) = 1111100000, \quad \text{bits}(B) = 1010101010.$$

Operation	Bitwise computation	Result
$A \cup B$	$1111100000 \vee 1010101010$	1111101010
$A \cap B$	$1111100000 \wedge 1010101010$	1010100000
$\overline{A}$	$\neg 1111100000$	0000011111
$A \triangle B$	$1111100000 \oplus 1010101010$	0101001010

Decoding: $A \cup B = \{1, 2, 3, 4, 5, 7, 9\}$, $A \cap B = \{1, 3, 5\}$, $\overline{A} = \{6, 7, 8, 9, 10\}$, $A \triangle B = \{2, 4, 7, 9\}$.

element	1	2	3	4	5	6	7	8	9	10
A	1	1	1	1	1	0	0	0	0	0
B	1	0	1	0	1	0	1	0	1	0
$A \cup B$	1	1	1	1	1	0	1	0	1	0
$A \cap B$	1	0	1	0	1	0	0	0	0	0

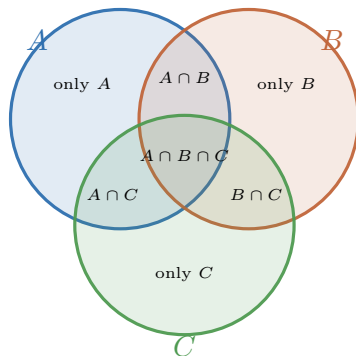
Figure 5.4: Bit-string representation. Union is a column-wise OR; intersection is a column-wise AND. On a 64-bit machine this handles a 64-element universe in a single instruction.

5.10 Counting: the inclusion–exclusion principle

Theorem 5.16 (Inclusion–exclusion). For finite sets,

$$|A \cup B| = |A| + |B| - |A \cap B|,$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$



Adding $|A| + |B| + |C|$ counts each double overlap *twice* and the triple overlap *three* times. Subtracting the three pairwise intersections removes the triple region entirely, so it must be added back once.

Figure 5.5: Why the signs alternate in inclusion–exclusion.

Example 5.17. Suppose $|A| = 28$, $|B| = 24$, $|C| = 19$, $|A \cap B| = 11$, $|A \cap C| = 8$, $|B \cap C| = 7$ and $|A \cap B \cap C| = 4$. Then

$$|A \cup B \cup C| = 28 + 24 + 19 - 11 - 8 - 7 + 4 = 49.$$

Consequently $A \cup B \cup C$ has 2^{49} subsets. The number of subsets containing every element of $A \cap B \cap C$ is $2^{49-4} = 2^{45}$, since the 4 elements of the triple intersection are forced in and the remaining 45 are free.

5.11 Chapter summary

- A set is a well-defined collection of distinct objects; order and repetition are irrelevant. Describe sets by roster, ellipsis, words, or set-builder notation.
- $A \subseteq B \iff \forall x (x \in A \rightarrow x \in B)$; $\emptyset \subseteq A$ vacuously, and $A \subseteq A$ always.
- $A = B \iff A \subseteq B$ and $B \subseteq A$. This double inclusion is the master proof template.
- $|\mathcal{P}(A)| = 2^{|A|}$.
- $\cup, \cap, -, \overline{}, \Delta$ are defined by $\vee, \wedge, \wedge \neg, \neg, \oplus$ respectively; set theory and propositional logic are the same Boolean algebra.
- Four proof methods: double inclusion, set-builder chain, membership table, and algebra with named identities. Venn diagrams illustrate and refute but do not prove.
- $A - B = A \cap \overline{B}$ is the first move for any expression containing a difference.
- Bit strings make set operations single machine instructions over a finite universe.
- Inclusion-exclusion: add the singles, subtract the pairs, add the triple.

CHAPTER 6

Functions

What this chapter is for. A function is a rule that assigns to every input *exactly one* output. Two properties dominate the chapter — injectivity (no two inputs share an output) and surjectivity (every possible output is used) — because together they give invertibility, and because they are the two properties you will be asked to prove or disprove again and again.

6.1 Definition and terminology

Definition 6.1 (Function). Let X and Y be non-empty sets. A *function* f from X to Y , written $f : X \rightarrow Y$, is an assignment of *exactly one* element of Y to each element of X . We write $f(a) = b$ when b is the unique element of Y assigned to $a \in X$. Functions are also called *mappings* or *transformations*.

Two requirements are hidden in “exactly one”:

1. **Totality.** Every element of X must be assigned something. (Otherwise you have a *partial* function — Section 6.11.)
2. **Single-valuedness.** No element of X may be assigned two different elements of Y .

There is *no* requirement that every element of Y be used, and no requirement that different elements of X get different values.

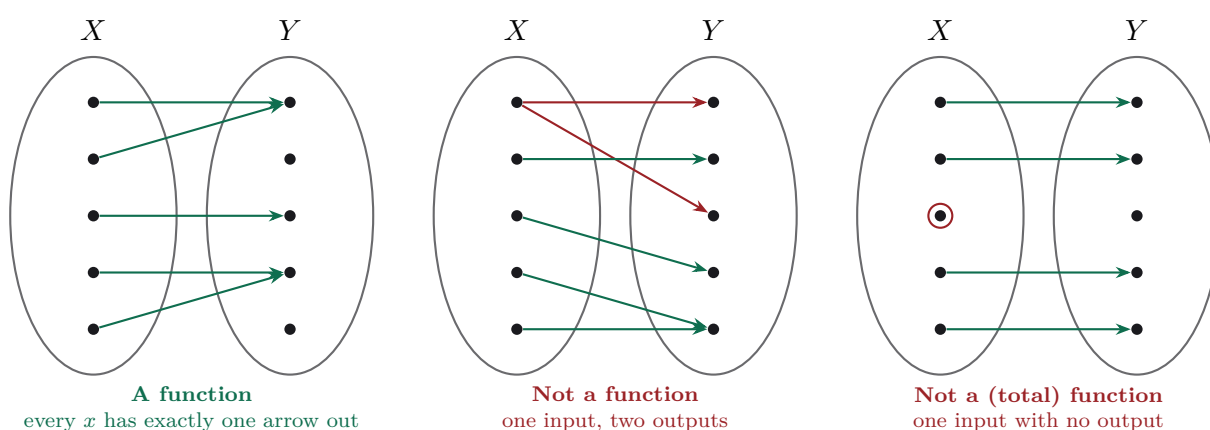


Figure 6.1: The two ways a diagram fails to define a function. Note that neither “two inputs sharing an output” nor “an unused output” is a failure.

Definition 6.2 (Domain, codomain, image, range). For $f : X \rightarrow Y$:

- X is the *domain*, Y the *codomain*.
- If $f(a) = b$ then b is the *image* of a , and a is a *pre-image* of b .
- The *range* (or *image*) of f is

$$\text{Range}(f) = \{y \in Y \mid y = f(x) \text{ for some } x \in X\}.$$

Always $\text{Range}(f) \subseteq Y$.

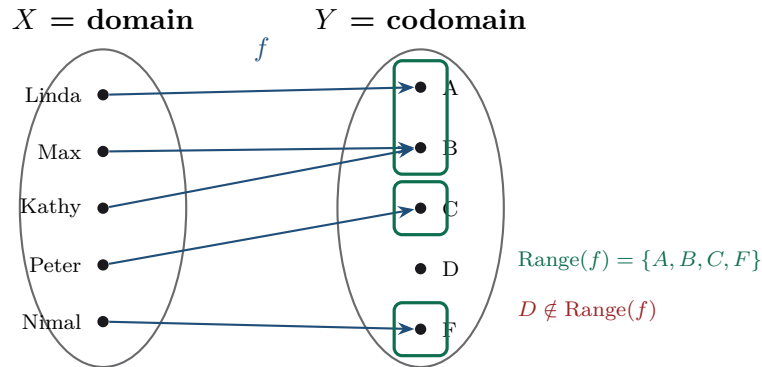


Figure 6.2: Domain, codomain and range. The range is what is actually hit; the codomain is what is allowed to be hit. D has no pre-image, so this f is not onto.

Example 6.1 (finding domain, codomain, range).

- (a) Let f assign to each bit string of length ≥ 2 its last two bits; e.g. $f(11010) = 10$.
Domain: all bit strings of length ≥ 2 . Codomain and range: $\{00, 01, 10, 11\}$.
- (b) Let $f : \mathbb{Z} \rightarrow \mathbb{Z}$ with $f(x) = x^2$. Domain $\mathbb{Z}$, codomain $\mathbb{Z}$, and $\text{Range}(f) = \{n^2 \mid n \in \mathbb{Z}\} = \{0, 1, 4, 9, 16, \dots\}$. Here $\text{Range}(f) \subsetneq \mathbb{Z}$.

6.2 One-to-one (injective) functions

Definition 6.3 (Injection). f is *one-to-one* (or an *injection*) if $f(a) = f(b)$ implies $a = b$ for all a, b in the domain:

$$f \text{ is one-to-one} \iff \forall a \forall b (f(a) = f(b) \rightarrow a = b) \iff \forall a \forall b (a \neq b \rightarrow f(a) \neq f(b)).$$

(The two forms are contrapositives of each other.)

Standard proof template (to show injective). “Suppose $f(x_1) = f(x_2)$ for some x_1, x_2 in the domain.” Then do algebra until you reach $x_1 = x_2$.

Standard disproof (to show not injective). Exhibit two distinct inputs with the same output.

Example 6.2.

- (a) $f : \{a, b, c, d\} \rightarrow \{1, 2, 3, 4, 5\}$ with $f(a) = 4$, $f(b) = 5$, $f(c) = 1$, $f(d) = 3$ is one-to-one: the four output values are distinct.
- (b) $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x + 1$. Suppose $f(x_1) = f(x_2)$. Then $x_1 + 1 = x_2 + 1$, so $x_1 = x_2$. Hence f is one-to-one.
- (c) $f : \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x) = x^2$, is **not** one-to-one: $f(-1) = f(1) = 1$ but $-1 \neq 1$.

6.3 Onto (surjective) functions

Definition 6.4 (Surjection). $f : A \rightarrow B$ is *onto* (or a *surjection*) if every element of B has at least one pre-image:

$$f \text{ is onto} \iff \forall y \in B \exists x \in A (f(x) = y) \iff \text{Range}(f) = B.$$

Standard proof template (to show onto.) “Let $y \in B$ be arbitrary.” Then *solve* $f(x) = y$ for x , *verify* that the x you found actually lies in the domain A , and conclude $f(x) = y$.

Standard disproof. Name one element of the codomain with no pre-image.

Example 6.3.

- (a) $f : \{a, b, c, d\} \rightarrow \{1, 2, 3\}$ with $f(a) = 3$, $f(b) = 2$, $f(c) = 1$, $f(d) = 3$ is onto: all three codomain elements are hit.
- (b) $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = 2x + 1$. Let $y \in \mathbb{R}$ be arbitrary and set $x = \frac{y-1}{2}$, which is a real number. Then $f(x) = 2(\frac{y-1}{2}) + 1 = y$. So f is onto.
- (c) $f : \mathbb{Z} \rightarrow \mathbb{Z}$, $f(x) = x^2$, is **not** onto: there is no integer x with $x^2 = -1$.

6.4 Bijections

Definition 6.5 (Bijection). $f : A \rightarrow B$ is a *bijection* (or *one-to-one correspondence*) if it is both one-to-one and onto.

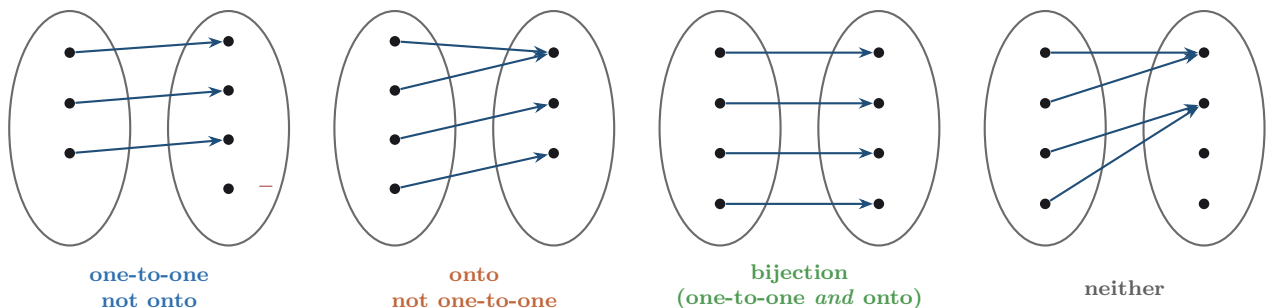


Figure 6.3: The four possibilities. Injectivity forbids two arrows landing on the same dot; surjectivity forbids a dot in the right oval with no arrow.

Example 6.4 (a bijection between punctured lines). Consider $f : \mathbb{R} - \{3\} \rightarrow \mathbb{R} - \{1\}$ defined by $f(x) = \frac{x-2}{x-3}$. Is f a bijection?

Solution. **One-to-one.** Suppose $f(x) = f(y)$ for $x, y \in \mathbb{R} - \{3\}$:

$$\begin{aligned} \frac{x-2}{x-3} = \frac{y-2}{y-3} &\implies (x-2)(y-3) = (x-3)(y-2) \\ &\implies xy - 3x - 2y + 6 = xy - 2x - 3y + 6 \\ &\implies -3x - 2y = -2x - 3y \implies x = y. \end{aligned}$$

So f is one-to-one.

Onto. Let $y \in \mathbb{R} - \{1\}$, so $y \neq 1$. Solve $f(x) = y$:

$$\begin{aligned} \frac{x-2}{x-3} = y &\implies x-2 = y(x-3) = xy - 3y \\ &\implies x - xy = 2 - 3y \implies x(1-y) = 2 - 3y \implies x = \frac{2-3y}{1-y}, \end{aligned}$$

which is a real number because $y \neq 1$. We must also check $x \neq 3$: if $\frac{2-3y}{1-y} = 3$ then $2 - 3y = 3 - 3y$, i.e. $2 = 3$, impossible. So $x \in \mathbb{R} - \{3\}$ and $f(x) = y$. Hence f is onto. Being one-to-one and onto, f is a **bijection**.

Example 6.5 (all four combinations on $\mathbb{Z}^+$). Give functions $\mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ that are:

- (a) **one-to-one but not onto:** $f(n) = n + 1$. Injective (if $n_1 + 1 = n_2 + 1$ then $n_1 = n_2$), but 1 has no pre-image in $\mathbb{Z}^+$, so not onto.
 (b) **onto but not one-to-one:**

$$f(n) = \begin{cases} 1 & n = 1, \\ n - 1 & n > 1. \end{cases}$$

Every $m \in \mathbb{Z}^+$ is $f(m + 1)$, so onto; but $f(1) = f(2) = 1$, so not injective.

- (c) **bijective but not the identity:**

$$f(n) = \begin{cases} n + 1 & n \text{ odd}, \\ n - 1 & n \text{ even}, \end{cases}$$

which swaps $1 \leftrightarrow 2$, $3 \leftrightarrow 4$, and so on. It is its own inverse.

- (d) **neither:** $f(n) = 1$ for all n .

Theorem 6.6 (Finite sets of equal size). *Let A, B be finite sets with $|A| = |B|$ and let $f : A \rightarrow B$. Then*

$$f \text{ one-to-one} \iff f \text{ onto} \iff f \text{ bijective}.$$

Idea. If f is one-to-one, the $|A|$ images are distinct, so $|\text{Range}(f)| = |A| = |B|$; a subset of B of size $|B|$ must be B itself, so f is onto. Conversely if f is onto then $|\text{Range}(f)| = |B| = |A|$; if two inputs collided the range would have fewer than $|A|$ elements. Hence f is one-to-one. ■

Finiteness is essential. $f : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$, $f(n) = n + 1$ is one-to-one but not onto; the case-defined f in (b) above is onto but not one-to-one. Both have “equal-sized” infinite domain and codomain.

6.5 Inverse functions

Definition 6.7 (Inverse). Let $f : A \rightarrow B$ be a bijection. The *inverse function* $f^{-1} : B \rightarrow A$ assigns to each $b \in B$ the unique $a \in A$ with $f(a) = b$. Thus

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

A function that has an inverse is *invertible*.

Theorem 6.8. f is invertible if and only if f is a bijection.

Why both conditions are needed. If f were not one-to-one, say $f(a_1) = f(a_2) = b$ with $a_1 \neq a_2$, then $f^{-1}(b)$ would have to be two different things — so f^{-1} would not be a function. If f were not onto, some $b \in B$ would have no pre-image, so $f^{-1}(b)$ would be undefined — so f^{-1} would not be total. ■

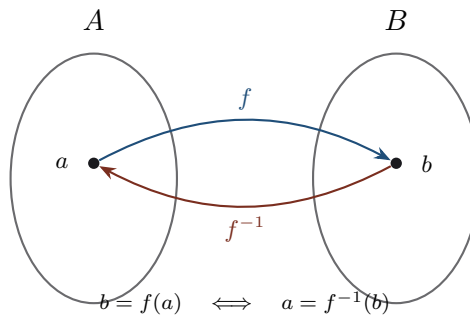


Figure 6.4: The inverse simply reverses every arrow. This is a function only when the original arrows form a bijection.

Example 6.6 (a finite inverse). $f : \{a, b, c\} \rightarrow \{1, 2, 3\}$ with $f(a) = 2$, $f(b) = 3$, $f(c) = 1$ is a bijection, so it is invertible, with

$$f^{-1}(1) = c, \quad f^{-1}(2) = a, \quad f^{-1}(3) = b.$$

Example 6.7 (restricting the domain to gain invertibility). $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x^2$ is **not** invertible, because $f(-1) = f(1) = 1$ means $f^{-1}(1)$ would have to be both 1 and -1 .

But let $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \geq 0\}$ and consider $f : \mathbb{R}^* \rightarrow \mathbb{R}^*$, $f(x) = x^2$.

One-to-one: if $x^2 = y^2$ then $(x - y)(x + y) = 0$, so $x = y$ or $x = -y$; since $x, y \geq 0$ the second forces $x = y = 0$. Either way $x = y$.

Onto: for $y \in \mathbb{R}^*$, take $x = \sqrt{y} \in \mathbb{R}^*$; then $f(x) = y$.

Hence f is a bijection and $f^{-1}(y) = \sqrt{y}$ for all $y \in \mathbb{R}^*$.

Finding f^{-1} in practice. Write $y = f(x)$, solve for x in terms of y , then rename. But this is only legitimate *after* you have shown f is a bijection — otherwise the “solution” may be ambiguous or undefined.

6.6 Composition

Definition 6.9 (Composition). Let $g : A \rightarrow B$ and $f : B \rightarrow C$. The *composition* $f \circ g : A \rightarrow C$ is defined by

$$(f \circ g)(a) = f(g(a)) \quad \text{for all } a \in A.$$

$f \circ g$ is defined only when $\text{Range}(g) \subseteq \text{dom}(f)$.

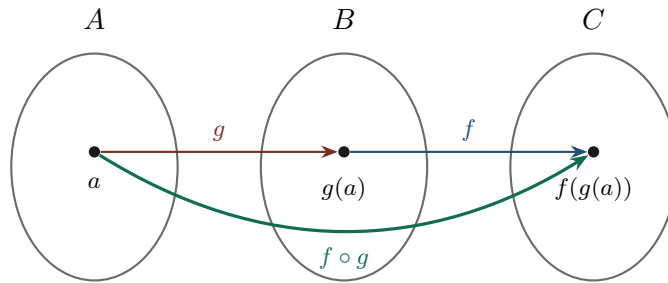


Figure 6.5: Composition. Read $f \circ g$ right-to-left: apply g first, then f .

Notation trap. In $f \circ g$ the function on the *right* acts *first*. (Relations in Chapter 7 follow the same convention: $S \circ R$ applies R first.)

Example 6.8 (composition need not commute — and may not exist). Let $g : \{a, b, c\} \rightarrow \{a, b, c\}$ with $g(a) = b$, $g(b) = c$, $g(c) = a$; and $f : \{a, b, c\} \rightarrow \{1, 2, 3\}$ with $f(a) = 3$, $f(b) = 2$, $f(c) = 1$.

Then $f \circ g : \{a, b, c\} \rightarrow \{1, 2, 3\}$ is

$$(f \circ g)(a) = f(b) = 2, \quad (f \circ g)(b) = f(c) = 1, \quad (f \circ g)(c) = f(a) = 3.$$

However $g \circ f$ is **not defined**, because $\text{Range}(f) = \{1, 2, 3\}$ is not a subset of $\text{dom}(g) = \{a, b, c\}$.

Example 6.9 (both defined but unequal). $f, g : \mathbb{Z} \rightarrow \mathbb{Z}$ with $f(x) = 2x + 3$ and $g(x) = 3x + 2$. For arbitrary $x \in \mathbb{Z}$:

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

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

Both are defined, but $f \circ g \neq g \circ f$. Composition is *associative* but not *commutative*.

Theorem 6.10 (Composition preserves injectivity and surjectivity). *Let $f : A \rightarrow B$ and $g : B \rightarrow C$.*

1. *If f and g are one-to-one, so is $g \circ f$.*
2. *If f and g are onto, so is $g \circ f$.*

Proof. (1) Suppose $(g \circ f)(a) = (g \circ f)(b)$ for $a, b \in A$. Then

$$\begin{aligned} g(f(a)) = g(f(b)) &\implies f(a) = f(b) && (g \text{ is one-to-one}) \\ &\implies a = b && (f \text{ is one-to-one}). \end{aligned}$$

Hence $g \circ f$ is one-to-one.

(2) Let $c \in C$ be arbitrary. Since g is onto, there is $b \in B$ with $g(b) = c$. Since f is onto, there is $a \in A$ with $f(a) = b$. Then $(g \circ f)(a) = g(f(a)) = g(b) = c$. Hence $g \circ f$ is onto. ■

Theorem 6.11 (Partial converses). *Let $f : A \rightarrow B$ and $g : B \rightarrow C$.*

1. *If $g \circ f$ is one-to-one, then f is one-to-one (but g need not be).*
2. *If $g \circ f$ is onto, then g is onto (but f need not be).*

Proof. (1) Suppose $f(a) = f(b)$. Applying g , $g(f(a)) = g(f(b))$, i.e. $(g \circ f)(a) = (g \circ f)(b)$; since $g \circ f$ is one-to-one, $a = b$.

(2) Let $c \in C$. Since $g \circ f$ is onto there is $a \in A$ with $g(f(a)) = c$. Then $b = f(a) \in B$ satisfies $g(b) = c$. ■

Counterexamples for the missing directions. Let $A = \{1\}$, $B = \{1, 2\}$, $C = \{1\}$, with $f(1) = 1$ and $g(1) = g(2) = 1$. Then $g \circ f$ is a bijection $A \rightarrow C$, yet g is not one-to-one and f is not onto.

6.7 The identity function

Definition 6.12. For a non-empty set A , the *identity function* $\iota_A : A \rightarrow A$ is $\iota_A(x) = x$ for all $x \in A$. It is a bijection.

Theorem 6.13. *If $f : A \rightarrow B$ is invertible then*

$$f^{-1} \circ f = \iota_A, \quad f \circ f^{-1} = \iota_B, \quad (f^{-1})^{-1} = f.$$

Both compositions must be checked. In general, verifying only $g(f(x)) = x$ does not prove $g = f^{-1}$: it shows f is injective and g is a *left* inverse, but g might be defined on a larger set and fail $f(g(y)) = y$. Only when f is already known to be a bijection does one identity suffice.

6.8 The graph of a function

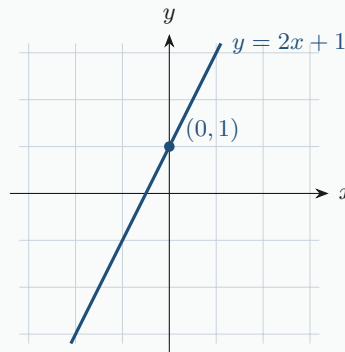
Definition 6.14. The *graph* of $f : A \rightarrow B$ is the set of ordered pairs

$$\mathcal{G}(f) = \{(a, b) \mid a \in A \text{ and } f(a) = b\} \subseteq A \times B.$$

This is the link to Chapter 7: the graph of a function is a special kind of relation — one in which every element of A appears as the first coordinate of *exactly one* pair.

Example 6.10. The graph of $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = 2x + 1$, is

$$\mathcal{G}(f) = \{(x, y) \mid x \in \mathbb{R}, y = 2x + 1\} = \{(x, 2x + 1) \mid x \in \mathbb{R}\}.$$



6.9 Images and inverse images of subsets

Definition 6.15. Let $f : A \rightarrow B$, $S \subseteq A$ and $T \subseteq B$.

$$f(S) = \{f(s) \mid s \in S\} \subseteq B \quad (\text{the image of } S),$$

$$f^{-1}(T) = \{a \in A \mid f(a) \in T\} \subseteq A \quad (\text{the inverse image / pre-image of } T).$$

The notation $f^{-1}(T)$ makes sense **even when f is not invertible**. It denotes a set of pre-images, not the value of an inverse function. Do not read $f^{-1}(\{1\}) = \{-1, 1\}$ as saying f^{-1} exists.

Example 6.11. Let $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x^2$.

$$f(\{-2, -1, 0, 1, 2\}) = \{0, 1, 4\},$$

$$f(\mathbb{Z}) = \{n^2 \mid n \in \mathbb{Z}\} = \{n^2 \mid n \in \mathbb{N}\},$$

$$f(\mathbb{R}) = \{x^2 \mid x \in \mathbb{R}\} = [0, \infty),$$

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

$$f^{-1}(\{x \mid 0 < x < 1\}) = \{x \mid -1 < x < 0\} \cup \{x \mid 0 < x < 1\}.$$

6.9.1 Images and set operations

Theorem 6.16. *Let $f : A \rightarrow B$ and $S, T \subseteq A$. Then*

$$f(S \cup T) = f(S) \cup f(T), \quad f(S \cap T) \subseteq f(S) \cap f(T).$$

Equality holds in the second for all S, T if and only if f is one-to-one.

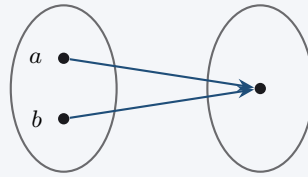
Proof. Union, $\subseteq$. Let $y \in f(S \cup T)$. Then there is $x \in S \cup T$ with $f(x) = y$, so $x \in S$ or $x \in T$, giving $y \in f(S)$ or $y \in f(T)$, i.e. $y \in f(S) \cup f(T)$.

Union, $\supseteq$. Let $y \in f(S) \cup f(T)$. Then there is $x \in S$ with $f(x) = y$, or there is $x \in T$ with $f(x) = y$; either way there is $x \in S \cup T$ with $f(x) = y$, so $y \in f(S \cup T)$.

Intersection, $\subseteq$. Let $y \in f(S \cap T)$. Then there is $x \in S \cap T$ with $f(x) = y$. Since $x \in S$ we get $y \in f(S)$; since $x \in T$ we get $y \in f(T)$. Hence $y \in f(S) \cap f(T)$.

