Precalculus: Algebra Part I

Polynomials

Gudfit

Contents

Chapter 1

Ideas & Motivations

Welcome to Algebra I by me (Gudfit). The point of these notes is to cover everything I think is important as I build up to my current math and physics knowledge, while keeping it free and accessible for everyone from kids to adults.

I aim for each set of notes to be max 150 pages (excluding exercise pages) [1], as rigorous as possible, and far-reaching too. That means I'll cover the axioms and proofs of the most interesting stuff, plus I'll pull in other subjects we've already touched on to show how math builds on itself like funky Lego. These notes build on my existing informal logic notes, and they're aimed at keeping the proofs, ideas, and build-up of algebra as informal as possible.

It'll be a mix of quick ideas and concepts, but in the appendix for each section, I'll go rigorous with the key axioms pulled from a bunch of books. For those theorems and ideas in the appendix, everything will be proved as we build towards writing proofs and set theory.

The original idea was a fully rigorous intro like Euler's Elements of Algebra, but that felt too grindy. Why slog through it when you can just read other people's notes, papers, or books? So this'll be more efficient (not totally deductive) assuming you've got some mathematical rigor. Either way, let's dive in and enjoy!

[1] Currently $\approx$ 76 pages of exercises.

Chapter 2

Introduction

Before we continue with algebra, it's important to note that, unlike other sciences that rely on experiments and observations of the real world, mathematics is built on a foundation of pure logic.

Think of it this way: if physics is the study of how the universe works, mathematics is the study of what must be true if we agree on a certain set of starting rules. This process of establishing undeniable truth from agreed-upon rules is called proof. This builds directly on the ideas discussed in my notes on Informal Logic. To get everyone on the same page, let's expand our vocabulary with the key terms that form the language of mathematical proof.

2.1 Our Dictionary

Every game needs rules. You can't play chess if the players don't agree on how the pieces move. Mathematics is the same — but before we talk about the rules, we need a shared vocabulary. Definitions tell us exactly what our words and symbols mean so that arguments and proofs are clear.

Note. As mentioned in my Informal Logic notes, we already talked about what definitions are and why they matter. Here is the quick version we will use in these notes.

Definition 2.1.1. ***(Definition)***. A definition fixes the meaning of a word or symbol for us. It is not something "we prove"; it is an agreement about how we will use a term so that later statements and proofs are clear.

Note. There are two helpful viewpoints:

- **Intensional**: tell the properties something must have to fit the term.
- **Extensional**: give examples the term applies to (good for intuition, but we usually cannot list them all).

Definition 2.1.2. ***(Well-defined)***. A rule is well-defined if the result does not depend on how something is written or named. The same object always gives the same outcome.

Example 2.1.1. Tiny examples.

- **Square (notation).** For any number x, define $x^2 := x \times x$. The symbol ":=" means "is defined to be."
- **Not well-defined (warning).** The rule "send a fraction a/b to the top number a" fails, because $\frac{1}{2}$ and $\frac{2}{4}$ name the same number but would give different results.

With our meanings fixed, we can now talk about the basic rules of the system. These are called axioms.

Definition 2.1.3. ***(Axiom)***. Axioms are agreed-upon statements or assumptions that are accepted as true without requiring proof.

Axioms are the starting points, the foundation upon which everything else is built. To see this in action, consider a classic puzzle:

Example 2.1.2. Suppose you need to transport a fox, a chicken, and a bag of grain across a river. The constraints (axioms) are:

(i) The boat can only hold you and one additional item (fox, chicken, or grain).
(ii) The chicken will eat the grain if left alone together.
(iii) The fox will eat the chicken if left alone together.
(iv) The fox does not eat grain.
(v) Neither the fox nor the chicken will run away.

In this example, the word problem is framed within a narrative, requiring the solver to apply the specified rules creatively to achieve the goal of transporting all items safely across the river.

Thus given these rules we argue if these axioms are universally true; we say, "IF we accept these axioms, THEN what is possible?"

Once we have our axioms, we use logic to see what they imply. The beautiful, proven statements we derive from axioms are called theorems.

Definition 2.1.4. ***(Theorem)***. A theorem is a mathematical statement that is true and can be (or has been) verified to be true.

A theorem normally has the form "If P, then Q," it can be regarded as a device that produces new information from P. Whenever we are dealing with a situation in which P is true, then the theorem guarantees that, in addition, Q is true. Since this kind of expansion of information is useful, theorems of the form, "If P, then Q", are very common.

But not every theorem is a conditional statement. Some have the form of the bi-conditional $P \iff Q$, which can be expressed as two conditional statements ("P, then Q" only if "Q then P"). Other theorems simply state facts about specific things. In general the word *theorem* is reserved for a statement that is considered important or significant:

Definition 2.1.5. ***(Lemma)***. A lemma is a theorem whose main purpose is to help prove another theorem.

Definition 2.1.6. ***(Corollary)***. A corollary is a result that follows almost immediately from a theorem. It's a direct consequence or a special case of a theorem that's already been proven. If a theorem is a major victory, a corollary is a quick bonus prize you get for free.

Note. As mentioned in my Informal Logic notes, there is one more term: a proposition. This is simply a statement that is proven to be true, but is often considered less significant or central than a theorem. It's a versatile term for a proven fact that might be a small standalone result or a stepping stone.

2.2 Definitions

At its core, the study of mathematics is built upon the study of increasing and decreasing quantities, or magnitudes[1], sometimes referred to as the science of quantity.

From the fruit that person X[2] purchases at a store, to the measurement of vast interstellar distances, the concept of quantity is ubiquitous. However, we cannot quantify or determine a specific amount except by comparing it to a similar magnitude of the same kind. For instance, when enumerating fruit, we might regard the collection as a single total or distinguish them by category (apples, pears, bananas). To formalise this comparison, we require a standard.

[1] We will study magnitudes in greater depth shortly.
[2] X is a variable; in this context, it acts as a placeholder for any person's name.

Definition 2.2.1. ***(Unit)***. A unit is a magnitude of a particular species, arbitrarily chosen and adopted as a fixed standard, to which all other magnitudes of that same species are referred for comparison.

Remark. A unit is the basic "one" for a kind of quantity. It is the smallest step we count by. If you change the unit, the number changes, but the quantity being measured remains the same.

Definition 2.2.2. ***(Measure)***. A measure is a standard, agreed-upon amount for a given quantity, adopted as a unit, to which other magnitudes of that species are compared. The number attached to a magnitude tells how many units of that species it contains.

Definition 2.2.3. ***(Number)***. A number, then, is nothing more than the proportion of one magnitude to another.

Example 2.2.1. (Sand on a beach). Stand at the edge of a beach and draw a small square in the sand. Everything inside that square is our amount of sand. Before we start, we choose a unit: one handful[3]. Now scoop the sand out, one handful at a time, saying the numbers out loud as you go. The last number you say is the measure of that sand in handfuls.

If you switch to a bigger scoop and repeat, you will finish sooner and stop at a smaller number. If you switch to a tiny spoon, you will take longer and stop at a bigger number. The sand did not change. Only the unit changed, so the number you report changed with it.

From these simple definitions, it should be easy to tell that numbers can express all magnitudes. Therefore, the very foundation of the mathematical sciences must be a complete science of numbers. We call this science **Algebra** [4].

In Algebra, we leave behind the different kinds of quantities and deal only with the numbers that represent them. This is what separates it from Arithmetic. While Arithmetic treats numbers specifically for specific calculations, Algebra is the general science that comprehends all possible cases in the doctrine and calculation of numbers.

[3]Use the same cup or scoop each time so that one handful always means the same amount.

[4]Some also call it Analysis, but I prefer to regard that subject, as distinct from Algebra, better viewed as a successor to Algebra.

Chapter 3

Basic Operators: Addition

From 2.2.3, a number records the unit count of a magnitude. The operation that adjoins more units is *addition*, denoted by $+$.

3.1 Operators, Operands, and Relations

Definition 3.1.1. ***(Operator)***. An operator is a symbol that prescribes an action or process to be performed (e.g., $+$).

Definition 3.1.2. ***(Operand)***. An operand is the subject or quantity on which an operator acts.

In the expression $a + 1$, `+1` acts as a single instruction: "add one unit" to the operand a. This link is vital; when rearranging expressions, the operator must accompany its operand.

Definition 3.1.3. ***(Relation)***. A relational symbol compares two quantities or expressions, producing a statement that is either true or false.

Equality

The symbol "$=$" denotes *equality*. The statement $A = B$ asserts that A and B denote the same value. Equality is reflexive ($x = x$), symmetric ($x = y \implies y = x$), and transitive ($x = y \land y = z \implies x = z$). Crucially, it satisfies the *substitution property*: if $A = B$, A may replace B in any expression without altering the value.

Remark. Ideally, one views an equation $L = R$ as a balance. Replacing a quantity on one side with an equal quantity maintains this balance.

3.2 Constructing Numbers

The fundamental family of numbers used for counting is generated by repeatedly adding one unit.

Definition 3.2.1. ***(Natural Numbers)***. The set of counting numbers $\{1, 2, 3, \dots\}$ is called the **natural numbers**, denoted by $\mathbb{N}$.

Definition 3.2.2. ***(Successor)***. For any number a, the expression $a + 1$ denotes the *successor* of a: the result of adjoining one unit. Chaining this action produces the sequence:

$$a \mapsto a + 1 \mapsto (a + 1) + 1 \mapsto \cdots$$

Definition 3.2.3. ***(Addition by Successive Unit Steps)***. For numbers a and b, the sum $a+b$ is the result of applying the successor action `+1` exactly b times to a. This is formalised by the rule:

$$a+(b+1) \coloneqq (a+b)+1$$

3.2.1 The Fundamental Laws of Addition

Addition, as built from the `+1` action, obeys two fundamental rules. These laws are axioms: rules accepted as true without proof. They are tools for rearranging and simplifying expressions involving addition.

The Law of Association

When adding several numbers, brackets (or parentheses) `()` indicate which part of the sum to perform first. This is called **grouping**. The Law of Association states that in a chain of additions, the grouping does not matter.

***Axiom* 3.2.1. (Associative Law of Addition).** For any numbers a, b, and c,

$$(a+b)+c = a+(b+c) \tag{3.1}$$

On the left side, we add a and b first. On the right, we add b and c first. The law states that both ways give the same answer.

Proof. We understand this law by remembering that numbers are collections of units. The sum $(2+3)+4$ means we first join a group of two units with a group of three, and then join a group of four to that new group. The sum $2+(3+4)$ means we first join the groups of three and four, and then join the group of two to that result. In either case, the process simply gathers all the individual units.

$$(2+3)+4 = (\underbrace{1+1}_{2}+\underbrace{1+1+1}_{3})+\underbrace{1+1+1+1}_{4}$$
$$2+(3+4) = \underbrace{1+1}_{2}+(\underbrace{1+1+1}_{3}+\underbrace{1+1+1+1}_{4})$$

Both sides are a chain of adding one nine times. The final collection of units is the same, so the results must be identical.[1] ■

This law allows us to write a sum like $a+b+c$ without brackets, as the order of calculation yields the same result.

The Law of Commutation

The second fundamental law states that the order in which we add numbers does not affect the outcome.

***Axiom* 3.2.2. (Commutative Law of Addition).** For any numbers a and b,

$$a+b = b+a \tag{3.2}$$

This law allows us to rearrange terms in a sum freely, a property that is invaluable for simplifying expressions.

Proof. We again appeal to the decomposition of numbers into units. To show that $2+3=3+2$, we expand both sides:

$$2+3 = (1+1)+(1+1+1)$$
$$3+2 = (1+1+1)+(1+1)$$

[1] Note that this is an observation rather than a formal proof. A full proof will be explored in the Set Theory Notes.

Both expressions represent joining a group of two units and a group of three units. The final result is a collection of five units. The order in which the groups are combined is irrelevant to the total number of units. ■

Definition 3.2.4. ***(Term)***. An algebraic expression can be written as a sum of parts. Each of these parts, along with its preceding sign, is called a term. For example, in the expression $3 + 5$, the terms are $+3$, and $+5$.

Calculation and Geometric View

The laws of addition provide the framework for calculation.

Example 3.2.1. (Calculating $2 + 3$). To find the sum of 2 and 3, we start at 2 and apply the `+1` operator three times, using the Associative Law to regroup the steps.

$$\begin{aligned} 2 + 3 &= 2 + (1 + 1 + 1) && \text{Since } 3 = 1 + 1 + 1 \\ &= (2 + 1) + 1 + 1 && \text{By 3.2.1} \\ &= 3 + 1 + 1 \\ &= (3 + 1) + 1 && \text{By 3.2.1} \\ &= 4 + 1 \\ &= 5 \end{aligned}$$

This algebraic construction has a direct geometric counterpart. We can represent our unit from 2.2.1 as a line segment of a fixed length. Starting from a point on a line, we mark off this unit segment. The endpoint is labelled 1. Repeating this step from the new endpoint yields the marks for $2, 3$, and so on, as illustrated in Figure 3.1.

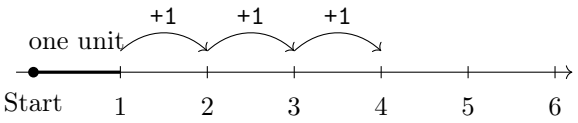


Figure 3.1: Constructing the number line from a chosen unit by successive applications of the `+1` operator. The marks $1, 2, 3, \ldots$ record how many unit steps have been taken from the start.

The position marked by the numeral n is reached by performing the successor action n times.

$$\underbrace{\texttt{+1};\texttt{+1};\cdots;\texttt{+1}}_{n \text{ times}} \quad = \quad n.$$

3.3 Zero

Every operation in algebra should have an inverse: an operation that undoes its effect. Before defining the inverse of addition, we must establish a starting point. If we add a unit and then immediately take it away, we return to where we began. This state of "no magnitude" is represented by a special number.

Definition 3.3.1. ***(Zero)***. The number that represents the absence of any units is called **zero**, denoted by the symbol 0. It is the number that results from subtracting any quantity from itself:

$$a - a = 0$$

A fundamental property of zero is that adding it to any number does not change that number's value, as it represents adding no units. This makes zero the *identity element*[2] for addition.

[2]This concept will be explained later.

***Axiom* 3.3.1. (Additive Identity).** For any number a,

$$a + 0 = 0 + a = a \tag{3.3}$$

3.4 Inverse of Addition

Addition combines magnitudes; its inverse takes them away. This inverse operation is called subtraction, denoted by the symbol $-$. Formally, subtraction is the inverse of addition, meaning the operation $-b$ undoes the effect of $+b$, and vice versa. This relationship is expressed by:

$$a + b - b = a \quad \text{and} \quad a - b + b = a \tag{3.4}$$

Remark. As mentioned in section 3.1, the symbols $+$ and $-$ act as signs that instruct how a quantity is to be treated. A preceding $+$ means "to be added"; a preceding $-$ means "to be subtracted". The expression $a + b$ means "to the quantity a, add the quantity b".

We can also view subtraction as finding a "missing addend".

Definition 3.4.1. ***(Subtraction as a Missing Addend).*** For numbers a and b, the difference $a - b$ is the unique number c that one must add to b to obtain a.

$$\begin{aligned} c + b &= a \\ c &= a - b. \end{aligned}$$

The mechanism for subtraction is the **predecessor** action, `-1`, which undoes a single successor step.

Definition 3.4.2. ***(`-1` as Predecessor).*** For any number a from which a unit can be removed, the expression $a - 1$ denotes the unique number c such that $c + 1 = a$.

The difference $a - b$ is therefore calculated by starting at a and applying the predecessor action `-1` exactly b times.

Example 3.4.1. (Calculating $5 - 3$). To find the difference $5 - 3$, we begin at 5 and apply the predecessor action `-1` three times.

$$\begin{aligned} 5 - 3 &= (5 - 1) - 1 - 1 && \text{First application of } \texttt{-1} \\ &= 4 - 1 - 1 \\ &= (4 - 1) - 1 && \text{Second application of } \texttt{-1} \\ &= 3 - 1 && \text{Third application of } \texttt{-1} \\ &= 2 \end{aligned}$$

The instruction -3 is carried out as a sequence of three `-1` actions. We can verify that $2 + 3 = 5$.

Geometrically, if addition is movement to the right on the number line, subtraction is movement to the left, as shown in Figure 3.2.

Note. A direct consequence of our definitions is that subtracting zero leaves a number unchanged. By 3.4.1, $a - 0$ is the number c such that $c + 0 = a$. From the additive identity axiom, $c + 0 = c$, which implies $c = a$. Therefore, $a - 0 = a$.

Remark. Finally from this we can conclude that if

$$a + 12 = 24$$

then $a = 12$.

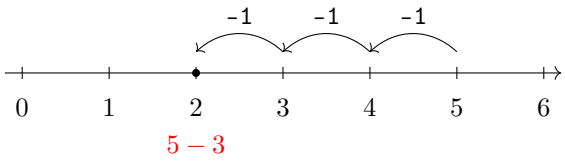


Figure 3.2: Subtraction on the number line as movement to the left. Each application of the `-1` operator moves one unit step back towards the start.

3.4.1 Laws of Commutation and Association Extended

The fundamental laws of association and commutation extend to expressions involving both addition and subtraction.

***Theorem* 3.4.1. (Commutative Law for Addition and Subtraction).** In any chain of additions and subtractions, the terms may be written in any order, provided each keeps its proper sign.

$$a + b - c = a - c + b \tag{3.5}$$

Proof. *By the definition of subtraction as an inverse operation, we can write* $a = a - c + c$.

$$\begin{aligned}
a + b - c &= (a + 0) + b - c && \textit{(3.3.1)} \\
a + b - c &= (a + (-c + c)) + b - c && \textit{Replace } a \textit{ with an equivalent expression} \\
&= a - c + (c + b) - c && \textit{By the Associative Law (3.2.1)} \\
&= a - c + (b + c) - c && \textit{By the Commutative Law (3.2.2)} \\
&= a - c + b + (c - c) && \textit{By the Associative Law} \\
&= a - c + b + 0 && \textit{By the definition of zero} \\
&= a - c + b
\end{aligned}$$

This shows that the operand c *and its operator* $-$ *can be moved together.* ■

Remark. The logic of this proof relies on the properties of zero. The rearrangement is made possible by introducing a pair of cancelling operations, $+c$ and $-c$. In the proof, this pair appears as the term $(c - c)$, which simplifies to 0 by 3.3.1. Since adding zero does not change the expression's value (3.3.1), the reordering is justified.

***Theorem* 3.4.2. (Associative Law for Addition and Subtraction).** If a bracketed expression is preceded by a + sign, the bracket may be removed without changing any signs. If it is preceded by a − sign, the bracket may be removed by changing the sign of every term inside.

$$\begin{aligned}
a + (b - c) &= a + b - c \\
a - (b - c) &= a - b + c
\end{aligned}$$

Proof. *The first case is straightforward. For the second, let* $x = a - (b - c)$. *By the definition of subtraction, this means:*

$$\begin{aligned}
x + (b - c) &= a \\
(x + b) - c &= a && \textit{By the Associative Law} \\
x + b &= a + c && \textit{Add } c \textit{ to both sides} \\
x &= a + c - b && \textit{Subtract } b \textit{ from both sides} \\
x &= a - b + c && \textit{By the Commutative Law}
\end{aligned}$$

Thus, $a - (b - c) = a - b + c$. ■

3.4.2 Negative Numbers

Our definition of subtraction, $a - b$, has so far assumed that a is larger than b. What about $3 - 5$? Using the missing addend definition from 3.4.1, we seek a number c such that $c + 5 = 3$. No such number exists on our current number line.

Algebra is the general theory of these operations; we establish laws and follow them. When results like $3 - 5$ cannot be interpreted with our current numbers, they force us to invent new concepts that are consistent with our laws.

Mechanically, calculating $3 - 5$ means starting at 3 and applying the predecessor action `-1` five times.

$$3 \xrightarrow{\texttt{-1}} 2 \xrightarrow{\texttt{-1}} 1 \xrightarrow{\texttt{-1}} 0 \xrightarrow{\texttt{-1}} ?$$

A step to the left from 0 takes us off our number line. To solve this, we must extend our system. A step of -1 from 0 lands on a point we call **negative one**, or -1. A further step lands on -2.

Definition 3.4.3. ***(Negative Number)***. A negative number, denoted $-a$, is the number that results from subtracting a positive number a from zero.

$$-a := 0 - a$$

With this, we can complete our calculation: $3 - 5 = (3 - 3) - 2 = 0 - 2 = -2$.

By extending our number line to include these new negative numbers, along with zero and the natural numbers, we form a more complete system of numbers.

Definition 3.4.4. ***(Integers)***. The system of numbers formed by combining the natural numbers ($\mathbb{N}$), their negative counterparts (additive inverses), and zero is called the **integers**. This collection of whole numbers, stretching infinitely in both positive and negative directions, is denoted by the symbol $\mathbb{Z}$.

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

3.4.3 The Additive Inverse

The most important property of a negative number is that it is the **opposite**, or **additive inverse**, of its positive counterpart.

***Axiom* 3.4.1. (Additive Inverse)**. For every number a, there exists a unique additive inverse, denoted $-a$, such that their sum is zero.

$$a + (-a) = 0 \tag{3.6}$$

This axiom holds for any number, including zero. If we let $a = 0$, the axiom states $0 + (-0) = 0$. By the Additive Identity property from 3.3.1, we know that $0 + (-0)$ is the same as -0. Thus we can conclude that $-0 = 0$. Zero is unique in that it is its own additive inverse.

The uniqueness of the additive inverse leads to a crucial theorem.

***Theorem* 3.4.3.** . If the sum of two numbers is zero, then each number is the additive inverse of the other.

$$\text{If } a + b = 0, \text{ then } a = -b \text{ and } b = -a.$$

Proof. We start with the given equation, $a + b = 0$. To show that $a = -b$, we must isolate a. We can achieve this by adding the additive inverse of b, which is $-b$, to both sides of the equation.

$$\begin{aligned}
(a + b) + (-b) &= 0 + (-b) && \text{Add } -b \text{ to both sides} \\
a + (b + (-b)) &= 0 + (-b) && \text{By the Associative Law (3.2.1)} \\
a + 0 &= -b && \text{By the Additive Inverse axiom (3.4.1)} \\
a &= -b && \text{By the Additive Identity axiom (3.3.1)}
\end{aligned}$$

The proof that $b = -a$ is symmetrical. We add $-a$ to both sides of $a + b = 0$. ■

This provides a powerful analogy. If positive numbers represent assets, negative numbers can represent debts. A possession of 100 crowns (+100) combined with a debt of 50 crowns (−50) results in a net worth of $100 - 50 = 50$ crowns. If the possession and debt are equal, for example +50 and −50, the net worth is $50 - 50 = 0$.

These new numbers allow us to extend our number line to the left of zero, creating a complete line that stretches infinitely in both positive and negative directions, as shown in Figure 3.3.

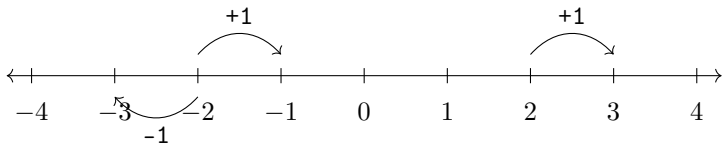


Figure 3.3: The extended number line: `+1` steps to the right, and `-1` steps to the left.