Intersection, $\supseteq$, when f is one-to-one. Let $y \in f(S) \cap f(T)$. Then there are $s \in S$ and $t \in T$ with $y = f(s) = f(t)$. Since f is one-to-one, $s = t$; so this common element lies in $S \cap T$ and $y = f(s) \in f(S \cap T)$. ■

Counterexample showing $\subseteq$ can be strict. Let $A = \{a, b\}$ and $f(a) = f(b)$. Put $S = \{a\}$, $T = \{b\}$. Then $S \cap T = \emptyset$ so $f(S \cap T) = \emptyset$, while $f(S) \cap f(T) = \{f(a)\} \neq \emptyset$.



6.9.2 Inverse images and set operations

Inverse images behave better — they commute with *all* the Boolean operations.

Theorem 6.17. *Let $f : A \rightarrow B$ and $S, T \subseteq B$. Then*

$$f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T), \quad f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T), \quad f^{-1}(B - S) = A - f^{-1}(S).$$

Proof. Each is a chain of biconditionals. For arbitrary $x \in A$:

$$\begin{aligned} x \in f^{-1}(S \cup T) &\iff f(x) \in S \cup T \iff f(x) \in S \vee f(x) \in T \\ &\iff x \in f^{-1}(S) \vee x \in f^{-1}(T) \iff x \in f^{-1}(S) \cup f^{-1}(T). \end{aligned}$$

Replacing $\vee$ by $\wedge$ throughout gives the intersection case. For the third,

$$\begin{aligned} x \in f^{-1}(B - S) &\iff f(x) \in B - S \iff f(x) \in B \wedge f(x) \notin S \\ &\iff x \in f^{-1}(B) \wedge x \notin f^{-1}(S) \\ &\iff x \in A \wedge x \notin f^{-1}(S) \iff x \in A - f^{-1}(S), \end{aligned}$$

using $f^{-1}(B) = A$ since f is total. ■

6.10 Floor and ceiling

Definition 6.18. The *floor* function $\lfloor \cdot \rfloor : \mathbb{R} \rightarrow \mathbb{Z}$ assigns to x the largest integer $\leq x$. The *ceiling* function $\lceil \cdot \rceil : \mathbb{R} \rightarrow \mathbb{Z}$ assigns to x the smallest integer $\geq x$. The floor function is also called the *greatest integer function*.

Example 6.12.

$$\begin{aligned} \lfloor 0.5 \rfloor &= 0, & \lfloor 7.25 \rfloor &= 7, & \lfloor -12.4 \rfloor &= -13, & \lfloor -10 \rfloor &= -10, \\ \lceil 0.5 \rceil &= 1, & \lceil 7.5 \rceil &= 8, & \lceil -3.4 \rceil &= -3, & \lceil -10 \rceil &= -10. \end{aligned}$$

Negative arguments are where mistakes happen. $\lfloor -12.4 \rfloor = -13$, *not* -12 : the floor moves *left* on the number line, always. Similarly $\lceil -3.4 \rceil = -3$, *not* -4 . Truncation-towards-zero is neither floor nor ceiling.

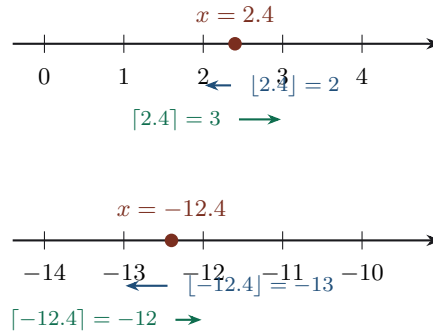


Figure 6.6: Floor always rounds *left*, ceiling always rounds *right*, on both halves of the number line.

Theorem 6.19 (Basic floor/ceiling identities). *For every $x \in \mathbb{R}$ and every $n \in \mathbb{Z}$:*

1. $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$ and $\lceil x \rceil - 1 < x \leq \lceil x \rceil$;
2. $\lfloor x \rfloor = n \iff n \leq x < n + 1$;
3. $\lceil x \rceil = -\lfloor -x \rfloor$ and $\lfloor x \rfloor = -\lceil -x \rceil$;
4. $\lfloor x + n \rfloor = \lfloor x \rfloor + n$ and $\lceil x + n \rceil = \lceil x \rceil + n$;
5. $\lfloor x \rfloor + \lfloor -x \rfloor = \begin{cases} 0 & x \in \mathbb{Z}, \\ -1 & x \notin \mathbb{Z}. \end{cases}$

Proof of (4). Let $m = \lfloor x \rfloor$, so $m \leq x < m + 1$ with $m \in \mathbb{Z}$. Adding n ,

$$m + n \leq x + n < m + n + 1,$$

and $m + n \in \mathbb{Z}$. By characterisation (2), $\lfloor x + n \rfloor = m + n = \lfloor x \rfloor + n$. ■

Proof of (5). If $x \in \mathbb{Z}$ then $\lfloor x \rfloor = x$ and $\lfloor -x \rfloor = -x$, so the sum is 0. If $x \notin \mathbb{Z}$, write $\lfloor x \rfloor = m$, so $m < x < m + 1$ (strict on both sides). Negating, $-m - 1 < -x < -m$, so $\lfloor -x \rfloor = -m - 1$, and the sum is $m + (-m - 1) = -1$. ■

6.11 Partial functions

Definition 6.20 (Partial function). A *partial function* f from A to B assigns to each element of some subset of A — the *domain of definition* of f — a unique element of B . A is still called the domain and B the codomain. f is *undefined* at elements of A outside the domain of definition. If the domain of definition is all of A , f is a *total* function.

Example 6.13. $f : \mathbb{Z} \rightarrow \mathbb{R}$ with $f(n) = \sqrt{n}$ is a partial function whose domain of definition is $\{n \in \mathbb{Z} \mid n \geq 0\}$; it is undefined for negative integers.

Partial functions are exactly what a computer program computes: a program that loops forever or crashes on some inputs implements a partial function, and proving totality is a distinct (and often hard) verification task.

6.12 Chapter summary

- $f : X \rightarrow Y$ assigns exactly one output to *every* input. $\text{Range}(f) \subseteq Y$, with equality iff f is onto.
- **Injective:** $f(x_1) = f(x_2) \rightarrow x_1 = x_2$. Prove by assuming $f(x_1) = f(x_2)$ and deriving $x_1 = x_2$; disprove by one colliding pair.
- **Surjective:** $\forall y \in Y \exists x \in X (f(x) = y)$. Prove by taking arbitrary y , solving for x , and checking x lies in the domain; disprove by one unhit y .
- **Bijective** = both; equivalently **invertible**. For finite sets of equal size the three notions coincide — but not for infinite sets.
- $(f \circ g)(a) = f(g(a))$: right function first. Composition is associative, not commutative, and preserves both injectivity and surjectivity. Conversely $g \circ f$ injective $\Rightarrow f$ injective; $g \circ f$ onto $\Rightarrow g$ onto.
- $f^{-1} \circ f = \iota_A$ and $f \circ f^{-1} = \iota_B$.
- $f(S \cup T) = f(S) \cup f(T)$ always, but $f(S \cap T) \subseteq f(S) \cap f(T)$, with equality iff f is injective. Inverse images commute with $\cup$, $\cap$ and complement without any hypothesis.
- $\lfloor x \rfloor$ rounds left, $\lceil x \rceil$ rounds right, always — watch negatives. $\lfloor x + n \rfloor = \lfloor x \rfloor + n$ for integer n .
- A partial function may be undefined on part of its domain.

CHAPTER 7

Relations

What this chapter is for. A relation is a set of ordered pairs — nothing more. That minimal definition is powerful precisely because it is so permissive: functions are relations, “ $\leq$ ” is a relation, “divides” is a relation, and a relational-database table is an n -ary relation. The chapter is dominated by four properties (reflexive, symmetric, anti-symmetric, transitive) which you must be able to *prove* when they hold and *refute* with a specific counterexample when they do not.

7.1 Cartesian products

Definition 7.1 (Cartesian product). For sets A and B ,

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

the set of all *ordered pairs* with first coordinate from A and second from B . More generally,

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i \text{ for } i = 1, 2, \dots, n\},$$

the set of ordered n -tuples.

Example 7.1. $A = \{1, 2\}$ and $B = \{a, b, c\}$ give

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\},$$

so $|A \times B| = 2 \times 3 = 6$. In general $|A \times B| = |A| \cdot |B|$.

Ordered pairs are *ordered*: $(1, a) \neq (a, 1)$, and in general $A \times B \neq B \times A$. Contrast with sets, where $\{1, a\} = \{a, 1\}$.

7.2 Binary relations

Definition 7.2 (Binary relation). A *binary relation from A to B* is a subset $R \subseteq A \times B$. A *binary relation on A* is a relation from A to A , i.e. a subset of $A \times A$.

Notation 7.3. We write $a R b$ for $(a, b) \in R$, and $a \not R b$ for $(a, b) \notin R$. When $(a, b) \in R$ we say *a is related to b by R* .

Example 7.2 (divisibility on a small set). Let $A = \{1, 2, 3, 4\}$ and $R = \{(a, b) \mid a \mid b\}$. Then

$$R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)\}.$$

Example 7.3 (strict order on a small set). With the same A and $R = \{(a, b) \mid a < b\}$,

$$R = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}.$$

7.2.1 How many relations are there?

Theorem 7.4. If $|A| = n$ then there are 2^{n^2} distinct binary relations on A .

Proof. A relation on A is a subset of $A \times A$, and $|A \times A| = n \cdot n = n^2$. A set with m elements has 2^m subsets, so there are 2^{n^2} subsets of $A \times A$. ■

For $n = 4$ this is $2^{16} = 65\,536$.

7.3 Representing relations

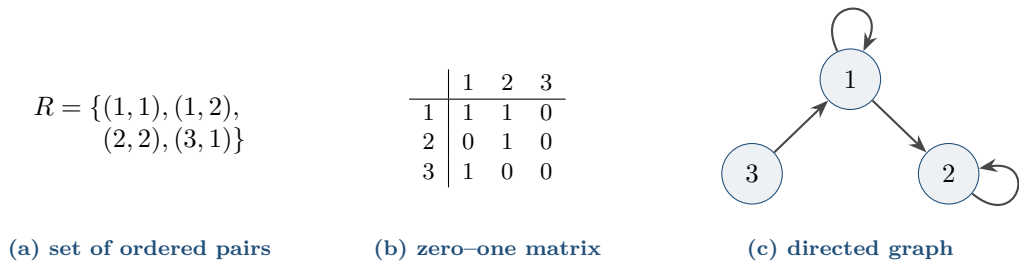


Figure 7.1: Three representations of the same relation R on $\{1, 2, 3\}$. The digraph has an arrow $a \rightarrow b$ exactly when $(a, b) \in R$; a *loop* at a means $(a, a) \in R$.

Reading properties off a digraph.

Property	Digraph signature
Reflexive	a loop at <i>every</i> vertex
Symmetric	every arrow has a matching reverse arrow
Anti-symmetric	<i>no</i> pair of opposite arrows between distinct vertices
Transitive	wherever $a \rightarrow b \rightarrow c$, there is also $a \rightarrow c$

7.4 Properties of relations

Definition 7.5. Let R be a relation on a set A .

R is *reflexive* $\iff \forall a ((a, a) \in R)$;

R is *symmetric* $\iff \forall a \forall b ((a, b) \in R \rightarrow (b, a) \in R)$;

R is *anti-symmetric* $\iff \forall a \forall b ((a, b) \in R \wedge (b, a) \in R \rightarrow a = b)$;

R is *transitive* $\iff \forall a \forall b \forall c ((a, b) \in R \wedge (b, c) \in R \rightarrow (a, c) \in R)$.

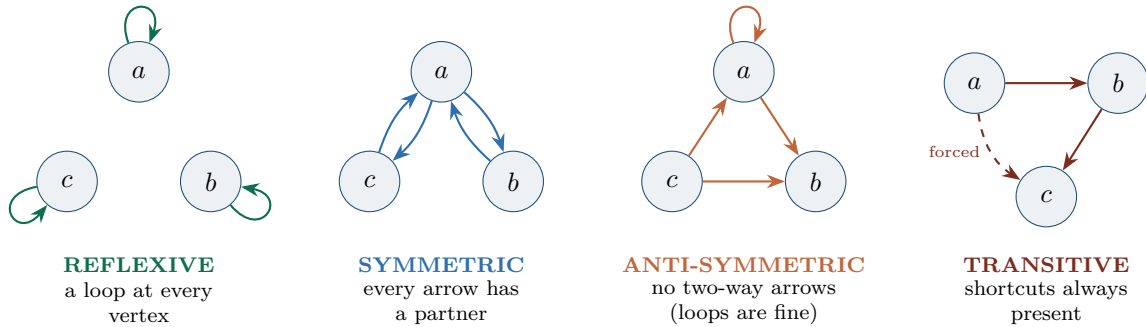


Figure 7.2: The four properties, seen in digraphs.

Anti-symmetric is not “not symmetric”.

- A relation can be **both**: e.g. the identity relation $\{(a, a) \mid a \in A\}$, or the empty relation.
- A relation can be **neither**: e.g. $\{(1, 2), (2, 1), (1, 3)\}$ on $\{1, 2, 3\}$ — not symmetric because $(1, 3)$ has no reverse, not anti-symmetric because $(1, 2)$ and $(2, 1)$ are both present with $1 \neq 2$.

Anti-symmetry only forbids *two-way* arrows between *distinct* elements; loops never violate it.

7.4.1 Worked classification: relations on a finite set

Example 7.4 (six relations on $\{1, 2, 3, 4\}$). Classify

$$R_1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\},$$

$$R_2 = \{(1, 1), (1, 2), (2, 1)\},$$

$$R_3 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\},$$

$$R_4 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\},$$

$$R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\},$$

$$R_6 = \{(3, 4)\}.$$

Solution.

	Reflexive	Symmetric	Anti-sym.	Transitive
R_1	no	no	no	no
R_2	no	yes	no	no
R_3	yes	yes	no	no
R_4	no	no	yes	yes
R_5	yes	no	yes	yes
R_6	no	no	yes	yes

Justifications for R_1 . Not reflexive: $(3, 3) \notin R_1$. Not symmetric: $(3, 4) \in R_1$ but $(4, 3) \notin R_1$. Not anti-symmetric: $(1, 2), (2, 1) \in R_1$ with $1 \neq 2$. Not transitive: $(3, 4), (4, 1) \in R_1$ but $(3, 1) \notin R_1$.

Justifications for R_2 . Not reflexive: $(2, 2) \notin R_2$. Symmetric: the only non-loop pairs are $(1, 2)$ and $(2, 1)$, and each has its partner. Not anti-symmetric: $(1, 2), (2, 1) \in R_2$ with $1 \neq 2$. Not transitive: $(2, 1), (1, 2) \in R_2$ but $(2, 2) \notin R_2$.

Justifications for R_5 . Reflexive: $(1, 1), (2, 2), (3, 3), (4, 4)$ are all present. Not symmetric: $(1, 4) \in R_5$ but $(4, 1) \notin R_5$. Anti-symmetric: there is no pair $a \neq b$ with both (a, b) and (b, a) in R_5 . Transitive: R_5 is precisely $\{(a, b) \mid a \leq b\}$ on $\{1, 2, 3, 4\}$, and $a \leq b \leq c$ implies $a \leq c$.

Answer format that earns full marks. For a *positive* claim, give a general argument. For a *negative* claim, give one specific counterexample of exactly the right shape:

To refute	Exhibit
reflexive	one a with $(a, a) \notin R$
symmetric	one pair with $(a, b) \in R, (b, a) \notin R$
anti-symmetric	$a \neq b$ with both $(a, b), (b, a) \in R$
transitive	$(a, b), (b, c) \in R$ but $(a, c) \notin R$

7.4.2 Worked classification: relations on $\mathbb{Z}$

Example 7.5. Classify these relations on $\mathbb{Z}$:

$$R_1 = \{(a, b) \mid a \leq b\}, \quad R_2 = \{(a, b) \mid a > b\}, \quad R_3 = \{(a, b) \mid a = b \text{ or } a = -b\},$$

$$R_4 = \{(a, b) \mid a = b\}, \quad R_5 = \{(a, b) \mid a = b + 1\}, \quad R_6 = \{(a, b) \mid a + b \leq 3\}.$$

Solution.

	Reflexive	Symmetric	Anti-sym.	Transitive
$R_1: a \leq b$	yes	no	yes	yes
$R_2: a > b$	no	no	yes	yes
$R_3: a = \pm b$	yes	yes	no	yes
$R_4: a = b$	yes	yes	yes	yes
$R_5: a = b + 1$	no	no	yes	no
$R_6: a + b \leq 3$	no	yes	no	no

R_1 **in detail.** Reflexive: $a \leq a$ for all $a \in \mathbb{Z}$. Not symmetric: $1 \leq 2$ but $2 \not\leq 1$. Anti-symmetric: $a \leq b$ and $b \leq a$ force $a = b$. Transitive: $a \leq b$ and $b \leq c$ force $a \leq c$.

R_5 **in detail.** Not reflexive: $1 \neq 1 + 1$, so $(1, 1) \notin R_5$. Not symmetric: $(2, 1) \in R_5$ but $(1, 2) \notin R_5$. Anti-symmetric: $a = b + 1$ and $b = a + 1$ would give $a = a + 2$, impossible; so the hypothesis never holds and the implication is vacuously true. Not transitive: $(3, 2), (2, 1) \in R_5$ but $(3, 1) \notin R_5$.

R_6 **in detail.** Not reflexive: $3 + 3 = 6 > 3$, so $(3, 3) \notin R_6$. Symmetric: $a + b \leq 3$ iff $b + a \leq 3$. Not anti-symmetric: $(1, 2), (2, 1) \in R_6$ but $1 \neq 2$. Not transitive: $(2, 1), (1, 2) \in R_6$ but $2 + 2 = 4 > 3$, so $(2, 2) \notin R_6$.

Vacuous anti-symmetry. A relation with no two-way pairs at all — like $a = b + 1$ — is anti-symmetric *vacuously*. This is a legitimate and complete justification; say so explicitly.

7.4.3 Counting relations with a given property

Theorem 7.6. Let $|A| = n$. The number of relations on A that are

<i>Property</i>	<i>Count</i>
(any)	2^{n^2}
reflexive	2^{n^2-n}
symmetric	$2^{n(n+1)/2}$
anti-symmetric	$2^n \cdot 3^{n(n-1)/2}$

Proof. Think of the $n \times n$ grid of cells (a, b) ; a relation chooses, independently, whether each cell is in R .

Any: n^2 free binary choices, giving 2^{n^2} .

Reflexive: the n diagonal cells are *forced* to be in R ; the other $n^2 - n$ are free, giving 2^{n^2-n} .

Symmetric: the n diagonal cells are free (2^n), and the $n(n-1)/2$ off-diagonal *pairs* $\{(a, b), (b, a)\}$ must be decided together — both in or both out ($2^{n(n-1)/2}$). Total $2^n \cdot 2^{n(n-1)/2} = 2^{n(n+1)/2}$.

Anti-symmetric: again 2^n for the diagonal. For each of the $n(n-1)/2$ unordered off-diagonal pairs there are *three* permitted configurations — (a, b) only, (b, a) only, or neither — the fourth (both) being forbidden. Total $2^n \cdot 3^{n(n-1)/2}$. ■

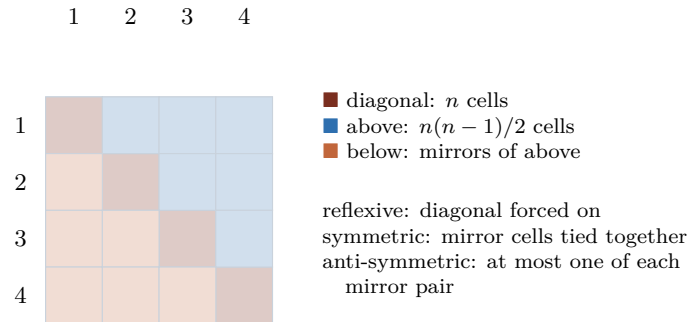


Figure 7.3: The counting argument as a grid. Each property constrains a different part of the $n \times n$ array of cells.

7.5 Combining relations

Relations are sets, so all the set operations apply.

Example 7.6. Let $A = \{1, 2, 3\}$, $B = \{1, 2, 3, 4\}$, $R_1 = \{(1, 1), (2, 2), (3, 3)\}$ and $R_2 = \{(1, 1), (1, 2), (1, 3), (1, 4)\}$.

$$R_1 \cup R_2 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (3, 3)\},$$

$$R_1 \cap R_2 = \{(1, 1)\},$$

$$R_1 - R_2 = \{(2, 2), (3, 3)\},$$

$$R_2 - R_1 = \{(1, 2), (1, 3), (1, 4)\}.$$

Example 7.7 (relations described in words). Let A be all students at UCSC and B all courses. Let R_1 be “ a has taken course b ” and R_2 be “ a requires course b to graduate”. Then

$$R_1 \cup R_2 = \{(a, b) \mid a \text{ has taken } b \text{ or } a \text{ needs } b \text{ to graduate}\},$$

$$R_1 \cap R_2 = \{(a, b) \mid a \text{ has taken } b \text{ and } a \text{ needs } b\},$$

$$R_1 - R_2 = \{(a, b) \mid a \text{ has taken } b \text{ but does not need it}\},$$

$$R_2 - R_1 = \{(a, b) \mid a \text{ needs } b \text{ but has not taken it}\},$$

$$R_1 \triangle R_2 = \text{courses taken-but-not-needed, together with needed-but-not-taken.}$$

The symmetric difference is exactly what a degree audit would flag.

Example 7.8 ($<$ and $>$ on $\mathbb{R}$). With $R_1 = \{(x, y) \mid x < y\}$ and $R_2 = \{(x, y) \mid x > y\}$:

$$R_1 \cup R_2 = \{(x, y) \mid x < y \text{ or } x > y\} = \{(x, y) \mid x \neq y\},$$

$$R_1 \cap R_2 = \{(x, y) \mid x < y \text{ and } x > y\} = \emptyset,$$

$$R_1 - R_2 = R_1, \quad R_2 - R_1 = R_2,$$

$$R_1 \triangle R_2 = R_1 \cup R_2 = \{(x, y) \mid x \neq y\}.$$

7.6 Composition of relations

Definition 7.7 (Composite). Let R be a relation from A to B and S a relation from B to C . The *composite* $S \circ R$ is the relation from A to C given by

$$S \circ R = \{(a, c) \in A \times C \mid \exists b \in B ((a, b) \in R \wedge (b, c) \in S)\}.$$

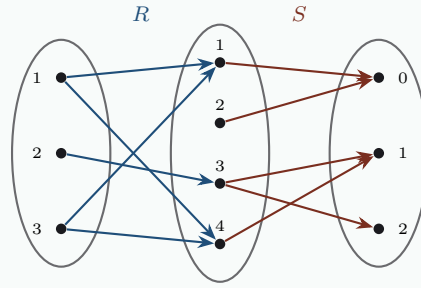
As with functions, the *right-hand* relation is applied *first*: in $S \circ R$ you travel along R and then along S .

Example 7.9 (composition by chasing arrows). R from $\{1, 2, 3\}$ to $\{1, 2, 3, 4\}$ is $R = \{(1, 1), (1, 4), (2, 3), (3, 1), (3, 4)\}$; S from $\{1, 2, 3, 4\}$ to $\{0, 1, 2\}$ is $S = \{(1, 0), (2, 0), (3, 1), (3, 2), (4, 1)\}$.

Solution. Chase each element of R through S :

$$\begin{aligned} (1, 1) \text{ then } (1, 0) &\Rightarrow (1, 0), & (1, 4) \text{ then } (4, 1) &\Rightarrow (1, 1), \\ (2, 3) \text{ then } (3, 1), (3, 2) &\Rightarrow (2, 1), (2, 2), & (3, 1) \text{ then } (1, 0) &\Rightarrow (3, 0), \\ (3, 4) \text{ then } (4, 1) &\Rightarrow (3, 1). \end{aligned}$$

Hence $S \circ R = \{(1, 0), (1, 1), (2, 1), (2, 2), (3, 0), (3, 1)\}$.



Example 7.10 (composition described by a formula). Let $A = \{1, 2, 3, 4\}$ with $D = \{(a, b) \mid b = 5 - a\} = \{(1, 4), (2, 3), (3, 2), (4, 1)\}$ and $S = \{(a, b) \mid a < b\} = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$.

Solution.

$$\begin{aligned} S \circ D &= \{(a, c) \mid \exists b \in A ((a, b) \in D \wedge (b, c) \in S)\} \\ &= \{(a, c) \mid \exists b \in A (b = 5 - a \wedge b < c)\} \\ &= \{(a, c) \mid c > 5 - a\} = \{(a, c) \mid a + c > 5\} \\ &= \{(2, 4), (3, 3), (3, 4), (4, 2), (4, 3), (4, 4)\}. \end{aligned}$$

Working with the defining condition rather than the pair list is much faster when the sets are large.

7.7 Powers of a relation

Definition 7.8. For a relation R on a set A , define recursively

$$R^1 = R, \quad R^{n+1} = R^n \circ R \quad (n \geq 1).$$

So $R^2 = R \circ R$, $R^3 = R^2 \circ R$, and so on.

$(a, b) \in R^n$ means exactly: *there is a path of length n from a to b in the digraph of R .*

Example 7.11. Let $R = \{(1, 1), (2, 1), (3, 2), (4, 3)\}$ on $\{1, 2, 3, 4\}$. Compute the powers.

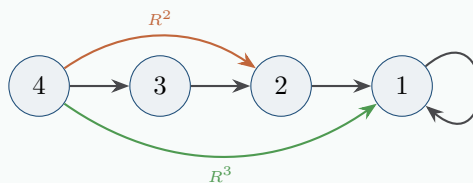
Solution. R is a chain $4 \rightarrow 3 \rightarrow 2 \rightarrow 1$ with a loop at 1.

$$R^2 = \{(1, 1), (2, 1), (3, 1), (4, 2)\},$$

$$R^3 = \{(1, 1), (2, 1), (3, 1), (4, 1)\},$$

$$R^4 = \{(1, 1), (2, 1), (3, 1), (4, 1)\} = R^3,$$

and therefore $R^n = R^3$ for all $n \geq 3$: once every vertex can reach the absorbing loop at 1, nothing changes.



Theorem 7.9. *A relation R on a set A is transitive if and only if $R^n \subseteq R$ for all $n \in \mathbb{Z}^+$.*

Proof. ($\Leftarrow$) Suppose $R^n \subseteq R$ for all n ; in particular $R^2 \subseteq R$. Let $(a, b) \in R$ and $(b, c) \in R$. By the definition of composition, $(a, c) \in R^2$, and since $R^2 \subseteq R$ we get $(a, c) \in R$. Hence R is transitive.

($\Rightarrow$) Suppose R is transitive. We show $R^n \subseteq R$ for all $n \in \mathbb{Z}^+$ by mathematical induction on n .

Base case. $R^1 = R \subseteq R$ trivially.

Inductive step. Assume $R^k \subseteq R$ for some $k \in \mathbb{Z}^+$. Let $(a, b) \in R^{k+1} = R^k \circ R$. Then there exists $x \in A$ with $(a, x) \in R$ and $(x, b) \in R^k$. By the inductive hypothesis $R^k \subseteq R$, so $(x, b) \in R$. Since R is transitive and $(a, x), (x, b) \in R$, we get $(a, b) \in R$. Hence $R^{k+1} \subseteq R$. By induction, $R^n \subseteq R$ for every $n \in \mathbb{Z}^+$. ■

Practical test for transitivity. Compute R^2 and check $R^2 \subseteq R$. If some pair of R^2 is missing from R , that pair *is* your counterexample — and you can read off the intermediate vertex from the composition.

7.8 Functions as relations

Theorem 7.10. *A relation R from A to B is the graph of a function $A \rightarrow B$ if and only if every element of A occurs as the first coordinate of exactly one ordered pair of R .*

Corresponding characterisations. Let R be the graph of $f : A \rightarrow B$.

- f is **one-to-one** $\iff$ every element of B occurs as the second coordinate of *at most one* pair of R .
- f is **onto** $\iff$ every element of B occurs as the second coordinate of *at least one* pair of R .
- f is a **bijection** $\iff$ every element of B occurs as the second coordinate of *exactly one* pair.

So “function”, “injective” and “surjective” are all statements about how many times an element appears as a coordinate.

7.9 Equivalence relations and partial orders

The four properties combine into the two structures that matter most.

Definition 7.11. Let R be a relation on A .

- R is an *equivalence relation* if it is reflexive, symmetric and transitive.
- R is a *partial order* if it is reflexive, anti-symmetric and transitive. The pair (A, R) is then a *poset*.

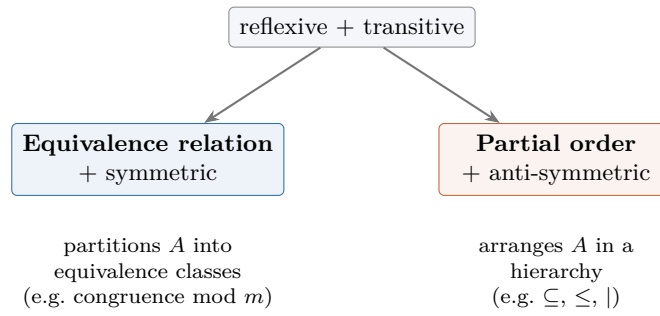


Figure 7.4: The two great families of relations, distinguished only by symmetry versus anti-symmetry.

Example 7.12 (congruence modulo 4). Define S on $\mathbb{Z}$ by $a S b \iff 4 \mid (a - b)$.

Reflexive: $a - a = 0 = 4 \cdot 0$, so $4 \mid (a - a)$.

Symmetric: if $a - b = 4k$ then $b - a = 4(-k)$, so $4 \mid (b - a)$.

Transitive: if $a - b = 4k$ and $b - c = 4m$ then $a - c = (a - b) + (b - c) = 4(k + m)$, so $4 \mid (a - c)$.

Hence S is an **equivalence relation**. It is *not* anti-symmetric: $(1, 5)$ and $(5, 1)$ are both in S but $1 \neq 5$.

Example 7.13 (divisibility on $\mathbb{Z}^+$). Define $a R b \iff a \mid b$.

Reflexive: $a = a \cdot 1$, so $a \mid a$.

Not symmetric: $2 \mid 4$ but $4 \nmid 2$.

Anti-symmetric: if $a \mid b$ and $b \mid a$ with $a, b \in \mathbb{Z}^+$, then $b = ak$ and $a = bm$ for positive integers k, m , so $a = ak m$, giving $km = 1$ and hence $k = m = 1$, i.e. $a = b$.

Transitive: if $b = ak$ and $c = bm$ then $c = a(km)$, so $a \mid c$.

Hence $(\mathbb{Z}^+, |)$ is a **poset**.

On $\mathbb{Z}$ (rather than $\mathbb{Z}^+$) divisibility is **not** anti-symmetric: $2 \mid -2$ and $-2 \mid 2$, yet $2 \neq -2$. The restriction to positive integers matters.

7.9.1 Hasse diagrams

A digraph of a partial order is cluttered with information you already know must be there: every loop (reflexivity) and every shortcut (transitivity). A *Hasse diagram* strips these away.

Constructing a Hasse diagram.

1. Draw the digraph of the partial order.
2. Delete every loop (reflexivity is understood).
3. Delete every edge implied by transitivity (if $a \rightarrow b \rightarrow c$, delete $a \rightarrow c$).
4. Arrange the remaining edges so that all point *upwards*, then delete the arrowheads.

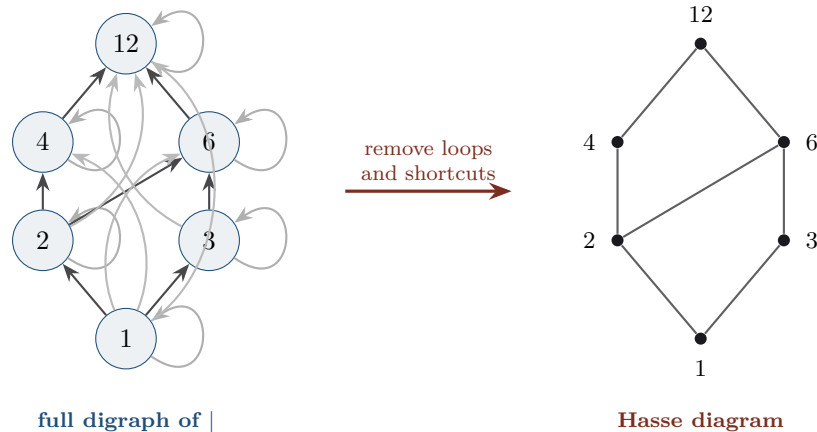


Figure 7.5: The divisibility poset on $\{1, 2, 3, 4, 6, 12\}$. All the information is preserved: $a \mid b$ iff there is an upward path from a to b . Note 2 and 3 are *incomparable* — neither divides the other — which is what makes the order *partial*.

Example 7.14 (the power set as a poset). Figure 5.2 in Chapter 5 is already a Hasse diagram: it depicts $(\mathcal{P}(\{a, b, c\}), \subseteq)$. The bottom element is $\emptyset$, the top is $\{a, b, c\}$, and $\{a\}$ and $\{b\}$ are incomparable.

7.10 n -ary relations

Definition 7.12 (n -ary relation). Let $A_1, A_2, \dots, A_n$ be sets. An n -ary relation on these sets is a subset of $A_1 \times A_2 \times \dots \times A_n$. The sets A_i are the *domains* of the relation and n is its *degree*.

Example 7.15. Let $R = \{(a, b, c) \mid a = 2b \wedge b = 2c, a, b, c \in \mathbb{Z}\}$. The degree of R is 3, so its elements are triples; all three domains are $\mathbb{Z}$. We have $(4, 2, 1) \in R$ (since $4 = 2 \cdot 2$ and $2 = 2 \cdot 1$) but $(2, 4, 8) \notin R$.

Why this matters. A table in a relational database *is* an n -ary relation: the columns are the domains, the degree is the number of columns, and each row is an n -tuple. **SELECT** is projection, **WHERE** is selection, and **JOIN** is a form of composition — so the whole of SQL rests on this definition.

7.11 Chapter summary

- $A \times B$ is the set of ordered pairs; a binary relation from A to B is any subset of it. On a set with n elements there are 2^{n^2} relations.
- Represent a relation as a set of pairs, a zero-one matrix, or a digraph. Digraph signatures: loops everywhere (reflexive), matched arrows (symmetric), no two-way

arrows (anti-symmetric), all shortcuts present (transitive).

- Anti-symmetric $\neq$ not symmetric. A relation can be both, either, or neither. Vacuous anti-symmetry is a valid justification.
- Counting: 2^{n^2-n} reflexive, $2^{n(n+1)/2}$ symmetric, $2^n 3^{n(n-1)/2}$ anti-symmetric relations.
- $S \circ R$ applies R first. $(a, b) \in R^n$ means there is a path of length n from a to b .
- R is transitive $\iff R^2 \subseteq R \iff R^n \subseteq R$ for all $n \geq 1$.
- A relation is a function iff every domain element is a first coordinate exactly once; injectivity and surjectivity are the “at most once” and “at least once” conditions on second coordinates.
- Reflexive + symmetric + transitive = equivalence relation. Reflexive + anti-symmetric + transitive = partial order, drawn as a Hasse diagram.
- n -ary relations are the mathematical content of relational database tables.

CHAPTER 8

Number Theory

What this chapter is for. Number theory studies the integers $\mathbb{Z}$ and, above all, what happens to *remainders*. That single idea — modular arithmetic — underlies hashing, checksums, pseudorandom number generation, and all of public-key cryptography. The chapter is also where every proof technique from Chapter 4 gets serious exercise.

8.1 Divisibility

Definition 8.1 (Divides). Let $a, b \in \mathbb{Z}$ with $a \neq 0$. We say a *divides* b , written $a \mid b$, if there exists $c \in \mathbb{Z}$ with $b = ac$. Then a is a *factor* or *divisor* of b , and b is a *multiple* of a . If no such c exists we write $a \nmid b$. Formally,

$$a \mid b \iff \exists c \in \mathbb{Z} (ac = b).$$

Example 8.1. $3 \nmid 7$, because $7/3$ is not an integer. $3 \mid 12$, because $12 = 3 \cdot 4$.

$a \mid b$ is a **statement**; a/b is a **number**. Do not write “ $a \mid b$ ” when you mean the fraction, and never “divide through” a divisibility statement as if it were an equation. Note also that the roles are the reverse of the fraction: $a \mid b$ means a is the *smaller-role* number.

Theorem 8.2 (Basic facts about division). Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. Then

- (a) if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$;
- (b) if $a \mid b$ then $a \mid bx$ for every $x \in \mathbb{Z}$;
- (c) if $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof. (a) Suppose $a \mid b$ and $a \mid c$. Then there are $s, t \in \mathbb{Z}$ with $b = as$ and $c = at$. Hence

$$b + c = as + at = a(s + t),$$

and $s + t \in \mathbb{Z}$, so $a \mid (b + c)$.

(b) Suppose $a \mid b$, say $b = as$. Then $bx = a(sx)$ with $sx \in \mathbb{Z}$, so $a \mid bx$.

(c) Suppose $b = as$ and $c = bt$. Then $c = (as)t = a(st)$ with $st \in \mathbb{Z}$, so $a \mid c$. ■

Corollary 8.3 (Linear combinations). If $a \mid b$ and $a \mid c$ (with $a \neq 0$), then $a \mid (mb + nc)$ for all $m, n \in \mathbb{Z}$.

Proof. By definition there are $k_1, k_2 \in \mathbb{Z}$ with $b = ak_1$ and $c = ak_2$. Then

$$mb + nc = m(ak_1) + n(ak_2) = a(mk_1 + nk_2) = ak_3,$$

where $k_3 = mk_1 + nk_2 \in \mathbb{Z}$. Hence $a \mid (mb + nc)$. ■

Corollary 8.3 is the workhorse of the chapter: any time you know two things are divisible by a , every integer combination of them is too. It is what makes the Euclidean algorithm and Euclid's proof of the infinitude of primes work.

8.2 The division algorithm

Theorem 8.4 (Division algorithm). *Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Then there exist unique integers q and r with*

$$a = dq + r, \quad 0 \leq r < d.$$

Notation 8.5. a is the *dividend*, d the *divisor*, q the *quotient* and r the *remainder*. We write

$$q = a \text{ div } d, \quad r = a \text{ mod } d.$$

Note $d \mid a$ if and only if $a \text{ mod } d = 0$.

The remainder is never negative. This is the point people get wrong on negative dividends.

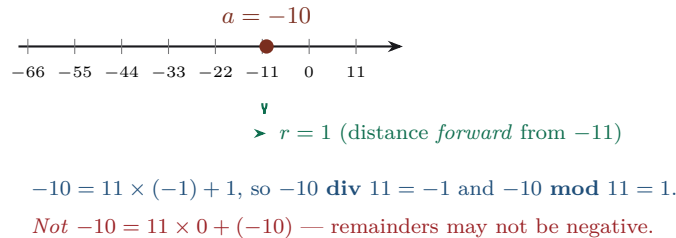


Figure 8.1: The division algorithm on the number line. Slide *down* to the nearest multiple of d at or below a ; the leftover distance is $r \in [0, d)$.

Example 8.2 (positive and negative dividends).

- (a) $101 = 11 \cdot 9 + 2$, so $101 \text{ div } 11 = 9$ and $101 \text{ mod } 11 = 2$.
- (b) $97 = 11 \cdot 8 + 9$, so $97 \text{ div } 11 = 8$ and $97 \text{ mod } 11 = 9$.
- (c) $-11 = 3 \cdot (-4) + 1$, so $-11 \text{ div } 3 = -4$ and $-11 \text{ mod } 3 = 1$. *Not* $-11 = 3 \cdot (-3) - 2$, since $-2 < 0$.
- (d) $-97 = 11 \cdot (-9) + 2$, so $-97 \text{ div } 11 = -9$ and $-97 \text{ mod } 11 = 2$.

8.3 Congruences

Definition 8.6 (Congruence). Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then a is *congruent to b modulo m* , written $a \equiv b \pmod{m}$, if $m \mid (a - b)$. The integer m is the *modulus*. If they are not congruent we write $a \not\equiv b \pmod{m}$.

Example 8.3. Is 17 congruent to 5 modulo 6? We have $17 - 5 = 12 = 6 \cdot 2$, so $6 \mid 12$ and hence $17 \equiv 5 \pmod{6}$.

Theorem 8.7. For $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$,

$$a \equiv b \pmod{m} \iff a \bmod m = b \bmod m.$$

Proof. ($\Rightarrow$) Suppose $a \equiv b \pmod{m}$, so $a - b = km$ for some $k \in \mathbb{Z}$. By the division algorithm write $a = q_1m + r_1$ and $b = q_2m + r_2$ with $0 \leq r_1, r_2 < m$. Subtracting,

$$km = a - b = (q_1 - q_2)m + (r_1 - r_2) \implies r_1 - r_2 = m(k - q_1 + q_2),$$

so $m \mid (r_1 - r_2)$. But $0 \leq r_1, r_2 < m$ forces $|r_1 - r_2| < m$, and the only multiple of m of absolute value less than m is 0. Hence $r_1 = r_2$, i.e. $a \bmod m = b \bmod m$.

($\Leftarrow$) Suppose $a \bmod m = b \bmod m = r$. Then $a = q_1m + r$ and $b = q_2m + r$, so $a - b = (q_1 - q_2)m$, giving $m \mid (a - b)$, i.e. $a \equiv b \pmod{m}$. ■

Theorem 8.8. $a \equiv b \pmod{m}$ if and only if $a = b + km$ for some $k \in \mathbb{Z}$.

Proof. ($\Rightarrow$) If $a \equiv b \pmod{m}$ then $m \mid (a - b)$, so $a - b = km$ for some $k \in \mathbb{Z}$, i.e. $a = b + km$.

($\Leftarrow$) If $a = b + km$ then $a - b = km$, so $m \mid (a - b)$ and $a \equiv b \pmod{m}$. ■

Definition 8.9 (Residue). If $a \equiv b \pmod{m}$ then b is a *residue* of a modulo m . When $0 \leq b < m$, b is the *least non-negative residue* of a modulo m .

8.3.1 Arithmetic with congruences

Theorem 8.10 (Congruences respect $+$ and $\times$). Let $m \in \mathbb{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

- (a) $a + c \equiv b + d \pmod{m}$;
- (b) $ac \equiv bd \pmod{m}$;
- (c) $a^n \equiv b^n \pmod{m}$ for every $n \geq 1$.

Proof. (a) By Theorem 8.8 there are $t, s \in \mathbb{Z}$ with $a = tm + b$ and $c = sm + d$. Adding,

$$a + c = (t + s)m + (b + d),$$

so by Theorem 8.8 again, $a + c \equiv b + d \pmod{m}$.

(b) With the same t, s ,

$$ac = (tm + b)(sm + d) = m(tsm + td + bs) + bd,$$

and $tsm + td + bs \in \mathbb{Z}$, so $ac \equiv bd \pmod{m}$.

(c) Immediate from (b) by induction on n . ■

Corollary 8.11. For $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$:

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m,$$

$$(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m.$$

In particular $a \equiv (a \bmod m) \pmod{m}$ for every a .

This is why modular arithmetic is computationally cheap. You may reduce *at every step* rather than computing a gigantic number and reducing once. It also licenses using *negative* residues, which often shortens the work dramatically: e.g. $9 \equiv -4 \pmod{13}$, and squaring -4 is easier than squaring 9 .

Division is *not* automatically allowed. From $14 \equiv 8 \pmod{6}$ you may *not* cancel the 2: $7 \not\equiv 4 \pmod{6}$. Cancellation needs Theorem 8.23 below and the condition $\gcd(c, m) = 1$.

8.3.2 Fast modular exponentiation

Example 8.4 ($4^{100} \bmod 13$). Compute the least non-negative residue of 4^{100} modulo 13.

Solution. Build up the powers of 2 in the exponent, reducing at each step and using negative residues where convenient:

$$4^2 \equiv 16 \equiv 3 \pmod{13}$$

$$4^4 \equiv 3^2 = 9 \equiv -4 \pmod{13}$$

$$4^8 \equiv (-4)^2 = 16 \equiv 3 \pmod{13}$$

$$4^{16} \equiv 3^2 = 9 \equiv -4 \pmod{13}$$

$$4^{32} \equiv (-4)^2 \equiv 3 \pmod{13}$$

$$4^{64} \equiv 3^2 \equiv -4 \pmod{13}$$

Now $100 = 64 + 32 + 4$, so

$$4^{100} = 4^{64} \cdot 4^{32} \cdot 4^4 \equiv (-4) \cdot 3 \cdot (-4) = 48 \equiv 9 \pmod{13}.$$

Hence $4^{100} \bmod 13 = 9$.

Example 8.5 (Euler's famous factorisation). Prove that $2^{2^5} + 1$ is divisible by 641.

Solution. Note $641 = 640 + 1 = 5 \times 2^7 + 1$, so

$$5 \times 2^7 \equiv -1 \pmod{641}$$

$$(5 \times 2^7)^4 \equiv (-1)^4 = 1 \pmod{641}$$

$$5^4 \times 2^{28} \equiv 1 \pmod{641}.$$

Now $5^4 = 625 \equiv -16 = -2^4 \pmod{641}$, so

$$-2^4 \times 2^{28} \equiv 1 \pmod{641} \implies 2^{32} \equiv -1 \pmod{641}.$$

Therefore $641 \mid (2^{32} + 1) = 2^{2^5} + 1$. (This disproved Fermat's conjecture that all numbers $2^{2^n} + 1$ are prime.)

8.3.3 Arithmetic on $\mathbb{Z}_m$

Definition 8.12. Let $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$. Define

$$a +_m b = (a + b) \bmod m, \quad a \times_m b = (a \times b) \bmod m,$$

for all $a, b \in \mathbb{Z}_m$. These are *addition and multiplication modulo m* .

Example 8.6. In $\mathbb{Z}_{11}$: $8 +_{11} 9 = 17 \bmod 11 = 6$ and $7 \times_{11} 9 = 63 \bmod 11 = 8$.

8.4 Primes

Definition 8.13. An integer $p > 1$ is *prime* if its only positive factors are 1 and p . An integer greater than 1 that is not prime is *composite*.

Theorem 8.14 (Fundamental theorem of arithmetic). *Every integer greater than 1 can be written uniquely as a prime, or as a product of two or more primes, with the prime factors written in non-decreasing order.*

For example $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$.

Theorem 8.15. *If n is composite, then n has a prime divisor $\leq \sqrt{n}$.*

This is what makes trial division practical: to test whether n is prime you need only try divisors up to $\sqrt{n}$. (It is also the contrapositive result proved in Chapter 4: if $n = ab$ then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.)

Theorem 8.16 (Euclid). *There are infinitely many primes.*

Proof by contradiction. Suppose there are only finitely many primes, $p_1, p_2, \dots, p_n$. Let

$$q = p_1 p_2 \cdots p_n + 1.$$

By the fundamental theorem of arithmetic, q is either prime or a product of primes. Suppose some p_j divides q . Since p_j also divides $p_1 p_2 \cdots p_n$, Corollary 8.3 gives

$$p_j \mid (q - p_1 p_2 \cdots p_n) = 1,$$

which is impossible for a prime $p_j > 1$. So no p_j divides q .

Hence there is a prime not in the list $p_1, \dots, p_n$: either q itself (if q is prime) or any prime factor of q . This contradicts the assumption that the list contained all primes. Therefore there are infinitely many primes. ■

The proof does *not* claim q is prime — it usually is not. E.g. $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \times 509$. The claim is only that q 's prime factors are all new.

8.5 Greatest common divisor and least common multiple

Definition 8.17. Let $a, b \in \mathbb{Z}$, not both zero. The *greatest common divisor* $\gcd(a, b)$ is the largest integer d with $d \mid a$ and $d \mid b$.
 a and b are *relatively prime* (coprime) if $\gcd(a, b) = 1$.
Integers $a_1, \dots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.
The *least common multiple* $\text{lcm}(a, b)$ of positive integers a, b is the smallest positive integer divisible by both.

Example 8.7. $\gcd(17, 22) = 1$, so 17 and 22 are relatively prime. The integers 10, 17, 21 are pairwise relatively prime.

From prime factorisations. If $a = p_1^{a_1} p_2^{a_2} \cdots$ and $b = p_1^{b_1} p_2^{b_2} \cdots$ (allowing zero exponents), then

$$\gcd(a, b) = \prod_i p_i^{\min(a_i, b_i)}, \quad \text{lcm}(a, b) = \prod_i p_i^{\max(a_i, b_i)}.$$

Lowest powers for gcd, *highest* powers for lcm.

Example 8.8. $150 = 2 \cdot 3 \cdot 5^2$ and $500 = 2^2 \cdot 5^3$. Hence

$$\gcd(150, 500) = 2^1 \cdot 3^0 \cdot 5^2 = 50, \quad \text{lcm}(150, 500) = 2^2 \cdot 3^1 \cdot 5^3 = 1500.$$

Check: $50 \times 1500 = 75\,000 = 150 \times 500$. ✓

Theorem 8.18. For positive integers a, b :

$$ab = \gcd(a, b) \cdot \text{lcm}(a, b).$$

Idea. For each prime p , $\min(a_i, b_i) + \max(a_i, b_i) = a_i + b_i$; multiplying over all primes gives the result. ■

8.6 The Euclidean algorithm

Factorising large numbers is hard; computing gcds is easy. The reason is the following lemma.

Lemma 8.19. If $a = bq + r$ with $a, b, q, r \in \mathbb{Z}$, then $\gcd(a, b) = \gcd(b, r)$.

Proof. It suffices to show that d is a common divisor of a and b if and only if d is a common divisor of b and r ; the two pairs then have the same set of common divisors and hence the same greatest one.

Suppose $d \mid a$ and $d \mid b$. Then by Corollary 8.3, $d \mid (a - bq) = r$, so d divides both b and r . Conversely suppose $d \mid b$ and $d \mid r$. Then $d \mid (bq + r) = a$, so d divides both a and b . ■

The algorithm. Let $a \geq b > 0$, $r_0 = a$, $r_1 = b$. Apply the division algorithm repeatedly:

$$\begin{aligned} r_0 &= r_1 q_1 + r_2, & 0 \leq r_2 < r_1 \\ r_1 &= r_2 q_2 + r_3, & 0 \leq r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, & 0 \leq r_n < r_{n-1} \\ r_{n-1} &= r_n q_n + 0. \end{aligned}$$

Since $a = r_0 > r_1 > r_2 > \cdots \geq 0$ is a strictly decreasing sequence of non-negative integers, it must terminate. By Lemma 8.19,

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_n, 0) = r_n.$$

$\gcd(a, b)$ is the last non-zero remainder.

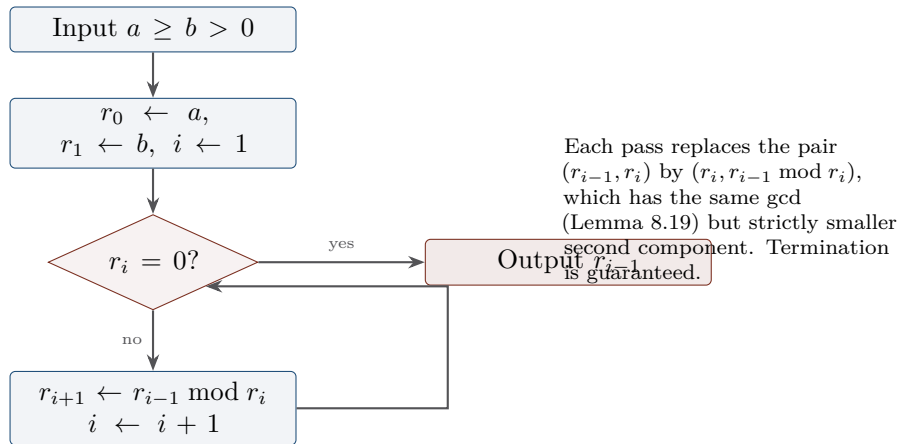


Figure 8.2: The Euclidean algorithm.

Example 8.9 ($\gcd(2415, 945)$).

Solution.

$$\begin{aligned} 2415 &= 945 \times 2 + 525 & \gcd(2415, 945) &= \gcd(945, 525) \\ 945 &= 525 \times 1 + 420 & &= \gcd(525, 420) \\ 525 &= 420 \times 1 + 105 & &= \gcd(420, 105) \\ 420 &= 105 \times 4 + 0. & &= 105 \end{aligned}$$

The last non-zero remainder is 105, so $\gcd(2415, 945) = 105$.

8.7 Bézout's theorem and the extended algorithm

Theorem 8.20 (Bézout). *If a and b are positive integers, then there exist $s, t \in \mathbb{Z}$ with*

$$\gcd(a, b) = sa + tb.$$

The integers s, t are Bézout coefficients and the equation is Bézout's identity.

Back-substitution. Run the Euclidean algorithm forwards, then work *backwards*: start from the equation giving the gcd, and at each stage substitute the previous remainder, always keeping the expression in the form

$$\gcd = (\text{integer}) \times (\text{one number}) + (\text{integer}) \times (\text{the next number}).$$

Never multiply the numbers out — keep them symbolic until the end.

Example 8.10 ($\gcd(252, 198)$ as a linear combination).