3.4.4 Operations with Signed Numbers

The extended laws of association give us the rules for all combinations of operations with signed numbers. A quantity to be added is called a *positive* quantity ($+a$), and a quantity to be subtracted is a *negative* quantity ($-a$). If a number at the beginning of an expression has no sign, it is assumed to be positive.

The rules are direct applications of removing brackets.

(i) **Adding a negative number:** $a + (-b) = a - b$. Adding a negative is the same as subtracting its positive counterpart.

Example 3.4.2. $(7 + (-3) = 4)$. The calculation $7 + (-3)$ is the same as $7 - 3$, which is 4.

(ii) **Subtracting a negative number:** $a - (-b) = a + b$. This is an application of the law $a - (x - y) = a - x + y$.

$$a - (-b) = a - (0 - b) = a - 0 + b = a + b$$

Subtracting a negative is the same as adding its positive counterpart.

Example 3.4.3. $(7 - (-3) = 10)$. The expression $7 - (-3)$ simplifies to $7 + 3$, which is 10.

The following theorems are fundamental for manipulating algebraic sums.

***Theorem* 3.4.4. (Distributive Property of Negation).** The additive inverse of a sum is the sum of the additive inverses.

$$-(a + b) = -a - b \tag{3.7}$$

Proof. By the additive inverse axiom (3.4.1), we know that $-(a+b)$ is the unique number that, when added to $(a + b)$, results in 0. To prove the theorem, we must show that $(a + b) + (-a - b)$ is indeed equal to 0.

$$\begin{aligned}
(a + b) + (-a - b) &= a + b - a - b && \textit{Unifying addition and subtraction} \\
&= a - a + b - b && \textit{By the Commutative Law (3.2.2)} \\
&= (a - a) + (b - b) && \textit{By the Associative Law} \\
&= 0 + 0 && \textit{By the definition of zero} \\
&= 0 && \textit{By the Additive Identity axiom}
\end{aligned}$$

Since $(a + b) + (-a - b) = 0$, it must be that $(-a - b)$ is the additive inverse of $(a + b)$. ■

***Theorem* 3.4.5.** . The sum of two negative numbers is the negative of their sum.

$$(-a) + (-b) = -(a + b) \tag{3.8}$$

Proof.

$$\begin{aligned}(-a)+(-b) &= -a-b && \textit{Unifying addition and subtraction}\\ &= -(a+b) && \textit{By the Distributive Property of Negation}\end{aligned}$$

■

***Axiom* 3.4.2. (Double Negative).** The negative of a negative number is the original positive number.

$$-(-a) = a \tag{3.9}$$

Proof. Using the definition of a negative number, $-(-a) = 0-(-a)$. *From the rule for subtracting a negative, this becomes* $0+a$, *which is simply* a. *Geometrically, taking the negative of a number reflects it across* 0 *on the number line. Reflecting* a *gives* $-a$. *Reflecting* $-a$ *brings us back to* a. ■

3.4.5 Simplifying Algebraic Sums

The commutative and associative laws lead to a practical rule for reducing a chain of additions and subtractions, an "algebraic sum", to its simplest value.

Consider the expression $+a-b+c+d-e-f+g$. By the commutative law, we can reorder the terms to group all positive and negative quantities.

$$+a+c+d+g-b-e-f$$

By the associative law, we can group these into two collections:

$$+(a+c+d+g)-(b+e+f)$$

This leads to the following rule: *To evaluate a chain of additions and subtractions, add all positive quantities, and separately add all positive counterparts of the negative quantities. Take the difference of the two sums and affix the sign of the greater.*

Example 3.4.4. $(+3-5+6+8-9-10+2)$.

$$\begin{aligned}+3-5+6+8-9-10+2 &= +(3+6+8+2)-(5+9+10)\\ &= +19-24\\ &= -(24-19) = -5\end{aligned}$$

3.5 Comments on Proofs

The proofs presented in this chapter all follow the same logical structure. The step-by-step process is driven by rules of inference, primarily modus ponens, as detailed in the companion notes on Informal Logic. If the reasoning in any of the proofs is difficult to follow, a review of those notes is the recommended way to clarify the steps.

3.6 Exercises

Note. Problems marked with a ⋆ are more challenging and may require combining several ideas from the chapter.

Part I: Foundational Identities and Properties

1. Justify each step in proving the following identities using only the commutative and associative laws of addition.

(a) $(a+b)+(c+d)=(a+c)+(b+d)$

(b) $(a+b)+(c+d)=(a+d)+(b+c)$

(c) $((x+y)+z)+w=(x+z)+(y+w)$

2. Justify each step in proving the following identities using the laws of addition and subtraction.

(a) $(a-b)+(c-d)=(a+c)-(b+d)$

(b) $(a-b)+(c-d)=(a-d)+(c-b)$

(c) $(a-b)+(c-d)=-(b+d)+(a+c)$

(d) $(x-y)-(z-w)=(x+w)-y-z$

(e) $(x-y)-(z-w)=(x-z)+(w-y)$

(f) $\star$ $(a-b)+(c-d)=-(b+d)-(-a-c)$

3. Prove the following properties of negation.

(a) $-(a+b+c)=-a-b-c$

(b) $-(a-b-c)=-a+b+c$

(c) $-(a-b)=b-a$

4. Prove the cancellation law for addition: If $a+b=a+c$, then $b=c$.

5. Prove: If $a+b=a$, then $b=0$.

6. Prove the following identities.

(a) Telescoping Sum: $(a-b)+(b-c)+(c-d)=a-d$.

(b) Cyclic Sum: $(a-b)+(b-c)+(c-a)=0$.

(c) $a-(b+c)=(a-b)-c$.

(d) $(a-b)-(c+d)=a-(b+c+d)$.

7. A System with Cancellation. If $(a+d=b+c)$ and $(a+c=b+d)$, prove that $a=b$ and $c=d$.

Part II: Numerical and Advanced Challenges

8. Without using a calculator, find the value of the following expression.

$$1-2+3-4+\cdots-100+101.$$

9. $\star$ Without using a calculator, solve: $1-(2-(3-(4-\cdots-(10-11)\cdots)))$.

10. $\star$ **Zero from a Balanced Sum.** If $a+b+c=0$, prove that $(-a)+(-b)+(-c)=0$ and conclude that $a=-(b+c)$.

Chapter 4

Basic Operators: Multiplication

Addition adjoins quantities; multiplication is the process of adding a quantity to itself a specified number of times. It is, in its primary sense, a shorthand for repeated addition.

4.1 Multiplication

Definition 4.1.1. ***(Multiplication)***. The result of adding a number a to itself n times is the **product** of a and n. This operation is called multiplication. Formally, for any number a and non-negative integer n, the product is defined recursively:

$$a \times 0 := 0$$
$$a \times (n+1) := (a \times n) + a$$

The number a is the **multiplicand**, and n is the **multiplier**.

Remark. We prove why $a \times 0 = 0$ later in the text.

From this definition, two immediate consequences are used constantly:

$$a \times 1 = a \times (0+1) = (a \times 0) + a = 0 + a = a$$
$$a \times 2 = a \times (1+1) = (a \times 1) + a = a + a$$

In general form, this is

$$a \times n = \underbrace{a + a + \cdots + a}_{n \text{ times}}$$

The product $a \times n$ can be written as $a \cdot n$ or, where no ambiguity arises, by simple apposition, as in an.

4.1.1 The Fundamental Laws of Multiplication

Just as addition is governed by its own laws, so too is multiplication. These laws are first observed with simple numbers but are then adopted as axiomatic rules for all algebraic quantities.

The Law of Commutation

In a product, the order of the numbers does not affect the result.

***Axiom* 4.1.1. (Commutative Law of Multiplication).** For any numbers a and b,

$$a \times b = b \times a \tag{4.1}$$

Proof. For integer multipliers, this law is easily visualised. The product 4×3 *means four groups of three units, while* 3×4 *means three groups of four units. Arranging these units in a rectangular grid, as in Figure 4.1, shows that we are merely viewing the same collection from a different perspective. One view shows four columns of 3, the other three rows of 4. The total number of units is identical.* ■

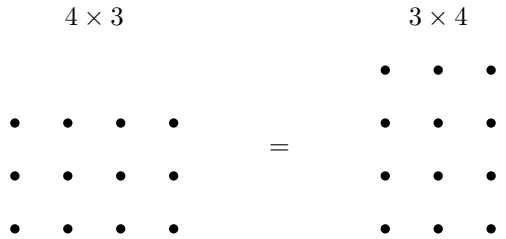


Figure 4.1: The product 4×3 (4 columns of 3) and 3×4 (3 columns of 4) represent the same total number of units.

The Law of Association

When multiplying several numbers in a chain, the manner in which they are grouped is immaterial.

***Axiom* 4.1.2. (Associative Law of Multiplication).** For any numbers a, b, and c,

$$(a \times b) \times c = a \times (b \times c) \tag{4.2}$$

Proof. This law can be visualised with a three-dimensional block of units. The product $(2 \times 3) \times 4$ *corresponds to creating a rectangular base of* 2×3 *units, and then stacking this base four units high. The product* $2 \times (3 \times 4)$ *corresponds to creating a vertical slice of* 3×4 *units, and then placing two such slices side by side. As shown in Figure 4.2, both constructions result in the same solid rectangular prism containing* 24 *units. The method of assembly does not alter the final object.* ■

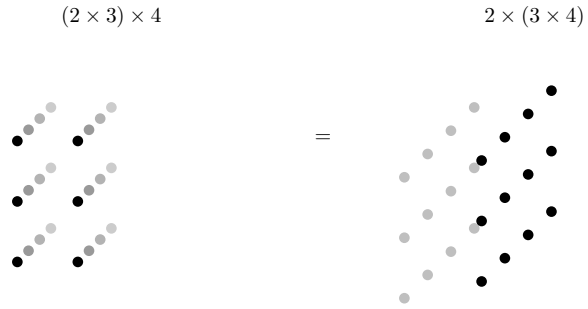


Figure 4.2: The product $(2 \times 3) \times 4$ and $2 \times (3 \times 4)$ produce the same arrangement of units.

***Corollary* 4.1.1.** . In any finite product, the order of factors is indifferent and brackets may be omitted:

$a_1 a_2 \cdots a_n$ is independent of the order and grouping of the a_i.

These laws, suggested by arithmetic, are now laid down as fundamental to all algebra, defining the operation of multiplication.

4.1.2 The Distributive Law: Connecting Addition and Multiplication

The third great law of algebra provides the connection between the operations of addition and multiplication.

***Axiom* 4.1.3. (Distributive Law).** The product of a number and a sum is equal to the sum of the products of that number with each term in the sum.

$$a \times (b + c) = (a \times b) + (a \times c) \tag{4.3}$$

Proof. *This law is best understood geometrically. The expression $a \times (b+c)$ represents the area of a rectangle with sides of length a and $(b + c)$. As shown in Figure 4.3, this area can be seen as the sum of the areas of two smaller rectangles: one with sides a and b (area ab), and another with sides a and c (area ac). The total area is the same whether calculated as a whole or as the sum of its parts.* ■

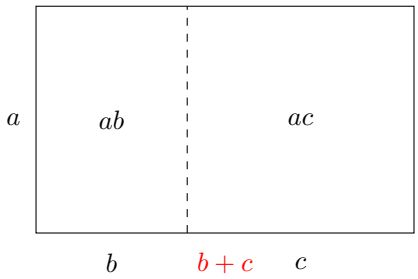


Figure 4.3: The area of the large rectangle $a(b+c)$ is the sum of the areas of the smaller rectangles, $ab+ac$.

The distributive law enables us to prove critical properties related to multiplication.

4.1.3 Properties of Multiplication

The fundamental laws lead directly to the rules for multiplication involving zero, one, and negative numbers.

***Theorem* 4.1.1. (Multiplication by Zero).** The product of any number and zero is zero.

$$a \times 0 = 0 \quad \text{and} \quad 0 \times a = 0 \tag{4.4}$$

Proof. *The first identity, $a \times 0 = 0$, is from our definition in 4.1.1. For the second, we use the fact that 0 can be written as $b - b$ for any b.*

$$\begin{aligned} 0 \times a &= (b - b) \times a && \textit{By the definition of zero in 3.3.1} \\ &= (b \times a) - (b \times a) && \textit{By the Distributive Law} \\ &= 0 && \textit{By the definition of zero} \end{aligned}$$

■

***Theorem* 4.1.2. (Multiplicative Identity).** For any number a,

$$a \times 1 = a \quad \text{and} \quad 1 \times a = a \tag{4.5}$$

Proof. *The identity $a \times 1 = a$ follows directly from the definition of multiplication. The second identity, $1 \times a = a$, then follows from the commutative law (4.1.1).* ■

***Theorem* 4.1.3. (The Law of Signs).** When multiplying two numbers, the sign of the product is determined by the following rules:

(i) A positive number times a positive number gives a positive product. $(+a) \times (+b) = +ab$

(ii) A positive number times a negative number gives a negative product. $(+a) \times (-b) = -ab$

(iii) A negative number times a positive number gives a negative product. $(-a) \times (+b) = -ab$

(iv) A negative number times a negative number gives a positive product. $(-a) \times (-b) = +ab$

In short, like signs produce a positive result, unlike signs a negative one.

Proof. *The proofs rely on the distributive law and the additive inverse property $x + (-x) = 0$.*

(i) This follows directly from the primary definition of multiplication as repeated addition of a positive quantity.

(ii) Consider the expression $a \times (b + (-b))$.

$$a \times (b + (-b)) = a \times 0 \qquad \textit{Since } b + (-b) = 0$$
$$(a \times b) + (a \times (-b)) = 0 \qquad \textit{By the Distributive Law}$$

This shows that $a \times (-b)$ is the additive inverse of $a \times b$. The unique additive inverse of ab is $-ab$, so we must have $a \times (-b) = -ab$.

(iii) By the commutative law (4.1.1), $(-a) \times b = b \times (-a)$. From the previous case, this is equal to $-ba$, which is $-ab$.

(iv) Consider the expression $(-a) \times (b + (-b))$.

$$(-a) \times (b + (-b)) = (-a) \times 0$$
$$(-a) \times b + (-a) \times (-b) = 0 \qquad \textit{By the Distributive Law}$$

From case (iii), we know that $(-a) \times b = -ab$. Substituting this gives:

$$-ab + (-a) \times (-b) = 0$$

This equation shows that the term $(-a) \times (-b)$ is the additive inverse of $-ab$. The unique additive inverse of $-ab$ is $+ab$. Therefore, it must be that $(-a) \times (-b) = +ab$.

■

***Corollary* 4.1.2.** . Distribution over subtraction is immediate from $b - c = b + (-c)$:

$$a(b - c) = ab - ac, \qquad (b - c)a = ba - ca.$$

***Corollary* 4.1.3.** . For any finite chain $\pm b_1 \pm b_2 \pm \cdots \pm b_n$,

$$a(\pm b_1 \pm \cdots \pm b_n) = \pm ab_1 \pm \cdots \pm ab_n,$$

each term keeping or changing sign according to its original sign.

***Corollary* 4.1.4.** . Reverse distribution (factorisation): if $ab + ac$ appears, one may write

$$ab + ac = a(b + c).$$

Proof. *By axiom 4.1.3 we have, for all a, b, c,*

$$a(b + c) = ab + ac.$$

Equality is symmetric, so

$$ab + ac = a(b + c).$$

Thus, reverse distribution (factorisation) holds. ■

The distributive law extends to expressions with any number of terms. To find the product of two expressions, each of which is a chain of additions and subtractions, we multiply every term in the first expression by every term in the second, and combine the resulting partial products according to the law of signs.

Example 4.1.1. $((a-b)(c-d))$. We can treat $(c-d)$ as a single quantity and distribute $(a-b)$ over it.

$$\begin{aligned}(a-b)(c-d) &= a(c-d) - b(c-d) \\ &= (ac-ad) - (bc-bd) && \text{Distribute } a \text{ and } b \\ &= ac - ad - bc + bd && \text{Remove brackets, changing signs for the second}\end{aligned}$$

The result is the sum of the products of each pair of terms: $(+a)(+c)$, $(+a)(-d)$, $(-b)(+c)$, and $(-b)(-d)$.

***Corollary* 4.1.5.** . The Product of Sum and Difference:

$$(a-b)(a+b) = a^2 - b^2$$

Proof. Using the method above: $(a-b)(a+b) = a(a+b) - b(a+b) = a^2 + ab - ab - b^2 = a^2 - b^2$. ■

4.2 Division

Just as subtraction is the inverse of addition, division is the inverse operation of multiplication.

Definition 4.2.1. ***(Division as a Missing Factor)***. For numbers a and b (where b is not zero), the quotient $a \div b$ is the unique number c that one must multiply by b to obtain a.

$$\begin{aligned}c \times b &= a \\ c &= a \div b.\end{aligned}$$

In the expression $a \div b$, a is the **dividend** and b is the **divisor**.

Another standard notation for division is the fraction bar, where $a \div b$ is written as $\frac{a}{b}$. This notation is familiar from arithmetic, where $\frac{a}{b}$ represents a of the b-th parts of a unit. We can see that these two ideas are the same. If we take b copies of the quantity $\frac{a}{b}$, we have $b \times \frac{a}{b}$, which by the arithmetical definition is a. Since this matches our algebraic definition, the notations are equivalent and can be used interchangeably.

4.2.1 The Multiplicative Identity

The inverse relationship between multiplication and division allows us to define the number **one**. Just as "zero" arises from subtracting a number from itself ($a-a=0$), "one" arises from dividing a non-zero number by itself.

Definition 4.2.2. ***(One)***. The number that represents the ratio of any non-zero quantity to itself is called **one**, denoted by the symbol 1.

$$a \div a = \frac{a}{a} = 1 \quad (\text{for } a \neq 0)$$

The fundamental property of one is that multiplying or dividing any number by it does not change that number's value. This makes one the *identity element* for multiplication.

***Axiom* 4.2.1.** **(Multiplicative Identity)**. For any number a,

$$a \times 1 = 1 \times a = a \quad \text{and} \quad a \div 1 = a \tag{4.6}$$

4.2.2 Fundamental Laws of Division

Since division is defined as the inverse of multiplication, its laws can be deduced from the laws we have already established.

***Theorem* 4.2.1.** **(Commutative Law for Multiplication and Division)**. In any chain of multiplications and divisions, the order of the operations is indifferent, provided each operand keeps its operator.

$$(a \times b) \div c = (a \div c) \times b \tag{4.7}$$

Proof. *Let $x = (a \div c) \times b$. To prove the theorem, we must show that $x \times c = a \times b$.*

$$\begin{aligned} x \times c &= ((a \div c) \times b) \times c && \text{Multiply both sides by } c \\ &= (a \div c) \times (b \times c) && \text{By the Associative Law (4.1.2)} \\ &= (a \div c) \times (c \times b) && \text{By the Commutative Law (4.1.1)} \\ &= ((a \div c) \times c) \times b && \text{By the Associative Law} \\ &= a \times b && \text{By definition of division, } (a \div c) \times c = a \end{aligned}$$

Since $x \times c = a \times b$, it follows from the definition of division that $x = (a \times b) \div c$. ■

***Theorem* 4.2.2. (Associative Law for Multiplication and Division)**. If a $\times$ sign precedes a bracketed expression containing a chain of multiplications and divisions, the bracket may be removed without changing any operators. If a $\div$ sign precedes it, the bracket may be removed by reversing the operator of every term inside ($\times$ becomes $\div$, and $\div$ becomes $\times$).

$$a \times (b \div c) = a \times b \div c$$
$$a \div (b \div c) = a \div b \times c$$

Proof. *For the second case, let $x = a \div (b \div c)$. By the definition of division, this means:*

$$\begin{aligned} x \times (b \div c) &= a \\ (x \times b) \div c &= a && \text{By the first case of this theorem} \\ x \times b &= a \times c && \text{Multiply both sides by } c \\ x &= (a \times c) \div b && \text{Divide both sides by } b \\ x &= (a \div b) \times c && \text{By the Commutative Law} \end{aligned}$$

Thus, $a \div (b \div c) = a \div b \times c$. ■

4.2.3 The Law of Signs for Division

The rules for the sign of a quotient are identical to those for a product and can be proven directly from them.

***Theorem* 4.2.3. (Law of Signs for Division)**. When dividing two numbers, the sign of the quotient is positive if the signs of the dividend and divisor are alike, and negative if they are unlike.

(i) $(+a) \div (+b) = +(a \div b)$

(ii) $(+a) \div (-b) = -(a \div b)$

(iii) $(-a) \div (+b) = -(a \div b)$

(iv) $(-a) \div (-b) = +(a \div b)$

Proof. *We prove case (ii) and leave the others as an exercise. Let $x = (+a) \div (-b)$. By the definition of division, we must have $x \times (-b) = +a$. According to the law of signs for multiplication, the product of two numbers is positive only if their signs are alike. Since $-b$ is negative, x must also be negative. Thus, the quotient is a negative number.* ■

4.2.4 The Distributive Law

The distributive law connects division to addition and subtraction, but its application is more limited than for multiplication.

***Theorem* 4.2.4. (Distributive Law for Division)**. Division distributes over addition and subtraction in the dividend.

$$(a+b) \div c = (a \div c) + (b \div c) \tag{4.8}$$

Proof. *Let $x = (a \div c) + (b \div c)$. We will show that $x \times c = a + b$.*

$$\begin{aligned} x \times c &= ((a \div c) + (b \div c)) \times c \\ &= (a \div c) \times c + (b \div c) \times c && \textit{By the Distributive Law (4.1.3)} \\ &= a + b && \textit{By the definition of division} \end{aligned}$$

Since $x \times c = a + b$, it must be that $x = (a+b) \div c$. ■

Remark. The divisor cannot be distributed. In general, $c \div (a+b)$ is **not** equal to $(c \div a) + (c \div b)$. A simple counterexample shows this: $12 \div (2+4) = 12 \div 6 = 2$, but $(12 \div 2) + (12 \div 4) = 6 + 3 = 9$.

***Theorem* 4.2.5. (Cancellation Law for Multiplication)**. If $ac = bc$ and $c \neq 0$, then $a = b$.

Proof. *We start with the given equation, $ac = bc$.*

$$\begin{aligned} ac - bc &= 0 && \textit{Subtract } bc \textit{ from both sides} \\ (a-b)c &= 0 && \textit{By the Distributive Law} \end{aligned}$$

The product of two numbers is zero only if at least one of the numbers is zero. We are given that $c \neq 0$. Therefore, it must be that the other factor is zero.

$$a - b = 0 \implies a = b$$

■

4.2.5 The Multiplicative Inverse (Reciprocal)

The concept of an inverse can be formalised. Just as every number a has an additive inverse $-a$, every non-zero number b has a multiplicative inverse.

Definition 4.2.3. ***(Reciprocal)***. For every non-zero number b, there exists a unique **reciprocal** or multiplicative inverse, denoted $\frac{1}{b}$ or b^{-1}, such that their product is one.

$$b \times \frac{1}{b} = 1$$

Using the reciprocal provides a powerful way to re-frame division.

***Theorem* 4.2.6.** . Dividing by a number is equivalent to multiplying by its reciprocal.

$$a \div b = a \times \frac{1}{b} \tag{4.9}$$

Proof. *Let $x = a \times \frac{1}{b}$. Multiplying both sides by b:*

$$\begin{aligned} x \times b &= \left(a \times \frac{1}{b}\right) \times b \\ &= a \times \left(\frac{1}{b} \times b\right) && \textit{By the Associative Law (4.1.2)} \\ &= a \times 1 && \textit{By the definition of a reciprocal} \\ &= a \end{aligned}$$

Since $x \times b = a$, we have $x = a \div b$ by definition. ■

This relationship is beneficial. It transforms every problem of division into one of multiplication, allowing us to use the more flexible laws of multiplication to simplify expressions. For example, the associative law $a \div (b \div c) = a \div b \times c$ becomes clearer:

$$a \div \left(b \times \frac{1}{c}\right) = a \times \frac{1}{b \times \frac{1}{c}} = a \times \left(1 \times \frac{c}{b}\right) = a \times \frac{1}{b} \times c = (a \div b) \times c$$

Remark. We will now examine the case of division by zero. To show that this operation is not permissible, we must consider all possibilities. This method of proof, where every case is examined, is known as proof by exhaustion.

4.2.6 Division by Zero

The definition of division requires the divisor to be non-zero. Let us examine why this must be so.

Note. There are in this case only two possible scenarios either $a \neq 0$ or $a = 0$.

1. **Case 1: Dividend is not zero.** Consider the expression $a \div 0$ where $a \neq 0$. By 4.2.1, this would be a number c such that $c \times 0 = a$. However, we proved that the product of any number and zero is always zero. Since $a \neq 0$, no such number c can exist. Therefore, division of a non-zero number by zero is **undefined**.
2. **Case 2: Dividend is zero.** Consider the expression $0 \div 0$. This would be a number c such that $c \times 0 = 0$. This statement is true for *every* number c. Since the result is not a unique, well-defined number, the expression $0 \div 0$ is also undefined, sometimes called **indeterminate**.

Because division by zero does not yield a consistent and unique result, it is not a permissible operation in algebra.

Geometric View and Examples

The rectangular grid model for multiplication also illustrates division and cancellation. A rectangle of $a \times b$ units contains a total of ab unit squares. If we divide this total area by the number of columns, b, we find the number of squares in each column, which is a. This is shown in Figure 4.4.

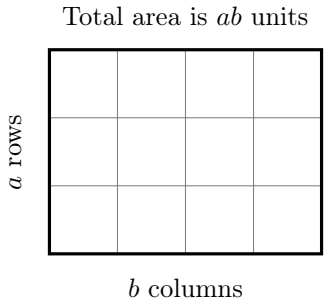


Figure 4.4: Dividing the total area ab by the number of columns b gives the area of one column, which is a. Thus $(ab) \div b = a$.

Example 4.2.1. (Combining operations).

$$\frac{(-6) \times 10}{(-5)} = (-6) \times \frac{10}{-5} = (-6) \times (-2) = 12$$

First, we perform the division, observing the law of signs. Then we perform the multiplication.

Example 4.2.2. (Distributing the dividend).

$$\frac{9x - 15y + 3}{3} = \frac{9x}{3} - \frac{15y}{3} + \frac{3}{3} = 3x - 5y + 1$$

4.3 Exercises

Part I: Foundational Identities and Properties

1. Expand the following products using the distributive law.

(a) $(x+3)(x+4)$

(b) $(2a-b)(a+5b)$

(c) $(p+q)(r+s)$

2. Apply the law of signs to compute the following products.

(a) $(-5)(3x-2)$

(b) $(3-2a)(-4)$

(c) $(-x)(-y-z)$

3. Use the properties of the multiplicative identity (1) and zero to simplify the following expressions.

(a) $1 \cdot (-2a+b-c)$

(b) $(3y+2) \cdot (x-x)$

(c) $a \times (b \div b)$, for $b \neq 0$

4. Factorise the following expressions by identifying the common factor.

(a) $6xy + 9xz$

(b) $ab^2 - ac + ad$

(c) $k(3-p) - k(2-p)$

5. Simplify the following quotients using the definition of division and the law of signs. State any restrictions on the variables.

(a) $\dfrac{-24x}{6}$

(b) $\dfrac{15a}{-3b}$

(c) $\dfrac{-ab}{-c}$

6. Apply the distributive law for division to simplify these expressions.

(a) $\dfrac{12a+18b}{6}$

(b) $\dfrac{xy-xz}{x}$

(c) $\dfrac{-9p+15q-3r}{3}$

Part II: Algebraic Manipulation

These problems require multiple steps, including rearranging, substituting, and simplifying fractions.

7. Factorise the expression $a(x-y)+b(y-x)$.

Remark. Recall from the notes on subtraction that $y-x=-(x-y)$.

8. By first rearranging the terms, use factorisation to show that $ax-by+bx-ay=(a+b)(x-y)$.

9. Expand and simplify the expression $(x+y)(a+b)-(x-y)(a-b)$.

10. Given that $x=a+b$, substitute this into the expression $x(c+d)-a(c+d)$ and simplify the result.

11. Simplify the following algebraic fractions by factorising and cancelling. State any restrictions on the variables.

(a) $\dfrac{2x}{3}\times\dfrac{9}{4x^2}$

(b) $\dfrac{a+1}{a-1}\times\dfrac{a^2-1}{a+1}$

(c) $\dfrac{(m-1)m}{m}\cdot\dfrac{1}{m-1}$

12. Simplify to a single fraction. State all restrictions on the variables.

$$\left(\frac{1}{a}+\frac{1}{b}\right)\div\left(\frac{1}{a}-\frac{1}{b}\right)$$

13. Simplify and condense.

$$2a-(3a-(a-(b-a)))$$

14. Distribute the following products:

(i) $(a+b)(a+b)$

(ii) $(a-b)(a+b)$

(iii) $(3a-6b)(3a+6b)$

(iv) $\left(\dfrac{1}{3}a-\dfrac{1}{6}\right)\left(\dfrac{1}{3}a+\dfrac{1}{6}b\right)$

Remark. Note the substitution, makes it easier.

15. Simplify and condense

$$\Big((m+1)a+(n+1)b\Big)\Big((m-1)a+(n-1)b\Big)+\Big((m+1)a-(n+1)b\Big)\Big((m-1)a-(n-1)b\Big).$$

16. Simplify and condense

$$\left(x+\frac{1}{x}\right)\left(y+\frac{1}{y}\right)+\left(x-\frac{1}{x}\right)\left(y-\frac{1}{y}\right).$$

and

$$\left(x+\frac{1}{x}\right)\left(y+\frac{1}{y}\right)\left(z+\frac{1}{z}\right)+\left(x-\frac{1}{x}\right)\left(y-\frac{1}{y}\right)\left(z-\frac{1}{z}\right).$$

Remark. Substituting $\dfrac{1}{x}$ for a makes it much easier, and you can substitute it back once you have your final equation.

Part III: Proof and Reasoning

Construct formal arguments for the following statements, justifying each step with a definition, axiom, or previously established theorem from the text.

17. Telescoping Product I. For any integer $n\geq 2$, evaluate the following product.

$$\frac{2}{1}\cdot\frac{3}{2}\cdot\frac{4}{3}\cdots\frac{n}{n-1}.$$

18. Prove the identity: $(a-b)c+(b-c)a+(c-a)b=0$.

19. ⋆ An algebraic operation, denoted by $\oplus$, is defined for any two numbers a and b as:

$$a \oplus b = a + b - ab$$

Using the standard laws of algebra, prove that this new operation is associative. That is, prove $a \oplus (b \oplus c) = (a \oplus b) \oplus c$.

Remark. Plug in the values and show that $L = R$.

20. ⋆ **An Identity by Grouping.** Prove the identity:

$$a(b-c) + b(c-d) + c(d-b) + d(a-c) = (a-c)(d-b)$$

Remark. Do not expand the right-hand side. Instead, rearrange and factor the terms on the left-hand side to match those on the right.

21. ⋆ **Telescoping Product II.** For any integer $n \geq 2$, evaluate the following product.

$$\frac{3}{4} \cdot \frac{8}{9} \cdot \frac{15}{16} \cdot \frac{24}{25} \cdots \frac{n^2-1}{n^2}$$

Remark. Write the numerator of each fraction as $k^2 - 1 = (k-1)(k+1)$ and observe the pattern of cancellation.

4.4 Monomials

A product formed by multiplying numbers and letters, without any addition or subtraction, is called a monomial. For example, $3 \times a \times x \times x \times b \times a$ is a monomial. Using the commutative and associative laws of multiplication, we can reorder and group the factors in this expression. It is conventional to group numerical factors together and identical letters together:

$$(3) \times (a \times a) \times (b) \times (x \times x)$$

This repeated multiplication becomes cumbersome to write. We introduce a shorthand notation for this process using indices, or exponents.

Definition 4.4.1. ***(Exponent)***. For a positive integer n, the expression a^n denotes the product of n factors of a.

$$a^n \coloneqq \underbrace{a \times a \times \cdots \times a}_{n \text{ times}}$$

Here, n is called the **index** or exponent, and a^n is called the n-th power of a. We also define $a^1 = a$.

With this notation, our example monomial simplifies from $3 \times a \times a \times b \times x \times x$ to the much neater expression $3a^2bx^2$.

4.4.1 The Laws of Indices

The definition of an exponent, combined with the fundamental laws of algebra, leads to a set of rules for manipulating powers. These are laid down as the general laws for all indices.

***Axiom* 4.4.1. (Laws of Indices)**. For any numbers a, b and positive integers m, n:

I. **Product of Powers:** $a^m \times a^n = a^{m+n}$

II. **Quotient of Powers:**

$$\frac{a^m}{a^n} = \begin{cases} a^{m-n} & \text{if } m \geq n \\ \dfrac{1}{a^{n-m}} & \text{if } m < n \end{cases}$$

Remark. This latter case naturally leads to the definition of negative exponents, where we define $a^{-k} \coloneqq \frac{1}{a^k}$.

III. **Power of a Power:** $(a^m)^n = a^{mn}$

IV. **Power of a Product:** $(ab)^m = a^m b^m$

V. **Power of a Quotient:** $(a \div b)^m = a^m \div b^m$

Proof.

I. *By the definition of an exponent:*

$$a^m \times a^n = \underbrace{(a \times \cdots \times a)}_{m \text{ factors}} \times \underbrace{(a \times \cdots \times a)}_{n \text{ factors}}$$

By the associative law of multiplication, we can remove the brackets to form a single product containing $m+n$ factors of a. This is, by definition, a^{m+n}.

II. *Using fraction notation and the definition of an exponent:*

$$\frac{a^m}{a^n} = \frac{\overbrace{a \times a \times \cdots \times a}^{m \text{ factors}}}{\underbrace{a \times a \times \cdots \times a}_{n \text{ factors}}}$$

If $m > n$, we cancel n factors of a, leaving $m - n$ factors in the numerator. The result is a^{m-n}. If $m < n$, we cancel m factors of a, leaving $n - m$ factors in the denominator, which gives $\frac{1}{a^{n-m}}$. If $m = n$, all factors cancel, resulting in $a^{m-m} = a^0 = 1$.

III. *We are taking the n-th power of the term a^m:*

$$(a^m)^n = \underbrace{(a^m) \times (a^m) \times \cdots \times (a^m)}_{n \text{ times}}$$

Each term a^m is a product of m factors of a. We have n such groups of factors. By the associative law, this is a single product with $m \times n$ factors of a, which is a^{mn}.

IV. *By definition, we have:*

$$(ab)^m = \underbrace{(ab) \times (ab) \times \cdots \times (ab)}_{m \text{ times}}$$

Using the commutative and associative laws, we can re-group all the a factors and all the b factors:

$$\underbrace{(a \times \cdots \times a)}_{m \text{ factors}} \times \underbrace{(b \times \cdots \times b)}_{m \text{ factors}} = a^m b^m$$

V. *Similar to the above, we have:*

$$\left(\frac{a}{b}\right)^m = \underbrace{\frac{a}{b} \times \frac{a}{b} \times \cdots \times \frac{a}{b}}_{m \text{ times}} = \frac{\overbrace{a \times \cdots \times a}^{m \text{ times}}}{\underbrace{b \times \cdots \times b}_{m \text{ times}}} = \frac{a^m}{b^m}$$

■

4.4.2 The Theory of Degree

Monomials can be classified based on the exponents of the letters they contain. A monomial is said to be **integral** if it involves no division by letters. For example, $3a^2b$ is integral, whereas $3a^2/b$ is fractional.

Definition 4.4.2. ***(Degree)***. The degree of an integral monomial in a particular letter is the index of that letter. The degree of the monomial itself is the sum of the degrees of its specified letters, called the **variables**.

Letters whose degrees are not counted are called **constants**. The numerical part of a monomial, along with any constants, is called the **coefficient**.

Example 4.4.1. Consider the monomial $5a^2x^4y^3$. If we specify x and y as the variables, then:

- The degree in x is 4.
- The degree in y is 3.
- The degree of the monomial is $4 + 3 = 7$.
- The coefficient is $5a^2$.

The concept of degree is fundamental for classifying and ordering expressions.

***Theorem* 4.4.1.** The degree of the product of two or more monomials is the sum of their respective degrees.

Proof. Let two monomials be $A = c_1x^ly^m$ and $B = c_2x^py^q$, where c_1, c_2 are coefficients and x, y are variables. The degree of A is $d_A = l + m$, and the degree of B is $d_B = p + q$. Their product is:

$$\begin{aligned} A \times B &= (c_1x^ly^m) \times (c_2x^py^q) \\ &= (c_1c_2)(x^lx^p)(y^my^q) && \textit{By Commutative and Associative Laws} \\ &= (c_1c_2)x^{l+p}y^{m+q} && \textit{By Law of Indices I} \end{aligned}$$

The degree of the product is $(l + p) + (m + q)$, which can be rearranged to $(l + m) + (p + q)$, or $d_A + d_B$. ■

***Theorem* 4.4.2.** If the quotient of two monomials is an integral monomial, its degree is the degree of the dividend minus the degree of the divisor.

Proof. Let A and B be two monomials with degrees d_A and d_B. Let the quotient $Q = A \div B$ be an integral monomial with degree d_Q. By the definition of division, $A = Q \times B$. From the previous theorem, the degree of the product $Q \times B$ must be the sum of the degrees of Q and B.

$$\begin{aligned} \deg(A) &= \deg(Q \times B) \\ d_A &= d_Q + d_B \end{aligned}$$

Rearranging this equation gives $d_Q = d_A - d_B$. ■

Example 4.4.2. (Degree arithmetic). If $A = 6x^{14}y^{10}$ and $B = 7x^7y^3$, then

$$AB = 42x^{21}y^{13} \quad (\deg = 21 + 13 = 34), \qquad \frac{A}{B} = \frac{6}{7}x^7y^7 \quad (\deg = 14 - 7 + 10 - 3 = 14).$$

Note. Reordering does not affect degree; only the exponents of the chosen variables matter. Coefficients (including lettered constants) do not contribute to the degree of the polynomial.

4.5 Exercises

Part I: Foundational Skills

These exercises focus on the direct application of one or two laws of indices at a time.

1. Simplify the following monomials.

(a) $a^5 \times a^8$

(b) $(b^4)^6$

(c) $c^{12} \div c^5$

(d) $(2x^3y^2)^4$

2. Are the expressions $(3^2)^4$ and $3^{(2^4)}$ equal? Calculate both to justify your answer.

3. Simplify the quotient of the following monomials, reducing the numerical coefficients to their simplest form:

$$\frac{36a^7b^5c^4}{81a^4b^3c^3}$$

4. Simplify the expression

$$\frac{2^{2^2}}{2(2^2)^2}.$$

5. Simplify the following product of monomial fractions:

$$\frac{45x^5y^6z^3}{27x^2y^5z^2} \times \frac{243x^4y^4z^2}{180x^3y^6z}$$

Part II: Combined Operations

6. Simplify the following expression involving products and powers:

$$\frac{(5a^3b^2)^2 \times (2a^2b^4)^3}{10a^{10}b^{15}}$$

7. Express the following as a single power of 3:

$$\frac{81^{x+1} \times 9^{2x-1}}{27^{3x}}$$

Remark. Express all numbers as powers of the same base.

8. Simplify the following expression involving a division of products:

$$\frac{(3xy^2)^2 \times x^4y^9}{x^6y^9} \div \left(\frac{3x^2y}{y^2x^2}\right)^2$$

9. Simplify the expression:

$$\frac{a^{2x+3}b^{x-1}c^4}{a^{x+2}b^{2x}c^{x-3}} \times \frac{a^{3-x}b^{1-x}c^{2x+1}}{a^4b^{-3}c^{5-x}}$$

10. The following expression appears complicated, but has a simple structure. Simplify it by first handling the typical exponent:

$$\frac{(x^3y^2z^3)^7 \times (y^3z^6x^2)^7 \times (x^2z^2y)^7}{(x^5y^2z)^7 \times (y^2z^3)^7 \times (x^3z^4)^7}$$

Part III: Problems with Variable Exponents

These exercises test your ability to apply the laws of indices in a more abstract setting.

11. Simplify the following expression. The result is straightforward.

$$\left(\frac{x^m}{x^n}\right)^{m+n} \times \left(\frac{x^n}{x^l}\right)^{n+l} \times \left(\frac{x^l}{x^m}\right)^{l+m}$$

Hint: Recall the algebraic identity for the difference of two squares.

12. Simplify the following by carefully collecting the exponents for each base:

$$(a^{p-q}b^{q-r}c^{r-p})^2 \times (a^{q-r}b^{r-p}c^{p-q})^3$$

13. Distribute the product and simplify the resulting expression:

$$(x^a - x^b + x^c)\left(x^{-a} + x^{-b}\right)$$

14. Simplify the following expression, which involves subtraction in the numerator and denominator:

$$\frac{a^{x+b} - a^{x+c}}{a^{x+c} - a^{x+b}}$$

Hint: This is not a monomial. Use the distributive law in reverse by factoring out a common term from the numerator and denominator.

Part IV: Challenge Problems and Proofs

These problems require careful reasoning and synthesis of multiple concepts.

15. ⋆ Prove that if $m = a^x$, $n = a^y$, and $a^2 = (m^y n^x)^z$ for $a > 0, a \neq 1$, then it must be that $xyz = 1$.

16. ⋆ Simplify the following complex expression by first simplifying the terms within each bracket and then applying the outer exponents.

$$\left(\frac{a^4b^4c^2}{a^3b^2c^3x^2y}\right)^2 \times \left(\frac{a^3b^3}{a^2b^6c^3x^3y^3}\right)^3 \times \left(\frac{b^6c^4x^2y}{a^4b^3x^3y^3}\right)^4$$

17. ⋆**Prove the identity:**

$$\left(\frac{x^p}{x^q}\right)^{p+q-r} \times \left(\frac{x^q}{x^r}\right)^{q+r-p} \times \left(\frac{x^r}{x^p}\right)^{r+p-q} = 1$$

4.5.1 An Introduction to Proof by Contradiction

Note. Thus far, our proofs have been direct constructions. We now introduce a powerful method of indirect proof. To prove a statement P is true, we can assume for a moment that it is false (i.e., assume *not* P is true). We then reason logically from this assumption until we arrive at a statement that is absurd or contradicts a known fact (e.g., $1 = 0$). This contradiction shows that our initial assumption must have been wrong, and therefore the original statement P must be true.

Worked Examples

1. **Uniqueness of the Additive Inverse.** Prove that for any number a, its additive inverse is unique.

   Proof. Statement to Prove: For a given a, there is only one number b such that $a + b = 0$.

   (i) ***The Assumption (Assume the Opposite):*** *Let's assume the additive inverse is not unique. This means there exist two different numbers, b and c (so $b \neq c$), that are both additive inverses of a.*

   (ii) ***Logical Steps from the Assumption:*** *If b and c are both additive inverses of a, then by 3.4.1, they must both satisfy the definition:*

   $$a + b = 0$$
   $$a + c = 0$$

   Since both expressions equal 0, they must be equal to each other:

   $$a + b = a + c$$

   Now, we add the additive inverse of a, which is $-a$, to both sides of the equation.

   $$\begin{aligned} (-a) + (a + b) &= (-a) + (a + c) && \text{Add } -a \text{ to both sides} \\ ((-a) + a) + b &= ((-a) + a) + c && \text{By the Associative Law (3.2.1)} \\ 0 + b &= 0 + c && \text{By the Additive Inverse axiom (3.4.1)} \\ b &= c && \text{By the Additive Identity axiom (3.3.1)} \end{aligned}$$

   (iii) ***The Contradiction:*** *Our result, $b = c$, directly contradicts our initial assumption that $b \neq c$.*

   Since our assumption led to a logical impossibility, the assumption must be false. Therefore, the additive inverse of any number a must be unique. ■

2. **The Zero-Product Property.** Prove that if $ab = 0$, then either $a = 0$ or $b = 0$.

   Proof. **Statement to Prove:** If a product is zero, at least one of its factors must be zero.

   (i) ***The Assumption (Assume the Opposite):*** *Assume the statement is false. This means we can have a situation where $ab = 0$, but* neither *a nor b is zero. So, we assume $ab = 0$ AND $a \neq 0$ AND $b \neq 0$.*

   (ii) ***Logical Steps from the Assumption:*** *We start with the equation $ab = 0$. Since we have assumed that $a \neq 0$, 4.2.3 guarantees that a has a unique reciprocal, $\frac{1}{a}$. We can multiply both sides of our equation by this reciprocal.*

   $$\begin{aligned} \frac{1}{a} \times (ab) &= \frac{1}{a} \times 0 && \text{Multiply both sides by the reciprocal of } a \\ \left(\frac{1}{a} \times a\right) \times b &= \frac{1}{a} \times 0 && \text{By the Associative Law (4.1.2)} \\ 1 \times b &= 0 && \text{By def. of reciprocal and Theorem 4.1.1} \\ b &= 0 && \text{By the Multiplicative Identity (Theorem 4.1.2)} \end{aligned}$$

   (iii) ***The Contradiction:*** *Our result, $b = 0$, contradicts our initial assumption that $b \neq 0$.*

   (iv) ***Conclusion:*** *The assumption that we can have $ab = 0$ while both factors are non-zero leads to a contradiction. Thus, the assumption is false, and the original statement must be true.*

   ■

Given that prove

18. **Uniqueness of the Reciprocal.** Prove by contradiction that for any non-zero number b, its reciprocal (multiplicative inverse) is unique.

Remark. Assume there are two different reciprocals, x and y (where $x \neq y$), such that $bx = 1$ and $by = 1$. Follow the logic of Example E1.

19. Uniqueness of the Additive Identity. Prove by contradiction that there is only one number that acts as the additive identity.

Remark. Assume there are two different additive identities, 0 and z (where $z \neq 0$). Use the definition of the additive identity ($a + 0 = a$ and $a + z = a$) to show that z must equal 0, a contradiction.