Solution. **Forward (Euclidean algorithm):**

$$\begin{aligned} 252 &= 1 \times 198 + 54 \\ 198 &= 3 \times 54 + 36 \\ 54 &= 1 \times 36 + 18 \\ 36 &= 2 \times 18 + 0 \end{aligned} \quad \Longrightarrow \quad \gcd(252, 198) = 18.$$

Backward (substitution):

$$\begin{aligned} 18 &= 54 - 1 \times 36 \\ &= 54 - 1 \times (198 - 3 \times 54) && \text{[substitute 36]} \\ &= 4 \times 54 - 1 \times 198 \\ &= 4 \times (252 - 1 \times 198) - 1 \times 198 && \text{[substitute 54]} \\ &= 4 \times 252 - 5 \times 198. \end{aligned}$$

Hence $\gcd(252, 198) = 18 = 4(252) - 5(198)$, with Bézout coefficients $s = 4$, $t = -5$.

Check: $4 \times 252 = 1008$ and $5 \times 198 = 990$, and $1008 - 990 = 18$. ✓

Lemma 8.21. *If a, b, c are positive integers with $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.*

Lemma 8.22. *If p is prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some i .*

Theorem 8.23 (Cancellation). *Let $m \in \mathbb{Z}^+$ and $a, b, c \in \mathbb{Z}$. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.*

Proof. Since $ac \equiv bc \pmod{m}$ we have $m \mid (ac - bc) = c(a - b)$. Because $\gcd(c, m) = 1$, Lemma 8.21 gives $m \mid (a - b)$, i.e. $a \equiv b \pmod{m}$. ■

The coprimality hypothesis is essential. $14 \equiv 8 \pmod{6}$ holds, but dividing both sides by 2 gives 7 and 4, and $7 \not\equiv 4 \pmod{6}$ — because $\gcd(2, 6) = 2 \neq 1$.

8.8 Linear congruences and modular inverses

Definition 8.24. A congruence $ax \equiv b \pmod{m}$ with $a, b, m \in \mathbb{Z}$, $m > 0$ and x a variable is a *linear congruence*. An integer a' with $a'a \equiv 1 \pmod{m}$ is an *inverse of a modulo m* .

Theorem 8.25. Let $m \geq 2$. If $\gcd(a, m) = 1$, then there is a unique $\bar{a}$ with $a\bar{a} \equiv 1 \pmod{m}$ and $0 < \bar{a} < m$.

Proof. Existence. Since $\gcd(a, m) = 1$, Bézout (Theorem 8.20) gives $s, t \in \mathbb{Z}$ with $sa + tm = 1$. Hence $sa + tm \equiv 1 \pmod{m}$; since $tm \equiv 0 \pmod{m}$, this reduces to $sa \equiv 1 \pmod{m}$. So s is an inverse of a modulo m , and its least positive residue lies in $(0, m)$.

Uniqueness. Suppose b and c are both inverses: $ba \equiv 1 \pmod{m}$ and $ca \equiv 1 \pmod{m}$. Then $ba \equiv ca \pmod{m}$, and since $\gcd(a, m) = 1$, Theorem 8.23 gives $b \equiv c \pmod{m}$. Two residues in $(0, m)$ that are congruent must be equal. ■

Example 8.11 (a small inverse). Find an inverse of 2 modulo 7. We need x with $2x \equiv 1 \pmod{7}$. Since $4 \times 2 = 8 \equiv 1 \pmod{7}$, 4 is an inverse. (So is -3 , since $-3 \times 2 = -6 \equiv 1 \pmod{7}$; the inverse is unique only among residues in $(0, 7)$.)

Example 8.12 (a large inverse via extended Euclid). Find an inverse of 101 modulo 4620.

Solution. Forward:

$$\begin{aligned}
 4620 &= 45 \times 101 + 75 \\
 101 &= 1 \times 75 + 26 \\
 75 &= 2 \times 26 + 23 \\
 26 &= 1 \times 23 + 3 & \gcd(101, 4620) = 1. \\
 23 &= 7 \times 3 + 2 \\
 3 &= 1 \times 2 + 1 \\
 2 &= 2 \times 1 + 0
 \end{aligned}$$

Backward:

$$\begin{aligned}
 1 &= 3 - 1 \times 2 \\
 &= 3 - 1 \times (23 - 7 \times 3) = -1 \times 23 + 8 \times 3 \\
 &= -1 \times 23 + 8 \times (26 - 1 \times 23) = 8 \times 26 - 9 \times 23 \\
 &= 8 \times 26 - 9 \times (75 - 2 \times 26) = -9 \times 75 + 26 \times 26 \\
 &= -9 \times 75 + 26 \times (101 - 1 \times 75) = 26 \times 101 - 35 \times 75 \\
 &= 26 \times 101 - 35 \times (4620 - 45 \times 101) = -35 \times 4620 + 1601 \times 101.
 \end{aligned}$$

So $1601 \times 101 \equiv 1 \pmod{4620}$, and $\bar{101} = 1601$.

Solving $ax \equiv b \pmod{m}$ when $\gcd(a, m) = 1$. Multiply both sides by $\bar{a}$:

$$\bar{a}ax \equiv \bar{a}b \pmod{m} \implies x \equiv \bar{a}b \pmod{m},$$

a single congruence class of solutions.

When $d = \gcd(a, m) > 1$: the congruence has a solution if and only if $d \mid b$, and then it has exactly d incongruent solutions modulo m . Divide the whole congruence (including the modulus) by d , solve the resulting coprime congruence, and generate the d solutions by adding multiples of m/d .

Example 8.13 (solving a linear congruence). Solve $2x \equiv 4 \pmod{7}$.

Solution. $\gcd(2, 7) = 1$, and 4 is an inverse of 2 modulo 7. Multiplying both sides by 4:

$$4 \cdot 2x \equiv 4 \cdot 4 \pmod{7} \implies x \equiv 16 \pmod{7} \equiv 2 \pmod{7}.$$

Verification. If $x \equiv 2 \pmod{7}$ then by Theorem 8.10, $2x \equiv 4 \pmod{7}$. So the solution set is exactly $\{x \in \mathbb{Z} \mid x \equiv 2 \pmod{7}\} = \{\dots, -12, -5, 2, 9, 16, \dots\}$.

8.9 The Chinese remainder theorem

Theorem 8.26 (Chinese remainder theorem). *Let $m_1, m_2, \dots, m_n$ be pairwise relatively prime integers greater than 1, and let $a_1, \dots, a_n$ be arbitrary integers. Then the system*

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \dots, \quad x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$.

Existence. For $k = 1, \dots, n$ let $M_k = m/m_k$. Since the moduli are pairwise coprime, $\gcd(M_k, m_k) = 1$, so by Theorem 8.25 an inverse y_k of M_k modulo m_k exists: $y_k M_k \equiv 1 \pmod{m_k}$. Put

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n.$$

Fix k . For $j \neq k$ we have $m_k \mid M_j$, so $M_j \equiv 0 \pmod{m_k}$ and every term except the k th vanishes modulo m_k . Since $M_k y_k \equiv 1 \pmod{m_k}$,

$$x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}.$$

As k was arbitrary, x solves all n congruences. ■

CRT recipe.

1. $m = m_1 m_2 \cdots m_n$.
2. $M_k = m/m_k$ for each k .
3. $y_k =$ inverse of M_k modulo m_k .
4. $x = \sum_k a_k M_k y_k$, then reduce modulo m .

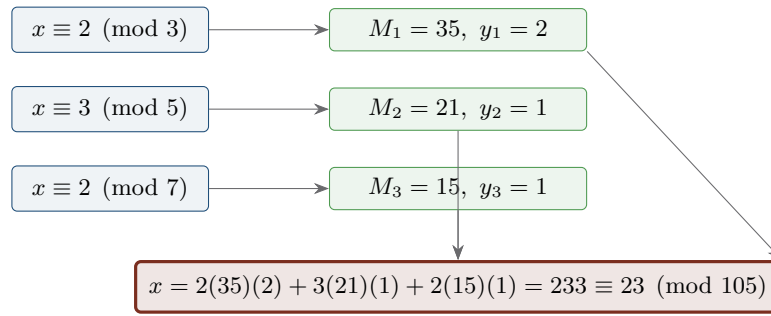


Figure 8.3: The CRT combining three congruences into one.

Example 8.14 (the classical example). Solve

$$x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 2 \pmod{7}.$$

Solution. The moduli 3, 5, 7 are pairwise coprime, so $m = 3 \times 5 \times 7 = 105$ and

$$M_1 = \frac{105}{3} = 35, \quad M_2 = \frac{105}{5} = 21, \quad M_3 = \frac{105}{7} = 15.$$

Inverses:

- $35 \equiv 2 \pmod{3}$ and $2 \times 2 = 4 \equiv 1 \pmod{3}$, so $y_1 = 2$.
- $21 \equiv 1 \pmod{5}$ and $1 \times 1 \equiv 1 \pmod{5}$, so $y_2 = 1$.
- $15 \equiv 1 \pmod{7}$ and $1 \times 1 \equiv 1 \pmod{7}$, so $y_3 = 1$.

Therefore

$$x = 2(35)(2) + 3(21)(1) + 2(15)(1) = 140 + 63 + 30 = 233 \equiv 23 \pmod{105}.$$

Check: $23 = 3 \cdot 7 + 2 \checkmark$; $23 = 5 \cdot 4 + 3 \checkmark$; $23 = 7 \cdot 3 + 2 \checkmark$. The smallest positive solution is 23, and the full solution set is $\{23 + 105k \mid k \in \mathbb{Z}\}$.

8.10 Euler's totient function

Definition 8.27. The *Euler φ -function* $\varphi : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ is defined by

$$\varphi(n) = \#\{k \in \{1, 2, \dots, n\} \mid \gcd(k, n) = 1\},$$

the number of positive integers up to n that are relatively prime to n .

Proposition 8.28. (a) If p is prime, $\varphi(p) = p - 1$.

(b) If p is prime and $n \geq 1$, $\varphi(p^n) = p^n - p^{n-1}$.

(c) If $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$ (multiplicativity).

(d) If $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ is the prime-power factorisation of $n > 1$, then

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_s}\right).$$

Example 8.15 ($\varphi(1000)$). $1000 = 2^3 \cdot 5^3$, so

$$\varphi(1000) = 1000 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 1000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400.$$

Example 8.16 ($\varphi(40)$). $40 = 2^3 \cdot 5$, so $\varphi(40) = 40 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 40 \cdot \frac{1}{2} \cdot \frac{4}{5} = 16$.

8.10.1 Residue systems

Definition 8.29. For $n \in \mathbb{Z}^+$:

- A *complete residue system mod n* is a set of n integers containing exactly one from each congruence class — canonically $\{0, 1, 2, \dots, n-1\}$.
- A *reduced residue system mod n* is a set $\{a_1, \dots, a_{\varphi(n)}\}$ such that (i) $a_i \not\equiv a_j \pmod{n}$ when $i \neq j$, and (ii) $\gcd(a_i, n) = 1$ for each i .

Example 8.17. $\{1, 5, 7, 11\}$ is a reduced residue system mod 12 (indeed $\varphi(12) = 4$). So is $\{-11, 17, 31, -1\}$, since $-11 \equiv 1$, $17 \equiv 5$, $31 \equiv 7$, $-1 \equiv 11 \pmod{12}$.

Lemma 8.30. Let $\varphi(n) = k$ and let $\{a_1, \dots, a_k\}$ be a reduced residue system mod n . Then

- $\{a_1 + mn, a_2 + mn, \dots, a_k + mn\}$ is a reduced residue system mod n for every m ;
- if $\gcd(m, n) = 1$, then $\{ma_1, ma_2, \dots, ma_k\}$ is a reduced residue system mod n .

8.11 Euler's theorem and Fermat's little theorem

Theorem 8.31 (Euler). *Let $n > 0$ and $\gcd(a, n) = 1$. Then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Proof. Let $k = \varphi(n)$ and let $\{a_1, \dots, a_k\}$ be a reduced residue system mod n , with each $a_i \in \{1, \dots, n-1\}$.

Since $\gcd(a, n) = 1$, Lemma 8.30(b) says $\{aa_1, aa_2, \dots, aa_k\}$ is also a reduced residue system mod n . Being the same set of residue classes as the original, the two systems have the same product modulo n :

$$(aa_1)(aa_2) \cdots (aa_k) \equiv a_1 a_2 \cdots a_k \pmod{n}.$$

Factoring out a from each of the k terms on the left,

$$a^k (a_1 a_2 \cdots a_k) \equiv a_1 a_2 \cdots a_k \pmod{n}.$$

Since $\gcd(a_i, n) = 1$ for each i , we have $\gcd(a_1 \cdots a_k, n) = 1$, so Theorem 8.23 lets us cancel the common factor:

$$a^k \equiv 1 \pmod{n}, \quad \text{i.e.} \quad a^{\varphi(n)} \equiv 1 \pmod{n}. \quad \blacksquare$$

Theorem 8.32 (Fermat's little theorem). *Let p be prime and $a \in \mathbb{Z}$ with $p \nmid a$. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Moreover, for every integer a , $a^p \equiv a \pmod{p}$.

Proof. Since $p \nmid a$, the residues $a, 2a, 3a, \dots, (p-1)a$ are all non-zero modulo p and pairwise incongruent, so they are a permutation of $1, 2, \dots, p-1$ modulo p . Multiplying,

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p},$$

that is,

$$a^{p-1} (p-1)! \equiv (p-1)! \pmod{p}.$$

Since p is prime, $\gcd((p-1)!, p) = 1$, so by Theorem 8.23 we may cancel $(p-1)!$ to obtain $a^{p-1} \equiv 1 \pmod{p}$.

(Alternatively: Fermat is the special case $n = p$ of Euler, since $\varphi(p) = p-1$.) $\blacksquare$

How to use these in computation. To evaluate $a^N \pmod{n}$:

1. Check $\gcd(a, n) = 1$.
2. Compute $\varphi(n)$.
3. Write $N = q\varphi(n) + r$ with $0 \leq r < \varphi(n)$.
4. Then $a^N = (a^{\varphi(n)})^q \cdot a^r \equiv 1^q \cdot a^r = a^r \pmod{n}$.

An exponent of a hundred million collapses to one smaller than $\varphi(n)$.

Example 8.18 ($9^{16} \pmod{40}$). $\varphi(40) = 16$ and $\gcd(9, 40) = 1$, so Euler's theorem gives immediately $9^{16} \equiv 1 \pmod{40}$.

Example 8.19 ($7^{222} \bmod 11$).

Solution. 11 is prime and $11 \nmid 7$, so Fermat gives $7^{10} \equiv 1 \pmod{11}$. Write $222 = 22 \times 10 + 2$:

$$7^{222} = (7^{10})^{22} \cdot 7^2 \equiv 1^{22} \cdot 49 \equiv 49 \equiv 5 \pmod{11}.$$

So $7^{222} \bmod 11 = 5$.

Example 8.20 ($7^{222} \bmod 100$).

Solution. $\gcd(7, 100) = 1$ and $100 = 2^2 \cdot 5^2$, so

$$\varphi(100) = 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40.$$

By Euler's theorem $7^{40} \equiv 1 \pmod{100}$. Now $222 = 5 \times 40 + 22$, so

$$7^{222} \equiv (7^{40})^5 \cdot 7^{22} \equiv 7^{22} \pmod{100}.$$

Reduce 7^{22} by repeated squaring modulo 100:

$$\begin{aligned} 7^2 &= 49, & 7^4 &\equiv 49^2 = 2401 \equiv 1, \\ 7^{20} &\equiv (7^4)^5 \equiv 1^5 = 1, & 7^{22} &\equiv 7^{20} \cdot 7^2 \equiv 1 \cdot 49 = 49. \end{aligned}$$

Hence $7^{222} \equiv 49 \pmod{100}$: the last two digits are **49**.

Example 8.21 (solving $15x \equiv 7 \pmod{32}$).

Solution. $\gcd(15, 32) = 1$, so a unique solution class exists. Find the inverse of 15 mod 32 by inspection or extended Euclid: $15 \times 15 = 225 = 7 \times 32 + 1 \equiv 1 \pmod{32}$, so $\overline{15} = 15$. Multiplying both sides by 15,

$$x \equiv 15 \times 7 = 105 = 3 \times 32 + 9 \equiv 9 \pmod{32}.$$

Check: $15 \times 9 = 135 = 4 \times 32 + 7 \equiv 7 \pmod{32}$. ✓

8.12 Applications

Where all this is used.

- **Hashing.** $h(k) = k \bmod m$ distributes keys across m buckets; m prime reduces clustering.
- **Pseudorandom numbers.** Linear congruential generators $x_{n+1} = (ax_n + c) \bmod m$.
- **Check digits.** ISBN and IBAN validity are congruence conditions.
- **Cryptography.** RSA encrypts by $c = M^e \bmod n$ and decrypts by $M = c^d \bmod n$, where $ed \equiv 1 \pmod{\varphi(n)}$. Correctness is *exactly* Euler's theorem; security rests on the difficulty of computing $\varphi(n)$ without factoring n .

8.13 Chapter summary

- $a \mid b \iff \exists c (b = ac)$. Divisibility is preserved under integer linear combinations (Corollary 8.3).
- Division algorithm: unique q, r with $a = dq + r$, $0 \leq r < d$. Remainders are never negative.
- $a \equiv b \pmod{m} \iff m \mid (a - b) \iff a \bmod m = b \bmod m \iff a = b + km$.
- Congruences may be added, multiplied and raised to powers; they may be *divided* only when the cancelled factor is coprime to the modulus.
- There are infinitely many primes (Euclid); every $n > 1$ factors uniquely into primes; a composite n has a prime factor $\leq \sqrt{n}$.
- gcd from lowest prime powers, lcm from highest; $ab = \gcd(a, b) \operatorname{lcm}(a, b)$.
- Euclidean algorithm: gcd is the last non-zero remainder. Run it backwards for Bézout coefficients s, t with $\gcd(a, b) = sa + tb$.
- a has an inverse mod m iff $\gcd(a, m) = 1$; find it with extended Euclid. Then $ax \equiv b \pmod{m}$ has the unique solution $x \equiv \bar{a}b \pmod{m}$.
- CRT: pairwise coprime moduli give a unique solution mod $m = \prod m_i$, via $x = \sum a_k M_k y_k$.
- Euler: $a^{\varphi(n)} \equiv 1 \pmod{n}$ when $\gcd(a, n) = 1$. Fermat is the prime case $a^{p-1} \equiv 1 \pmod{p}$. Both collapse huge exponents.

Part III Worked Solutions and Reference Tables

APPENDIX A

Worked Solutions: Tutorials 01–04

Solutions are written at the level of detail expected in a submitted answer. Where a question asks you to “determine” or “decide”, the reasoning is given in full, not just the verdict. Cross-references point back to the chapter where the technique was introduced.

A.1 Tutorial 01 — Propositional Logic

1. What is meant by a “proposition”? A declarative sentence that is either true or false, but not both (Chapter 1). Two conditions: it must declare a fact (not ask or command), and its truth value must be determinate.

2. Which are propositions?

	Proposition?	Reason / truth value
(a) Do not pass go.	No	Imperative.
(b) What time is it?	No	Interrogative.
(c) $4 + x = 5$.	No	Truth value depends on x .
(d) The moon is made of green cheese.	Yes	False.
(e) $2^n \geq 100$.	No	Depends on n .

3. Negations.

- (a) Steve does *not* have more than 100 GB free disk space on his laptop (i.e. he has at most 100 GB free).
- (b) Steve does not block emails and texts from Jennifer. (Reading the original as the single act “blocks emails-and-texts”. If it is read as a conjunction $b_e \wedge b_t$, De Morgan gives “Steve does not block emails from Jennifer or he does not block texts from her”.)
- (c) Jennifer did not send more than 100 text messages yesterday (she sent at most 100).
- (d) Jennifer did not ride her bicycle 100 miles on Sunday.

4. Are these propositions? (a) Yes, false. (b) No, imperative. (c) Yes, true. (d) No, contains a free variable. (e) No, interrogative.

5. p = “the election is decided”, q = “the votes have been counted”.

(a) $\neg p$	The election is not decided.
(b) $p \vee q$	The election is decided or the votes have been counted (or both).
(c) $\neg p \wedge q$	The election is not decided but the votes have been counted.
(d) $q \rightarrow p$	If the votes have been counted, then the election is decided.
(e) $\neg q \rightarrow \neg p$	If the votes have not been counted, then the election is not decided.
(f) $\neg p \rightarrow \neg q$	If the election is not decided, then the votes have not been counted.
(g) $p \leftrightarrow q$	The election is decided if and only if the votes have been counted.
(h) $\neg q \vee (\neg p \wedge q)$	Either the votes have not been counted, or the election is not decided but the votes have been counted.

6. Well-formed formulas? (a) $p \vee q$ — **yes**. (b) $\neg(p \rightarrow (q \wedge p))$ — **yes**. (c) $\neg(p \rightarrow (q = p))$ — **no**: “=” is not a logical connective. (d) $\neg(\blacklozenge(q \vee p))$ — **no**: undefined symbol. (e) $(p \wedge \neg q) \vee (q \rightarrow r)$ — **yes**. (f) $p \neg r$ — **no**: no binary connective between p and $\neg r$.

7. Does $v(p) = \mathbf{F}$, $v(q) = \mathbf{T}$, $v(r) = \mathbf{T}$ satisfy ...?

- (a) $(p \rightarrow \neg q) \vee \neg(r \wedge q)$: $p \rightarrow \neg q = \mathbf{F} \rightarrow \mathbf{F} = \mathbf{T}$. Whole formula **T. Satisfied**.
 (b) $(\neg p \vee \neg q) \rightarrow (p \vee \neg r)$: antecedent = $\mathbf{T} \vee \mathbf{F} = \mathbf{T}$; consequent = $\mathbf{F} \vee \mathbf{F} = \mathbf{F}$. Formula = **F. Not satisfied**.
 (c) $\neg(\neg p \rightarrow \neg q) \wedge r$: $\neg p \rightarrow \neg q = \mathbf{T} \rightarrow \mathbf{F} = \mathbf{F}$, so $\neg(\cdot) = \mathbf{T}$; and $r = \mathbf{T}$. Formula = **T. Satisfied**.
 (d) $\neg(\neg p \rightarrow (q \wedge \neg r))$: $q \wedge \neg r = \mathbf{T} \wedge \mathbf{F} = \mathbf{F}$; $\neg p \rightarrow \mathbf{F} = \mathbf{T} \rightarrow \mathbf{F} = \mathbf{F}$; negating gives **T. Satisfied**.

8. Truth table of $(p \vee q) \wedge \neg(p \wedge q)$.

p	q	$p \vee q$	$p \wedge q$	$\neg(p \wedge q)$	$(p \vee q) \wedge \neg(p \wedge q)$
0	0	0	0	1	0
0	1	1	0	1	1
1	0	1	0	1	1
1	1	1	1	0	0

This is exactly $p \oplus q$.

9. $p = \mathbf{A}$ on final, $q = \mathbf{every\ exercise}$, $r = \mathbf{A\ in\ class}$. (a) $r \wedge \neg q$. (b) $p \wedge q \wedge r$. (c) $r \rightarrow p$. (d) $p \wedge \neg q \wedge r$. (e) $(p \wedge q) \rightarrow r$. (f) $r \leftrightarrow (q \vee p)$.

10. Inclusive or exclusive? (a) Inclusive — knowing both languages is not disqualifying. (b) Exclusive — you choose one. (c) Inclusive — having both documents is fine. (d) Inclusive in form (both can happen), though used exclusively in rhetoric.

11. Rewrite as “if and only if”. (a) You buy an ice cream cone if and only if it is hot outside. (b) The trains run late if and only if I take them.

12. Converse, contrapositive, inverse.

(a) “If it snows tonight, then I will stay at home.”

Converse If I stay at home tonight, then it will snow.

Contrapositive If I do not stay at home tonight, then it will not snow.

Inverse If it does not snow tonight, then I will not stay at home.

(b) “I go to the beach whenever it is a sunny summer day,” i.e. $s \rightarrow b$.

Converse If I go to the beach, then it is a sunny summer day.

Contrapositive If I do not go to the beach, then it is not a sunny summer day.

Inverse If it is not a sunny summer day, then I do not go to the beach.

(c) “When I stay up late, it is necessary that I sleep until noon,” i.e. $l \rightarrow n$.

Converse If I sleep until noon, then I stayed up late.

Contrapositive If I do not sleep until noon, then I did not stay up late.

Inverse If I do not stay up late, then I do not sleep until noon.

13. Truth tables.

p	q	(a) $p \wedge \neg p$	(b) $(p \vee \neg q) \rightarrow q$	(c) $p \oplus (p \vee q)$	(d) $(p \leftrightarrow q) \oplus (p \leftrightarrow \neg q)$
0	0	0	0	0	1
0	1	0	1	1	1
1	0	0	0	0	1
1	1	0	1	0	1

(a) is a contradiction; (d) is a tautology — $p \leftrightarrow q$ and $p \leftrightarrow \neg q$ always disagree.

p	q	r	(e) $p \rightarrow (\neg q \vee r)$	(f) $(p \rightarrow q) \wedge (\neg p \rightarrow r)$	(g) $(p \leftrightarrow q) \vee (\neg q \leftrightarrow r)$
0	0	0	1	0	1
0	0	1	1	1	1
0	1	0	1	0	1
0	1	1	1	1	0
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	0	1	1
1	1	1	1	1	1

(g) is a *contingency*: it fails exactly in the two bold rows $(p, q, r) = (\mathbf{F}, \mathbf{T}, \mathbf{T})$ and $(\mathbf{T}, \mathbf{F}, \mathbf{F})$, where $p \neq q$ makes the first disjunct false and $\neg q \neq r$ makes the second false too.

14. Is $(\neg p \vee q) \wedge (q \rightarrow (\neg r \wedge \neg p)) \wedge (p \vee r)$ satisfiable? Take $p = \mathbf{F}$, $q = \mathbf{F}$, $r = \mathbf{T}$. Then $\neg p \vee q = \mathbf{T} \vee \mathbf{F} = \mathbf{T}$; the second conjunct has a false hypothesis so is vacuously $\mathbf{T}$; and $p \vee r = \mathbf{F} \vee \mathbf{T} = \mathbf{T}$. All three conjuncts hold, so the formula is **satisfiable**. (It is not a tautology: $p = \mathbf{T}$, $q = \mathbf{T}$ makes the second conjunct false.)