20. A Property of Zero. Prove by contradiction that if $a + x = a$, then $x = 0$.

Remark. Assume that $a + x = a$ is true, but that $x \neq 0$. Use the laws of algebra to isolate x and show that it must be 0, which contradicts your assumption.

21. A Property of One. Using the laws of multiplication, prove by contradiction that if $ax = a$ for a non-zero number a, then $x = 1$.

Remark. This is the multiplicative version of the previous problem. Assume $ax = a$ and $a \neq 0$, but that $x \neq 1$. Use the reciprocal of a to find a contradiction.

22. Impossibility of a Solution. Prove by contradiction that there is no number x for which $3(x + 2) = 3x + 5$.

Remark. Assume such a number x does exist. Simplify until you reach a statement that is clearly false.

4.6 Integers and Divisibility

The collection of positive integers $\{1, 2, 3, \dots\}$ can be separated into two distinct kinds of numbers.

Definition 4.6.1. ***(Even and Odd Numbers)***. An integer is even if it can be written in the form $2n$ for some integer n. An integer is odd if it can be written in the form $2n + 1$ for some integer n.

The even integers are $\dots, -4, -2, 0, 2, 4, \dots$ and the odd integers are $\dots, -3, -1, 1, 3, \dots$.

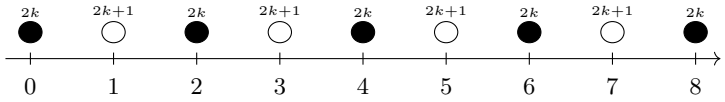


Figure 4.5: Parity classes on the number line: even $= 2k$, odd $= 2k + 1$.

***Theorem* 4.6.1. (Properties of Even and Odd Numbers)**. Let a, b be integers.

(i) If a, b are both even, their sum $a + b$ is even.

(ii) If a, b are both odd, their sum $a + b$ is even.

(iii) If one is even and one is odd, their sum $a + b$ is odd.

(iv) If a is even, its square a^2 is even.

(v) If a is odd, its square a^2 is odd.

Proof. We prove (iii) and (v) and leave the rest as exercises.

(i) Let a be even and b be odd. Then $a = 2n$ and $b = 2k + 1$ for some integers n, k.

$$a + b = 2n + (2k + 1) = 2(n + k) + 1$$

Since $n + k$ is an integer, the sum is of the form $2m + 1$ and is therefore odd.

(ii) Let a be odd. Then $a = 2n + 1$ for some integer n.

$$a^2 = (2n+1)^2 = (2n)^2 + 2(2n)(1) + 1^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1$$

Since $2n^2 + 2n$ is an integer, the square is of the form $2k + 1$ and is therefore odd.

■

***Corollary* 4.6.1.** *(Parity Converse).* If n^2 is even, then n is even. If n^2 is odd, then n is odd.

Proof. If n were odd, $n = 2k + 1$ and $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ would be odd. So if n^2 is even, n cannot be odd; hence n is even. If n^2 is odd, it is not even, so by the first part n is not even; thus n is odd. ■

The idea of an even number being a multiple of 2 can be generalised.

Definition 4.6.2. ***(Divisibility)***. An integer m is divisible by a non-zero integer d if there exists an integer k such that $m = dk$. If this is the case, we say that d divides m, or d is a factor of m.

4.6.1 The Division Algorithm

When we divide one integer by another, we are left with a quotient and a remainder. This simple idea is formalised in what is known as the Division Algorithm, a cornerstone for the theory of numbers.

***Theorem* 4.6.2. (The Division Algorithm)**. For any integer a (the dividend) and any positive integer b (the divisor), there exist unique integers q (the quotient) and r (the remainder) such that

$$a = qb + r, \quad \text{where } 0 \leq r < b$$

Proof. This proof has two parts: first showing that such a q and r exist, and second, showing they are the only pair that works.

(i) **Existence.** Consider the collection of numbers formed by subtracting multiples of b from a: $\ldots, a - 2b, a - b, a, a + b, \ldots$. Within this collection, there must be a smallest non-negative number. Let us call this number r. Since it is part of the collection, it must be of the form $a - qb$ for some integer q. So, we have $r = a - qb$, which rearranges to $a = qb + r$. By our choice, r is non-negative, so $r \geq 0$. We must also show $r < b$. Let us suppose for a moment that $r \geq b$. Then we could form the number $r - b$. Substituting what r is, we get $r - b = (a - qb) - b = a - (q + 1)b$. This number is still in our collection. Also, since $r \geq b$, the number $r - b$ must be non-negative. However, $r - b$ is smaller than r, which contradicts our choice of r as the smallest non-negative number in the collection. Our supposition must be false, so it must be that $r < b$. Thus, q and r exist with $0 \leq r < b$.

(ii) **Uniqueness.** To prove there is only one such pair, we suppose there are two pairs that both satisfy the conditions. Let them be (q, r) and (q', r').

$$a = qb + r, \quad \text{with } 0 \leq r < b$$
$$a = q'b + r', \quad \text{with } 0 \leq r' < b$$

Since both expressions equal a, they must equal each other:

$$qb + r = q'b + r'$$

Rearranging this equation to group terms with b gives:

$$(q - q')b = r' - r$$

This equation tells us two things. First, the left side is a multiple of b. Therefore, the right side, $r' - r$, must also be a multiple of b. Second, let's consider how large $r' - r$ can be. We know that both r and

r' are trapped in the range from 0 to $b-1$. The greatest possible value for $r'-r$ would be if r' is as large as possible $(b-1)$ and r is as small as possible (0), giving a difference of $b-1$. The smallest value would be if r' is 0 and r is $b-1$, giving a difference of $-(b-1)$. So, the number $r'-r$ must be strictly between $-b$ and b.

Now we combine these two facts. We have a number, $r'-r$, which is a multiple of b, but it is also in the range from $-(b-1)$ to $b-1$. The only multiple of b within this range is 0. Therefore, it must be that $r'-r=0$, which means $r'=r$.

Substituting this back into our rearranged equation gives $(q-q')b=0$. Since we know the divisor b is positive and not zero, the only way for this product to be zero is if $q-q'=0$, which means $q'=q$. The two pairs (q,r) and (q',r') are identical. The quotient and remainder are unique.

■

Remark. This is probably the hardest thing to understand right now so take your time, read it multiple times to truly understand what i mean; you might be wondering why all of this but you will see why in a few chapters.

Example 4.6.1. Take $a=47$ and $b=6$. Subtract 6 step by step:

$$47, 41, 35, 29, 23, 17, 11, 5, -1.$$

Stop just before going negative. We subtracted 6 seven times and have $r=5$. Thus

$$47 = 7\cdot 6 + 5, \qquad 0 \le 5 < 6.$$

***Corollary* 4.6.2.** For any integer $b \ge 2$, every integer a can be expressed in exactly one of the forms

$$qb, \quad qb+1, \quad qb+2, \quad \ldots, \quad qb+(b-1)$$

for some integer q.

Example 4.6.2. With $b=7$, every integer is one of $7q, 7q+1, \ldots, 7q+6$. For instance,

$$23 = 3\cdot 7 + 2,$$

so 23 is of the form $7q+2$ with $q=3$.

4.7 Exercises

Note. In these exercises, the notation $d \mid a$ means "d divides a", i.e. there exists an integer k with $a=dk$. You may use any definitions, axioms, or theorems previously established in the text.

Part I: Foundational Properties

1. If $d \mid a$ and $d \mid b$, prove that $d \mid (ma+nb)$ for any integers m, n.

   Remark. Write out a and b using the definition of divisibility and substitute.

2. If $d \mid a$ and $a \mid b$, prove that $d \mid b$.

3. If $a \mid b$ and $b \mid a$, show that $a = \pm b$. If in addition $a, b > 0$, conclude that $a = b$.

4. Prove the remaining parts of the theorem on properties of even and odd numbers from the text, namely:

   (a) The sum of two even integers is even.

   (b) The sum of two odd integers is even.

(c) The square of an even integer is even.

5. Let $a = qb + r$ with $0 \leq r < b$. Prove that $b \mid a$ if and only if $r = 0$. This provides a direct connection between the Division Algorithm and divisibility.

6. Apply the Division Algorithm to find the unique quotient q and remainder r for the following pairs (a, b):

(a) $(137, 11)$

(b) $(-137, 17)$

Remark. Remember, the remainder r must satisfy $0 \leq r < 17$.

(c) $(2024, 42)$

(d) $(100, -13)$

Remark. The definition requires the divisor b to be positive. How should you handle this?

7. Prove that for any integer n, the product of two consecutive integers, $n(n + 1)$, is always even.

Remark. Use the Division Algorithm with $b = 2$. An integer n is either of the form $2k$ or $2k + 1$. Consider each case.

8. By considering the possible remainders when an integer is divided by 3, prove that the square of any integer must be of the form $3k$ or $3k + 1$ for some integer k.

Remark. An integer n can be written as $3q$, $3q + 1$, or $3q + 2$. Square each form.

9. Use the result from the previous problem to prove that an integer of the form $3k + 2$ can never be a perfect square. Can the number $111\ldots11$ (containing $3k + 2$ digits) be a perfect square?

10. What are the possible remainders when a perfect square is divided by 4? Use this to prove that no number of the form $100k + 7$ can be a perfect square.

11. Prove that the product of three consecutive integers, $n(n + 1)(n + 2)$, is always divisible by 6.

Remark. To be divisible by 6, a number must be divisible by 2 and by 3. You have already shown one part in problem 7. For divisibility by 3, use the same case-by-case method.

4.8 Prime and Composite Numbers

Every integer greater than one has at least two divisors: one and itself. Some numbers have no others. This distinction is the basis for number theory.

Definition 4.8.1. ***(Prime and Composite Numbers)***. An integer $p > 1$ is a prime number if its only positive divisors are 1 and p. An integer $n > 1$ that is not prime is called a composite number.

The first few primes are $2, 3, 5, 7, 11, \ldots$. The numbers $4 = 2 \times 2$, $6 = 2 \times 3$, and $9 = 3 \times 3$ are composite. The number 1 is a unit, neither prime nor composite.

4.8.1 The Fundamental Theorem of Arithmetic

Composite numbers can be broken down into a product of their factors. This process can be continued until all factors are prime. For instance, $360 = 36 \times 10 = (4 \times 9) \times (2 \times 5) = (2^2 \times 3^2) \times (2 \times 5) = 2^3 \times 3^2 \times 5$. This leads to one of the most important results in mathematics.

***Theorem* 4.8.1. (The Fundamental Theorem of Arithmetic)**. Every integer greater than 1 is either a prime number itself or can be expressed as a product of prime numbers. This factorisation is unique, apart from the order in which the factors are written.

The proof has two parts: first, we show that such a factorisation always exists, and second, we show it is unique. The existence proof is straightforward, but the uniqueness proof requires more powerful tools.

For now, lets just prove Existence:

Proof. Let N be a composite number. Since it is composite, it has a divisor other than 1 and N. Let the smallest such divisor be a. This divisor a must be a prime number. If it were not, it would have a smaller divisor, which would also be a divisor of N, contradicting that a was the smallest. So, we can write $N = aN_1$ where a is prime. If N_1 is prime, we are done. If N_1 is composite, we repeat the process. Since the sequence $N, N_1, N_2, \ldots$ is strictly decreasing, this must terminate, leaving a product of primes. ■

4.8.2 Greatest Common Divisor and the Euclidean Algorithm

To prove uniqueness, we must first develop a method for finding the greatest common divisor of two integers.

Definition 4.8.2. ***(Greatest Common Divisor)***. A common divisor of two integers a and b is an integer that divides both. The largest of these is the greatest common divisor (GCD), denoted $\gcd(a, b)$. If $\gcd(a, b) = 1$, the integers are said to be **coprime**.

The Euclidean Algorithm is an efficient method for finding the GCD, which relies on the following property derived from the Division Algorithm.

***Theorem* 4.8.2. (Key Step of the Algorithm)**. If $a = qb + r$, where a, b, q, r are all integers, then $\gcd(a, b) = \gcd(b, r)$.

Proof.

- *Let d divide both b and r. Then $b = dk$ and $r = dt$ for some integers k, t. Since q is an integer, $qb = qdk$ is also a multiple of d. Hence*

$$a = qb + r = qdk + dt = d(qk + t),$$

  so d divides a as well. Therefore every common divisor of b and r is also a common divisor of a and b.
- *Conversely, Let d' divide both a and b. Then $a = d'u$ and $b = d'v$ for some integers u, v. Using $a = qb + r$ we get*

$$r = a - qb = d'u - qd'v = d'(u - qv)$$

  so d' divides r. Therefore every common divisor of a and b is also a common divisor of b and r.

Since the common divisors are the same in both directions, the greatest one is the same: $\gcd(a, b) = \gcd(b, r)$. ■

The algorithm applies this theorem repeatedly. To find $\gcd(a, b)$, we divide a by b to get a remainder r_0. We replace (a, b) with (b, r_0) and repeat. The sequence of remainders decreases until one is zero. The last non-zero remainder is the GCD.

Example 4.8.1. (Euclidean Algorithm). Find the GCD of 565 and 60.

$$\begin{aligned} 565 &= 9 \times 60 + 25 && \implies \gcd(565, 60) = \gcd(60, 25) \\ 60 &= 2 \times 25 + 10 && \implies \gcd(60, 25) = \gcd(25, 10) \\ 25 &= 2 \times 10 + 5 && \implies \gcd(25, 10) = \gcd(10, 5) \\ 10 &= 2 \times 5 + 0 && \implies \gcd(10, 5) = 5 \end{aligned}$$

The last non-zero remainder is 5, so $\gcd(565, 60) = 5$.

4.8.3 Bézout's Identity and Euclid's Lemma

The Euclidean algorithm has profound consequences. By working backwards through its steps, we can express the GCD as a combination of the original numbers.

***Theorem* 4.8.3. (Bézout's Identity)**. For any two integers a and b, there exist integers x and y such that

$$ax + by = \gcd(a, b)$$

Proof. The proof is constructive. We demonstrate by finding x and y for the previous example by rearranging the algorithm's equations:

$$\begin{aligned}
5 &= 25 - 2 \times 10 && \text{From line 3} \\
&= 25 - 2 \times (60 - 2 \times 25) && \text{Substitute for } 10 \text{ from line 2} \\
&= 25 - 2(60) + 4(25) = 5 \times 25 - 2 \times 60 \\
&= 5 \times (565 - 9 \times 60) - 2 \times 60 && \text{Substitute for } 25 \text{ from line 1} \\
&= 5(565) - 45(60) - 2(60) \\
&= 5(565) - 47(60)
\end{aligned}$$

Thus we have $565(5) + 60(-47) = 5$, demonstrating the identity with $x = 5$ and $y = -47$. ■

***Corollary* 4.8.1.** If a and b are coprime, there exist integers x and y such that $ax + by = 1$.

Proof. Run the Euclidean algorithm on a and b:

$$a = q_0 b + r_0, \qquad b = q_1 r_0 + r_1, \qquad r_0 = q_2 r_1 + r_2, \ \ldots, \ r_{k-1} = q_{k+1} r_k + 0.$$

Since a and b are coprime, the last non-zero remainder is $r_k = 1$ (by Theorem 4.8.2 applied step by step). Now express each remainder as an integer combination of a and b. This is done by back-substitution.

Start:

$$a = 1 \cdot a + 0 \cdot b, \qquad b = 0 \cdot a + 1 \cdot b.$$

Step: whenever

$$r_i = r_{i-2} - q_{i-1} r_{i-1}$$

and

$$r_{i-2} = s, a + t, b, \qquad r_{i-1} = s', a + t', b$$

for some integers s, t, s', t', then

$$r_i = (s - q_{i-1} s'), a + (t - q_{i-1} t'), b,$$

so r_i is again of the form $xa + yb$ with integers x, y. Repeating this along the chain ends with

$$1 = r_k = xa + yb$$

for some integers x and y. This is the required identity. ■

This leads to a crucial property of divisibility.

***Corollary* 4.8.2.** If a divides the product bc and $\gcd(a, b) = 1$, then a must divide c.

Proof. Since $gcd(a, b) = 1$, by 4.8.1 we can find integers x, y such that $ax + by = 1$. Multiply by c:

$$c(ax + by) = c \implies acx + bcy = c$$

The term acx is clearly divisible by a. The term bcy is also divisible by a, since we are given that a divides bc. As a divides both terms on the left, it must divide their sum, which is c. ■

We now have the tool required to prove the final piece of the Fundamental Theorem.

***Theorem* 4.8.4. (Euclid's Lemma)**. If a prime number p divides the product ab, then p must divide a or p must divide b.

Proof. Suppose p divides ab. If p divides a, we are done. If p does not divide a, its only positive divisors are 1 and p. Therefore, $gcd(p, a)$ must be 1. By 4.8.2, since p divides ab and is coprime to a, it must divide b. ■

4.8.4 Uniqueness of Prime Factorisation

With Euclid's Lemma established, we can finally prove the uniqueness part of Theorem 4.8.1.

Proof. Suppose for the sake of contradiction that an integer N could be factored into primes in two different ways. Let's call these two factorisations:

$$N = p_1 \times p_2 \times \cdots \times p_k \quad \textit{and} \quad N = q_1 \times q_2 \times \cdots \times q_m$$

Our goal is to show that these two collections of primes must be identical. Let's start with the first prime in the first list, p_1. Since p_1 is a factor of N, it must divide the second product as well:

$$p_1 \textit{ divides } (q_1 \times q_2 \times \cdots \times q_m)$$

Now we use Theorem 4.8.4. It tells us that if a prime divides a product, it must divide at least one of the factors. Applying this repeatedly, p_1 must divide one of the primes in the list $q_1, q_2, \ldots, q_m$. Let's say it divides q_j.
But q_j is a prime number, so its only positive divisors are 1 and itself. Since p_1 is also a prime, it is greater than 1. Therefore, if p_1 divides q_j, it must be that $p_1 = q_j$.
We have found a match. The prime p_1 from the first list is identical to one of the primes in the second list. Since the order of factors does not matter, we can re-arrange the second list to put this q_j first. So, we can say $p_1 = q_1$.
Now we can divide both sides of our original equation $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$ by this common prime. This leaves us with a new, simpler equation:

$$p_2 \times \cdots \times p_k = q_2 \times \cdots \times q_m$$

We can repeat this exact same argument for the next prime, p_2. It must divide the product on the right, so it must be equal to one of the remaining primes. We cancel them and continue.
We proceed like this, matching each prime from the p-list with a prime from the q-list and cancelling them out one by one.
What happens if the lists have different lengths? Suppose the p-list is longer than the q-list ($k > m$). After we have matched and cancelled all m of the q primes, we would be left with:

$$p_{m+1} \times \cdots \times p_k = 1$$

This is impossible. The product of any collection of prime numbers must be greater than 1. Similarly, if the q-list were longer ($m > k$), we would end up with $1 = q_{k+1} \times \cdots \times q_m$, which is also impossible.
The only way to avoid this contradiction is if the lists have the same length ($k = m$) and every prime in the first list is matched with an identical prime in the second. Therefore, the two factorisations were not different after all; they are just rearrangements of the same collection of primes. The prime factorisation of N is unique. ■

4.8.5 The Infinitude of Primes

A natural question, first answered by Euclid, is whether the list of prime numbers ever ends.

***Theorem* 4.8.5. (Euclid's Theorem)**. The number of prime numbers is infinite.

Proof. This is a proof by contradiction. Assume there is a finite number of primes. Let us list them all: $p_1, p_2, p_3, \ldots, p_k$. *Now consider the number formed by multiplying all these primes together and adding one:*

$$N = (p_1 p_2 p_3 \cdots p_k) + 1$$

This number N *must have a prime factor. However, dividing* N *by any prime* p_i *in our list gives a remainder of* 1. *Thus, none of the primes in our supposedly complete list can be a factor of* N. *This means that either* N *is itself a prime not in our list, or it has a prime factor that is not in our list. In either case, we have found a prime not on our list. This contradicts our assumption that the list of primes was complete. Therefore, the assumption must be false, and the number of primes is infinite.* ■

4.9 Exercises

Part I: Mechanics of Primes and Divisors

1. Find the complete prime factorisation for each of the following integers.

(a) 45738

(b) 297675

(c) 1729 (The Hardy-Ramanujan number)

2. Use the Euclidean Algorithm to compute the greatest common divisor for the following pairs. Then, use the "backwards" substitution method described in the proof of Bézout's Identity to find one pair of integers (x, y) satisfying $ax + by = \gcd(a, b)$.

(a) $(420, 132)$

(b) $(610, 987)$

3. The Euclidean Algorithm with Negative Remainders.

Note. The Division Algorithm states $a = qb + r$ where $0 \leq r < b$. However, we could also write $a = (q + 1)b + (r - b)$. The term $r - b$ is a negative remainder. Sometimes, the algorithm proceeds faster if we choose whichever remainder, r or $r - b$, is closer to zero. For instance, to divide 100 by 37:

$$100 = 2 \times 37 + 26 \quad \text{or} \quad 100 = 3 \times 37 - 11$$

Since -11 is closer to zero than 26 is, it is more efficient to use the negative remainder. The next step would be $\gcd(37, -11)$, which is the same as $\gcd(37, 11)$.

Use the Euclidean Algorithm, allowing for negative remainders where advantageous, to find the GCD of 54643 and 91319.

Part II: Properties of Fractions and Coprimality

4. A rational number $\frac{a}{b}$ is in lowest terms if $\gcd(a, b) = 1$. Suppose that $\frac{A}{B} = \frac{a}{b}$, where $\frac{a}{b}$ is in lowest terms. Prove that there must exist an integer k such that $A = ka$ and $B = kb$.

Remark. From the equality, we have $Ab = Ba$. Since a divides Ba, it must divide Ab. Use 4.8.2.

5. Let $\frac{a}{b}$ and $\frac{c}{d}$ be two fractions in lowest terms. Prove that their sum, $\frac{ad+bc}{bd}$, cannot be an integer unless their denominators are equal $(b = d)$.

Part III: Divisibility and Number Forms

6. Prove that the difference of the squares of any two odd numbers is divisible by 8.

Remark. Let the odd numbers be $2k+1$ and $2j+1$. Expand the difference of their squares and factor the result.

7. Prove that the sum of the squares of three consecutive odd numbers, when increased by 1, is a multiple of 12.

8. Let a and b be coprime integers. Prove the following:

(a) $\gcd(a+b, a-b)$ is either 1 or 2.

(b) $\star$ $\gcd(a+b, a^2-ab+b^2)$ is either 1 or 3.

Remark. Note that $a^3+b^3 = (a+b)(a^2-ab+b^2)$. Let d be the gcd and show that d must divide $3a^2$ and $3b^2$.

9. Consider the statement from the Division Algorithm, $x = uy + v$ with $0 \leq v < y$. Show that if one divides both x and uy by the remainder v, the new remainders will be identical, but the new quotients will differ by exactly one.

Part IV: The Least Common Multiple

11. We define the least common multiple of two positive integers a and b, written $\text{lcm}(a, b)$, as the smallest positive integer that is a multiple of both a and b.

(a) By listing multiples, find $\text{lcm}(12, 18)$ and $\text{lcm}(7, 13)$.

(b) Prove the fundamental relationship: $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$.

Remark. Consider the prime factorisation of a and b. For any prime p, let $a = p^{\alpha} \cdots$ and $b = p^{\beta} \cdots$. The exponent of p in $\gcd(a, b)$ is $\min(\alpha, \beta)$ and in $\text{lcm}(a, b)$ is $\max(\alpha, \beta)$. The identity $\alpha + \beta = \min(\alpha, \beta) + \max(\alpha, \beta)$ proves the result.

(c) Use the formula from part (b) and the Euclidean Algorithm to calculate $\text{lcm}(3054, 12378)$.

12. $\star$ Let a, b, c be three positive integers. Let $G = \gcd(a, b, c)$ and $L = \text{lcm}(a, b, c)$. Let $g_1 = \gcd(b, c)$, $g_2 = \gcd(c, a)$, $g_3 = \gcd(a, b)$. Prove the identity:

$$L = \frac{abcG}{g_1 g_2 g_3}$$

Remark. As in the previous problem, prove this identity by considering the exponent of an arbitrary prime p on each side of the equation.

Part V: Further Problems and Applications

13. A perfect number is a positive integer that is equal to the sum of its proper positive divisors (divisors excluding the number itself). For example, 6 is perfect because its proper divisors are $1, 2, 3$ and $1 + 2 + 3 = 6$.

(a) Verify that 28 is a perfect number.

(b) Euclid proved that if $2^p - 1$ is a prime number (a Mersenne prime), then $2^{p-1}(2^p - 1)$ is a perfect number. Prove this theorem.

Remark. List all the divisors of $2^{p-1}(2^p - 1)$ and sum them up.

14. $\star$ **Arbitrarily Large Gaps Between Primes.** This problem guides you through a proof that there can be arbitrarily large gaps between consecutive prime numbers.

(a) We define the **factorial** of a positive integer k, written $k!$, as the product of all integers from 1 to k. For example, $4! = 1 \times 2 \times 3 \times 4 = 24$. Prove that for any integer j such that $2 \leq j \leq k$, the number j must divide $k!$.

(b) Consider the number $M = 5! + 2$. Explain why M must be a composite number without calculating its value.

(c) Now consider the sequence of four numbers: $5! + 2, 5! + 3, 5! + 4, 5! + 5$. Prove that every number in this sequence is composite.

(d) Generalise your argument. To prove that there is a sequence of n consecutive composite integers for any $n \geq 2$, consider the sequence starting with the number $(n + 1)! + 2$. Write out the full sequence and prove that every term in it must be composite.

4.10 Operations with Fractions

A fraction is a number of the form $a \div b$ or $\frac{a}{b}$. The laws of algebra provide the framework for manipulating them.

***Theorem* 4.10.1. (Simplifying Fractions)**. Multiplying or dividing the numerator and denominator of a fraction by the same non-zero quantity does not change the value of the fraction.

$$\frac{a}{b} = \frac{a \times c}{b \times c} \quad (\text{for } c \neq 0) \tag{4.10}$$

Proof. Using the laws of association and commutation for multiplication and division:

$$\begin{aligned}
\frac{a \times c}{b \times c} &= (a \times c) \div (b \times c) \\
&= a \times c \div b \div c && \textit{By the Associative Law} \\
&= a \div b \times c \div c && \textit{By the Commutative Law} \\
&= (a \div b) \times (c \div c) \\
&= (a \div b) \times 1 = \frac{a}{b} && \textit{Since } c \div c = 1
\end{aligned}$$

■

This principle is fundamental to arithmetic with fractions. To add or subtract fractions, we must first express them with a common denominator.

***Theorem* 4.10.2. (Addition and Subtraction of Fractions)**. To add or subtract two fractions, rewrite them with a common denominator, then add or subtract their numerators.

$$\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd} \tag{4.11}$$

Proof.

$$\begin{aligned}
\frac{a}{b} \pm \frac{c}{d} &= \frac{a \times d}{b \times d} \pm \frac{c \times b}{d \times b} && \textit{Create a common denominator } bd \\
&= \frac{ad}{bd} \pm \frac{bc}{bd} \\
&= (ad \div bd) \pm (bc \div bd) \\
&= (ad \pm bc) \div bd && \textit{By the Distributive Law for Division} \\
&= \frac{ad \pm bc}{bd}
\end{aligned}$$

■

Example 4.10.1. (Three terms).

$$\frac{a}{b} \pm \frac{c}{d} \pm \frac{e}{f} = \frac{adf \pm cbf \pm ebd}{bdf},$$

by the same device.

Note. If b and d share common factors, we can find a **lowest common denominator** (LCD), which is the least common multiple of b and d. For example, if $b = 6$ and $d = 10$, their LCD is 30, not 60. Using the LCD makes calculations simpler.

The rules for multiplication and division follow directly from the laws of association and commutation.

***Theorem* 4.10.3. (Multiplication of Fractions)**. To multiply two fractions, multiply their numerators and multiply their denominators.

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd} \tag{4.12}$$

Proof.

$$\begin{aligned} \frac{a}{b} \times \frac{c}{d} &= (a \div b) \times (c \div d) \\ &= a \div b \times c \div d \\ &= (a \times c) \div (b \times d) && \textit{By the Commutative Law} \\ &= \frac{ac}{bd} \end{aligned}$$

■

***Theorem* 4.10.4. (Division of Fractions)**. To divide one fraction by another, multiply the first fraction by the reciprocal of the second.

$$\frac{a}{b} \div \frac{c}{d} = \frac{a}{b} \times \frac{d}{c} = \frac{ad}{bc} \tag{4.13}$$

Proof.

$$\begin{aligned} \frac{a}{b} \div \frac{c}{d} &= (a \div b) \div (c \div d) \\ &= a \div b \div c \times d && \textit{By the Associative Law for Division} \\ &= (a \times d) \div (b \times c) && \textit{By the Commutative Law} \\ &= \frac{ad}{bc} \end{aligned}$$

■

4.11 Rational and Irrational Numbers

By taking quotients of the integers we have studied, we form a larger and more powerful system of numbers.

Definition 4.11.1. ***(Rational Numbers)***. A rational number is a number that can be written as a quotient $\frac{m}{n}$, where m and n are integers and $n \neq 0$. The collection of all rational numbers is denoted by the symbol $\mathbb{Q}$.

Examples of rational numbers include $\frac{1}{2}$, $\frac{-3}{7}$, and any integer m, since we can write $m = \frac{m}{1}$. The representation of a rational number is not unique; for example, $\frac{1}{2} = \frac{2}{4} = \frac{-5}{-10}$. This leads to a necessary rule for determining when two different-looking fractions represent the same number.

***Theorem* 4.11.1.** (Rule for Equality of Fractions)Two rational numbers $\frac{a}{b}$ and $\frac{c}{d}$ are equal if and only if $ad = bc$.

Proof. *First, assume* $\frac{a}{b} = \frac{c}{d}$. *We multiply both sides by the product of the denominators,* bd.

$$\begin{aligned}
\frac{a}{b} \times (bd) &= \frac{c}{d} \times (bd) \\
(a \div b) \times (b \times d) &= (c \div d) \times (d \times b) && \text{Notation change} \\
a \times (b \div b) \times d &= c \times (d \div d) \times b && \text{Commutative and Associative Laws} \\
a \times 1 \times d &= c \times 1 \times b && \text{By 4.2.2} \\
ad &= cb
\end{aligned}$$

The reverse proof, starting from $ad = bc$ *and dividing both sides by* bd, *is left as an exercise.* ■

This method of checking equality is often called **cross-multiplication**. It is a direct consequence of the laws of algebra.

4.11.1 Lowest Form

Any rational number can be simplified to a standard representation called its lowest form.

Definition 4.11.2. ***(Lowest Form)***. A positive rational number $\frac{m}{n}$ is in its lowest form if its numerator m and denominator n are positive integers whose only common factor is 1.

***Theorem* 4.11.2.** . Any positive rational number has a unique expression in lowest form.

Proof. *Let a rational number be given as* $\frac{m}{n}$ *with* m, n *positive integers. Let* d *be the greatest common factor of* m *and* n. *We can then write* $m = dr$ *and* $n = ds$ *for some positive integers* r, s. *Our rational number is equal to*

$$\frac{m}{n} = \frac{dr}{ds} = \frac{r}{s}$$

We now show that $\frac{r}{s}$ *is in lowest form. Suppose* $e > 1$ *is a common factor of* r *and* s. *Then* $r = ex$ *and* $s = ey$ *for some integers* x, y. *This would mean* $m = dex$ *and* $n = dey$, *so* de *is a common factor of* m *and* n. *Since* $e > 1$, $de > d$. *This is impossible, as* d *was defined to be the greatest common factor. Thus, the only common factor of* r *and* s *is* 1. *This final step is justified by the Theorem 4.10.1.* ■

4.11.2 The Discovery of Irrational Numbers

A natural question arises: can all numbers be represented as a ratio of two integers? For centuries, this was assumed to be true. However, a simple geometric problem reveals this to be false. Consider an isosceles right-angled triangle with sides of length 1. By the Pythagorean theorem, the hypotenuse has a length whose square is $1^2 + 1^2 = 2$. Is this length a rational number?

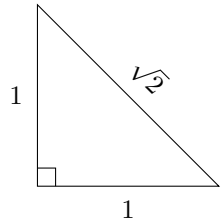


Figure 4.6: An isosceles right-angled triangle with sides of length 1. The hypotenuse has a length of $\sqrt{2}$.

***Theorem* 4.11.3.** There is no rational number whose square is 2.

Proof. *This is a proof by contradiction. We assume the opposite of what we want to prove and show it leads to an impossible conclusion.*

1. ***Assumption:*** *Suppose there exists a rational number whose square is* 2.
2. *By the previous theorem, we can write this number in its lowest form,* $\frac{p}{q}$*, where* p *and* q *are positive integers with no common factors other than* 1*. This means that not both* p *and* q *can be even.*
3. *We have* $\left(\frac{p}{q}\right)^2 = 2$*, which means* $\frac{p^2}{q^2} = 2$*.*
4. *Multiplying by* q^2 *gives* $p^2 = 2q^2$*. This shows that* p^2 *is an even number.*
5. *By the corollary to our theorem on even and odd numbers, if* p^2 *is even, then* p *must be even.*
6. *Since* p *is even, we can write it as* $p = 2k$ *for some integer* k*.*
7. *Substituting this into the equation from step 4:* $(2k)^2 = 2q^2$*, which simplifies to* $4k^2 = 2q^2$*.*
8. *Dividing by* 2*, we get* $2k^2 = q^2$*. This shows that* q^2 *is also an even number.*
9. *As before, if* q^2 *is even, then* q *must be even.*
10. ***Contradiction:*** *We have shown that both* p *and* q *must be even. This contradicts our initial condition in step 2 that* $\frac{p}{q}$ *was in lowest form and not both numbers could be even.*

Since our initial assumption leads to a logical impossibility, the assumption must be false. Therefore, there is no rational number whose square is 2. ■

Definition 4.11.3. ***(Irrational Number)***. A number that cannot be expressed as a ratio of two integers is called an irrational number.

The number whose square is 2, denoted $\sqrt{2}$, is our first example of an irrational number. The collection of all rational and irrational numbers together form the **real numbers**, $\mathbb{R}$.

4.12 Exercises

Part I: Foundational Manipulation of Algebraic Fractions

Prove the following relations.

1.
$$\frac{1}{2x+y} + \frac{1}{2x-y} = \frac{4x}{4x^2-y^2}..$$

2.
$$\frac{2x}{x+5} - \frac{3x+1}{2x+1} = \frac{x^2-14x-5}{2x^2+11x+5}.$$

3.
$$\frac{1}{x+3y} + \frac{1}{x-3y} = \frac{2x}{x^2-9y^2}.$$

4.
$$\frac{1}{3x-2y} + \frac{x}{x+y} = \frac{x+y+3x^2-2xy}{3x^2+xy-2y^2}.$$

5.
$$\frac{x^3-y^3}{x-y} = x^2+xy+y^2.$$

6.
$$\frac{x^4-y^4}{x-y} = x^3+x^2y+xy^2+y^3.$$

7. Let

$$x = \frac{1-t^2}{1+t^2} \quad \text{and} \quad y = \frac{2t}{1+t^2}.$$

Show that $x^2 + y^2 = 1$.

8.

$$\frac{x^3+1}{x+1} = x^2 - x + 1, \quad \frac{x^5+1}{x+1} = x^4 - x^3 + x^2 - x + 1.$$

Simplify the following expressions to their most reduced form.

9.

$$\frac{m+1}{n+1} - \frac{m}{n},$$

given $m = n - 1$.

10.

$$\frac{1}{2}\left(\frac{1}{x-3} - \frac{1}{x+1}\right),$$

with $(x \neq 3, -1)$.

11.

$$\frac{x}{x-y} + \frac{y}{y-x}, \quad \frac{x^2}{x-y} + \frac{y^2}{y-x}$$

Remark. Remember that $y - x = -(x - y)$, and you can substitute $(x - y)$ as z.

12.

$$\frac{a}{a-b} + \frac{b}{b-a}$$

13.

$$\frac{1}{4x^2+4x+1} \div \frac{1}{4x^2-1}$$

14.

$$4 - \left((x+3) \div \frac{x^2+5x+6}{x-2}\right)$$

15.

$$\frac{1 - \dfrac{x(1-y)}{x+y}}{1 + \dfrac{1-y}{x+y}}$$

16. Simplify the expression where $P = x + y$ and $Q = x - y$.

$$\frac{P+Q}{P-Q} \times \frac{P-Q}{P+Q}$$

17.

$$\left(a - \frac{b^2}{a+b}\right) \times \left(a + \frac{b^2}{a-b}\right)$$

Remark. This one doesn't end up pretty, that's on purpose.

18.

$$\left(\frac{a}{b} - \frac{b}{a}\right) \div \left(\frac{a^2}{b^2} - \frac{b^2}{a^2}\right)$$

Part II: Advanced Problems and Identities

Simplify the following complex expressions and prove the given identity.

Remark. Some of these ones aren't pretty, that's on purpose stop when you think there isn't anymore simplification to do.

19. Prove the following identity:

$$\frac{x}{x-y}+\frac{x}{x+y}+\frac{2x^2}{x^2+y^2}$$

20.

$$\frac{1}{p-q}-\frac{1}{p+q}+\frac{2p}{p^2-q^2}$$

21.

$$\frac{1+\dfrac{x}{1+x}}{x+\dfrac{1}{1+x}} \div \frac{(x+1)^2-x^2}{x^2+x+1}$$

22.

$$\frac{a^2+b^2}{(a+b)^2}+\frac{\dfrac{2}{ab}\left(\dfrac{1}{a}+\dfrac{1}{b}\right)}{\left(\dfrac{1}{a}+\dfrac{1}{b}\right)^3}$$

Remark. You can always substitute $\left(\frac{1}{a}+\frac{1}{b}\right)$ as z to make this easier to solve.

23.

$$\left(b+\frac{a^2}{b-a}\right)\times\left(b-\frac{a^2}{b+a}\right)$$

24.

$$\frac{1}{ab}-\frac{1}{ac}-\left(\frac{1}{bc}\div\frac{a^2-(b-c)^2}{a}\right)$$

25.

$$\left(\frac{a}{b}-\frac{b}{a}\right)^2\div\left(\frac{x^2}{b^2}-\frac{y^2}{a^2}\right)$$

26.

$$\left(\frac{x}{y}+\frac{y}{z}\right)\left(\frac{a}{b}+\frac{b}{a}\right)-\left(\frac{x}{y}-\frac{y}{z}\right)\left(\frac{a}{b}-\frac{b}{a}\right)$$

Part III: Proof and $\star$ Problems

Prove that

27. If n is an odd integer, prove that

$$\frac{x^n+1}{x+1}=x^{n-1}-x^{n-2}+x^{n-3}-\cdots-x+1.$$

Remark. Cross-multiply.

28. there is no positive rational number a such that $a^3=2$

29. there is no positive rational number a such that $a^4=2$

30. there is no positive rational number a such that $a^2 = 3$, $a^2 = 5$ and $a^2 = 6$

Remark. You may assume that a positive integer can be written in one of the forms $3k, 3k+1, 3k+2$ for some integer k. Prove that if the square of a positive integer is divisible by 3, then so is the integer. Then use a similar proof as for $\sqrt{2}$.

31. $\star$ Why does the proof based on the remark above not work for $\sqrt{4}$.

32. $\star\star$ there is no positive rational number a such that $a = \sqrt{2} + \sqrt{6}$

Remark. Square both sides, and show using contradiction that $\sqrt{3}$ is equal to a rational number.

33. $\star\star$ there is no positive rational number a such that $a = \sqrt{2} + \sqrt{3}$

34. $\star\star$ Let p be a prime number. Adapt the logic used to prove the uniqueness of prime factorisation to prove that $\sqrt{p}$ is irrational.

Remark. Assume $\sqrt{p} = a/b$ where the fraction is in lowest terms. Show this leads to p dividing both a and b, a contradiction.

Chapter 5

Generalised Distribution and Its Consequences

We have seen that the distributive law connects addition and multiplication. For two expressions, the rule is simple: multiply every term in the first expression by every term in the second.

$$(a-b)(c-d) = ac - ad - bc + bd$$

This principle can be extended to any number of expressions.

5.1 The Generalised Law of Distribution

Consider the product of three factors, such as $(a+b)(c+d)(e+f)$. We can first multiply the first two factors, and then multiply the result by the third:

$$\begin{aligned}(a+b)(c+d)(e+f) &= (ac+ad+bc+bd)(e+f)\\ &= ace + acf + ade + adf + bce + bcf + bde + bdf\end{aligned}$$

Notice that each term in the final result, such as adf, is formed by choosing exactly one term from each of the original brackets: a from the first, d from the second, and f from the third. This reveals the general rule.

***Theorem* 5.1.1. (Generalised Law of Distribution)**. To find the product of several bracketed expressions, form all possible partial products by taking exactly one term from each bracket. The sign of each partial product follows the usual law of signs.

Proof. This is just 4.1.3 done repeatedly.
Let's start with two brackets: $(a+b)(c+d)$. The distributive law tells us to multiply every term in the first bracket by every term in the second:

$$(a+b)(c+d) = ac + ad + bc + bd.$$

Notice that each resulting term (e.g., ad) is formed by choosing exactly one term from the first bracket (a) and one from the second (d). The rule holds.
Now, let's multiply this result by a third bracket, $(e+f)$:

$$((a+b)(c+d))(e+f) = (ac+ad+bc+bd)(e+f).$$

To expand this, we must distribute each term from the new, larger first bracket into the second bracket:

$$ac(e+f) + ad(e+f) + bc(e+f) + bd(e+f).$$

Distributing one final time gives:

$$(ace + acf) + (ade + adf) + (bce + bcf) + (bde + bdf).$$

Let's examine a typical final term, for example, bcf. It was formed from the term bc (which came from picking b from the first original bracket and c from the second) multiplied by f (from the third bracket). Therefore, bcf is formed by taking exactly one term from each of the three original brackets. This same logic applies to every other term in the final expansion.
If we were to multiply by a fourth bracket, the same process would repeat: each of these eight terms would be multiplied by each term in the fourth bracket, extending the pattern. The process demonstrates that the rule holds for any number of brackets. ■

***Corollary* 5.1.1.** If the brackets contain $l, m, n, \ldots$ terms respectively, then the total number of terms in the distributed product, before any collection of like terms, is $l \times m \times n \times \ldots$.

Proof. For each of the l choices from the first bracket, there are m choices from the second, giving $l \times m$ pairs. For each of these pairs, there are n choices from the third bracket, giving $(l \times m) \times n$ triplets, and so on. ■

Remark. The proof of this requires counting you can pretty much skip it if you don't understand it.

Example 5.1.1.

(i) $(a - b)(c - d)(e - f)$. The product will contain $2 \times 2 \times 2 = 8$ terms. A typical term is, for example, $(-b)(c)(-f) = +bcf$. The full expansion is:

$$ace - acf - ade + adf - bce + bcf + bde - bdf$$

Note. Combining like terms can shrink the list. For example, $(a + b)^2$ doesn't leave 4 distinct terms, because the two ab terms combine.

(ii) $(x + y)(x - y)(a + b + c)$. The product will contain (at most) $2 \times 2 \times 3 = 12$ terms.

$$x^2a + x^2b + x^2c - y^2a - y^2b - y^2c$$

Here we performed the first multiplication $(x + y)(x - y) = x^2 - y^2$ mentally to simplify the process.

5.1.1 Important Identities from Reduction

In the most general case, all the partial products are different. However, when the terms in the brackets are related, many partial products become identical and can be collected. This reduction leads to some of the most important formulae in algebra.

Consider the product $(a + b)(a + b)$, or $(a + b)^2$. The general rule gives four terms: aa, ab, ba, bb. Since multiplication is commutative, $ab = ba$. Collecting these like terms gives the result:

$$(a + b)^2 = a^2 + 2ab + b^2$$

This is the formula for a **perfect square**. Similarly, we can establish three fundamental identities that must be committed to memory.

$$(a + b)^2 = a^2 + 2ab + b^2 \tag{5.1}$$

$$(a - b)^2 = a^2 - 2ab + b^2 \tag{5.2}$$

$$(a + b)(a - b) = a^2 - b^2 \tag{5.3}$$

The last identity is called the difference of two squares. Its power lies in multiplying a sum by a difference.

This principle of combining recurring terms can be applied to higher powers. Consider $(a+b)^3 = (a+b)(a+b)(a+b)$. The general distribution gives $2 \times 2 \times 2 = 8$ terms. The possible distinct products using only letters a and b are a^3, a^2b, ab^2, b^3.

- To get a^3, we must choose a from all three brackets. This can be done in only one way.
- To get a^2b, we must choose b from one bracket and a from the other two. We can take b from the first, second, or third bracket. There are three ways to do this.
- Similarly, there are three ways to form ab^2.
- There is only one way to form b^3.

This gives the expansion for the cube of a binomial:

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 \tag{5.4}$$
$$(a-b)^3 = a^3 - 3a^2b + 3ab^2 - b^3 \tag{5.5}$$

The second formula is derived from the first by substituting $-b$ for b.

The same method extends to expressions with more terms. For $(a+b+c)^2$, the distinct types of terms are squares like a^2 and products like ab.

- A term like a^2 is formed by picking a from both brackets. This occurs once.
- A term like ab is formed by picking a from the first bracket and b from the second, or b from the first and a from the second. This occurs twice.

This leads to the identity:

$$(a+b+c)^2 = a^2 + b^2 + c^2 + 2ab + 2bc + 2ca$$

Example 5.1.2. .

$$(b+c)(c+a)(a+b) = a^2b + ab^2 + b^2c + bc^2 + c^2a + ca^2 + 2abc.$$

5.1.2 Abbreviative Notations: Σ and Π

Writing out long sums and products is laborious. To abbreviate them, we use the Greek letters Σ (Sigma, for Sum) and Π (Pi, for Product). There are two main ways this is done: a formal, indexed notation, and an informal shorthand for symmetric expressions.