15. Tautology, satisfiable, or unsatisfiable?

	Verdict	Reason
(a) $((p \rightarrow q) \wedge \neg q) \rightarrow \neg p$	Tautology	This is modus tollens; the antecedent is true only when p is false.
(b) $(p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r))$	Tautology	Standard axiom of propositional logic (distribution of $\rightarrow$).
(c) $((p \vee q) \rightarrow r) \vee p \vee q$	Tautology	If $p \vee q$ is false the first disjunct is vacuously true; if true, the last two cover it.
(d) $(p \vee q) \wedge (p \rightarrow (r \wedge q)) \wedge (q \rightarrow (\neg r \wedge p))$	Unsat.	Suppose it is true. If p holds then $r \wedge q$ holds, so q holds, so $\neg r \wedge p$ holds — giving $r \wedge \neg r$. If p fails then $p \vee q$ forces q , so $\neg r \wedge p$ holds, contradicting $\neg p$. No assignment survives.
(e) $(p \rightarrow q) \rightarrow (p \rightarrow \neg q)$	Satisfiable (contin- gency)	True at $p = \mathbf{F}$; false at $p = \mathbf{T}, q = \mathbf{T}$.
(f) $(\neg p \rightarrow q) \vee ((p \wedge \neg r) \leftrightarrow q)$	Tautology	If $p \vee q$ holds, the first disjunct is true. If both p and q are false, then $p \wedge \neg r$ is false and q is false, so the biconditional is true. All 8 rows check out.
(g) $(p \vee q) \wedge (\neg q \wedge \neg p)$	Unsatisfiable	$\neg q \wedge \neg p$ forces both false, killing $p \vee q$. (By De Morgan the second conjunct is $\neg(p \vee q)$.)

16. Logical consequences and equivalences.

	Correct?	Justification
(a) $(p \rightarrow q) \models \neg p \rightarrow \neg q$	No	Counterexample $p = \mathbf{F}, q = \mathbf{T}$: premise $\mathbf{T}$, conclusion $\mathbf{T} \rightarrow \mathbf{F} = \mathbf{F}$. (This is the inverse fallacy.)
(b) $p \rightarrow (q \wedge r) \models (p \rightarrow q) \rightarrow r$	No	$p = \mathbf{F}, q = \mathbf{F}, r = \mathbf{F}$: premise $\mathbf{T}$; $(p \rightarrow q) = \mathbf{T}$ so conclusion $= \mathbf{T} \rightarrow \mathbf{F} = \mathbf{F}$.
(c) $(p \rightarrow q) \wedge \neg q \models \neg p$	Yes	Modus tollens.
(d) $p \vee (\neg q \wedge r) \models (q \vee \neg r) \rightarrow p$	Yes	If the premise holds and p is false, then $\neg q \wedge r$ holds, so q is false and r is true, making $q \vee \neg r$ false and the conclusion vacuously true. If p is true the conclusion is trivially true.
(e) $(p \vee q) \wedge (\neg p \rightarrow \neg q) \equiv p$	Yes	$\neg p \rightarrow \neg q \equiv q \rightarrow p$; with $p \vee q$ this forces p . Conversely p makes both conjuncts true.
(f) $(p \wedge q) \vee r \equiv (p \rightarrow \neg q) \rightarrow r$	Yes	$(p \rightarrow \neg q) \rightarrow r \equiv \neg(\neg p \vee \neg q) \vee r \equiv (p \wedge q) \vee r$.
(g) $(p \vee q) \wedge (\neg p \rightarrow \neg q) \equiv q$	No	By (e) the left side is p , and $p \not\equiv q$ (take $p = \mathbf{T}, q = \mathbf{F}$).
(h) $((p \rightarrow q) \rightarrow q) \rightarrow q \equiv p \rightarrow q$	Yes	Both sides are false exactly when $p = \mathbf{T}, q = \mathbf{F}$; check the other three rows.

17. $p = \text{Paola happy}, q = \text{Paola paints}, r = \text{Renzo happy}$. (a) $(p \wedge q) \rightarrow \neg r$. (b) $p \rightarrow q$. (c) $p \rightarrow q$ ("only if" puts q on the right).

18. $p = \text{Aldo is Italian}, q = \text{Bob is English}$. (a) $\neg p$. (b) $p \wedge q$. (c) $p \rightarrow \neg q$. (d) $p \vee (\neg p \rightarrow q)$. (e) $(p \wedge q) \vee (\neg p \wedge \neg q)$, i.e. $p \leftrightarrow q$.

19. $p, q, r = \text{Aldo} / \text{Bruno} / \text{Carlo passed}$.

(a)	$\neg p \wedge \neg q \wedge r$
(b)	$\neg p \wedge q \wedge r$
(c)	$(p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r)$
(d)	$p \vee q \vee r$
(e)	$(p \wedge q) \vee (p \wedge r) \vee (q \wedge r)$
(f)	$\neg(p \wedge q \wedge r)$
(g)	$[(p \wedge q) \vee (p \wedge r) \vee (q \wedge r)] \wedge \neg(p \wedge q \wedge r)$

20. $p, q, r, s = \text{Angelo} / \text{Bruno} / \text{Carlo} / \text{Davide come}$.

(a)	$s \rightarrow (q \wedge r)$
(b)	$r \rightarrow (\neg p \wedge \neg q)$
(c)	$s \leftrightarrow (r \wedge \neg p)$
(d)	$s \rightarrow (\neg r \rightarrow p)$
(e)	$(\neg s \rightarrow r) \wedge (s \rightarrow \neg q)$
(f)	$p \rightarrow ((\neg q \wedge \neg r) \rightarrow s)$
(g)	$[(p \wedge q \wedge r) \leftrightarrow \neg s] \wedge [(\neg p \wedge \neg q) \rightarrow (s \rightarrow r)]$

21. DNF and CNF. See Chapter 1. A DNF is a disjunction of elementary products, e.g. $(p \wedge q) \vee (\neg p \wedge r)$. A CNF is a conjunction of elementary sums, e.g. $(p \vee q) \wedge (\neg p \vee r)$.

22. Normal forms. Method: eliminate $\leftrightarrow$ and $\rightarrow$, push negations inwards, distribute.

(a) $\neg[(\neg p \rightarrow q) \rightarrow r] \equiv \neg[\neg(p \vee q) \vee r] \equiv (p \vee q) \wedge \neg r$ (CNF; DNF is $(p \wedge \neg r) \vee (q \wedge \neg r)$).

(b) $p \rightarrow (q \wedge r) \equiv \neg p \vee (q \wedge r) \equiv (\neg p \vee q) \wedge (\neg p \vee r)$ (CNF); DNF is $\neg p \vee (q \wedge r)$.

(c) For $(p \wedge r) \leftrightarrow (\neg q \vee r)$,

$$\begin{aligned} &\equiv [(p \wedge r) \wedge (\neg q \vee r)] \vee [\neg(p \wedge r) \wedge \neg(\neg q \vee r)] \\ &\equiv (p \wedge r) \vee (q \wedge \neg r) \quad (\text{DNF}), \end{aligned}$$

since $(p \wedge r) \rightarrow (\neg q \vee r)$ always holds.

(d) $\neg[(\neg p \rightarrow \neg q) \wedge \neg r] \equiv (p \wedge \neg q) \vee r$ (DNF), using $\neg(\neg p \rightarrow \neg q) \equiv \neg p \wedge q$ — take care with the double negation.

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

(f) $(p \rightarrow (\neg q \wedge r)) \wedge (p \rightarrow \neg q) \equiv p \rightarrow (\neg q \wedge r) \equiv \neg p \vee (\neg q \wedge r)$; CNF: $(\neg p \vee \neg q) \wedge (\neg p \vee r)$.

(g) $\neg[(p \rightarrow q) \rightarrow ((q \rightarrow r) \rightarrow (p \rightarrow r))]$ **F**, because the inner formula is the hypothetical-syllogism tautology. Its DNF/CNF is the contradiction.

(h) $[(p \rightarrow (\neg q \rightarrow r)) \wedge (p \rightarrow \neg q)] \rightarrow (p \rightarrow r) \equiv \mathbf{T}$: assuming p and the two premises yields $\neg q$ and hence r .

A.2 Tutorial 02 — Predicate Logic

1. $P(x)$: “ x is a perfect square”, domain $\mathbb{Z}$. (a) $P(9)$: true ($9 = 3^2$). (b) $P(0)$: true ($0 = 0^2$). (c) $P(-4)$: false (no integer squares to a negative). (d) $P(2)$: false.

2. if $P(x)$ then $x := x*2$, $P(x)$: $x^2 > 10$. (a) $x = 3$: $9 > 10$ false, so x stays 3.

(b) $x = 4$: $16 > 10$ true, so x becomes 8.

(c) $x = -2$: $4 > 10$ false, so x stays -2 .

3. Quantified translations. (a) With $T(x)$ = “ x has travelled by train”, domain all students in the university:

(i) $\forall x T(x)$: every student has travelled by train.

(ii) $\exists x T(x)$: some student has travelled by train.

(iii) $\exists x \neg T(x)$: some student has not travelled by train.

(iv) $\neg \forall x T(x)$: not every student has travelled by train — logically the same as (iii).

(b) Domain all animals:

- (i) $\forall x (F(x) \rightarrow S(x))$: every fish can swim.
(ii) $\exists x (F(x) \wedge \neg S(x))$: there is a fish that cannot swim.

- 4. L, P, C over software engineering students in the class.** (a) $\forall x (P(x) \vee C(x))$.
(b) $\exists x (L(x) \wedge P(x) \wedge \neg C(x))$.
(c) $\neg \exists x (L(x) \wedge P(x) \wedge C(x))$, equivalently $\forall x \neg (L(x) \wedge P(x) \wedge C(x))$.
(d) $\exists x L(x) \wedge \exists x P(x) \wedge \exists x C(x)$.

5. Domain $\{-3, -1, 1, 3, 5\}$, expand without quantifiers.

- (a) $Q(-3) \vee Q(-1) \vee Q(1) \vee Q(3) \vee Q(5)$
(b) $Q(-3) \wedge Q(-1) \wedge Q(1) \wedge Q(3) \wedge Q(5)$
(c) $Q(1) \wedge Q(3) \wedge Q(5)$ (only 1, 3, 5 are > 0 ; the others make the hypothesis false)
(d) $\neg Q(-3) \vee \neg Q(-1) \vee \neg Q(3) \vee \neg Q(5)$

6. Domains making each statement true / false.

Statement	True over	False over
$\forall x (x < x^2)$	$\{2, 3, 4\}$	$\{0\}$ or $\{1\}$
$\exists x (x + x = x)$	$\{0, 1\}$	$\mathbb{Z}^+$
$\forall x \forall y (x \cdot y = 1)$	$\{1\}$	$\{1, 2\}$

7. Two domains. Write $L(x) = "x \text{ is in your lecture hall}"$, and E, A, B, U for the four properties.

	Domain = lecture hall	Domain = all people
(a)	$\exists x E(x)$	$\exists x (L(x) \wedge E(x))$
(b)	$\forall x A(x)$	$\forall x (L(x) \rightarrow A(x))$
(c)	$\exists x \neg B(x)$	$\exists x (L(x) \wedge \neg B(x))$
(d)	$\forall x U(x)$	$\forall x (L(x) \rightarrow U(x))$

8. Properties of propositions, formalised. Let the domain be compound propositions, with $\text{Tau}(x)$, $\text{Con}(x)$, $\text{Cont}(x)$, $\text{Cond}(x)$ meaning tautology / contradiction / contingency / conditional.

- (a) $\forall x \forall y (\text{Cont}(x) \wedge \text{Con}(y) \rightarrow \text{Con}(x \wedge y))$.
(b) $\forall x \forall y (\text{Tau}(x) \wedge \text{Tau}(y) \rightarrow \text{Tau}(x \vee y))$.
(c) $\exists x (\text{Cond}(x) \wedge \text{Cont}(x))$.

- 9. Truth sets.** (a) $\{x \in \mathbb{R} \mid x^2 - 5x + 6 = 0\} = \{2, 3\}$ (since $(x - 2)(x - 3) = 0$).
(b) $\{x \in \mathbb{Z}^+ \mid 2x + 1 < 7\} = \{x \in \mathbb{Z}^+ \mid x < 3\} = \{1, 2\}$.
(c) $\{x \in \mathbb{Z} \mid x^2 < 0\} = \emptyset$.

10. M, E, O, P over $\mathbb{Z}$. (a) $\forall x (M(x) \rightarrow E(x))$.

(b) $\exists x (\neg E(x) \wedge \neg M(x))$.

(c) $\forall x (\neg E(x) \rightarrow O(x))$.

(d) $\forall x (E(x) \wedge P(x) \rightarrow x = 2)$.

11. Are these equivalent?

(a) $\exists x (P(x) \wedge Q(x))$ vs. $\exists x P(x) \wedge \exists x Q(x)$: **not equivalent**. The first implies the second, but not conversely. *Counterexample*: domain $\mathbb{Z}^+$, P = “is prime”, Q = “is composite”. Then $\exists x P \wedge \exists x Q$ is true (2 and 4), yet $\exists x (P \wedge Q)$ is false.

(b) $\forall x (P(x) \rightarrow Q(x))$ vs. $\forall x P(x) \rightarrow \forall x Q(x)$: **not equivalent**. *Counterexample*: domain $\mathbb{Z}$, P = “even”, Q = “odd”. The right-hand side is vacuously true (its hypothesis is false), the left-hand side is false at $x = 2$.

12. Proofs of the two valid distributions. See the theorem and proof in Chapter 2. Briefly:

(a) $\forall x (P(x) \wedge Q(x))$ holds iff $P(a) \wedge Q(a)$ for all a , iff $(P(a) \text{ for all } a)$ and $(Q(a) \text{ for all } a)$, iff $\forall x P(x) \wedge \forall x Q(x)$.

(b) $\exists x (P(x) \vee Q(x))$ holds iff $P(a) \vee Q(a)$ for some a , iff $(P(a) \text{ for some } a)$ or $(Q(a) \text{ for some } a)$, iff $\exists x P(x) \vee \exists x Q(x)$.

13. Nested quantifiers over $\mathbb{R}$. (a) $\exists z \forall x (x + z = x)$.

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

(c) $\forall x \forall y \forall z (x(y + z) = xy + xz)$.

14. $W(x, y)$ = “ x has watched movie y ”. (a) $\exists x \forall y W(x, y)$: *there is a student who has watched every movie ever released*.

(b) $\forall y \exists x W(x, y)$: *every movie has been watched by at least one student in the class*.

The order is decisive. (a) demands a single hyper-cinephile; (b) allows a different student for each film. (a) implies (b), never the reverse.

15. Negations with $\neg$ pushed inside.

$$(a) \neg \forall x \exists y (x \cdot y > x) \equiv \exists x \forall y (x \cdot y \leq x),$$

$$(b) \neg \exists x \forall y (x + y = y) \equiv \forall x \exists y (x + y \neq y),$$

$$(c) \neg \forall x \exists y (P(x, y) \rightarrow Q(x, y)) \equiv \exists x \forall y (P(x, y) \wedge \neg Q(x, y)).$$

A.3 Tutorial 03 — Arguments

1. “If George does not have eight legs, then he is not a spider. George is a spider. Therefore George has eight legs.” Let e = “George has eight legs”, s = “George is a spider”. Form:

$$\neg e \rightarrow \neg s, \quad s \quad \therefore \quad e.$$

This is **valid** — it is modus tollens applied to $\neg e \rightarrow \neg s$ with $\neg(\neg s) = s$:

1	$\neg e \rightarrow \neg s$	Premise
2	$s \rightarrow e$	Contrapositive of (1)
3	s	Premise
4	e	Modus ponens, (2),(3)

Yes: if the premises are true, the conclusion is true.

2. “If Nimal does not study hard, then he will not pass. Nimal passed. Therefore Nimal studied hard.” Let h = “studies hard”, p = “passes”. Form $\neg h \rightarrow \neg p$, $p \therefore h$. **Valid** — modus tollens: from $\neg h \rightarrow \neg p$ and p (i.e. $\neg\neg p$) we get $\neg\neg h$, i.e. h .

3. “No man is an island. Manhattan is an island. Therefore Manhattan is not a man.” Let $M(x)$ = “ x is a man”, $I(x)$ = “ x is an island”. Premises $\forall x (M(x) \rightarrow \neg I(x))$ and $I(\text{Manhattan})$.

Rules used: **universal instantiation** (to get $M(m) \rightarrow \neg I(m)$ for $m = \text{Manhattan}$), then **modus tollens** with $I(m)$ to conclude $\neg M(m)$.

4. Which rule of inference?

(a) Kangaroos live in Australia <i>and</i> are marsupials $\therefore$ marsupials	Simplification
(b) $p \vee q$, $\neg p \therefore q$	Disjunctive syllogism
(c) p , $p \rightarrow q \therefore q$	Modus ponens
(d) $p \therefore p \vee q$	Addition
(e) $p \rightarrow q$, $q \rightarrow r \therefore p \rightarrow r$	Hypothetical syllogism

5. Sailing race. Let r = “it rains”, f = “it is foggy”, s = “the sailing race is held”, l = “the lifesaving demonstration goes on”, t = “the trophy is awarded”. Premises:

$$(\neg r \vee \neg f) \rightarrow (s \wedge l), \quad s \rightarrow t, \quad \neg t.$$

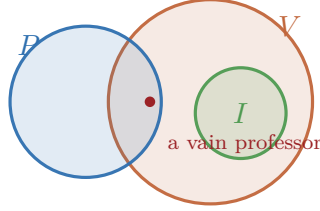
1	$\neg t$	Premise
2	$s \rightarrow t$	Premise
3	$\neg s$	Modus tollens, (1),(2)
4	$\neg s \vee \neg l$	Addition, (3)
5	$\neg(s \wedge l)$	De Morgan, (4)
6	$(\neg r \vee \neg f) \rightarrow (s \wedge l)$	Premise
7	$\neg(\neg r \vee \neg f)$	Modus tollens, (5),(6)
8	$r \wedge f$	De Morgan, (7)
9	r	Simplification, (8)

Hence **it rained** — and, as a bonus, it was foggy.

6. “No professors are ignorant. All ignorant people are vain. Therefore no professors are vain.” Form:

$$\forall x (P(x) \rightarrow \neg I(x)), \quad \forall x (I(x) \rightarrow V(x)) \quad \therefore \quad \forall x (P(x) \rightarrow \neg V(x)).$$

Invalid. Countermodel: let P and V overlap while I is disjoint from P .



Here no professor is ignorant ✓; all ignorant people are vain ✓; but the marked element is a professor who *is* vain, falsifying the conclusion.

7. Graph theory enrolment. Domain: CS students at UCSC. $F(x)$ = first year, $T(x)$ = third year, $G(x)$ = enrolled in graph theory. Premises

$$\forall x ((F(x) \vee T(x)) \rightarrow \neg G(x)), \quad G(n)$$

where n = Nimal; conclusion $\neg T(n)$.

1	$\forall x ((F(x) \vee T(x)) \rightarrow \neg G(x))$	Premise
2	$(F(n) \vee T(n)) \rightarrow \neg G(n)$	Universal instantiation, (1)
3	$G(n)$	Premise
4	$\neg \neg G(n)$	Double negation, (3)
5	$\neg (F(n) \vee T(n))$	Modus tollens, (2),(4)
6	$\neg F(n) \wedge \neg T(n)$	De Morgan, (5)
7	$\neg T(n)$	Simplification, (6)

Valid.

8. Alan at the park. Let a, b, c, d = Alan / Bill / Chandra / Denesh is at the park, and f = “today is Friday”, t = “today is Saturday”. Premises:

$$(c \wedge \neg b) \rightarrow a, \quad (f \vee t) \rightarrow c, \quad b \rightarrow d, \quad f \rightarrow \neg d, \quad f.$$

1	f	Premise
2	$f \rightarrow \neg d$	Premise
3	$\neg d$	Modus ponens, (1),(2)
4	$b \rightarrow d$	Premise
5	$\neg b$	Modus tollens, (3),(4)
6	$f \vee t$	Addition, (1)
7	$(f \vee t) \rightarrow c$	Premise
8	c	Modus ponens, (6),(7)
9	$c \wedge \neg b$	Conjunction, (8),(5)
10	$(c \wedge \neg b) \rightarrow a$	Premise
11	a	Modus ponens, (9),(10)

Valid: Alan will be at the park.

9. $p \rightarrow (q \wedge r), s \rightarrow r, r \rightarrow p \therefore s \rightarrow q$.

1	$s \rightarrow r$	Premise
2	$r \rightarrow p$	Premise
3	$s \rightarrow p$	Hypothetical syllogism, (1),(2)
4	$p \rightarrow (q \wedge r)$	Premise
5	$s \rightarrow (q \wedge r)$	Hypothetical syllogism, (3),(4)
6	$(q \wedge r) \rightarrow q$	Simplification (as a tautology)
7	$s \rightarrow q$	Hypothetical syllogism, (5),(6)

Valid.

10. **Giraffes, bears and rabbits.** b = bears are brown, g = giraffes are green, r = rabbits are red.

- (i) Symbolic argument: $g \rightarrow (b \vee \neg r), r \wedge \neg b \therefore \neg g$.
(ii) As one proposition: $[(g \rightarrow (b \vee \neg r)) \wedge (r \wedge \neg b)] \rightarrow \neg g$.
(iii) Truth table (columns: $P_1 = g \rightarrow (b \vee \neg r), P_2 = r \wedge \neg b, C = \neg g$):

b	g	r	$b \vee \neg r$	P_1	P_2	$(P_1 \wedge P_2) \rightarrow C$
0	0	0	1	1	0	1
0	0	1	0	1	1	1
0	1	0	1	1	0	1
0	1	1	0	0	1	1
1	0	0	1	1	0	1
1	0	1	1	1	0	1
1	1	0	1	1	0	1
1	1	1	1	1	0	1

- (iv) The last column is all 1s, so the argument is **valid**. (Directly: $r \wedge \neg b$ makes $b \vee \neg r$ false, and then $g \rightarrow \mathbf{F}$ forces $\neg g$ — modus tollens.)

A.4 Tutorial 04 — Sets, Functions, Relations, Number Theory

Sets

1. $(A - B) \cup (A - C) = A - (B \cap C)$, **three ways.** (i) **Usual method (double inclusion).** Let $x \in (A - B) \cup (A - C)$. Then $x \in A - B$ or $x \in A - C$, i.e. $(x \in A \text{ and } x \notin B)$ or $(x \in A \text{ and } x \notin C)$. In either case $x \in A$, and $x \notin B$ or $x \notin C$, i.e. $\neg(x \in B \wedge x \in C)$, i.e. $x \notin B \cap C$. So $x \in A - (B \cap C)$.

Conversely let $x \in A - (B \cap C)$: then $x \in A$ and $x \notin B \cap C$, so $x \notin B$ or $x \notin C$, giving $x \in A - B$ or $x \in A - C$. Both inclusions hold, so the sets are equal.

(ii) **Set-builder method.**

$$\begin{aligned}
 (A - B) \cup (A - C) &= \{x \mid (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C)\} \\
 &= \{x \mid x \in A \wedge (x \notin B \vee x \notin C)\} && \text{distributive} \\
 &= \{x \mid x \in A \wedge \neg(x \in B \wedge x \in C)\} && \text{De Morgan} \\
 &= \{x \mid x \in A \wedge x \notin B \cap C\} = A - (B \cap C).
 \end{aligned}$$

(iii) Set identities.

$$\begin{aligned}
(A - B) \cup (A - C) &= (A \cap \overline{B}) \cup (A \cap \overline{C}) & (X - Y &= X \cap \overline{Y}) \\
&= A \cap (\overline{B} \cup \overline{C}) & \text{distributive} \\
&= A \cap \overline{B \cap C} & \text{De Morgan} \\
&= A - (B \cap C) & (X \cap \overline{Y} &= X - Y).
\end{aligned}$$

2. Δ is associative; odd-membership. Encode membership by bits: for x , let $\alpha = [x \in A]$, $\beta = [x \in B]$, $\gamma = [x \in C]$ in $\{0, 1\}$. Then $x \in A \Delta B$ iff $\alpha \oplus \beta = 1$. Since $\oplus$ is associative on $\{0, 1\}$,

$$(\alpha \oplus \beta) \oplus \gamma = \alpha \oplus (\beta \oplus \gamma),$$

so $(A \Delta B) \Delta C = A \Delta (B \Delta C)$.

Moreover $\alpha \oplus \beta \oplus \gamma = 1$ exactly when an *odd* number of α, β, γ equal 1. Hence $x \in A \Delta B \Delta C$ iff x belongs to an odd number (one or three) of A, B, C .

3. $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$; when does $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$? For the first:

$$S \in \mathcal{P}(A \cap B) \iff S \subseteq A \cap B \iff (S \subseteq A) \wedge (S \subseteq B) \iff S \in \mathcal{P}(A) \wedge S \in \mathcal{P}(B).$$

For the second, the inclusion $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$ always holds.

Sufficiency. If $A \subseteq B$ then $A \cup B = B$ and $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(B)$, so equality holds. Symmetrically if $B \subseteq A$.

Necessity. Suppose $A \not\subseteq B$ and $B \not\subseteq A$. Pick $a \in A - B$ and $b \in B - A$. Then $\{a, b\} \subseteq A \cup B$, so $\{a, b\} \in \mathcal{P}(A \cup B)$; but $\{a, b\} \not\subseteq A$ (as $b \notin A$) and $\{a, b\} \not\subseteq B$ (as $a \notin B$), so $\{a, b\} \notin \mathcal{P}(A) \cup \mathcal{P}(B)$.

Conclusion: $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$ if and only if $A \subseteq B$ or $B \subseteq A$.

4. $A_n = \{k \in \mathbb{Z} : n \mid k\}$. $\bigcap_{n=1}^{\infty} A_n = \{k \in \mathbb{Z} \mid \forall n \geq 1, n \mid k\}$. If $k \neq 0$, take $n = |k| + 1 > |k|$: then $n \nmid k$. And 0 is divisible by every n . Hence the intersection is $\{0\}$.

$\bigcup_{n=2}^{\infty} A_n = \{k \in \mathbb{Z} \mid \exists n \geq 2, n \mid k\}$. Every k with $|k| \geq 2$ is divisible by itself; 0 is divisible by 2. But $k = 1$ and $k = -1$ have no divisor ≥ 2 . Hence the union is $\mathbb{Z} - \{1, -1\}$.

5. $U = \{1, \dots, 16\}$; bit strings.

$$\begin{aligned}
A = \{2, 4, 6, 8, 10, 12, 14, 16\} &\rightarrow 0101010101010101 \\
B = \{3, 6, 9, 12, 15\} &\rightarrow 0010010010010010 \\
C = \{2, 3, 5, 7, 11, 13\} &\rightarrow 0110101000101000
\end{aligned}$$

(b) Bitwise.

$$\begin{aligned}
A \vee B &= 0111010111010111 \\
\neg C &= 1001010111010111 \\
(A \cup B) - C &= (A \vee B) \wedge \neg C = 0001010111010111 \\
A \oplus B &= 0111000111000111
\end{aligned}$$

(c) Decoded. $(A \cup B) - C = \{4, 6, 8, 9, 10, 12, 14, 15, 16\}$ and $A \Delta B = \{2, 3, 4, 8, 9, 10, 14, 15, 16\}$.