Indexed Notation

This is the standard, precise way to write sums and products.

Definition 5.1.1. ***(Summation)***. For a list of terms $t_1, t_2, \ldots, t_n$, the symbol

$$\sum_{i=1}^{n} t_i \quad \text{means} \quad t_1 + t_2 + \cdots + t_n.$$

The letter i is the index of summation.

Definition 5.1.2. ***(Product)***. For the same list of terms, the symbol

$$\prod_{i=1}^{n} t_i \quad \text{means} \quad t_1 \cdot t_2 \cdots t_n.$$

These notations follow the standard laws of algebra.

***Theorem* 5.1.2. (Fundamental Properties of Summation)**. Let a_k and b_k be sequences of terms, and let c be a constant. The following properties hold:

$$\sum_{k=1}^{n}(a_k + b_k) = \sum_{k=1}^{n} a_k + \sum_{k=1}^{n} b_k \qquad \text{(Additive Property)} \tag{5.6}$$

$$\sum_{k=1}^{n}(ca_k) = c\sum_{k=1}^{n} a_k \qquad \text{(Homogeneous Property)} \tag{5.7}$$

$$\sum_{k=1}^{n}(a_k - a_{k-1}) = a_n - a_0 \qquad \text{(Telescoping Property)} \tag{5.8}$$

Proof. The proofs are a matter of writing out the sums and regrouping.

- ***Additive Property:*** *We expand the sum and then use the associative and commutative laws of addition to re-order the terms.*

$$\begin{aligned}\sum_{k=1}^{n}(a_k + b_k) &= (a_1 + b_1) + (a_2 + b_2) + \cdots + (a_n + b_n)\\ &= (a_1 + a_2 + \cdots + a_n) + (b_1 + b_2 + \cdots + b_n)\\ &= \sum_{k=1}^{n} a_k + \sum_{k=1}^{n} b_k.\end{aligned}$$

- ***Homogeneous Property:*** *This is just the distributive law, as we have already seen.*

$$\sum_{k=1}^{n} ca_k = ca_1 + ca_2 + \cdots + ca_n = c(a_1 + a_2 + \cdots + a_n) = c\sum_{k=1}^{n} a_k.$$

- ***Telescoping Property:*** *This elegant property is best seen by writing out the terms. Most of them cancel in pairs.*

$$\begin{aligned}\sum_{k=1}^{n}(a_k - a_{k-1}) &= (a_1 - a_0) + (a_2 - a_1) + (a_3 - a_2) + \cdots + (a_n - a_{n-1})\\ &= -a_0 + (a_1 - a_1) + (a_2 - a_2) + \cdots + (a_{n-1} - a_{n-1}) + a_n\\ &= a_n - a_0.\end{aligned}$$

  The sum collapses like an old-fashioned spyglass, leaving only the ends visible. This property is a surprisingly powerful tool for deriving summation formulae.

■

⋆⋆Symmetry and Shorthand Notation

Note. If you're here for A-level skip this section, if you also don't understand set theory skip this section.

Let us re-examine an identity we derived earlier:

$$(a + b + c)^2 = a^2 + b^2 + c^2 + 2ab + 2bc + 2ca$$

Notice a remarkable property of the expanded expression. If we swap the variables a and b, we get:

$$b^2 + a^2 + c^2 + 2ba + 2ac + 2cb$$

By the commutative laws of addition and multiplication, this is exactly the same expression we started with. The terms have merely been rearranged. This property of being unchanged by the swapping of variables is called symmetry.

Definition 5.1.3. ***(Symmetric Expression)***. An expression is called symmetric in a set of variables if its value remains unchanged when any two of those variables are interchanged. This implies it is unchanged by any permutation of the variables.

Example 5.1.3. .

- $a + b + c$ is symmetric in $\{a, b, c\}$.
- $a^2b + ab^2 + b^2c + bc^2 + c^2a + ca^2$ is symmetric in $\{a, b, c\}$.
- $a^2b + c$ is **not** symmetric in $\{a, b, c\}$. If we swap a and c, the expression becomes $c^2b + a$, which is different.

Expressions with this property are so fundamental in algebra that a compact notation has been developed specifically for them. This is the second, more informal, use of the Σ and Π symbols.

Definition 5.1.4. ***(Σ and Π for Symmetric Expressions)***. First, we establish a set of variables, for instance $\{a, b, c\}$.

- The symbol Σ, without indices, stands for the "sum of all distinct terms that can be formed by permuting the variables within a sample term."
- Similarly, the symbol Π stands for the "product of all such distinct terms."

The power of this method is its brevity, but it requires the context (the set of variables) to be clear.

Example 5.1.4. Let the context be the three variables $\{a, b, c\}$..

- To understand Σa^2, we start with the sample term a^2. By swapping the variables, we can also form b^2 and c^2. The sum of all these is:
$$\Sigma a^2 = a^2 + b^2 + c^2.$$
- For Σab, the sample term is ab. Swapping variables gives us ab, ac, ba, bc, ca, cb. The distinct products are ab, ac, bc. Thus:
$$\Sigma ab = ab + ac + bc.$$
- For $\Pi(a + b)$, the sample term is $(a + b)$. The other distinct terms of this type are $(b + c)$ and $(c + a)$. The product is:
$$\Pi(a + b) = (a + b)(b + c)(c + a).$$

This shorthand makes our earlier identities much cleaner. For variables a, b, c:

$$(a + b + c)^2 = a^2 + b^2 + c^2 + 2(ab + bc + ca) = \Sigma a^2 + 2\Sigma ab$$
$$(a + b + c)^3 = \Sigma a^3 + 3\Sigma a^2 b + 6abc$$

The term $\Sigma a^2 b$ expands to $a^2b + ab^2 + b^2c + bc^2 + c^2a + ca^2$. Notice there are six terms, as this is the sum over all distinct permutations.

5.1.3 Techniques of Expansion

The fundamental identities can be applied to more complex expressions through substitution and grouping.

The Principle of Substitution

The letters in our identities can stand for any algebraic quantity.

Example 5.1.5. $((3x^2 - 4y)^3)$. We use the identity for $(a-b)^3$ from Equation 5.5, letting $a = 3x^2$ and $b = 4y$.

$$\begin{aligned}(3x^2 - 4y)^3 &= (3x^2)^3 - 3(3x^2)^2(4y) + 3(3x^2)(4y)^2 - (4y)^3 \\ &= 27x^6 - 3(9x^4)(4y) + 3(3x^2)(16y^2) - 64y^3 \\ &= 27x^6 - 108x^4y + 144x^2y^2 - 64y^3\end{aligned}$$

Example 5.1.6. Generating new identities via substitution. Start with $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$ and substitute b with $b + c$:

$$(a + (b + c))^3 = a^3 + 3a^2(b + c) + 3a(b + c)^2 + (b + c)^3,$$

which tidies to

$$a^3 + b^3 + c^3 + 3(a^2b + a^2c + ab^2 + ac^2 + b^2c + bc^2) + 6abc.$$

Expansion by Grouping

We can simplify complex multiplications by grouping terms and treating them as single units. This often allows us to reuse the fundamental identities.

Example 5.1.7. $((a+b-c+d)(a-b-c-d))$. Instead of multiplying term by term (which would produce 16 partial products), we can group the terms to create the difference of two squares form from Equation 5.3.

$$\begin{aligned}(a+b-c+d)(a-b-c-d) &= ((a-c)+(b+d))((a-c)-(b+d)) \\ &= (a-c)^2 - (b+d)^2 && \text{Using } (X+Y)(X-Y) = X^2 - Y^2 \\ &= (a^2 - 2ac + c^2) - (b^2 + 2bd + d^2) && \text{Using perfect square identities} \\ &= a^2 - b^2 + c^2 - d^2 - 2ac - 2bd\end{aligned}$$

This method can also be used to derive results. For example, $(a+b+c)^2$ can be found by grouping it as $((a+b)+c)^2$.

$$\begin{aligned}((a+b)+c)^2 &= (a+b)^2 + 2(a+b)c + c^2 \\ &= (a^2 + 2ab + b^2) + 2ac + 2bc + c^2 \\ &= a^2 + b^2 + c^2 + 2ab + 2bc + 2ac\end{aligned}$$

5.1.4 A Useful Check: The Sum of Coefficients

Mistakes are common in lengthy expansions. A simple check can often catch them.

***Theorem* 5.1.3.** The algebraic sum of the coefficients in the expansion of any product can be found by substituting the value 1 for every variable in the original expression.

Proof. If you replace each variable by 1*, every monomial's value becomes its coefficient, so the whole polynomial evaluates to the sum of its coefficients.* ■

Example 5.1.8. Check the expansion of $(x - 2y + 3z)^2 = x^2 + 4y^2 + 9z^2 - 4xy - 12yz + 6xz.$. Substitute $x = 1, y = 1, z = 1$ into both sides.

- **Left Side:** $(1 - 2(1) + 3(1))^2 = (1 - 2 + 3)^2 = 2^2 = 4$.

- **Right Side:** $1^2 + 4(1)^2 + 9(1)^2 - 4(1)(1) - 12(1)(1) + 6(1)(1) = 1 + 4 + 9 - 4 - 12 + 6 = 4$.

Since both sides evaluate to 4, the expansion is likely correct. If the results were different, the expansion would be certainly wrong.

Example 5.1.9.

$$(1 + 1)^4 = 16 \Rightarrow \text{coefficients of } (a + b)^4 \text{ add to } 16.$$

5.2 Polynomials: The Building Blocks of Algebra

So far, we have been multiplying expressions without giving them a proper name. These expressions, like $a^2 + 2ab + b^2$ or $27x^6 - 108x^4y + 144x^2y^2 - 64y^3$, are examples of a very important class of objects in algebra called polynomials. It is time to formalise what they are.

5.2.1 Definitions

Definition 5.2.1. ***(Term)***. A term of a polynomial is a product of a coefficient and any number of variables raised to positive whole-number powers. The coefficient must not contain any of the variables.

Example 5.2.1. .

- $3x^2y^3$ is a term. The variables are x and y, the coefficient is 3.
- $-7a^2b$ is a term if the variables are considered to be a and b. The coefficient is -7.
- cx^4 is a term in the variable x. Here, the coefficient is c, which we treat as a constant that is independent of x.
- $\frac{x}{a}$ is a valid term for a polynomial in x, since it can be written as $(\frac{1}{a})x^1$. However, an expression containing this would not be a polynomial in a, because a is in the denominator.

Definition 5.2.2. ***(Polynomial)***. A polynomial is the algebraical sum of one or more terms. In old textbooks, you might see this called a rational integral algebraical function, but that is a mouthful!

Example 5.2.2. .

- $3x^2 + 5xy - 7y^2$ is a polynomial in the variables x and y.
- $ax^2 + bxy + cy^2$ is a polynomial in x and y. The coefficients are a, b, c.
- $x^3 - \frac{1}{2}x^2 + 8x - 1$ is a polynomial in the single variable x.

5.2.2 The Degree of a Polynomial

Every term in a polynomial has a 'degree', which tells us how 'powerful' it is. The degree of the whole polynomial is determined by its most powerful term.

Definition 5.2.3. ***(Degree)***.

- The degree of a term is the sum of the powers of its variables. For example, the degree of $3x^2y^3z^1$ is $2 + 3 + 1 = 6$.
- The degree of a polynomial is the degree of its term of highest degree.
- A constant term, like $+1$, is considered to have a degree of zero, as it could be written as $1x^0$.

Example 5.2.3. Let's find the degrees of the polynomials from our last example.

- For $3x^2 + 5xy - 7y^2$: The term $3x^2$ has degree 2. The term $5xy$ (or $5x^1y^1$) has degree $1 + 1 = 2$. The term $-7y^2$ has degree 2. The highest degree present is 2, so the polynomial is of the 2nd degree.
- For $x^3 - \frac{1}{2}x^2 + 8x - 1$: The terms have degrees $3, 2, 1$, and 0 respectively. The highest is 3, so this is a 3rd degree polynomial in x.

5.2.3 Multiplying Polynomials

We can now state a powerful and fundamental rule about what happens when we multiply these polynomials together. It follows directly from the Theorem 5.1.1 we established earlier.

***Theorem* 5.2.1. (Product of Polynomials).**

1. The product of any number of polynomials is also a polynomial.
2. The degree of the product is the sum of the degrees of the individual polynomials.
3. The highest-degree term in the product is the product of the highest-degree terms of the factors.
4. The lowest-degree term in the product is the product of the lowest-degree terms of the factors.

Proof. Let's think about multiplying two polynomials, say P_1 and P_2.

1. The Generalised Law of Distribution tells us that every term in the final product is formed by multiplying one term from P_1 by one term from P_2. Since all terms in P_1 and P_2 are valid polynomial terms, their product will also be a valid term (the powers of variables simply add). The final result is a sum of these new terms, which by definition is a polynomial.
2. Let the degree of P_1 be d_1, and let its highest-degree term be T_1. Similarly, let the degree of P_2 be d_2 with highest-degree term T_2. When we multiply, one of the resulting terms will be $T_1 \times T_2$. The degree of this term is $d_1 + d_2$. Now, consider any other combination, like multiplying T_1 by a term from P_2 with degree less than d_2. The resulting degree would be less than $d_1 + d_2$. The same happens if we pick a term from P_1 with degree less than d_1. The only way to get the maximum possible degree is by multiplying the two highest-degree terms together. Therefore, the highest-degree term of the product is $T_1 \times T_2$, and the degree of the product polynomial is $d_1 + d_2$.
3. The same logic applies in reverse for the lowest-degree terms. Let the lowest-degree terms be L_1 and L_2 with degrees l_1 and l_2. The product $L_1 \times L_2$ will have degree $l_1 + l_2$. Any other product of terms will involve a term of higher degree, resulting in a product of higher degree. Thus, L_1L_2 is the lowest-degree term of the final expansion.

This logic extends to a product of any number of polynomials. ■

Remark. These properties are cornerstones of the theory of algebraic forms. Every expansion you have done so far is an example of this theorem in action.

Example 5.2.4. Verify the theorem for $(x^2 + 2x + 3)(x - 1)$.

- The factors are polynomials of degrees 2 and 1. The theorem predicts the product will be a polynomial of degree $2 + 1 = 3$.
- The highest-degree terms of the factors are x^2 and x. Their product is x^3.
- The lowest-degree terms are 3 and -1. Their product is -3.
- Let us expand: $(x^2 + 2x + 3)(x - 1) = x^3 - x^2 + 2x^2 - 2x + 3x - 3 = x^3 + x^2 + x - 3$.
- The result is indeed a polynomial. Its degree is 3. Its highest-degree term is x^3, and its lowest-degree term is -3. The theorem holds perfectly.

5.3 Polynomials in One Variable

We have defined a polynomial as an algebraical sum of terms. A particularly important case is when the polynomial involves only one variable, say x. The general form of such a polynomial is

$$p_n x^n + p_{n-1}x^{n-1} + \cdots + p_1 x + p_0,$$

where the coefficients $p_0, p_1, \ldots, p_n$ are constants and n, the index of the highest power of x, is the degree of the polynomial.

The product rules already established (4.1.3, Theorem 5.1.1) let us expand and then collect like powers of x.

Product of Two Linear Factors

***Theorem* 5.3.1.** For any numbers a, b,

$$(x + a)(x + b) = x^2 + (a + b)x + ab. \tag{5.9}$$

Proof. *By 4.1.3,*

$$(x + a)(x + b) = x(x + b) + a(x + b) = x^2 + bx + ax + ab = x^2 + (a + b)x + ab.$$

■

Example 5.3.1.

$$(x - 2)(x + 3) = x^2 + (-2 + 3)x + (-2)(3) = x^2 + x - 6.$$

This virtually includes all possible cases; for example, setting $a = -b$ gives the difference of two squares identity from Equation 5.3.

$$(x - b)(x + b) = x^2 + (-b + b)x + (-b)(b) = x^2 - b^2.$$

The identity (5.9) admits a geometric picture that mirrors Figure 4.3.

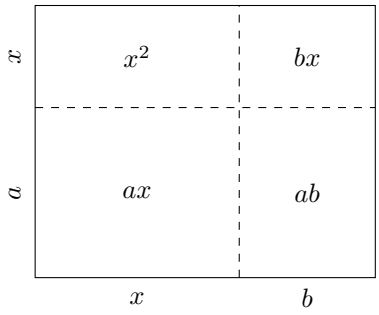


Figure 5.1: Area model for $(x + a)(x + b)$. The four sub-rectangles correspond to the terms x^2, ax, bx, ab.

Example 5.3.2. With coefficients on x, the expansion is direct..

$$\begin{aligned}(px + q)(rx + s) &= px(rx + s) + q(rx + s)\\ &= prx^2 + psx + qrx + qs\\ &= prx^2 + (ps + qr)x + qs.\end{aligned}$$

Product of Three Linear Factors

We extend the process to three factors, say $(x+a_1)(x+a_2)(x+a_3)$, by applying the previous result.

$$\begin{aligned}(x+a_1)(x+a_2)(x+a_3) &= \left(x^2+(a_1+a_2)x+a_1a_2\right)(x+a_3)\\ &= x\left(x^2+(a_1+a_2)x+a_1a_2\right)+a_3\left(x^2+(a_1+a_2)x+a_1a_2\right)\\ &= x^3+(a_1+a_2)x^2+a_1a_2x+a_3x^2+a_3(a_1+a_2)x+a_1a_2a_3\end{aligned}$$

Collecting the terms by powers of x:

$$x^3+(a_1+a_2+a_3)x^2+(a_1a_2+a_1a_3+a_2a_3)x+a_1a_2a_3.$$

A pattern emerges in the coefficients. The coefficient of x^2 is the sum of the constants a_i taken one at a time. The coefficient of x is the sum of all possible products of the constants taken two at a time. The final term is the product of all three.

5.3.1 The Product of n Linear Factors

The pattern observed for three factors generalises to the product of n linear factors, $(x+a_1)(x+a_2)\cdots(x+a_n)$. According to the Theorem 5.1.1, every term in the final expansion is formed by choosing either x or a constant a_i from each of the n brackets. The power of x in any resulting term indicates from how many brackets x was chosen.

To find the coefficient of x^{n-k}, we must sum the contributions from all terms formed by choosing x from $n-k$ brackets and constants from the remaining k brackets. Each such contribution is a product of k distinct constants chosen from $a_1,\ldots,a_n$.

We denote these coefficient sums by P_k.

- The coefficient of x^{n-1} is the sum of the constants taken one at a time:

$$P_1=\sum_{i=1}^{n}a_i=a_1+a_2+\cdots+a_n.$$

- The coefficient of x^{n-2} is the sum of all products of two distinct constants:

$$P_2=\sum_{i<j}a_ia_j=a_1a_2+a_1a_3+\cdots+a_{n-1}a_n.$$

  This abbreviated sum stands for all products of distinct pairs.

In general, the coefficient P_k is the sum of all possible products formed by taking k of the constants $a_1,\ldots,a_n$ at a time. This leads to the general formula:

$$(x+a_1)(x+a_2)\cdots(x+a_n)=\prod_{i=1}^{n}(x+a_i)=x^n+\left(\sum_{i=1}^{n}a_i\right)x^{n-1}+\left(\sum_{i<j}a_ia_j\right)x^{n-2}+\cdots+P_n, \quad (5.10)$$

where the last term, P_n, is the product of all n constants, $a_1a_2\cdots a_n$ otherwise known as

$$P_n=\prod_{i=1}^{n}a_i.$$

Example 5.3.3. Expand $(x+1)(x+2)(x+3)(x+4)$ using the general formula. Here $n=4$ and the constants are $1,2,3,4$. We calculate the coefficients P_k:

- $P_1=1+2+3+4=10$.

- $P_2 = (1 \cdot 2) + (1 \cdot 3) + (1 \cdot 4) + (2 \cdot 3) + (2 \cdot 4) + (3 \cdot 4) = 2 + 3 + 4 + 6 + 8 + 12 = 35$.
- $P_3 = (1 \cdot 2 \cdot 3) + (1 \cdot 2 \cdot 4) + (1 \cdot 3 \cdot 4) + (2 \cdot 3 \cdot 4) = 6 + 8 + 12 + 24 = 50$.
- $P_4 = 1 \cdot 2 \cdot 3 \cdot 4 = 24$.

Substituting these into Equation 5.10, we get:

$$(x+1)(x+2)(x+3)(x+4) = x^4 + 10x^3 + 35x^2 + 50x + 24.$$

Remark. When expanding any product of polynomials in x, the term of highest degree is the product of the terms of highest degree from each factor. The constant term (or absolute term) is the product of the constant terms from each factor. This agrees with the general product rule for degrees.

Example 5.3.4. In the product $(2x-1)(x+5)(x-3)$, the term of highest degree is $(2x)(x)(x) = 2x^3$. The constant term is $(-1)(5)(-3) = 15$.

5.4 The Elementary Symmetric Polynomials

The simplest and most fundamental symmetric polynomials, such as Σa and Σab, are the ones we already encountered as the coefficients in the expansion of $\prod(x + a_i)$. They are so important that they are given their own formal definition and notation.

Definition 5.4.1. ***(Elementary Symmetric Polynomial).*** Let A be a collection of n variables, for instance $A = \{a_1, a_2, \ldots, a_n\}$. The **elementary symmetric polynomial of degree** k in these variables, denoted $P_k(A)$, is formed by a two-step process:

1. First, list all possible sub-collections of k distinct variables that can be chosen from A.
2. Second, form the product of the variables in each sub-collection.
3. Finally, add all these products together.

By convention, there is only one way to choose zero variables, and its product is defined to be 1. So, $P_0(A) = 1$.

Example 5.4.1.

1. Let's trace this process for the collection of three variables a, b, c, where $A = \{a, b, c\}$.

- **For $P_1(A)$ (degree $k = 1$):** The sub-collections of size one are $\{a\}$, $\{b\}$, $\{c\}$. The sum of their products is $P_1(A) = a + b + c$.
- **For $P_2(A)$ (degree $k = 2$):** The sub-collections of size two are $\{a, b\}$, $\{a, c\}$, $\{b, c\}$. The sum of their products is $P_2(A) = ab + ac + bc$.
- **For $P_3(A)$ (degree $k = 3$):** The only sub-collection of size three is $\{a, b, c\}$. The product is $P_3(A) = abc$.
- **For $P_4(A)$ (degree $k = 4$):** It is impossible to choose four distinct variables from a collection of three, so $P_4(A) = 0$. In general, $P_k(A) = 0$ if k is greater than the number of variables in A.

You should see the crucial connection immediately. For the variables $\{a, b, c\}$, the formal $P_1(A)$ is identical to our shorthand Σa, and $P_2(A)$ is identical to Σab. This new, formal notation is what we will use for precision in advanced problems.

2. Now consider a collection of four variables, $B = \{w, x, y, z\}$. Let's find $P_2(B)$.

- We need to list all possible pairs of variables. Systematically: start with w and pair it with the others (wx, wy, wz), then move to x and pair it with the remaining ones (xy, xz), and finally pair y with what's left (yz).

- The sum of these products is:

$$P_2(B) = wx + wy + wz + xy + xz + yz.$$

3. Let the variables be the first five positive integers, $C = \{1, 2, 3, 4, 5\}$. Find the numerical value of $P_1(C)$ and $P_5(C)$.

- $P_1(C)$ is the sum of all variables taken one at a time:

$$P_1(C) = 1 + 2 + 3 + 4 + 5 = 15.$$

- $P_5(C)$ is the product of all variables taken five at a time. There is only one way to do this:

$$P_5(C) = 1 \times 2 \times 3 \times 4 \times 5 = 120.$$

Remark. The definition of $P_k(A)$ is a formal restatement of how the coefficients are built in the expansion of n linear factors from Equation 5.10.

$$\prod_{i=1}^{n}(x + a_i) = x^n + P_1(A)x^{n-1} + P_2(A)x^{n-2} + \cdots + P_n(A).$$

5.5 Exercises

Part I: Direct Expansion

Remark. These are for warming up. Focus on applying the Theorem 5.1.1 directly and accurately. Don't rush.

1. Expand the following products. Before you begin, state how many terms the expansion will have before any like terms are collected.

(a) $(x + 2)(y + z)$
(b) $(a - 4)(b - c)$
(c) $(p + q)(p - q + r)$
(d) $(x^2 + x + 1)(y - 1)$
(e) $(a + b - c)(d - e)$
(f) $(2x + 3y)(x - y + z)$

2. Expand the following products of three factors.

(a) $(x + 1)(x + 2)(x + 3)$
(b) $(a - b)(c - d)(e - f)$
(c) $(x + y)(x - y)(x + y)$
(d) $(2a + b)(a - 2b)(a + b)$

3. How many terms will the expansion of $(a_1 + a_2)(b_1 + b_2 + b_3)(c_1 + c_2 + c_3 + c_4)(d_1 + d_2)$ contain, before any terms are collected?

4. Find the product of $(x^2 - xy + y^2)$ and $(x + y)$. What does this remind you of?

5. Find the product of $(x^2 + xy + y^2)$ and $(x - y)$.

6. Expand $(a + b + c)(a + b - c)$. Can you do this by grouping terms to make it faster?

Part II: Using the Fundamental Identities

7. Use the perfect square and difference of squares identities to expand:

(a) $(3x + 4)^2$
(b) $(2y - 5z)^2$
(c) $(a^2 + b^2)^2$
(d) $(7p + 2q)(7p - 2q)$
(e) $(\frac{1}{2}x - \frac{1}{3}y)^2$
(f) $(xy + yz)(xy - yz)$

8. Use the cubic identities to expand:

(a) $(x + 2)^3$
(b) $(2a - b)^3$
(c) $(x^2 + 1)^3$
(d) $(3p - 2q)^3$

9. Use the principle of substitution to expand the following. Clearly state what you are substituting for 'a' and 'b' in the standard identities.

(a) $((x + y) + z)^2$
(b) $((a - b) - c)^2$
(c) $((2x + y) - (x - y))^2$
(d) $(x^m + y^n)^2$
(e) $((a + b) + (c + d))^2$
(f) $(a^2 + b^2 - ab)(a^2 + b^2 + ab)$

10. Expand and simplify the following expressions.

(a) $(x + y)^2 + (x - y)^2$
(b) $(x + y)^2 - (x - y)^2$
(c) $(a + b + c)^2 - (a + b - c)^2$
(d) $(m + n)^3 - (m - n)^3$

11. Expand $(a + b + c + d)^2$ by grouping it as $((a + b) + (c + d))^2$.

12. Expand $(x + y - z - w)(x - y - z + w)$.

Part III: The Summation Symbol

13. Find the numerical values of the following sums:

(a)
$$\sum_{k=1}^{4} k.$$

(b)
$$\sum_{n=0}^{5} 2^{n-2}.$$

(c)
$$\sum_{r=0}^{3} 2^{r+1}.$$

(d)
$$\sum_{n=1}^{4} n^n.$$

(e)
$$\sum_{i=0}^{5}(2i+1)$$

(f)
$$\sum_{k=1}^{6} \frac{1}{k(k+1)}.$$

Remark. $\frac{1}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$.

Part IV: The Product Symbol

Remark. The product symbol, behaves similarly to its cousin Σ, but its rules are based on multiplication, not addition.

14. Find the numerical values of the following products by writing them out.

(a)
$$\prod_{k=1}^{4} k. \quad \text{(This is also written as 4!, "4 factorial".)}$$

(b)
$$\prod_{k=1}^{5}(k-3). \quad \text{(Be careful!)}$$

(c)
$$\prod_{i=1}^{n} c, \text{ where } c \text{ is a constant.}$$

(d)
$$\prod_{j=2}^{5} \frac{j}{j-1}.$$

15. Establish the following fundamental properties of the product notation:

(a)
$$\prod_{k=1}^{n}(a_k b_k) = \left(\prod_{k=1}^{n} a_k\right)\left(\prod_{k=1}^{n} b_k\right). \quad \text{(Multiplicative Property)}$$

(b)
$$\prod_{k=1}^{n}(ca_k) = c^n \prod_{k=1}^{n} a_k. \quad \text{(Power Property)}$$

Remark. Note the crucial difference from the summation property. Why does the constant become c^n instead of just c?

(c)
$$\prod_{k=1}^{n} \frac{a_k}{a_{k-1}} = \frac{a_n}{a_0}, \quad \text{provided } a_k \neq 0 \text{ for all } k. \quad \text{(Telescoping Product)}$$

Remark. Write out the first few terms of the product to see how the cancellation occurs. It is the multiplicative analogue of the telescoping sum.

16. ⋆ Use the properties you just proved to establish the following identities for the product of the first n even and odd integers.

(a) First, prove that the product of the first n even integers is $\prod_{k=1}^{n}(2k) = 2^n n!$.

(b) The product of all integers up to $2n$ is $(2n)!$. This product can be separated into the product of its even parts and its odd parts:
$$(2n)! = \left(\prod_{k=1}^{n}(2k)\right)\left(\prod_{k=1}^{n}(2k-1)\right).$$
Using this fact and the result from part (a), prove that the product of the first n odd integers is:
$$\prod_{k=1}^{n}(2k-1) = \frac{(2n)!}{2^n n!}.$$

Part V: Properties of Polynomials

17. For each polynomial, state its degree.

(a) $3x^4 - 5x^2 + 2x - 10$

(b) $a^2b^3 + 3a^4b - 7b^5 + a^2b^2$

(c) $p^7 + 2p^3q^5 - 4q^3$

18. Consider the polynomials $P(x) = 3x^3 - 2x^2 + x - 5$ and $Q(x) = 2x^2 + 4x - 1$. Without finding the full product $P(x)Q(x)$, determine:

(a) The degree of the product.

(b) The term of highest degree in the product.

(c) The term of lowest degree (the constant term) in the product.

19. Repeat the previous question for the product of three polynomials: $A(z) = z^4+2z$, $B(z) = -z^5+z^2-3$, $C(z) = 2z^3 + 1$.

20. Use the sum of coefficients check for the following expansions. State whether the expansion is possibly correct or certainly incorrect.

(a) $(x - y + 1)^2 = x^2 + y^2 + 1 - 2xy + 2x - 2y$

(b) $(a - 2b)^3 = a^3 - 6a^2b + 12ab^2 - 8b^3$

(c) $(x + y)(x - y + 1) = x^2 - y^2 + x + y$

(d) $(2a - b - c)^2 = 4a^2 + b^2 + c^2 - 4ab - 4ac + 2bc$

21. Find the sum of the coefficients of the expansion of $(x^3 - 3x + 2)^4$.

Part VI: Deriving Summation Formulae

Remark. Use the properties from the previous part whenever possible to derive these classic and essential formulae.

3. Prove that

$$\sum_{i=1}^{j} 1 = n.$$

4. Prove that

$$\sum_{k=1}^{n} (2k-1) = n^2.$$

Remark. Use the identity $2k - 1 = k^2 - (k-1)^2$ and the telescoping property.

5. Prove that

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Remark. Use the results from the previous two problems.

6. Prove that

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}..$$

Remark. Sum the identity $k^3 - (k-1)^3 = 3k^2 - 3k + 1$ from $k = 1$ to n.

7. Prove the formula for a geometric series: if $x \neq 1$, then

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

Remark. Let $S = \sum_{k=0}^{n} x^k$. Now expand $S - xS$ and see what happens.

Part VII: The Product of n Linear Factors and Coefficient Hunting

12. Let $P(x) = (x-1)(x+2)(x-3)(x+4)$. Write the coefficients of x^3, x^2, and x as sums (P_1, P_2, P_3), and then compute their values to expand $P(x)$.

13. Consider the polynomial

$$P(x) = \prod_{k=1}^{5} (x-k) = (x-1)(x-2)(x-3)(x-4)(x-5).$$

Without expanding the entire polynomial, find the coefficient of x^4 and x^3.

14. Let $P(x) = \prod_{i=1}^{7} (x + a_i)$, where the constants $a_1, \ldots, a_7$ are the numbers $-3, -2, -1, 1, 2, 3, 4$.

(a) Find the coefficient of x^6.

(b) Find the constant term.

15. Let the polynomial be $P(x) = (x-1)(x+2)(x-4)(x+8)(x-16)$. Find the coefficient of x^3.

16. Let $P(x) = \prod_{k=1}^{n} (x-k)$. What is the sign of the constant term? Express your answer in terms of n.

Part VIII: Properties of Symmetric Polynomials

17. For n variables $a_1, \ldots, a_n$, prove the identity:

$$\left(\sum_{i=1}^{n} a_i \right)^2 = \sum_{i=1}^{n} a_i^2 + 2 \sum_{1 \leq i < j \leq n} a_i a_j.$$

Remark. Try it with $(x+y)(x+y)$, and $(x+y+z)(x+y+z)$ notice the pattern and generalise it using distributive property.

18. Let $P(x) = \prod_{i=1}^{n}(x - a_i) = x^n - P_1x^{n-1} + P_2x^{n-2} - \cdots + (-1)^nP_n$.

(a) Find the expansion for $P(-x)$ in terms of x and the coefficients P_k.

(b) Let $Q(x) = \prod_{i=1}^{n}(x + a_i)$. How do the coefficients of $Q(x)$ relate to the coefficients, P_k, of the original polynomial $P(x)$?

19. ⋆ Prove the Brahmagupta-Fibonacci identity: for any four numbers a, b, c, d:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

This shows that the product of two sums of two squares is itself a sum of two squares. Prove this by direct, brutal expansion of both sides.

20. ⋆ Consider the expression $E = (a+b+c)(a+b-c)(a-b+c)(-a+b+c)$.

(a) Expand this product.

(b) Show that the result is symmetric in a, b, c, and can be written as $2(a^2b^2+b^2c^2+c^2a^2)-(a^4+b^4+c^4)$, or more compactly as $2\Sigma a^2b^2 - \Sigma a^4$.

21. ⋆ **Part I: Combining Factors.** This problem is the first step in discovering a powerful rule for expanding polynomials. Let us consider two separate products: $P_A = (x+a_1)$ and $P_B = (x+b_1)(x+b_2)$.

(a) Expand P_A and P_B separately, what are $P_1(B)$ and $P_2(B)$ in terms of b_1 and b_2?

(b) Now form the combined product, $P_{AB} = P_A \cdot P_B = (x + a_1)(x + b_1)(x + b_2)$. Expand this full product.

(c) Now look at your final expansion from part (b). Show by direct substitution that the coefficient of x^1 in the final product P_{AB} is equal to $a_1P_1(B) + P_2(B)$.

Remark. This may seem obscure, but you have just verified a single case of a deep and elegant theorem that we will prove fully in a later chapter.

22. ⋆ **Newton's Identities.** Let us define the power sums

$$s_k = \sum_{i=1}^{n} a_i^k = a_1^k + a_2^k + \cdots + a_n^k.$$

These are symmetric, just like the elementary symmetric polynomials P_k. For example, for variables a, b, c ($n = 3$):

- $s_1 = a + b + c = P_1$
- $s_2 = a^2 + b^2 + c^2$
- $P_2 = ab + bc + ca$

Notice that while $s_1 = P_1$, s_2 is different from P_2. However, they are deeply connected. These exercises guide you to discover and prove the remarkable relations between them, known as Newton's Identities.

(a) **The First Two Identities by Expansion.**

i. The first identity is the simplest. Just note by i guess observation of their definitions that for any number of variables, $s_1 = P_1$.

ii. Prove the second identity:

$$s_2 = P_1s_1 - 2P_2$$

Remark. If you'd like to prove it the long way use the result from question 17, to solve this.

(b) **A New Method for the Third Identity.** Proving the next identities by direct expansion becomes very difficult. We need a more clever approach.

i. For three variables a, b, c, prove the next relation by expanding the Right Hand Side (RHS) and showing it equals the Left Hand Side (LHS): >

$$s_3 = P_1 s_2 - P_2 s_1 + 3P_3.$$

ii. Consider the polynomial defined by the product $F(t) = (t-a)(t-b)(t-c)$, which we know expands to $t^3 - P_1 t^2 + P_2 t - P_3$.

- The structure of the product $F(t)$ ensures that if we substitute a, b, or c for t, the result is zero. For example, $F(a) = (a-a)(a-b)(a-c) = 0$. Write out the expanded form of the three equations $F(a) = 0$, $F(b) = 0$, and $F(c) = 0$.
- By summing these three equations, $F(a) + F(b) + F(c) = 0$, and collecting terms, derive the third Newton's Identity:

$$s_3 = P_1 s_2 - P_2 s_1 + 3P_3.$$

(c) **Generalising the Method.** The elegant method from part (b) can be generalised to find a relationship between the power sums for any number of variables. We again consider n variables $a_1, \ldots, a_n$ and the polynomial

$$F(t) = \prod_{i=1}^{n}(t - a_i) = t^n - P_1 t^{n-1} + P_2 t^{n-2} - \cdots + (-1)^n P_n.$$

i. The starting point is the same: for any variable a_j from our collection, $F(a_j) = 0$. Writing this out using the expansion of $F(t)$ gives:

$$a_j^n - P_1 a_j^{n-1} + P_2 a_j^{n-2} - \cdots + (-1)^n P_n = 0.$$

ii. To generate a relation involving s_k for $k > n$, multiply this entire equation by a_j^{k-n}. Show that this transforms the equation into:

$$a_j^k - P_1 a_j^{k-1} + P_2 a_j^{k-2} - \cdots + (-1)^n P_n a_j^{k-n} = 0.$$

iii. This equation is true for each of the n variables. Our goal is to combine these n separate equations into a single equation relating the sums of their powers. We do this by summing them all together.

a. First, apply the summation operator $\sum_{j=1}^{n}$ to the entire equation from part (ii).

b. In each term of the equation you got from the problem above, the coefficients P_m are constants with respect to the summation index j. Use the homogeneous property of summation to factor these coefficients out of their respective sums.

c. Recognize that each remaining summation is, by definition, a power sum and thus finally derive the general recurrence relation, which holds for all $k > n$:

$$s_k - P_1 s_{k-1} + P_2 s_{k-2} - \cdots + (-1)^n P_n s_{k-n} = 0.$$

(d) **Application.** The numbers $1, 2, 3$ are the roots of the polynomial equation $F(t) = t^3 - 6t^2 + 11t - 6 = 0$.

i. By comparing $F(t)$ to the general form $t^3 - P_1 t^2 + P_2 t - P_3$, state the numerical values of P_1, P_2, P_3 for the set of variables $\{1, 2, 3\}$.

ii. Use the identities you proved in parts (a) and (b) to calculate the values of the power sums s_1, s_2, s_3.

iii. Check your answers by calculating $s_1 = 1 + 2 + 3$, $s_2 = 1^2 + 2^2 + 3^2$, and $s_3 = 1^3 + 2^3 + 3^3$ directly.

iv. The power sum s_4 involves a power $k = 4$, which is greater than $n = 3$. Use the general recurrence relation you proved in part (c) to predict the value of $s_4 = 1^4 + 2^4 + 3^4$.

Chapter 6

Set Theory and Counting

Throughout the previous chapters, we have constructed arguments and proofs using plain English, supplemented with algebraic symbols. This approach relies on our shared understanding of the meaning of words like "and", "or", "if...then", and "for any". While this is often sufficient, mathematics strives for a level of precision that everyday language can sometimes lack. To build more complex and certain arguments, we must first formalise the language we use to reason.

Remark. You will see that we have been using these ideas of logic and sets all along; we are now simply giving them names and symbols to make our reasoning sharper, clearer, and more powerful.

6.1 Logic: The Language of Reasoning

At the heart of any mathematical argument is the *proposition*, a statement that can be definitively judged as either true (**T**) or false (**F**).

6.1.1 Propositions and Logical Connectives

We combine simple propositions to form more complex ones using logical connectives. The precise meaning of these connectives is defined by a truth table, which shows the truth value of the combined statement for all possible truth values of its components. Let P and Q be propositions.

P	Q	$P \wedge Q$ (and)	$P \vee Q$ (or)	$\neg P$ (not)	$P \implies Q$ (if...then)	$P \iff Q$ (if and only if)
T	**T**	**T**	**T**	**F**	**T**	**T**
T	**F**	**F**	**T**	**F**	**F**	**F**
F	**T**	**F**	**T**	**T**	**T**	**F**
F	**F**	**F**	**F**	**T**	**T**	**T**

The connectives for conjunction ($P \wedge Q$, "P and Q"), disjunction ($P \vee Q$, "P or Q"), and negation ($\neg P$, "not P") behave as their English names suggest. The most important, and sometimes surprising, is the material implication ($P \implies Q$, "if P then Q").

A statement $P \implies Q$ is only false when a true hypothesis P leads to a false conclusion Q. If the hypothesis P is false, the implication makes no claim about Q, and so the statement as a whole is considered true.

Example 6.1.1. Consider the promise, "If you tidy your room, then you will get ice cream." Let P be 'you tidy your room' and Q be 'you get ice cream'. The promise is only broken if you tidy your room (P is true) but you do not get ice cream (Q is false). If you do not tidy your room (P is false), the promise remains unbroken whether you get ice cream or not.

Finally, the biconditional ($P \iff Q$, read "P if and only if Q") is true precisely when P and Q have the same truth value. The statement $P \iff Q$ is logically equivalent to proving the implication in both directions: $(P \implies Q) \wedge (Q \implies P)$. This is why proving an "if and only if" statement requires two distinct steps: proving the "if" part $(Q \implies P)$ and the "only if" part $(P \implies Q)$.

6.1.2 Quantifiers

Many mathematical statements apply to entire classes of objects. To express these ideas precisely, we use quantifiers.

- The **universal quantifier** $\forall x$ is read "for all x" or "for every x".
- The **existential quantifier** $\exists x$ is read "there exists an x".

Using this notation, the additive inverse axiom (3.4.1) can be written with full precision:

$$(\forall a \in \mathbb{Z})(\exists (-a) \in \mathbb{Z}) \text{ such that } a + (-a) = 0.$$

This reads, "For every integer a, there exists an integer $(-a)$ such that their sum is zero."

Negating a quantified statement follows specific rules. The negation of "all things have property P" is not "no things have property P", but rather "at least one thing does not have property P". Symbolically:

$$\neg(\forall x, P(x)) \iff \exists x, \neg P(x)$$
$$\neg(\exists x, P(x)) \iff \forall x, \neg P(x)$$

To disprove a universal claim, you need only find one instance where it fails (a counterexample).

6.2 Sets: The Idea of a Collection

The most basic organisational tool in mathematics is the set. With a system of logical notation under our belt, we can define this concept with greater precision.

Definition 6.2.1. ***(Set, Element, Membership)***. A *set* is a collection of distinct objects, viewed as a single entity. The objects in the collection are called the elements or members of the set. To avoid certain logical paradoxes, we assume all our sets are collections of objects from some large, pre-defined **universal set**, denoted $\mathcal{U}$. If A is a set and x is an object, we write $x \in A$ when x is an element of A, and $x \notin A$ when it is not.

6.2.1 Specifying Sets

We can describe a set in several ways.

- **Roster Form.** We can simply list the elements in curly braces: $\{1, 2, 3\}$. The order of elements does not matter, and duplicates are ignored, so $\{1, 2, 3\}$ is the same set as $\{3, 1, 2, 1\}$.
- **Implied Lists.** For large or infinite sets, we use an ellipsis $(\dots)$ to imply a pattern, such as the set of the first 100 square numbers, $\{1, 4, 9, \dots, 10000\}$, or the natural numbers, $\mathbb{N} = \{1, 2, 3, \dots\}$.
- **Set-Builder Notation.** The most precise method defines a set by a property its elements must satisfy. The notation $\{x \in A \mid P(x)\}$ is read as "the set of all x in set A such that the proposition $P(x)$ is true".

Example 6.2.1. Let our universal set be the integers, $\mathbb{Z}$.

- The set of all even integers can be written as $\{n \in \mathbb{Z} \mid n \text{ is even}\}$.

- An alternative form specifies the structure of the elements directly: $\{2k \mid k \in \mathbb{Z}\}$. This is read as "the set of all numbers of the form $2k$, where k is an integer".
- The set $\{n \in \mathbb{Z} \mid -2 \leq n < 3\}$ is $\{-2, -1, 0, 1, 2\}$ in roster form.

Definition 6.2.2. ***(Empty Set)***. The set with no elements is called the empty set, denoted by $\emptyset$. Its defining property is that no object is an element of it. Symbolically, this is expressed as $\forall x, x \notin \emptyset$

6.2.2 Subsets and Equality

Definition 6.2.3. ***(Subset)***. A set A is a subset of a set B, written $A \subseteq B$, if every element of A is also an element of B. Formally, $A \subseteq B \iff \forall x, (x \in A \implies x \in B)$. If $A \subseteq B$ but $A \neq B$, we call A a **proper subset** of B and write $A \subsetneq B$.

Remark. To prove $A \subseteq B$, the standard method is to take an arbitrary element $x \in A$ and, using only the properties of A, demonstrate that x must also be an element of B.

***Theorem* 6.2.1.** The empty set is a subset of every set. That is, for any set A, it is true that $\emptyset \subseteq A$.

Proof. To prove $\emptyset \subseteq A$, we must satisfy the formal definition of a subset, which is the proposition $\forall x, (x \in \emptyset \implies x \in A)$.
Consider the implication within the universal statement: $x \in \emptyset \implies x \in A$. The hypothesis, $x \in \emptyset$, is false for any object x by the very definition of the empty set. By our truth table, an implication with a false hypothesis is always true, regardless of the truth of the conclusion.
Since the implication holds true for any choice of x, the universal statement is true. Therefore, $\emptyset \subseteq A$. ■

Remark. For any proposition $P(x)$, the statement $\forall x, (x \in \emptyset \implies P(x))$ is true.

Note. Such a statement, which is true only because the condition of its hypothesis can never be met, is called vacuously true.

Definition 6.2.4. ***(Set Equality)***. Two sets A and B are equal, written $A = B$, if and only if they have exactly the same elements. This is equivalent to showing that $A \subseteq B$ and $B \subseteq A$.

Remark. This two-part proof strategy, showing $A \subseteq B$ and $B \subseteq A$ separately, is called proof by double containment.

6.2.3 The Power Set

Definition 6.2.5. ***(Power Set)***. The power set of a set A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.