6. Inclusion–exclusion.

- (a) $|A \cup B \cup C| = 28 + 24 + 19 - 11 - 8 - 7 + 4 = \mathbf{49}$.
 (b) Number of subsets $= 2^{49}$.
 (c) Subsets containing all 4 elements of $A \cap B \cap C$: the other $49 - 4 = 45$ elements are free, giving 2^{45} .

7. Truth sets over $\mathbb{Z}$. $P(x)$: $2 \mid (x^2 - x)$. Since $x^2 - x = x(x - 1)$ is a product of consecutive integers, one factor is even; so P holds for *every* integer. Truth set $= \mathbb{Z}$.

$Q(x)$: $4 \mid x$. Truth set $= \{4k \mid k \in \mathbb{Z}\} = 4\mathbb{Z}$.

$R(x)$: $x^2 \equiv 0$ or $1 \pmod{4}$. If $x = 2k$ then $x^2 = 4k^2 \equiv 0$; if $x = 2k + 1$ then $x^2 = 4(k^2 + k) + 1 \equiv 1$. So R holds for every integer; truth set $= \mathbb{Z}$.

Do P and R have the same truth set? Yes, both are $\mathbb{Z}$, proved above by cases on the parity of x .

8. Prove or give the smallest counterexample.

- (a) $\mathcal{P}(A - B) = \mathcal{P}(A) - \mathcal{P}(B)$ is **false**. Smallest counterexample: $A = B = \emptyset$. Then $A - B = \emptyset$ so LHS $= \{\emptyset\}$, while $\mathcal{P}(A) - \mathcal{P}(B) = \{\emptyset\} - \{\emptyset\} = \emptyset$. (The empty set is always in the left side but never in the right when $\emptyset \in \mathcal{P}(B)$, which is always.)
 (b) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$ is **true**. In membership bits, $\alpha \wedge (\beta \oplus \gamma) = (\alpha \wedge \beta) \oplus (\alpha \wedge \gamma)$, i.e. $\wedge$ distributes over $\oplus$. (Check all 8 rows.)
 (c) “ $A \cup C = B \cup C \Rightarrow A = B$ ” is **false**. Smallest counterexample: $A = \emptyset$, $B = C = \{1\}$. Then $A \cup C = \{1\} = B \cup C$ but $A \neq B$.
 (d) “ $A \cap C = B \cap C$ and $A \cup C = B \cup C \Rightarrow A = B$ ” is **true**. Let $x \in A$. If $x \in C$ then $x \in A \cap C = B \cap C \subseteq B$. If $x \notin C$ then $x \in A \cup C = B \cup C$, and since $x \notin C$ we get $x \in B$. So $A \subseteq B$; by symmetry $B \subseteq A$.

Proof techniques

9. $5 \mid (n^5 - n)$ for every $n \in \mathbb{Z}$. Work modulo 5; the complete residue system is $\{0, 1, 2, 3, 4\}$.

$n \bmod 5$	n^2	n^4	$n^5 - n = n(n^4 - 1)$
0	0	0	$0 \cdot (\cdot) \equiv 0$
1	1	1	$1(1 - 1) \equiv 0$
2	4	$16 \equiv 1$	$2(1 - 1) \equiv 0$
3	$9 \equiv 4$	$16 \equiv 1$	$3(1 - 1) \equiv 0$
4	$16 \equiv 1$	1	$4(1 - 1) \equiv 0$

In all five cases $n^5 - n \equiv 0 \pmod{5}$. The cases are exhaustive, so $5 \mid (n^5 - n)$ for every integer n .

10. If $3 \mid n^2$ then $3 \mid n$. Original: $\forall n \in \mathbb{Z} (3 \mid n^2 \rightarrow 3 \mid n)$. **Contrapositive:** $\forall n \in \mathbb{Z} (3 \nmid n \rightarrow 3 \nmid n^2)$.

Proof of the contrapositive. Suppose $3 \nmid n$. By the division algorithm $n = 3k + 1$ or $n = 3k + 2$ for some $k \in \mathbb{Z}$.

- If $n = 3k + 1$: $n^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$, so $n^2 \equiv 1 \pmod{3}$.

- If $n = 3k + 2$: $n^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$, so again $n^2 \equiv 1 \pmod{3}$.

In both cases n^2 leaves remainder 1, so $3 \nmid n^2$. The key fact about residues mod 3 is that a non-multiple of 3 squares to something $\equiv 1$.

11. $\sqrt{p}$ is irrational for p prime. Suppose not: $\sqrt{p} = a/b$ with $a, b \in \mathbb{Z}$, $b \neq 0$, $\gcd(a, b) = 1$. Then $a^2 = pb^2$, so $p \mid a^2$.

Why $p \mid a^2$ implies $p \mid a$: $a^2 = a \cdot a$, so by Lemma 8.22 (a prime dividing a product divides a factor), $p \mid a$. Write $a = pk$.

Then $pb^2 = a^2 = p^2k^2$, so $b^2 = pk^2$, giving $p \mid b^2$ and hence $p \mid b$. But then $p \mid \gcd(a, b) = 1$, impossible for a prime $p \geq 2$. Contradiction; therefore $\sqrt{p}$ is irrational.

12. n odd $\iff n^2$ odd $\iff n^3$ odd. Prove the cycle (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (a).

(a) $\Rightarrow$ (b): $n = 2k + 1 \Rightarrow n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, odd.

(b) $\Rightarrow$ (c): if n^2 is odd then (by the contrapositive argument of Chapter 4) n is odd, say $n = 2k + 1$; then $n^3 = n^2 \cdot n$ is a product of two odd numbers, hence odd (explicitly $n^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$).

(c) $\Rightarrow$ (a), by contraposition: if n is even, $n = 2k$, then $n^3 = 8k^3 = 2(4k^3)$ is even.

A cycle of implications proves equivalence because any $p_i \rightarrow p_j$ follows by chaining round the cycle using hypothetical syllogism.

13. $|x + y| \leq |x| + |y|$. Recall $|t| = t$ if $t \geq 0$ and $-t$ if $t < 0$; in particular $t \leq |t|$ and $-t \leq |t|$ always.

Case 1: $x + y \geq 0$. Then $|x + y| = x + y \leq |x| + |y|$, using $x \leq |x|$ and $y \leq |y|$.

Case 2: $x + y < 0$. Then $|x + y| = -(x + y) = (-x) + (-y) \leq |x| + |y|$, using $-x \leq |x|$ and $-y \leq |y|$.

The two cases are exhaustive, so the inequality holds for all real x, y .

14. Uniqueness in the division algorithm. Suppose $a = q_1d + r_1 = q_2d + r_2$ with $d > 0$ and $0 \leq r_1, r_2 < d$. Subtracting,

$$(q_1 - q_2)d = r_2 - r_1.$$

From $0 \leq r_1 < d$ and $0 \leq r_2 < d$ we get $-d < r_2 - r_1 < d$, so $|(q_1 - q_2)d| < d$. Since $d > 0$ this forces $|q_1 - q_2| < 1$, and as $q_1 - q_2 \in \mathbb{Z}$ we conclude $q_1 = q_2$. Then $r_2 - r_1 = 0$, i.e. $r_1 = r_2$.

Where the bounds are used: precisely in deducing $|r_2 - r_1| < d$, which is what pins the integer $q_1 - q_2$ to zero. Without the bounds infinitely many representations exist.

15. Existence proofs.

(a) **Constructive:** $1729 = 1^3 + 12^3 = 9^3 + 10^3$.

(b) **Non-constructive:** consider $\sqrt{2}^{\sqrt{2}}$. If it is rational take $x = y = \sqrt{2}$; if irrational take $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$, whence $x^y = \sqrt{2}^2 = 2$.

It is non-constructive because the argument splits on a disjunction whose truth we never settle: at the end we know a suitable pair exists but cannot say which of the two candidate pairs it is.

16. Diagnosing a flawed proof. The student writes: “ $n^2 = 2k$, so $n = 2(k/n)$, hence n is even.”

Flaws. (i) k/n need not be an integer, so “ $n = 2 \times \text{integer}$ ” is unjustified — the definition of even requires an *integer* witness. (ii) Division by n is illegitimate when $n = 0$ (and in any case leaves the integrality question open).

Repair — proof by contraposition is the natural choice, because the negation of the conclusion (“ n is odd”) gives an explicit form $n = 2m + 1$ to compute with, whereas the hypothesis “ $n^2 = 2k$ ” gives nothing to substitute.

Proof. Suppose n is odd, $n = 2m + 1$. Then $n^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$ is odd. Contrapositively, if n^2 is even then n is even.

Functions

17. $f : \mathbb{Z} \rightarrow \mathbb{Z}$, $f(n) = n^2 + n$.

- (a) **Not one-to-one:** $f(0) = 0 = f(-1)$ and $0 \neq -1$.
- (b) **Not onto:** $f(n) = n(n+1)$ is a product of consecutive integers, hence always even and ≥ 0 ; so 1 (indeed any odd or any negative integer) has no pre-image.
- (c) $m \in \text{Range}(f)$ iff $n^2 + n - m = 0$ has an integer root. Completing the square, $4m + 1 = (2n + 1)^2$. So if $m = f(n)$ then $4m + 1$ is the square of the odd integer $2n + 1$. Conversely if $4m + 1 = (2t + 1)^2$ for an integer t , then $4m = 4t^2 + 4t$, i.e. $m = t^2 + t = f(t)$.

18. $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = (x - 2)^2 - 3$.

- (a) **Not one-to-one:** $f(1) = f(3) = -2$. **Not onto:** $(x - 2)^2 \geq 0$ so $f(x) \geq -3$; the value -4 is never attained.
- (b) Restrict to $f : [2, \infty) \rightarrow [-3, \infty)$. *Injective:* if $(x - 2)^2 = (y - 2)^2$ with $x, y \geq 2$, then $x - 2, y - 2 \geq 0$, so taking non-negative square roots gives $x - 2 = y - 2$, i.e. $x = y$. *Surjective:* for $y \geq -3$ put $x = 2 + \sqrt{y + 3} \geq 2$; then $f(x) = (\sqrt{y + 3})^2 - 3 = y$.
- (c) $f^{-1}(y) = 2 + \sqrt{y + 3}$. Check both ways:

$$f^{-1}(f(x)) = 2 + \sqrt{(x - 2)^2} = 2 + (x - 2) = x \quad (x \geq 2),$$

$$f(f^{-1}(y)) = (2 + \sqrt{y + 3} - 2)^2 - 3 = (y + 3) - 3 = y \quad (y \geq -3).$$

19. $f(x) = 3x - 5$, $g(x) = (x + 5)/3$ on $\mathbb{R}$.

- (a) $(f \circ g)(x) = 3\left(\frac{x+5}{3}\right) - 5 = x$; $(g \circ f)(x) = \frac{(3x-5)+5}{3} = x$.
- (b) Both composites are the identity, so for every y , $f(g(y)) = y$ shows f is onto, and $g(f(x)) = x$ shows f is one-to-one. Hence f is a bijection and, by uniqueness of inverses, $g = f^{-1}$.
- (c) In general a one-sided identity is not enough: g could be a left inverse without being a right inverse (this happens when f is injective but not surjective). Checking both compositions rules that out.

20. Composition and the two properties.

- (a) If $g \circ f$ is one-to-one then f is: suppose $f(a) = f(b)$; applying g gives $(g \circ f)(a) = (g \circ f)(b)$, hence $a = b$.

- (b) If $g \circ f$ is onto then g is: given $c \in C$ there is a with $g(f(a)) = c$, so $b = f(a)$ satisfies $g(b) = c$.
- (c) **Counterexamples for the converses.** Take $A = \{1\}$, $B = \{1, 2\}$, $C = \{1\}$, $f(1) = 1$, $g(1) = g(2) = 1$. Then $g \circ f$ is a bijection $A \rightarrow C$; but g is *not* one-to-one and f is *not* onto.

21. Images of unions and intersections. Parts (a) and (b) are proved as theorems in Chapter 6.

- (c) *If f is one-to-one then equality holds:* let $y \in f(S) \cap f(T)$, so $y = f(s) = f(t)$ with $s \in S$, $t \in T$; injectivity gives $s = t \in S \cap T$, so $y \in f(S \cap T)$.

If equality always holds then f is one-to-one: suppose $f(a) = f(b)$ with $a \neq b$. Take $S = \{a\}$, $T = \{b\}$. Then $f(S \cap T) = f(\emptyset) = \emptyset$, while $f(S) \cap f(T) = \{f(a)\} \neq \emptyset$ — contradicting equality. Hence f must be injective.

22. Floor and ceiling identities.

- (a) $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$: by definition $\lfloor x \rfloor$ is the largest integer $\leq x$, so $\lfloor x \rfloor \leq x$; and if $x \geq \lfloor x \rfloor + 1$ then $\lfloor x \rfloor + 1$ would be a larger integer $\leq x$, a contradiction.
- (b) $\lceil x \rceil = -\lfloor -x \rfloor$: let $m = \lfloor -x \rfloor$, so $m \leq -x < m + 1$. Negating (which reverses inequalities), $-m - 1 < x \leq -m$. Thus $-m$ is an integer $\geq x$, and no smaller integer is $\geq x$ (since $-m - 1 < x$). Hence $\lceil x \rceil = -m = -\lfloor -x \rfloor$.
- (c) If $x \in \mathbb{Z}$ then $\lfloor x \rfloor = x$, $\lfloor -x \rfloor = -x$, sum 0. If $x \notin \mathbb{Z}$ then $\lfloor x \rfloor < x < \lfloor x \rfloor + 1$ strictly; writing $m = \lfloor x \rfloor$, negation gives $-m - 1 < -x < -m$, so $\lfloor -x \rfloor = -m - 1$ and the sum is $m + (-m - 1) = -1$.

23. Partial function $h(n) = 12/(n - 3)$.

- (a) Domain of definition: $n - 3$ must be a non-zero divisor of 12, so $n - 3 \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$, giving
- $$\{-9, -3, -1, 0, 1, 2, 4, 5, 6, 7, 9, 15\}.$$
- (b) Range: the corresponding values $12/(n - 3)$ are $\{-1, -2, -3, -4, -6, -12, 12, 6, 4, 3, 2, 1\}$, i.e. $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$.
- (c) **One-to-one** on its domain of definition: if $12/(m - 3) = 12/(n - 3)$ then $m - 3 = n - 3$, so $m = n$.
- (d) Two total extensions: (i) $h_1(n) = h(n)$ where defined and $h_1(n) = 0$ otherwise; (ii) $h_2(n) = h(n)$ where defined and $h_2(n) = n$ otherwise. Both are functions $\mathbb{Z} \rightarrow \mathbb{Z}$.

24. Finite sets of equal size. Let $|A| = |B| = n$ and $f : A \rightarrow B$.

- (a) $\Rightarrow$ (b): if f is one-to-one, the n images are distinct, so $|f(A)| = n = |B|$; a subset of B with $|B|$ elements must equal B , so f is onto.
- (b) $\Rightarrow$ (a): if f is onto, $|f(A)| = n$; but $f(A)$ has at most $|A| = n$ elements, with equality only if no two inputs collide. So f is one-to-one.
- (a) $\wedge$ (b) $\Leftrightarrow$ (c) is the definition of bijection.

Finiteness is essential because the counting step “ $|f(A)| = |A|$ unless two inputs collide” has no infinite analogue. Indeed $f : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$, $f(n) = n + 1$, is injective but not surjective.

Relations

25. Counting relations on an n -element set. Consider the $n \times n$ grid of cells (a, b) .

- (a) All relations: each of the n^2 cells is independently in or out: 2^{n^2} .
- (b) Reflexive: the n diagonal cells are forced in; the remaining $n^2 - n$ are free: 2^{n^2-n} .
- (c) Symmetric: n free diagonal cells, and the $n(n-1)/2$ mirror pairs must agree: $2^n \cdot 2^{n(n-1)/2} = 2^{n(n+1)/2}$.
- (d) Anti-symmetric: 2^n for the diagonal, and for each of the $n(n-1)/2$ mirror pairs there are 3 allowed configurations ((a, b) only, (b, a) only, neither): $2^n \cdot 3^{n(n-1)/2}$.

26. $aRb \iff a \mid b$ on $\mathbb{Z}^+$. **Reflexive:** $a = a \cdot 1$, so $a \mid a$. ✓

Not symmetric: $2 \mid 4$ but $4 \nmid 2$.

Anti-symmetric: if $b = ak$ and $a = bm$ with $k, m \in \mathbb{Z}^+$ then $a = akm$, so $km = 1$, hence $k = m = 1$ and $a = b$. ✓

Transitive: $b = ak$ and $c = bm$ give $c = a(km)$, so $a \mid c$. ✓

So $(\mathbb{Z}^+, \mid)$ is a partial order.

27. $aRb \iff 2 \mid (a - b)$; $aSb \iff 3 \mid (a - b)$ on $\mathbb{Z}$.

- (a) Both are equivalence relations (reflexive, symmetric, transitive) — the proof for modulus m is in Chapter 7. Neither is anti-symmetric: $(0, 2), (2, 0) \in R$ with $0 \neq 2$; $(0, 3), (3, 0) \in S$ with $0 \neq 3$.
- (b) $R \cap S = \{(a, b) \mid 2 \mid (a - b) \wedge 3 \mid (a - b)\} = \{(a, b) \mid 6 \mid (a - b)\}$, congruence modulo 6 (since $\gcd(2, 3) = 1$).
 $R \cup S = \{(a, b) \mid 2 \mid (a - b) \text{ or } 3 \mid (a - b)\}$.
 $R - S = \{(a, b) \mid 2 \mid (a - b) \text{ and } 3 \nmid (a - b)\}$.
- (c) $R \cap S$ is congruence mod 6, hence reflexive, symmetric, transitive, not anti-symmetric (e.g. $(0, 6), (6, 0)$).
 $R \cup S$ is reflexive and symmetric but **not transitive**: $(0, 2) \in R$ and $(2, 5) \in S$ (since $3 \mid -3$), yet $0 - 5 = -5$ is divisible by neither 2 nor 3, so $(0, 5) \notin R \cup S$. It is not anti-symmetric either (same example as above).

28. $aRb \iff a^2 \leq b^2$ on $\mathbb{R}$. **Reflexive:** $a^2 \leq a^2$. ✓

Not symmetric: $1R2$ (as $1 \leq 4$) but not $2R1$.

Not anti-symmetric: $1R(-1)$ and $(-1)R1$ (both give $1 \leq 1$) yet $1 \neq -1$. This example isolates the failure precisely: distinct numbers with equal squares.

Transitive: $a^2 \leq b^2$ and $b^2 \leq c^2$ give $a^2 \leq c^2$. ✓

29. $S \circ R$. $R = \{(1, a), (1, b), (2, b), (3, c), (4, a)\}$, $S = \{(a, 0), (b, 0), (b, 1), (c, 1)\}$.

$$\begin{array}{lll}
 1 \rightarrow a \rightarrow 0, & 1 \rightarrow b \rightarrow 0, 1 & \Rightarrow (1, 0), (1, 1) \\
 2 \rightarrow b \rightarrow 0, 1 & & \Rightarrow (2, 0), (2, 1) \\
 3 \rightarrow c \rightarrow 1 & & \Rightarrow (3, 1) \\
 4 \rightarrow a \rightarrow 0 & & \Rightarrow (4, 0)
 \end{array}$$

So $S \circ R = \{(1, 0), (1, 1), (2, 0), (2, 1), (3, 1), (4, 0)\}$, with domain $\{1, 2, 3, 4\}$ and range $\{0, 1\}$.

30. Powers of $R = \{(1, 2), (2, 3), (3, 1), (3, 4), (4, 4)\}$ on $\{1, 2, 3, 4\}$.

$$R^2 = \{(1, 3), (2, 1), (2, 4), (3, 2), (3, 4), (4, 4)\},$$

$$R^3 = \{(1, 1), (1, 4), (2, 2), (2, 4), (3, 3), (3, 4), (4, 4)\},$$

$$R^4 = \{(1, 2), (1, 4), (2, 3), (2, 4), (3, 1), (3, 4), (4, 4)\}.$$

R is **not transitive**: $(1, 2), (2, 3) \in R$ but $(1, 3) \notin R$ — equivalently $R^2 \not\subseteq R$.

$(a, b) \in R^n$ means there is a directed path of length exactly n from a to b in the digraph of R .

31. R transitive $\iff R^2 \subseteq R$, and induction. See the theorem and its proof in Chapter 7. The inductive step: assuming $R^k \subseteq R$, take $(a, b) \in R^{k+1} = R^k \circ R$; then $(a, x) \in R$ and $(x, b) \in R^k \subseteq R$ for some x , so transitivity gives $(a, b) \in R$.

32. Ordered-pair characterisations.

- (a) $R \subseteq A \times B$ is the graph of a function iff every $a \in A$ is the first coordinate of exactly one pair. ($\Rightarrow$) A function assigns exactly one value to each a , giving exactly one pair. ($\Leftarrow$) Define $f(a)$ to be the unique b with $(a, b) \in R$; totality and single-valuedness are precisely the “exactly one” condition.
- (b) One-to-one $\iff$ every $b \in B$ is the second coordinate of *at most one* pair. If two pairs $(a_1, b), (a_2, b)$ existed with $a_1 \neq a_2$ then $f(a_1) = f(a_2)$, contradicting injectivity; conversely a collision produces two such pairs.
- (c) Onto $\iff$ every $b \in B$ is the second coordinate of *at least one* pair.

Number theory

33. Division algorithm for -2027 by 37 . $37 \times 55 = 2035 > 2027$ and $37 \times 54 = 1998$, so $2027 = 37 \times 54 + 29$. Hence

$$-2027 = -37 \times 54 - 29 = 37 \times (-55) + (37 - 29) = 37 \times (-55) + 8.$$

So $q = -55$ and $r = 8$, with $0 \leq 8 < 37$. *Check:* $37 \times (-55) = -2035$ and $-2035 + 8 = -2027$.
✓

A representation with a negative remainder, e.g. $-2027 = 37 \times (-54) + (-29)$, is *not* the division-algorithm representation because the theorem requires $0 \leq r < d$; that requirement is exactly what makes q and r unique.

34. $a \equiv b \pmod{m} \iff a \bmod m = b \bmod m$, and an application. The proof is Theorem 8.7 in Chapter 8.

Application: is $2^{50} + 3^{50} \equiv 0 \pmod{5}$? By Fermat, $2^4 \equiv 1$ and $3^4 \equiv 1 \pmod{5}$. Since $50 = 4 \times 12 + 2$,

$$2^{50} \equiv 2^2 = 4, \quad 3^{50} \equiv 3^2 = 9 \equiv 4 \pmod{5},$$

so $2^{50} + 3^{50} \equiv 8 \equiv 3 \pmod{5}$. Hence $2^{50} + 3^{50} \not\equiv 0 \pmod{5}$.

(If the expression is instead read as the plain sum $250 + 350 = 600$, then $600 = 5 \times 120$ and the congruence *does* hold. State which reading you are using.)

35. gcd(10672, 4147) and Bézout. Euclidean algorithm:

$$\begin{aligned}
10672 &= 2 \times 4147 + 2378 \\
4147 &= 1 \times 2378 + 1769 \\
2378 &= 1 \times 1769 + 609 \\
1769 &= 2 \times 609 + 551 & \text{gcd} = \mathbf{29}. \\
609 &= 1 \times 551 + 58 \\
551 &= 9 \times 58 + 29 \\
58 &= 2 \times 29 + 0
\end{aligned}$$

Back-substitution:

$$\begin{aligned}
29 &= 551 - 9 \times 58 \\
&= 551 - 9(609 - 551) = 10 \times 551 - 9 \times 609 \\
&= 10(1769 - 2 \times 609) - 9 \times 609 = 10 \times 1769 - 29 \times 609 \\
&= 10 \times 1769 - 29(2378 - 1769) = 39 \times 1769 - 29 \times 2378 \\
&= 39(4147 - 2378) - 29 \times 2378 = 39 \times 4147 - 68 \times 2378 \\
&= 39 \times 4147 - 68(10672 - 2 \times 4147) = 175 \times 4147 - 68 \times 10672.
\end{aligned}$$

So $s = -68$, $t = 175$: $\text{gcd}(10672, 4147) = 29 = -68(10672) + 175(4147)$.

Verification: $-68 \times 10672 = -725\,696$ and $175 \times 4147 = 725\,725$; the difference is 29. ✓

36. Solve $84x \equiv 30 \pmod{138}$. $d = \text{gcd}(84, 138) = 6$ and $6 \mid 30$, so solutions exist and there are exactly $d = 6$ incongruent ones modulo 138.

Divide everything (including the modulus) by 6:

$$14x \equiv 5 \pmod{23}.$$

$\text{gcd}(14, 23) = 1$; find the inverse of 14 mod 23: $14 \times 5 = 70 = 3 \times 23 + 1$, so $\overline{14} = 5$. Hence

$$x \equiv 5 \times 5 = 25 \equiv 2 \pmod{23}.$$

Lifting back to modulus 138 by adding multiples of $138/6 = 23$:

$$x \in \{2, 25, 48, 71, 94, 117\} \pmod{138}.$$

Check: $84 \times 2 = 168 = 138 + 30$. ✓

Why gcd governs the count: $ax \equiv b \pmod{m}$ is solvable iff $d = \text{gcd}(a, m)$ divides b ; dividing through by d produces a congruence with coprime coefficient and modulus m/d , which has one solution class mod m/d . That class splits into exactly d classes modulo m .

37. Inverse of 101 mod 4620, and $101x \equiv 73 \pmod{4620}$. From the extended Euclidean computation in Chapter 8,

$$1 = 1601 \times 101 - 35 \times 4620 \implies \overline{101} = 1601.$$

Verification: $1601 \times 101 = 161\,701 = 35 \times 4620 + 1 = 161\,700 + 1$. ✓

Then

$$x \equiv 1601 \times 73 = 116\,873 \pmod{4620}.$$

Since $4620 \times 25 = 115\,500$, we get $x \equiv 116\,873 - 115\,500 = \mathbf{1373} \pmod{4620}$.

Check: $101 \times 1373 = 138\,673$, and $138\,673 = 30 \times 4620 + 73 = 138\,600 + 73$. ✓

38. $\varphi(7560)$. $7560 = 2^3 \cdot 3^3 \cdot 5 \cdot 7$. Hence

$$\varphi(7560) = 7560 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right) = 7560 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = \mathbf{1728}.$$

So exactly 1728 integers in $\{1, \dots, 7560\}$ are relatively prime to 7560, and $7560 - 1728 = \mathbf{5832}$ are not.

39. $7^{222} \bmod 100$. $\gcd(7, 100) = 1$ (7 is prime and $7 \nmid 100$), so Euler's theorem applies. $100 = 2^2 \cdot 5^2$, so $\varphi(100) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$ and $7^{40} \equiv 1 \pmod{100}$.

Write $222 = 5 \times 40 + 22$:

$$7^{222} = (7^{40})^5 \cdot 7^{22} \equiv 1^5 \cdot 7^{22} = 7^{22} \pmod{100}.$$

Now $7^2 = 49$ and $7^4 = 2401 \equiv 1 \pmod{100}$, so $7^{20} = (7^4)^5 \equiv 1$ and

$$7^{22} = 7^{20} \cdot 7^2 \equiv 1 \times 49 = 49 \pmod{100}.$$

Hence $7^{222} \bmod 100 = \mathbf{49}$.

40. Infinitely many primes. Suppose only $p_1, \dots, p_k$ are prime and let $N = p_1 p_2 \cdots p_k + 1$.

- (a) If some p_i divided N , then since p_i also divides the product $p_1 \cdots p_k$, it would divide the difference $N - p_1 \cdots p_k = 1$ (Corollary 8.3). But no prime divides 1, since every prime is ≥ 2 . So no listed prime divides N .
- (b) $N \geq 3 > 1$, so by the fundamental theorem of arithmetic N is either prime or has a prime factorisation. Either way N has a prime divisor q . By (a), q is not among $p_1, \dots, p_k$ — a new prime.

This contradicts the assumption that the list was complete. Hence there are infinitely many primes.

APPENDIX B

Worked Solutions: Assignments 01–02

These are model solutions provided as a study aid. Assignment instructions require *your own* complete reasoning, every theorem or identity named, and a counterexample wherever a claim fails — so work each problem yourself first and use these to check method and answer, not as a substitute.

B.1 Assignment 01

Question 01 — Propositional logic

(a) Are $(p \wedge \neg q) \rightarrow r$ and $(p \rightarrow q) \rightarrow r$ logically equivalent?

p	q	r	$\neg q$	$p \wedge \neg q$	$p \rightarrow q$	$(p \wedge \neg q) \rightarrow r$	$(p \rightarrow q) \rightarrow r$
0	0	0	1	0	1	1	0
0	0	1	1	0	1	1	1
0	1	0	0	0	1	1	0
0	1	1	0	0	1	1	1
1	0	0	1	1	0	0	1
1	0	1	1	1	0	1	1
1	1	0	0	0	1	1	0
1	1	1	0	0	1	1	1

The two final columns disagree in four rows (shown in bold), so the propositions are **not logically equivalent**.

Column 7 contains both 1s and 0s, so $(p \wedge \neg q) \rightarrow r$ is a **contingency**. It is therefore **not valid** (a proposition is valid only if every row is true).

(b) “If Yomal is concerned about his cholesterol levels, then he will walk 2 km every day.” Let c = “Yomal is concerned about his cholesterol levels”, w = “Yomal walks 2 km every day”; the statement is $c \rightarrow w$.

Converse	$w \rightarrow c$	If Yomal walks 2 km every day, then he is concerned about his cholesterol levels.
Contrapositive	$\neg w \rightarrow \neg c$	If Yomal does not walk 2 km every day, then he is not concerned about his cholesterol levels.
Inverse	$\neg c \rightarrow \neg w$	If Yomal is not concerned about his cholesterol levels, then he does not walk 2 km every day.

(c) $(p \vee q) \wedge p \equiv p$.

$$\begin{aligned} (p \vee q) \wedge p &\equiv p \wedge (p \vee q) && \text{Commutative law} \\ &\equiv p && \text{Absorption law.} \end{aligned}$$

(Alternatively, expand by the distributive law: $(p \vee q) \wedge p \equiv (p \wedge p) \vee (q \wedge p) \equiv p \vee (p \wedge q) \equiv p$, using idempotent, commutative and absorption laws.)

(d) $\neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg q$.

$$\begin{aligned} \neg(p \vee (\neg p \wedge q)) &\equiv \neg p \wedge \neg(\neg p \wedge q) && \text{De Morgan's law} \\ &\equiv \neg p \wedge (\neg(\neg p) \vee \neg q) && \text{De Morgan's law} \\ &\equiv \neg p \wedge (p \vee \neg q) && \text{Double negation law} \\ &\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) && \text{Distributive law} \\ &\equiv \mathbf{F} \vee (\neg p \wedge \neg q) && \text{Negation law} \\ &\equiv \neg p \wedge \neg q && \text{Identity law.} \end{aligned}$$

Question 02 — Predicates and quantifiers

(a) $p(x) : x < -1$ and $q(x) : x \geq 1$, domain $\mathbb{R}$. First record the negations: $\neg p(x)$ is $x \geq -1$ and $\neg q(x)$ is $x < 1$.

(i) $\neg \forall x (\neg p(x) \wedge \neg q(x))$.

The inner predicate $\neg p(x) \wedge \neg q(x)$ says $-1 \leq x < 1$. This is *not* true of every real (take $x = 5$), so $\forall x(\dots)$ is false and its negation is **TRUE**.

(ii) $\neg \exists x (\neg p(x) \vee \neg q(x))$.

$\neg p(x) \vee \neg q(x)$ says $x \geq -1$ or $x < 1$, which holds for *every* real (if $x < -1$ then certainly $x < 1$). So the existential is true and its negation is **FALSE**.

(iii) $\neg \forall x \neg p(x) \vee \neg \exists x q(x)$.

$\forall x \neg p(x)$ says every real is ≥ -1 , which is false (take $x = -2$); so $\neg \forall x \neg p(x)$ is **true** and the whole disjunction is **TRUE**. (For completeness, $\exists x q(x)$ is true — take $x = 1$ — so the second disjunct is false; the first alone carries the disjunction.)

(iv) $\neg \exists x \neg p(x) \wedge \neg \exists x \neg q(x)$.

$\neg \exists x \neg p(x) \equiv \forall x p(x)$, i.e. every real is < -1 , which is false. A conjunction with a false conjunct is **FALSE**.

(b) N, E, O, P over $\mathbb{Z}$.

-
- (i) There exists an odd prime integer. $\exists x (P(x) \wedge O(x))$
- (ii) If an integer is not even, then it is odd. $\forall x (\neg E(x) \rightarrow O(x))$
- (iii) The only even prime is 2. $\forall x (P(x) \wedge E(x) \rightarrow x = 2)$
- (iv) The addition of two primes need not be prime. $\exists x \exists y (P(x) \wedge P(y) \wedge \neg P(x + y))$
- (v) The product of any two primes is not prime. $\forall x \forall y (P(x) \wedge P(y) \rightarrow \neg P(xy))$
-

Note the contrast between (iv) and (v): “need not be” is an existential claim, “any two” is a universal one.

Question 03 — Arguments

(a) $(m \wedge n) \rightarrow (p \vee \neg q)$, $m \rightarrow (r \wedge \neg p)$, $q \rightarrow \neg r \therefore \neg n$. The argument is **invalid**. A truth assignment making all three premises true and the conclusion false:

$$m = \mathbf{T}, \quad n = \mathbf{T}, \quad p = \mathbf{F}, \quad q = \mathbf{F}, \quad r = \mathbf{T}.$$

Verification.

Formula	Evaluation	Value
$(m \wedge n) \rightarrow (p \vee \neg q)$	$(\mathbf{T} \wedge \mathbf{T}) \rightarrow (\mathbf{F} \vee \mathbf{T}) = \mathbf{T} \rightarrow \mathbf{T}$	$\mathbf{T}$
$m \rightarrow (r \wedge \neg p)$	$\mathbf{T} \rightarrow (\mathbf{T} \wedge \mathbf{T}) = \mathbf{T} \rightarrow \mathbf{T}$	$\mathbf{T}$
$q \rightarrow \neg r$	$\mathbf{F} \rightarrow \mathbf{F}$ (vacuously true)	$\mathbf{T}$
$\neg n$	$\neg \mathbf{T}$	$\mathbf{F}$

All premises are true while the conclusion is false, so the argument form is invalid.

(b) **AI systems.** Let e = “AI systems are ethical”, u = “programmers are unbiased”, s = “regulations are strict”.

(i) **Symbolic form.**

$$\text{Premise: } e \rightarrow (u \vee s); \quad \text{Conclusion: } (\neg s \wedge \neg u) \rightarrow \neg e.$$

(ii) **As a single conditional.**

$$[e \rightarrow (u \vee s)] \rightarrow [(\neg s \wedge \neg u) \rightarrow \neg e].$$

(iii) **Truth table.** Write $P = e \rightarrow (u \vee s)$ and $C = (\neg s \wedge \neg u) \rightarrow \neg e$.

e	u	s	$u \vee s$	P	$\neg s \wedge \neg u$	C	$P \rightarrow C$
0	0	0	0	1	1	1	1
0	0	1	1	1	0	1	1
0	1	0	1	1	0	1	1
0	1	1	1	1	0	1	1
1	0	0	0	0	1	0	1
1	0	1	1	1	0	1	1
1	1	0	1	1	0	1	1
1	1	1	1	1	0	1	1

- (iv) The final column is all 1s, so the conditional is a tautology and the argument is **valid**. The reason is structural: the conclusion is precisely the *contrapositive* of the premise, since $\neg(u \vee s) \equiv \neg u \wedge \neg s$ by De Morgan. And $A \rightarrow B \equiv \neg B \rightarrow \neg A$.

(c) “If $n > 4$ then $n^2 > 16$. Suppose $n^2 \leq 16$. Then $n \leq 4$.” Let p be “ $n > 4$ ” and q be “ $n^2 > 16$ ”. The argument has the form

$$p \rightarrow q, \quad \neg q \quad \therefore \quad \neg p,$$

which is **modus tollens** — a valid rule of inference. Its application is justified because $\neg q$ is literally “ $n^2 \leq 16$ ” and $\neg p$ is literally “ $n \leq 4$ ” (the negations of strict inequalities over $\mathbb{R}$). Hence the argument is **valid**.

Question 04 — The submission portal (resolution)

(a) Symbolic knowledge base.

$$\text{KB} = \{ V \rightarrow U, \quad U \rightarrow R, \quad R \rightarrow A, \quad E \rightarrow U, \quad E \rightarrow \neg R, \quad E \}.$$

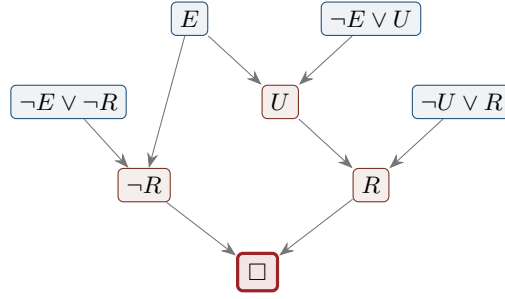
(b) Clausal form. Using $X \rightarrow Y \equiv \neg X \vee Y$:

Clause	Form	Clause	Form
C_1	$\neg V \vee U$	C_4	$\neg E \vee U$
C_2	$\neg U \vee R$	C_5	$\neg E \vee \neg R$
C_3	$\neg R \vee A$	C_6	E

(c) Resolution refutation.

Step	Clause	Derivation
1	E	C_6 (premise)
2	$\neg E \vee U$	C_4 (premise)
3	U	Resolution of (1) and (2) on E
4	$\neg U \vee R$	C_2 (premise)
5	R	Resolution of (3) and (4) on U
6	$\neg E \vee \neg R$	C_5 (premise)
7	$\neg R$	Resolution of (1) and (6) on E
8	$\square$	Resolution of (5) and (7) on R

The empty clause is derived, so the knowledge base is **unsatisfiable**: the recorded requirements are **inconsistent**.



(d) Minimal culprit set and a repair. The refutation used only clauses C_6 (E), C_4 ($E \rightarrow U$), C_2 ($U \rightarrow R$) and C_5 ($E \rightarrow \neg R$). That four-element set is already inconsistent, and no proper subset is: dropping any one of them leaves a satisfiable set (e.g. dropping C_2 allows $E = U = \mathbf{T}$, $R = \mathbf{F}$). So

$$\{U \rightarrow R, E \rightarrow U, E \rightarrow \neg R, E\}$$

is a **minimal inconsistent subset**. In plain terms: emergency mode forces an upload, an upload forces a receipt, and emergency mode forbids a receipt.

Minimal revision. Requirement (2) is the one whose scope is too broad. Replace

$$U \rightarrow R \quad \text{by} \quad (U \wedge \neg E) \rightarrow R,$$

i.e. “if the script is uploaded *and the portal is not in emergency recovery mode*, then a receipt is generated”. To preserve the portal’s purpose (accepting valid submissions) also add

$$(E \wedge U) \rightarrow A,$$

“an upload in emergency mode is accepted”.

Demonstration that the conflict is gone. Take

$$V = \mathbf{F}, \quad U = \mathbf{T}, \quad R = \mathbf{F}, \quad A = \mathbf{T}, \quad E = \mathbf{T}.$$

Requirement	Evaluation	Value
$V \rightarrow U$	$\mathbf{F} \rightarrow \mathbf{T}$	$\mathbf{T}$
$(U \wedge \neg E) \rightarrow R$	$(\mathbf{T} \wedge \mathbf{F}) \rightarrow \mathbf{F} = \mathbf{F} \rightarrow \mathbf{F}$	$\mathbf{T}$
$R \rightarrow A$	$\mathbf{F} \rightarrow \mathbf{T}$	$\mathbf{T}$
$E \rightarrow U$	$\mathbf{T} \rightarrow \mathbf{T}$	$\mathbf{T}$
$E \rightarrow \neg R$	$\mathbf{T} \rightarrow \mathbf{T}$	$\mathbf{T}$
E	—	$\mathbf{T}$
$(E \wedge U) \rightarrow A$	$\mathbf{T} \rightarrow \mathbf{T}$	$\mathbf{T}$

Every requirement is satisfied simultaneously, so the revised set is consistent — and the submission is still accepted ($A = \mathbf{T}$), preserving the portal’s main purpose.

Question 05 — Research project funding

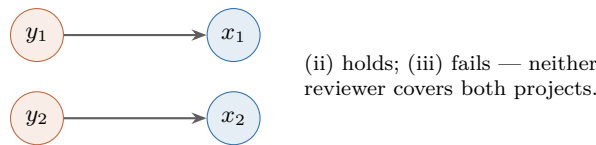
(a) Translations.

-
- (i) Every funded project has $\forall x (F(x) \rightarrow E(x))$ passed ethics review.
 - (ii) For every AI project, there is $\forall x (A(x) \rightarrow \exists y (C(y) \wedge R(y, x)))$ a certified reviewer who reviewed it.
 - (iii) There is a certified reviewer $\exists y (C(y) \wedge \forall x (A(x) \rightarrow R(y, x)))$ who reviewed every AI project.
 - (iv) At least one AI project has $\exists x (A(x) \wedge \neg E(x))$ not passed ethics review.
-

(b) Are (ii) and (iii) equivalent? No. Statement (iii) implies (ii) — if one reviewer covers every AI project, then each AI project certainly has *some* certified reviewer — but the converse fails.

Finite countermodel.

Projects: x_1, x_2 with $A(x_1), A(x_2)$ both true,
 Reviewers: y_1, y_2 with $C(y_1), C(y_2)$ both true,
 Review relation: $R = \{(y_1, x_1), (y_2, x_2)\}$.



Statement (ii) is true: x_1 was reviewed by the certified y_1 and x_2 by the certified y_2 . Statement (iii) is false: y_1 did not review x_2 and y_2 did not review x_1 , so no single certified reviewer reviewed *every* AI project.

(c) Does “some AI project is not funded” follow? Premises: $\forall x (F(x) \rightarrow E(x))$ and $\exists x (A(x) \wedge \neg E(x))$. Conclusion: $\exists x (A(x) \wedge \neg F(x))$. **Valid.**

Step	Statement	Reason
1	$\exists x (A(x) \wedge \neg E(x))$	Premise
2	$A(a) \wedge \neg E(a)$	Existential instantiation, (1)
3	$A(a)$	Simplification, (2)
4	$\neg E(a)$	Simplification, (2)
5	$\forall x (F(x) \rightarrow E(x))$	Premise
6	$F(a) \rightarrow E(a)$	Universal instantiation, (5) <i>at the same witness a</i>
7	$\neg F(a)$	Modus tollens, (4) and (6)
8	$A(a) \wedge \neg F(a)$	Conjunction, (3) and (7)
9	$\exists x (A(x) \wedge \neg F(x))$	Existential generalisation, (8)

(d) Negation of (iii).

$$\begin{aligned}
\neg \exists y \left(C(y) \wedge \forall x (A(x) \rightarrow R(y, x)) \right) &\equiv \forall y \neg \left(C(y) \wedge \forall x (A(x) \rightarrow R(y, x)) \right) \\
&\equiv \forall y \left(\neg C(y) \vee \neg \forall x (A(x) \rightarrow R(y, x)) \right) \\
&\equiv \forall y \left(\neg C(y) \vee \exists x (A(x) \wedge \neg R(y, x)) \right) \\
&\equiv \forall y \left(C(y) \rightarrow \exists x (A(x) \wedge \neg R(y, x)) \right).
\end{aligned}$$

In English: *for every certified reviewer there is some AI project that they did not review* — i.e. no certified reviewer has covered the whole AI portfolio.

Question 06 — Software regulation

(a) Premises.

- (1) $\forall x (S(x) \wedge D(x) \rightarrow T(x))$
- (2) $\forall x (C(x) \rightarrow T(x))$
- (3) $\exists x (S(x) \wedge \neg T(x))$

(b) Does $\exists x (S(x) \wedge \neg D(x))$ follow? **Yes — valid.**

Step	Statement	Reason
1	$\exists x (S(x) \wedge \neg T(x))$	Premise (3)
2	$S(a) \wedge \neg T(a)$	Existential instantiation, (1)
3	$S(a)$	Simplification, (2)
4	$\neg T(a)$	Simplification, (2)
5	$\forall x (S(x) \wedge D(x) \rightarrow T(x))$	Premise (1)
6	$S(a) \wedge D(a) \rightarrow T(a)$	Universal instantiation, (5) <i>at a</i>
7	$\neg(S(a) \wedge D(a))$	Modus tollens, (4) and (6)
8	$\neg S(a) \vee \neg D(a)$	De Morgan, (7)
9	$\neg D(a)$	Disjunctive syllogism, (3) and (8)
10	$S(a) \wedge \neg D(a)$	Conjunction, (3) and (9)
11	$\exists x (S(x) \wedge \neg D(x))$	Existential generalisation, (10)

(c) Does $\exists x (S(x) \wedge \neg C(x))$ follow? **Yes — valid.**

Step	Statement	Reason
1	$\exists x (S(x) \wedge \neg T(x))$	Premise (3)
2	$S(a) \wedge \neg T(a)$	Existential instantiation, (1)
3	$S(a)$	Simplification, (2)
4	$\neg T(a)$	Simplification, (2)
5	$\forall x (C(x) \rightarrow T(x))$	Premise (2)
6	$C(a) \rightarrow T(a)$	Universal instantiation, (5) at a
7	$\neg C(a)$	Modus tollens, (4) and (6)
8	$S(a) \wedge \neg C(a)$	Conjunction, (3) and (7)
9	$\exists x (S(x) \wedge \neg C(x))$	Existential generalisation, (8)

(d) **Why the same witness must be used.** Existential instantiation licenses only this: *some* object satisfies the predicate, and we give it a name. The name is a placeholder for one particular but unknown object.

If, having introduced a from $\exists x (S(x) \wedge \neg T(x))$, we then instantiated the universal premise at a *different* constant b , the resulting statements $S(a) \wedge \neg T(a)$ and $C(b) \rightarrow T(b)$ would concern possibly different systems, and modus tollens could not be applied — there would be no shared subject to reason about. Conversely, if two *separate* existential premises were both instantiated at the same name, we would be illegitimately asserting that one object witnesses both, which the premises do not guarantee.

Hence the rule: each existential instantiation introduces a **fresh** constant, and every subsequent step about that witness must use **that same** constant.

B.2 Assignment 02

Question 01 — Sets

(a) $U = \{1, \dots, 20\}$.

$$A = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20\} \quad (\text{multiples of } 2)$$

$$B = \{3, 6, 9, 12, 15, 18\} \quad (\text{multiples of } 3)$$

$$C = \{2, 3, 5, 7, 11, 13, 17, 19\} \quad (\text{primes})$$

Expression	Roster form
$(A \cup B)^c$	$\{1, 5, 7, 11, 13, 17, 19\}$
$(A \cap B) \cup C$	$\{2, 3, 5, 6, 7, 11, 12, 13, 17, 18, 19\}$
$(A - C) \triangle (B - C)$	$\{4, 8, 9, 10, 14, 15, 16, 20\}$
$((A \cup C) \cap (B \cup C)) - C$	$\{6, 12, 18\}$

Working. $A \cup B = \{2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20\}$, so the complement is as stated. $A \cap B = \{6, 12, 18\}$ (multiples of 6). $A - C = \{4, 6, 8, 10, 12, 14, 16, 18, 20\}$ and $B - C = \{6, 9, 12, 15, 18\}$; the symmetric difference keeps the elements in exactly one of them.

Verification of $(A \cup C) \cap (B \cup C) = (A \cap B) \cup C$.

$$A \cup C = \{2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 16, 17, 18, 19, 20\},$$

$$B \cup C = \{2, 3, 5, 6, 7, 9, 11, 12, 13, 15, 17, 18, 19\},$$

so

$$(A \cup C) \cap (B \cup C) = \{2, 3, 5, 6, 7, 11, 12, 13, 17, 18, 19\} = (A \cap B) \cup C. \quad \checkmark$$

This is an instance of the distributive law $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

(b) $X = \{a, b, c, d, e\}$, $|X| = 5$.

(i) **Containing a :** a is forced in; the other 4 elements are free, giving $2^4 = 16$.

(ii) **Containing both a and b :** two forced, three free: $2^3 = 8$.

(iii) **Exactly three elements:** choose which 3 of the 5 to include: $\binom{5}{3} = 10$.

(iv) **Containing a but not e :** a forced in, e forced out, three free: $2^3 = 8$.

The counting argument in (i), (ii) and (iv) is the same each time: every element is an *independent* binary decision, and each constraint removes one element from the pool of free decisions.

(c) $A - (B \cup C) = (A - B) \cap (A - C)$, **by element membership.** ($\subseteq$) Let $x \in A - (B \cup C)$. Then $x \in A$ and $x \notin B \cup C$, i.e. $\neg(x \in B \vee x \in C)$. By De Morgan, $x \notin B$ and $x \notin C$. Hence $x \in A$ and $x \notin B$, so $x \in A - B$; and $x \in A$ and $x \notin C$, so $x \in A - C$. Therefore $x \in (A - B) \cap (A - C)$.

($\supseteq$) Let $x \in (A - B) \cap (A - C)$. Then $x \in A - B$ and $x \in A - C$, so $x \in A$, $x \notin B$ and $x \notin C$. By De Morgan, $\neg(x \in B \vee x \in C)$, i.e. $x \notin B \cup C$. Hence $x \in A - (B \cup C)$.

Both inclusions hold, so the sets are equal. ■

(d) $U = \{1, \dots, 12\}$, **bit strings.**

$$A : 101101001011 = \{1, 3, 4, 6, 9, 11, 12\}$$

$$B : 011011100101 = \{2, 3, 5, 6, 7, 10, 12\}$$

$$C : 110010011010 = \{1, 2, 5, 8, 9, 11\}$$

Computing $(A \cap B^c) \cup C$.

$$B = 011011100101$$

$$B^c = \neg B = 100100011010$$

$$A = 101101001011$$

$$A \wedge B^c = 100100001010$$

$$C = 110010011010$$

$$(A \wedge B^c) \vee C = \mathbf{110110011010}$$

Decoding: $(A \cap B^c) \cup C = \{1, 2, 4, 5, 8, 9, 11\}$.

Computing $(A \triangle B) \cap C^c$, bit by bit:

position	1	2	3	4	5	6	7	8	9	10	11	12
A	1	0	1	1	0	1	0	0	1	0	1	1
B	0	1	1	0	1	1	1	0	0	1	0	1
$A \oplus B$	1	1	0	1	1	0	1	0	1	1	1	0
C^c	0	0	1	1	0	1	1	0	0	1	0	1
$(A \oplus B) \wedge C^c$	0	0	0	1	0	0	1	0	0	1	0	0

Reading off the last two rows:

$$A \triangle B = 110110101110 = \{1, 2, 4, 5, 7, 9, 10, 11\}, \quad (A \triangle B) \cap C^c = 000100100100 = \{4, 7, 10\}.$$

(e) **Simplify** $[(A \cup B) \cap (A \cup B^c)] \cup [A^c \cap (B \cup B^c)]$.

$$\begin{aligned}
 & [(A \cup B) \cap (A \cup \overline{B})] \cup [\overline{A} \cap (B \cup \overline{B})] \\
 &= [A \cup (B \cap \overline{B})] \cup [\overline{A} \cap \mathbb{U}] && \text{Distributive law; Complement law} \\
 &= [A \cup \emptyset] \cup \overline{A} && \text{Complement law; Identity law} \\
 &= A \cup \overline{A} && \text{Identity law} \\
 &= \mathbb{U} && \text{Complement law.}
 \end{aligned}$$

Element-membership verification. Let x be arbitrary.

- If $x \in A$: then $x \in A \cup B$ and $x \in A \cup \overline{B}$, so x is in the first bracket, hence in the union.
- If $x \notin A$: then $x \in \overline{A}$, and x is in B or in $\overline{B}$, so $x \in \overline{A} \cap (B \cup \overline{B})$, hence in the union.

Every $x \in \mathbb{U}$ falls into one of these two cases, so the expression equals $\mathbb{U}$. ✓

Question 02 — Functions

(a) $A = \{-2, -1, 0, 1, 2\}$, $f(x) = x^2 - x$.

x	-2	-1	0	1	2
$f(x)$	6	2	0	0	2

Range = $\{0, 2, 6\}$.

Not one-to-one: $f(0) = 0 = f(1)$ but $0 \neq 1$. (Also $f(-1) = 2 = f(2)$.)

Now let $B = f(A) = \{0, 2, 6\}$ and regard $f : A \rightarrow B$. By construction every element of B is an image, so f is **onto**. But it is still *not* one-to-one (same counterexample), so it is **not a bijection**.

(b) $f : \mathbb{R} \setminus \{-1\} \rightarrow \mathbb{R} \setminus \{2\}$, $f(x) = \frac{2x-3}{x+1}$. **One-to-one.** Suppose $f(x) = f(y)$ with $x, y \neq -1$:

$$\begin{aligned}
 \frac{2x-3}{x+1} &= \frac{2y-3}{y+1} \implies (2x-3)(y+1) = (2y-3)(x+1) \\
 &\implies 2xy + 2x - 3y - 3 = 2xy + 2y - 3x - 3 \\
 &\implies 2x - 3y = 2y - 3x \implies 5x = 5y \implies x = y.
 \end{aligned}$$

Onto. Let $y \in \mathbb{R} \setminus \{2\}$ and solve $f(x) = y$:

$$\begin{aligned} \frac{2x-3}{x+1} = y &\implies 2x-3 = y(x+1) = xy+y \\ &\implies 2x-xy = y+3 \implies x(2-y) = y+3 \implies x = \frac{y+3}{2-y}, \end{aligned}$$

which is a real number since $y \neq 2$. We must check $x \neq -1$: if $\frac{y+3}{2-y} = -1$ then $y+3 = y-2$, i.e. $3 = -2$, impossible. So $x \in \mathbb{R} \setminus \{-1\}$ and $f(x) = y$.

Hence f is a bijection with

$$\boxed{f^{-1}(y) = \frac{y+3}{2-y}}$$

Verification of $f^{-1}(f(x)) = x$. Put $t = \frac{2x-3}{x+1}$. Then

$$f^{-1}(t) = \frac{t+3}{2-t} = \frac{\frac{2x-3}{x+1} + 3}{2 - \frac{2x-3}{x+1}} = \frac{\frac{2x-3+3x+3}{x+1}}{\frac{2x+2-2x+3}{x+1}} = \frac{5x}{5} = x. \quad \checkmark$$

(c) $f(x) = 2x - 1$, $g(x) = x^2 + 2$ on $\mathbb{Z}$.

$$\begin{aligned} (f \circ g)(x) &= f(x^2 + 2) = 2(x^2 + 2) - 1 = 2x^2 + 3, \\ (g \circ f)(x) &= g(2x - 1) = (2x - 1)^2 + 2 = 4x^2 - 4x + 3, \\ (f \circ f)(x) &= f(2x - 1) = 2(2x - 1) - 1 = 4x - 3. \end{aligned}$$

Setting the first two equal:

$$2x^2 + 3 = 4x^2 - 4x + 3 \iff 0 = 2x^2 - 4x = 2x(x - 2) \iff x = 0 \text{ or } x = 2.$$

Both are integers, so the solution set is $\{0, 2\}$. Check: $(f \circ g)(0) = 3 = (g \circ f)(0)$; $(f \circ g)(2) = 11 = (g \circ f)(2)$. $\checkmark$

(d) Images of unions and intersections.

- (i) $f(S \cup T) = f(S) \cup f(T)$.
 $(\subseteq)$ Let $y \in f(S \cup T)$. Then $y = f(x)$ for some $x \in S \cup T$, so $x \in S$ or $x \in T$, giving $y \in f(S)$ or $y \in f(T)$; hence $y \in f(S) \cup f(T)$.
 $(\supseteq)$ Let $y \in f(S) \cup f(T)$. Then $y = f(s)$ for some $s \in S$, or $y = f(t)$ for some $t \in T$. In either case the witness lies in $S \cup T$, so $y \in f(S \cup T)$.
- (ii) $f(S \cap T) \subseteq f(S) \cap f(T)$.
 Let $y \in f(S \cap T)$. Then $y = f(x)$ for some $x \in S \cap T$. Since $x \in S$ we get $y \in f(S)$; since $x \in T$ we get $y \in f(T)$. Hence $y \in f(S) \cap f(T)$.
- (iii) **Counterexample to equality.** Let $A = \{a, b\}$, $B = \{1\}$ and $f(a) = f(b) = 1$. Take $S = \{a\}$, $T = \{b\}$. Then

$$f(S \cap T) = f(\emptyset) = \emptyset, \quad f(S) \cap f(T) = \{1\} \cap \{1\} = \{1\}.$$

The inclusion is strict. (The obstruction is exactly the failure of injectivity, as proved in Chapter 6.)

(e) **Floor, ceiling, and** $\lfloor x + n \rfloor = \lfloor x \rfloor + n$.

$$\left\lfloor -\frac{17}{4} \right\rfloor = \lfloor -4.25 \rfloor = -5, \quad \left\lceil -\frac{17}{4} \right\rceil = \lceil -4.25 \rceil = -4,$$

$$\lfloor \sqrt{20} \rfloor = \lfloor 4.472 \dots \rfloor = 4, \quad \lceil \sqrt{20} \rceil = 5.$$

(Recall $4^2 = 16 < 20 < 25 = 5^2$.)

Proof that $\lfloor x + n \rfloor = \lfloor x \rfloor + n$ **for** $x \in \mathbb{R}$, $n \in \mathbb{Z}$. Let $m = \lfloor x \rfloor$, so $m \in \mathbb{Z}$ and, by the characterising property of the floor,

$$m \leq x < m + 1.$$

Adding the integer n to all three parts,

$$m + n \leq x + n < m + n + 1,$$

and $m + n \in \mathbb{Z}$. But the floor of a real number is the *unique* integer k with $k \leq x + n < k + 1$. Hence

$$\lfloor x + n \rfloor = m + n = \lfloor x \rfloor + n. \quad \blacksquare$$

Question 03 — Relations

(a) $A = \{1, 2, 3, 4, 6, 12\}$, $aRb \iff a \mid b$.

$$\begin{aligned} R = \{ & (1, 1), (1, 2), (1, 3), (1, 4), (1, 6), (1, 12), \\ & (2, 2), (2, 4), (2, 6), (2, 12), \\ & (3, 3), (3, 6), (3, 12), \\ & (4, 4), (4, 12), \\ & (6, 6), (6, 12), \\ & (12, 12) \} \end{aligned}$$

— eighteen ordered pairs.

Property	Holds?	Proof / counterexample
Reflexive	Yes	$a = a \cdot 1$, so $a \mid a$ for every $a \in A$.
Symmetric	No	$(1, 2) \in R$ but $(2, 1) \notin R$, since $2 \nmid 1$.
Anti-symmetric	Yes	If $a \mid b$ and $b \mid a$ with a, b positive, then $b = ak$ and $a = bm$ give $a = akm$, so $km = 1$, hence $k = m = 1$ and $a = b$.
Transitive	Yes	If $b = ak$ and $c = bm$ then $c = a(km)$, so $a \mid c$.

Reflexive + anti-symmetric + transitive means $(A, \mid)$ is a **partial order**. Its Hasse diagram is Figure 7.5.

(b) $aSb \iff 4 \mid (a - b)$ **on** $\mathbb{Z}$. **Reflexive:** $a - a = 0 = 4 \cdot 0$, so $4 \mid (a - a)$ and $(a, a) \in S$ for every $a \in \mathbb{Z}$.

Symmetric: suppose $(a, b) \in S$, so $a - b = 4k$ for some $k \in \mathbb{Z}$. Then $b - a = 4(-k)$ with $-k \in \mathbb{Z}$, so $4 \mid (b - a)$ and $(b, a) \in S$.

Transitive: suppose $(a, b), (b, c) \in S$, so $a - b = 4k$ and $b - c = 4m$ with $k, m \in \mathbb{Z}$. Then

$$a - c = (a - b) + (b - c) = 4k + 4m = 4(k + m),$$

so $4 \mid (a - c)$ and $(a, c) \in S$.

Hence S is an **equivalence relation** (it is congruence modulo 4).

Anti-symmetric? No. Counterexample: $(0, 4) \in S$ and $(4, 0) \in S$ (both differences are ± 4), yet $0 \neq 4$.

(c) $S \circ R$. $R = \{(1, a), (1, b), (2, b), (3, c), (4, a)\}$ from $A = \{1, 2, 3, 4\}$ to $B = \{a, b, c\}$; $S = \{(a, x), (a, z), (b, y), (c, x), (c, z)\}$ from B to $C = \{x, y, z\}$.

Chasing each pair of R through S :

$$1 \rightarrow a \rightarrow x, z; \quad 1 \rightarrow b \rightarrow y \implies (1, x), (1, z), (1, y)$$

$$2 \rightarrow b \rightarrow y \implies (2, y)$$

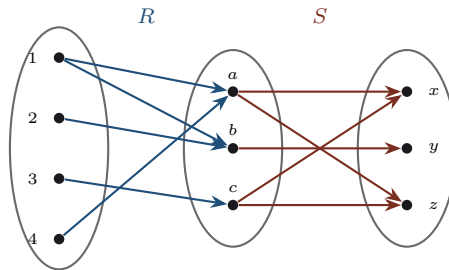
$$3 \rightarrow c \rightarrow x, z \implies (3, x), (3, z)$$

$$4 \rightarrow a \rightarrow x, z \implies (4, x), (4, z)$$

$$S \circ R = \{(1, x), (1, y), (1, z), (2, y), (3, x), (3, z), (4, x), (4, z)\}.$$

Is R a function $A \rightarrow B$? No: the element 1 is the first coordinate of two pairs, $(1, a)$ and $(1, b)$, violating single-valuedness.

Is $S \circ R$ a function $A \rightarrow C$? No, for the same reason — 1 appears as a first coordinate three times (and 3 and 4 twice each).



(d) **Powers of $R = \{(1, 2), (2, 3), (3, 1), (3, 4), (4, 4)\}$ on $A = \{1, 2, 3, 4\}$.**

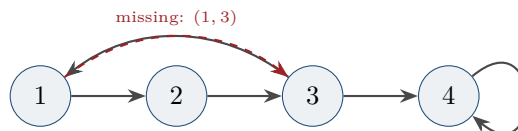
$$R^2 = R \circ R = \{(1, 3), (2, 1), (2, 4), (3, 2), (3, 4), (4, 4)\},$$

$$R^3 = R^2 \circ R = \{(1, 1), (1, 4), (2, 2), (2, 4), (3, 3), (3, 4), (4, 4)\}.$$

How R^2 was obtained: follow two arrows. $1 \rightarrow 2 \rightarrow 3$ gives $(1, 3)$; $2 \rightarrow 3 \rightarrow 1$ and $2 \rightarrow 3 \rightarrow 4$ give $(2, 1), (2, 4)$; $3 \rightarrow 1 \rightarrow 2$ and $3 \rightarrow 4 \rightarrow 4$ give $(3, 2), (3, 4)$; $4 \rightarrow 4 \rightarrow 4$ gives $(4, 4)$.

Is R transitive? No. By the criterion R transitive $\iff R^2 \subseteq R$, it suffices that $(1, 3) \in R^2$ but $(1, 3) \notin R$.

Demonstrating pair: $(1, 2) \in R$ and $(2, 3) \in R$, yet $(1, 3) \notin R$.



(e) $|A| = 4$.

- (i) **All relations.** A relation is a subset of $A \times A$, which has $4 \times 4 = 16$ elements. Each of the 16 cells is independently in or out: $2^{16} = \mathbf{65\,536}$.
- (ii) **Reflexive relations.** The 4 diagonal pairs $(1, 1), \dots, (4, 4)$ must all be present — no choice there. The remaining $16 - 4 = 12$ cells are free: $2^{12} = \mathbf{4096}$.
- (iii) **Symmetric relations.** The 4 diagonal cells are free (2^4 choices). The $\binom{4}{2} = 6$ off-diagonal pairs $\{(a, b), (b, a)\}$ must be decided together — both in or both out (2^6 choices). Total $2^4 \cdot 2^6 = 2^{10} = \mathbf{1024}$.

Question 04 — Number theory

(a) If $a \mid b$ and $a \mid c$ then $a \mid (5b - 3c)$.

Proof. Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$, and suppose $a \mid b$ and $a \mid c$. By the *definition of divisibility* there exist integers k_1, k_2 with

$$b = ak_1, \quad c = ak_2.$$

Then

$$5b - 3c = 5(ak_1) - 3(ak_2) = a(5k_1 - 3k_2) = ak_3,$$

where $k_3 = 5k_1 - 3k_2 \in \mathbb{Z}$ because the integers are closed under multiplication and subtraction. By the definition of divisibility, $a \mid (5b - 3c)$. ■

(b) $\sqrt{3}$ is irrational.

Proof by contradiction. Suppose $\sqrt{3}$ is rational. Then we may write

$$\sqrt{3} = \frac{a}{b}, \quad a, b \in \mathbb{Z}, \quad b \neq 0, \quad \gcd(a, b) = 1$$

(any rational can be reduced to lowest terms). Squaring and clearing denominators,

$$a^2 = 3b^2,$$

so $3 \mid a^2$. Using the given fact, $3 \mid a$; write $a = 3k$ with $k \in \mathbb{Z}$. Substituting,

$$3b^2 = a^2 = 9k^2 \implies b^2 = 3k^2,$$

so $3 \mid b^2$ and hence, by the same fact, $3 \mid b$.

But now 3 is a common divisor of a and b , so $\gcd(a, b) \geq 3$, contradicting $\gcd(a, b) = 1$.

The contradiction is precisely $\gcd(a, b) = 1$ and $\gcd(a, b) \geq 3$ holding simultaneously. Therefore the assumption is false and $\sqrt{3}$ is irrational. ■

(c) $\gcd(414, 662)$ and Bézout coefficients. Euclidean algorithm.

$$\begin{aligned} 662 &= 1 \times 414 + 248 \\ 414 &= 1 \times 248 + 166 \\ 248 &= 1 \times 166 + 82 & \gcd(414, 662) = \mathbf{2}. \\ 166 &= 2 \times 82 + 2 \\ 82 &= 41 \times 2 + 0 \end{aligned}$$

Back-substitution.

$$\begin{aligned}
2 &= 166 - 2 \times 82 \\
&= 166 - 2(248 - 166) = 3 \times 166 - 2 \times 248 \\
&= 3(414 - 248) - 2 \times 248 = 3 \times 414 - 5 \times 248 \\
&= 3 \times 414 - 5(662 - 414) = 8 \times 414 - 5 \times 662.
\end{aligned}$$

So $s = 8$ and $t = -5$:

$$\gcd(414, 662) = 2 = 8(414) + (-5)(662).$$

Verification: $8 \times 414 = 3312$ and $5 \times 662 = 3310$; $3312 - 3310 = 2$. ✓

(d) Solve $18x \equiv 30 \pmod{42}$. Let $d = \gcd(18, 42) = 6$. Since $6 \mid 30$, the congruence is **solvable**, and it has exactly $d = 6$ incongruent solutions modulo 42.

Divide the congruence *and the modulus* by 6:

$$3x \equiv 5 \pmod{7}.$$

Now $\gcd(3, 7) = 1$. An inverse of 3 modulo 7 is 5, because $3 \times 5 = 15 = 2 \times 7 + 1 \equiv 1 \pmod{7}$. Multiplying,

$$x \equiv 5 \times 5 = 25 \equiv 4 \pmod{7}.$$

Lifting back to modulus 42 by adding multiples of $42/6 = 7$:

$$x \equiv 4, 11, 18, 25, 32, 39 \pmod{42}.$$

Verification.

x	$18x$	$18x \pmod{42}$
4	72	$72 - 42 = 30$ ✓
11	198	$198 - 4(42) = 30$ ✓
18	324	$324 - 7(42) = 30$ ✓
25	450	$450 - 10(42) = 30$ ✓
32	576	$576 - 13(42) = 30$ ✓
39	702	$702 - 16(42) = 30$ ✓

(e) $p \mid a^n \Rightarrow p \mid a$, by induction; then $\sqrt{p}$ irrational. **Claim.** For every prime p and every integer a : for all $n \geq 1$, if $p \mid a^n$ then $p \mid a$.

Proof by induction on n . Base case $n = 1$. If $p \mid a^1 = a$ then $p \mid a$. Trivially true.

Inductive step. Assume the statement holds for some $k \geq 1$: if $p \mid a^k$ then $p \mid a$. Suppose now $p \mid a^{k+1} = a \cdot a^k$. Since p is prime, by Lemma 8.22 (a prime dividing a product divides one of the factors) either

- $p \mid a$, and we are done; or
- $p \mid a^k$, in which case the inductive hypothesis gives $p \mid a$.

Either way $p \mid a$, so the statement holds for $k + 1$.

By the principle of mathematical induction it holds for all $n \geq 1$. ■

Consequence: $\sqrt{p}$ is irrational.

Proof by contradiction. Suppose $\sqrt{p}$ is rational and write it *in lowest terms*:

$$\sqrt{p} = \frac{a}{b}, \quad a, b \in \mathbb{Z}, \quad b \neq 0, \quad \gcd(a, b) = 1.$$

Squaring gives $a^2 = p b^2$, so $p \mid a^2$. By the claim (with $n = 2$), $p \mid a$; write $a = pk$. Substituting,

$$pb^2 = a^2 = p^2 k^2 \implies b^2 = pk^2,$$

so $p \mid b^2$ and, by the claim again, $p \mid b$.

The contradiction: p divides both a and b , so $\gcd(a, b) \geq p \geq 2$; but we assumed $\gcd(a, b) = 1$. The assumption that $\sqrt{p}$ is rational in lowest terms is therefore untenable, and $\sqrt{p}$ is irrational. ■

Notice that part (b) is the special case $p = 3$ of part (e). Writing the general proof first and then specialising is usually cleaner than repeating the argument.

APPENDIX C

Quick Reference

Everything that is worth having on one page during revision. Each entry points back to the chapter where it is derived.

C.1 Truth tables and equivalences

p	q	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \rightarrow q$	$p \leftrightarrow q$
0	0	0	0	0	1	1
0	1	0	1	1	1	0
1	0	0	1	1	0	0
1	1	1	1	0	1	1

Precedence: $\neg > \wedge > \vee > \rightarrow > \leftrightarrow$ (right-associative).

Law	Logic	Sets
Identity	$p \wedge \mathbf{T} \equiv p$	$A \cap \mathbb{U} = A$
Domination	$p \vee \mathbf{T} \equiv \mathbf{T}$	$A \cup \mathbb{U} = \mathbb{U}$
Idempotent	$p \vee p \equiv p$	$A \cup A = A$
Double negation	$\neg\neg p \equiv p$	$\overline{\overline{A}} = A$
Commutative	$p \vee q \equiv q \vee p$	$p \wedge q \equiv q \wedge p$
Associative	$(p \vee q) \vee r \equiv p \vee (q \vee r)$	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
Distributive	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
De Morgan	$\neg(p \vee q) \equiv \neg p \wedge \neg q$	$\neg(p \wedge q) \equiv \neg p \vee \neg q$
Absorption	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Negation	$p \vee \neg p \equiv \mathbf{T}$	$p \wedge \neg p \equiv \mathbf{F}$

Conditional identities

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

C.2 Rules of inference

p $\frac{p \rightarrow q}{\therefore q}$	Modus ponens	$\frac{p}{\therefore p \vee q}$	Addition
$\neg q$ $\frac{p \rightarrow q}{\therefore \neg p}$	Modus tollens	$\frac{p \wedge q}{\therefore p}$	Simplification
$\frac{p \rightarrow q}{q \rightarrow r}$ $\therefore p \rightarrow r$	Hypothetical syll.	$\frac{p}{q}$ $\therefore p \wedge q$	Conjunction
$\frac{p \vee q}{\neg p}$ $\therefore q$	Disjunctive syll.	$\frac{p \vee q}{\neg p \vee r}$ $\therefore q \vee r$	Resolution

Fallacies. Affirming the consequent ($p \rightarrow q, q \therefore p$) and denying the antecedent ($p \rightarrow q, \neg p \therefore \neg q$) are *invalid*.

Quantifier rule	Side condition
UI: $\forall x P(x) \therefore P(c)$	any c
UG: $P(c)$ for arbitrary $c \therefore \forall x P(x)$	c must be <i>arbitrary</i>
EI: $\exists x P(x) \therefore P(c)$	c must be <i>fresh</i> , used consistently
EG: $P(c) \therefore \exists x P(x)$	any c

C.3 Quantifier rules

$$\begin{aligned}
 \neg \forall x P(x) &\equiv \exists x \neg P(x), & \neg \exists x P(x) &\equiv \forall x \neg P(x). \\
 \forall x (P \wedge Q) &\equiv \forall x P \wedge \forall x Q, & \exists x (P \vee Q) &\equiv \exists x P \vee \exists x Q. \\
 \forall x (P \vee Q) &\not\equiv \forall x P \vee \forall x Q, & \exists x (P \wedge Q) &\not\equiv \exists x P \wedge \exists x Q. \\
 \exists x \forall y P(x, y) &\rightarrow \forall y \exists x P(x, y) & (\text{never the converse}).
 \end{aligned}$$

Translation patterns: “all A s are B s” $\rightsquigarrow \forall x (A(x) \rightarrow B(x))$; “some A is a B ” $\rightsquigarrow \exists x (A(x) \wedge B(x))$.

C.4 Proof methods

Method	Assume	Derive
Vacuous	—	p false
Trivial	—	q true
Direct	p	q
Contraposition	$\neg q$	$\neg p$
Contradiction	$p \wedge \neg q$	$r \wedge \neg r$
Cases	each p_i	q each time (cases must be exhaustive)
Equivalence (n statements)	—	the cycle $p_1 \rightarrow p_2 \rightarrow \cdots \rightarrow p_n \rightarrow p_1$
Counterexample	—	one x with $\neg P(x)$
Uniqueness	$P(y)$	$y = x$, after proving existence
Set equality	$x \in A / x \in B$	the reverse membership, both ways

Definitions to unfold. n even $\iff n = 2k$; n odd $\iff n = 2k+1$; r rational $\iff r = a/b$ with $a \in \mathbb{Z}, b \in \mathbb{Z}^+$.

C.5 Sets

$$\begin{aligned}
A \cup B &= \{x \mid x \in A \vee x \in B\}, & A \cap B &= \{x \mid x \in A \wedge x \in B\}, \\
A - B &= \{x \mid x \in A \wedge x \notin B\} = A \cap \overline{B}, & A \triangle B &= (A - B) \cup (B - A), \\
\overline{A} &= \mathbb{U} - A, & |\mathcal{P}(A)| &= 2^{|A|}. \\
A \subseteq B &\iff \forall x(x \in A \rightarrow x \in B), & A = B &\iff A \subseteq B \wedge B \subseteq A. \\
|A \cup B| &= |A| + |B| - |A \cap B|, \\
|A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.
\end{aligned}$$

Bit-string operations (fixed universe of size n): $\cup \rightarrow$ bitwise OR, $\cap \rightarrow$ bitwise AND, $\neg \rightarrow$ bitwise NOT, $\triangle \rightarrow$ bitwise XOR.

C.6 Functions

Property	Definition	Proof template
One-to-one	$f(a) = f(b) \rightarrow a = b$	Assume $f(x_1) = f(x_2)$; derive $x_1 = x_2$
Onto	$\forall y \in B \exists x \in A : f(x) = y$	Take arbitrary y ; solve for x ; check $x \in A$
Bijection	one-to-one and onto	Both of the above
Invertible	$\iff$ bijection	$f^{-1} \circ f = \iota_A, f \circ f^{-1} = \iota_B$

$$(f \circ g)(x) = f(g(x)) \quad (\text{right one first}).$$

$$\begin{aligned}
f(S \cup T) &= f(S) \cup f(T), & f(S \cap T) &\subseteq f(S) \cap f(T) \text{ (equality iff } f \text{ injective),} \\
f^{-1}(S \cup T) &= f^{-1}(S) \cup f^{-1}(T), & f^{-1}(S \cap T) &= f^{-1}(S) \cap f^{-1}(T), & f^{-1}(B - S) &= A - f^{-1}(S). \\
\lfloor x \rfloor &\leq x < \lfloor x \rfloor + 1, & \lceil x \rceil &= -\lfloor -x \rfloor, & \lfloor x + n \rfloor &= \lfloor x \rfloor + n \quad (n \in \mathbb{Z}).
\end{aligned}$$

C.7 Relations

Property	Definition	Refute by
Reflexive	$\forall a (a, a) \in R$	one a with $(a, a) \notin R$
Symmetric	$(a, b) \in R \rightarrow (b, a) \in R$	$(a, b) \in R, (b, a) \notin R$
Anti-symmetric	$(a, b), (b, a) \in R \rightarrow a = b$	$a \neq b$ with both in R
Transitive	$(a, b), (b, c) \in R \rightarrow (a, c) \in R$	$(a, b), (b, c) \in R, (a, c) \notin R$

Relations on $ A = n$	Count	Structure	Properties
all	2^{n^2}	Equivalence relation	refl. + sym. + trans.
reflexive	2^{n^2-n}	Partial order	refl. + anti-sym. + trans.
symmetric	$2^{n(n+1)/2}$		
anti-symmetric	$2^n 3^{n(n-1)/2}$		

$$\begin{aligned}
S \circ R &= \{(a, c) \mid \exists b: (a, b) \in R \wedge (b, c) \in S\}, & R^1 &= R, & R^{n+1} &= R^n \circ R. \\
R \text{ transitive} &\iff R^2 \subseteq R \iff R^n \subseteq R \quad \forall n \geq 1.
\end{aligned}$$

C.8 Number theory

$$\begin{aligned}
a \mid b &\iff \exists c \in \mathbb{Z} (b = ac); & a \mid b, a \mid c &\implies a \mid (mb + nc). \\
a &= dq + r, \quad 0 \leq r < d; & q &= a \text{ div } d, \quad r = a \text{ mod } d. \\
a \equiv b \pmod{m} &\iff m \mid (a - b) \iff a \text{ mod } m = b \text{ mod } m \iff a = b + km.
\end{aligned}$$

Result	Statement
Congruence arithmetic	$a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}, ac \equiv bd \pmod{m}$
Cancellation	$ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1 \Rightarrow a \equiv b \pmod{m}$
gcd/lcm from factorisations	lowest powers for gcd, highest for lcm
Product rule	$ab = \gcd(a, b) \cdot \text{lcm}(a, b)$
Euclid's lemma	$a = bq + r \Rightarrow \gcd(a, b) = \gcd(b, r)$
Euclidean algorithm	gcd = last non-zero remainder
Bézout	$\exists s, t : \gcd(a, b) = sa + tb$
Inverse	$\bar{a}$ exists mod $m \iff \gcd(a, m) = 1$
Linear congruence	$ax \equiv b \pmod{m}$ solvable iff $\gcd(a, m) \mid b$; then $\gcd(a, m)$ solutions
CRT	pairwise coprime m_i : $x = \sum a_k M_k y_k \pmod{m}$, $M_k = m/m_k$, $y_k = \overline{M_k} \pmod{m_k}$
Euler	$\gcd(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$
Fermat	p prime, $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$
Totient	$\varphi(n) = n \prod_{p \mid n} (1 - \frac{1}{p})$

C.9 Common pitfalls

1. $p \rightarrow q$ is *true* whenever p is false.
2. The converse and inverse are *not* equivalent to the original; only the contrapositive is.
3. “ p only if q ” is $p \rightarrow q$, not $q \rightarrow p$.
4. $\equiv$ is not a connective and never gets a truth-table column.
5. Negating a quantified statement flips *every* quantifier the negation passes.
6. $\forall$ does not distribute over $\vee$; $\exists$ does not distribute over $\wedge$.
7. $\exists x \forall y \neq \forall y \exists x$.
8. Universal generalisation needs an *arbitrary* constant; existential instantiation needs a *fresh* one.
9. Anti-symmetric $\neq$ not symmetric; a relation may be both or neither.
10. $f(S \cap T)$ may be strictly smaller than $f(S) \cap f(T)$.
11. $\lfloor -4.25 \rfloor = -5$, not -4 .
12. Remainders in the division algorithm are never negative.
13. You may not cancel a factor in a congruence unless it is coprime to the modulus.
14. In $f \circ g$ and $S \circ R$, the *right-hand* one acts first.
15. Venn diagrams illustrate and refute, but do not prove.
16. Checking many instances never proves a universal statement.