Example 6.2.2. Let $A = \{1, 2\}$. The subsets of A are $\emptyset, \{1\}, \{2\}, \{1, 2\}$. The power set is therefore $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

Note. Be careful to distinguish between membership ($\in$) and subsethood ($\subseteq$). For the set $A = \{1, 2\}$, we have $\{1\} \subseteq A$ but $\{1\} \in \mathcal{P}(A)$.

6.3 Operations on Sets

We can combine sets to form new ones using several fundamental operations. Let A and B be subsets of some universe $\mathcal{U}$.

Definition 6.3.1. ***(Union, Intersection, Difference, Complement)***.

$$A \cup B \coloneqq \{x \in \mathcal{U} \mid x \in A \vee x \in B\} \quad \text{(Union)}$$
$$A \cap B \coloneqq \{x \in \mathcal{U} \mid x \in A \wedge x \in B\} \quad \text{(Intersection)}$$
$$A \setminus B \coloneqq \{x \in \mathcal{U} \mid x \in A \wedge x \notin B\} \quad \text{(Difference)}$$
$$A^c \coloneqq \mathcal{U} \setminus A = \{x \in \mathcal{U} \mid x \notin A\} \quad \text{(Complement)}$$

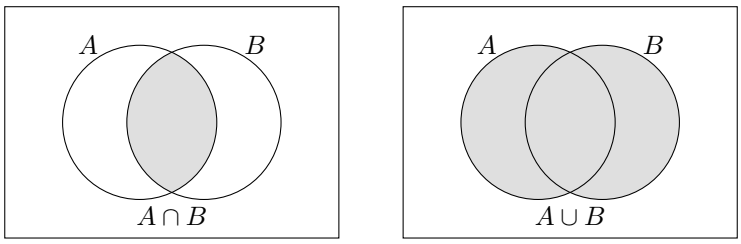


Figure 6.1: The intersection and union of two sets.

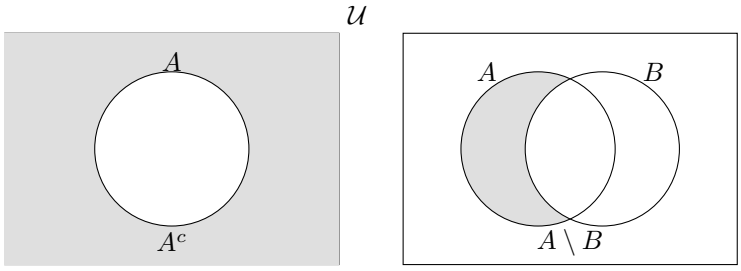


Figure 6.2: The complement of a set A and the difference $A \setminus B$.

If $A \cap B = \emptyset$, the sets are said to be **disjoint**. These operations are illustrated in Figure 6.1 and Figure 6.2.

Definition 6.3.2. ***(Cartesian Product)***. The Cartesian product of two sets A and B, denoted $A \times B$, is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$.

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

Example 6.3.1. If $A = \{1, 2\}$ and $B = \{H, T\}$, their Cartesian product is

$$A \times B = \{(1, H), (1, T), (2, H), (2, T)\}.$$

The set $\mathbb{R} \times \mathbb{R}$, often written $\mathbb{R}^2$, is the set of all coordinates in the Cartesian plane.

6.4 Reasoning with Sets and Logic

The definitions of set operations reveal a deep connection to the connectives of logic. A statement about an element's membership in a set is a logical proposition, and the rules governing sets are direct parallels of the rules governing logic.

Set Notation		Logical Equivalent
$x \in A \cap B$	$\iff$	$(x \in A) \wedge (x \in B)$
$x \in A \cup B$	$\iff$	$(x \in A) \vee (x \in B)$
$x \in A^c$	$\iff$	$\neg(x \in A)$
$A \subseteq B$	$\iff$	$\forall x, (x \in A \implies x \in B)$

This correspondence allows us to prove general laws about sets by manipulating logical symbols.

***Theorem* 6.4.1. (Laws of Set Operations)**. For any sets A, B, C that are subsets of a universe $\mathcal{U}$:

(i) **Commutative Laws:** $A \cup B = B \cup A$ and $A \cap B = B \cap A$.

(ii) **Associative Laws:** $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$.

(iii) **Distributive Laws:** $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

(iv) **De Morgan's Laws:** $(A \cup B)^c = A^c \cap B^c$ and $(A \cap B)^c = A^c \cup B^c$.

Proof. We prove the first of De Morgan's Laws. To show $(A \cup B)^c = A^c \cap B^c$, we use double containment.

($\subseteq$) Let $x \in (A \cup B)^c$. By definition of complement, this means $x \notin (A \cup B)$. This is equivalent to $\neg(x \in A \cup B)$. By definition of union, this is $\neg((x \in A) \vee (x \in B))$. By De Morgan's law for logic, this is equivalent to $(\neg(x \in A)) \wedge (\neg(x \in B))$. This means $(x \notin A) \wedge (x \notin B)$, which is the same as $(x \in A^c) \wedge (x \in B^c)$. Finally, by definition of intersection, this means $x \in A^c \cap B^c$.

($\supseteq$) To prove the reverse containment, $A^c \cap B^c \subseteq (A \cup B)^c$, one simply reverses each step of the argument above, as each step was an equivalence ($\iff$).

Since the membership conditions for the two sets are logically equivalent, the sets must be equal. The other laws are proven using similar arguments. ■

This equivalence can also be proven geometrically using Venn diagrams, as shown in Figure 6.3, which demonstrates that the region for $(A \cup B)^c$ is identical to the region for $A^c \cap B^c$.

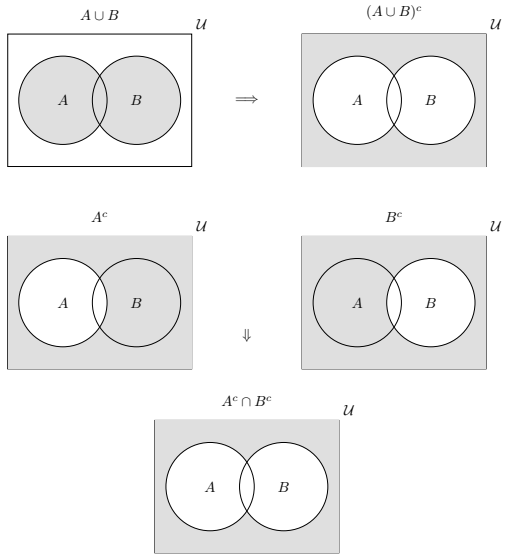


Figure 6.3: A geometric proof of De Morgan's law. The top row shows the construction of $(A \cup B)^c$. The middle row shows the individual complements, A^c and B^c. The bottom diagram shows their intersection, which is identical to the final diagram in the top row.

6.5 A Review of Proof Strategies

A mathematical proof is a sequence of logical deductions starting from axioms that establishes the truth of a statement. The proofs in this book follow these formal patterns.

1. **Direct Proof:** To prove $P \implies Q$, we assume P is true and construct a chain of logical steps that concludes with Q.
2. **Proof by Cases:** We partition a problem into exhaustive cases and prove the claim for each one.

   Example 6.5.1. For any integer n, either n is even or $n+1$ is even. In either case, their product $n(n+1)$ must contain a factor of 2 and is therefore even.
3. **Proof by Contrapositive:** To prove $P \implies Q$, it is sometimes easier to prove its logical equivalent: $\neg Q \implies \neg P$.

Example 6.5.2. To prove "if n^2 is even, then n is even", we can prove the contrapositive: "if n is odd, then n^2 is odd". If $n = 2k + 1$, then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd.

4. **Proof by Contradiction:** To prove a statement P, we assume its negation $\neg P$ is true and show this leads to a logical impossibility. The proof that $\sqrt{2}$ is irrational is a classic example.

5. **Counterexample:** To disprove a universal claim $(\forall x)P(x)$, we need only produce a single instance of an x for which $P(x)$ is false.

   Example 6.5.3. Claim: $(\forall n \in \mathbb{N}), n^2 > n$.
   Counterexample: take $n = 1$. Then $1^2 = 1 \not> 1$, so the universal claim is false.

6.6 The Principle of Mathematical Induction

The set of natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$ has a unique structure: it starts at a definite point (0) and proceeds in discrete steps, one after the other. This step-by-step nature allows for a powerful method of proof called mathematical induction.

Imagine an infinitely long line of dominoes, one for each natural number. To ensure they all fall, we need to do two things:

1. Push over the first domino (domino 0).
2. Ensure that the dominoes are arranged such that each one, upon falling, will knock over the next one.

If both conditions are met, the entire chain reaction is guaranteed. This is the essence of induction.

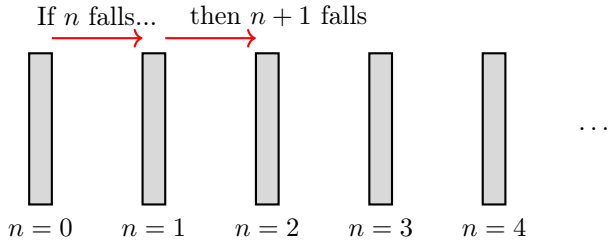


Figure 6.4: The domino analogy for induction.

***Theorem* 6.6.1. (The Principle of Weak Induction).** Let $P(n)$ be a statement concerning a natural number n, and let $b \in \mathbb{N}$ be a starting value. If

(i) $P(b)$ is true, and

(ii) for all $n \geq b$, the implication $P(n) \implies P(n + 1)$ is true,

then $P(n)$ is true for all natural numbers $n \geq b$.

Remark. This principle is taken as a fundamental axiom of the natural numbers. It is the formal rule that captures their step-by-step character.

To prove a statement using induction, we must perform two distinct tasks.

The Method of Proof by Induction

To prove that a statement $P(n)$ is true for all natural numbers $n \geq b$:

- **Base Case (BC):** Prove that the statement $P(b)$ is true.
- **Inductive Step (IS):** Assume that $P(n)$ is true for some arbitrary but fixed integer $n \geq b$. This assumption is called the **induction hypothesis (IH)**. Using this assumption, prove that $P(n+1)$ must also be true.

Example 6.6.1. Prove that for all $n \in \mathbb{N}$, the sum of the first n non-negative integers is given by the formula $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$. Let $P(n)$ be the statement "$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$". We are proving this for all $n \geq 0$, so our base case is $b = 0$.

- **(BC)** We must show $P(0)$ is true. The statement $P(0)$ asserts that $\sum_{i=0}^{0} i = \frac{0(0+1)}{2}$. The left side is simply 0. The right side is $\frac{0\times 1}{2} = 0$. Since $0 = 0$, the base case holds.
- **(IS)** Let $n \geq 0$ be an integer and assume $P(n)$ is true. This means we assume:

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2} \quad \text{(IH)}$$

Our goal is to use this fact to prove that $P(n+1)$ is true. The statement $P(n+1)$ is:

$$\sum_{i=0}^{n+1} i = \frac{(n+1)((n+1)+1)}{2} = \frac{(n+1)(n+2)}{2}$$

We start with the left side of our goal and use the (IH) to simplify it.

$$\begin{aligned}
\sum_{i=0}^{n+1} i &= \left(\sum_{i=0}^{n} i\right) + (n+1) && \text{By definition of summation} \\
&= \frac{n(n+1)}{2} + (n+1) && \text{By the Induction Hypothesis (IH)} \\
&= (n+1)\left(\frac{n}{2} + 1\right) && \text{Factor out } (n+1) \\
&= (n+1)\left(\frac{n}{2} + \frac{2}{2}\right) && \text{Create a common denominator} \\
&= (n+1)\left(\frac{n+2}{2}\right) \\
&= \frac{(n+1)(n+2)}{2}
\end{aligned}$$

This is exactly the right-hand side of $P(n+1)$. Thus, we have shown that $P(n) \implies P(n+1)$.

By the principle of induction, the formula is true for all $n \geq 0$.

Example 6.6.2. Prove that for all $n \in \mathbb{N}$, the number $n^3 - n$ is divisible by 3. Let $P(n)$ be the statement "$n^3 - n$ is divisible by 3". We use $b = 0$.

- **(BC)** For $n = 0$, we have $0^3 - 0 = 0$. Since $0 = 3 \times 0$, it is divisible by 3. The base case holds.
- **(IS)** Assume $P(n)$ is true for some $n \geq 0$. This means $n^3 - n = 3k$ for some integer k (IH). We want

to prove that $(n+1)^3 - (n+1)$ is also divisible by 3.

$$\begin{aligned}
(n+1)^3 - (n+1) &= (n^3 + 3n^2 + 3n + 1) - (n+1) && \text{Expand the cube} \\
&= n^3 + 3n^2 + 2n \\
&= (n^3 - n) + (3n^2 + 3n) && \text{Rearrange to use the (IH)} \\
&= 3k + 3(n^2 + n) && \text{By (IH) and factorisation} \\
&= 3(k + n^2 + n)
\end{aligned}$$

Since $k + n^2 + n$ is an integer, we have shown that $(n+1)^3 - (n+1)$ is a multiple of 3. Thus $P(n) \implies P(n+1)$.

By induction, the statement is true for all $n \in \mathbb{N}$.

6.6.1 Inductive Proofs of Algebraic Formulae

Many of the algebraic laws and summation formulae we have already established can be proven with rigour using induction. This method provides a formal check on our reasoning and is particularly suited to statements defined recursively, such as indexed sums and products.

Formulae for Sums

***Theorem* 6.6.2. (Linearity of Finite Sums)**. For any constant c and sequences a_i, b_i,

$$\sum_{i=1}^{n}(a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i, \qquad \sum_{i=1}^{n} ca_i = c\sum_{i=1}^{n} a_i \qquad (\text{for } n \in \mathbb{N}).$$

Proof. We prove the first identity.

- ***(BC)** For $n = 0$, the sums are empty and defined to be 0. So $0 = 0 + 0$, which is true.*
- ***(IS)** Assume the claim holds for n. Then*

$$\begin{aligned}
\sum_{i=1}^{n+1}(a_i + b_i) &= \left(\sum_{i=1}^{n}(a_i + b_i)\right) + (a_{n+1} + b_{n+1}) && \textit{by definition of sum} \\
&= \left(\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i\right) + a_{n+1} + b_{n+1} && \textit{by (IH)} \\
&= \left(\sum_{i=1}^{n} a_i + a_{n+1}\right) + \left(\sum_{i=1}^{n} b_i + b_{n+1}\right) && \textit{by associative law} \\
&= \sum_{i=1}^{n+1} a_i + \sum_{i=1}^{n+1} b_i
\end{aligned}$$

The second identity is proven similarly. ■

***Theorem* 6.6.3. (Sum of an Arithmetic Progression)**. For all $n \in \mathbb{N}$,

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}.$$

Proof.

- ***(BC)*** *For $n = 0$: $0 = \frac{0 \cdot 1}{2}$, which is true.*
- ***(IS)*** *Assume $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$. Then*

$$\sum_{k=0}^{n+1} k = \left(\sum_{k=0}^{n} k \right) + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}.$$

■

***Theorem* 6.6.4. (Geometric Series)**. For $x \neq 1$ and $n \in \mathbb{N}$,

$$x^{n+1} - 1 = (x-1) \sum_{k=0}^{n} x^k.$$

Proof.

- ***(BC)*** *For $n = 0$: $x - 1 = (x-1) \sum_{k=0}^{0} x^k = (x-1)x^0 = (x-1) \cdot 1$. True.*
- ***(IS)*** *Assume $x^{n+1} - 1 = (x-1) \sum_{k=0}^{n} x^k$. Consider the next case:*

$$\begin{aligned}
(x-1) \sum_{k=0}^{n+1} x^k &= (x-1) \left(\sum_{k=0}^{n} x^k + x^{n+1} \right) \\
&= (x-1) \sum_{k=0}^{n} x^k + (x-1)x^{n+1} && \text{by distributive law} \\
&= (x^{n+1} - 1) + (x^{n+2} - x^{n+1}) && \text{by (IH) and distribution} \\
&= x^{n+2} - 1
\end{aligned}$$

■

Products, Powers, and Divisibility

***Theorem* 6.6.5. (Law of Indices Revisited)**. For any a, b, $(ab)^n = a^n b^n$ for all $n \in \mathbb{N}$.

Proof.

- ***(BC)*** *For $n = 0$: $(ab)^0 = 1$ and $a^0 b^0 = 1 \cdot 1 = 1$. True.*
- ***(IS)*** *Assume $(ab)^n = a^n b^n$. Then*

$$(ab)^{n+1} = (ab)^n (ab) = (a^n b^n)(ab) = a^n a b^n b = a^{n+1} b^{n+1},$$

by the commutative and associative laws of multiplication.

■

Example 6.6.3. (Divisibility). For all $n \geq 1$, $7^n - 1$ is divisible by 6.

- **(BC)** For $n = 1$: $7^1 - 1 = 6$, which is divisible by 6.

- **(IS)** Assume $7^n - 1$ is divisible by 6. This means $7^n - 1 = 6k$ for some integer k, or $7^n = 6k + 1$. Consider $7^{n+1} - 1$:

$$7^{n+1} - 1 = 7 \cdot 7^n - 1 = 7(6k + 1) - 1 = 42k + 7 - 1 = 42k + 6 = 6(7k + 1).$$

  Since $7k + 1$ is an integer, $7^{n+1} - 1$ is divisible by 6.

Example 6.6.4. (A Basic Inequality). For all $n \in \mathbb{N}$, $2^n \geq n + 1$.

- **(BC)** For $n = 0$: $2^0 = 1$ and $0 + 1 = 1$. Since $1 \geq 1$, it is true.
- **(IS)** Assume $2^n \geq n + 1$ for some $n \geq 0$. We wish to show $2^{n+1} \geq (n + 1) + 1 = n + 2$.

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n && \text{by definition of powers} \\ &\geq 2(n + 1) && \text{by (IH)} \\ &= 2n + 2 = (n + 2) + n \end{aligned}$$

  Since $n \geq 0$, we know $(n + 2) + n \geq n + 2$. Therefore, $2^{n+1} \geq n + 2$.

A Geometric Example

Induction is not limited to algebraic sums. It can prove geometric facts as well.

Example 6.6.5. Prove that for any integer $n \geq 3$, the sum of the interior angles of a convex polygon with n sides is $(n - 2) \times 180°$. Let $P(n)$ be the statement "the sum of interior angles of a convex n-gon is $(n - 2) \times 180°$". Our base case is a triangle, so $b = 3$.

- **(BC)** For $n = 3$, the polygon is a triangle. The sum of its interior angles is known to be 180°. The formula gives $(3 - 2) \times 180° = 180°$. The base case holds.
- **(IS)** Assume for some $n \geq 3$ that the formula holds for any convex n-gon (IH). Now consider a convex polygon with $n + 1$ sides. Let its vertices be $V_1, V_2, \ldots, V_{n+1}$. We can draw a line segment from V_1 to V_n, as in Figure 6.5. This splits the polygon into two smaller shapes: a triangle ($\triangle V_1 V_n V_{n+1}$) and a convex n-gon ($V_1 V_2 \ldots V_n$). The sum of the interior angles of the $(n + 1)$-gon is the sum of the angles

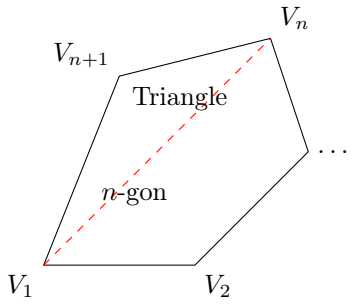


Figure 6.5: Splitting an $(n + 1)$-gon into an n-gon and a triangle.

  in the triangle plus the sum of the angles in the n-gon.

$$\begin{aligned} \text{Sum for } (n+1)\text{-gon} &= (\text{Sum for } n\text{-gon}) + (\text{Sum for triangle}) \\ &= (180° \times (n - 2)) + 180° && \text{By (IH) and base case} \\ &= 180° \times ((n - 2) + 1) && \text{By Distributive property} \\ &= (n - 1) \times 180° \\ &= ((n + 1) - 2) \times 180° \end{aligned}$$

  This is exactly the formula for $P(n + 1)$. Therefore $P(n) \implies P(n + 1)$.

By induction, the formula is true for all polygons with $n \geq 3$ sides.

In fact, some algebraic identities have elegant geometric interpretations that constitute an inductive proof in themselves.

Example 6.6.6. (Sum of Integers). The formula $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ corresponds to counting the dots in a triangular arrangement. As shown in Figure 6.6, two such triangles can be fitted together to form an $n \times (n+1)$ rectangle of dots. The total number of dots is $n(n+1)$, so the number in one triangle is half of this.

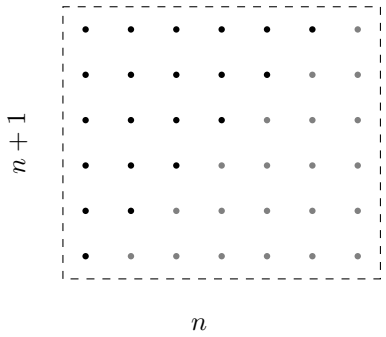


Figure 6.6: Two triangular arrays form an $n \times (n+1)$ rectangle, so $2\sum_{k=1}^{n} k = n(n+1)$.

A Cautionary Tale: The Flawed Induction

A faulty inductive step can lead to absurd conclusions. Consider the following famous 'proof'.

Example 6.6.7. (Fallacious Proof). 'Prove' that all horses are the same colour

Let $P(n)$ be the statement "in any set of n horses, all horses are the same colour".

- **(BC)** For $n = 1$, any set with one horse contains only horses of a single colour. $P(1)$ is true.
- **(IS)** Assume $P(n)$ is true. Consider a set of $n+1$ horses. Remove the first horse; the remaining n horses are all the same colour by the (IH). Now, put the first horse back and remove the last horse. This new set of n horses must also be the same colour. Therefore, the first horse is the same colour as the middle horses, who are the same colour as the last horse. Thus all $n+1$ horses are the same colour.

The logic seems plausible, yet the conclusion is clearly false. The error lies in the inductive step. The argument that the first horse's colour matches the last horse's colour relies on there being 'middle' horses that overlap between the two groups. This works for any set of 3 or more horses. But it fails completely when moving from a set of size $n = 1$ to $n = 2$. In a set of two horses, $\{H_1, H_2\}$, removing one leaves a set of one, and removing the other leaves a different set of one. There is no overlap to transfer the property of 'same colour'. The implication $P(1) \implies P(2)$ is false, and the domino chain breaks before it even begins.

6.6.2 Strong Induction

Sometimes, to prove a statement for $n+1$, we need to know it is true not just for n, but for several preceding values. This requires a seemingly more powerful form of induction.

***Theorem* 6.6.6. (The Principle of Strong Induction)**. Let $P(n)$ be a statement concerning a natural number n, and let $b \in \mathbb{N}$. If

(i) $P(b)$ is true, and

(ii) for all $n \geq b$, if $P(k)$ is true for all k such that $b \leq k \leq n$, then $P(n+1)$ is true,

then $P(n)$ is true for all natural numbers $n \geq b$.

Despite its name, strong induction is logically equivalent to weak induction. The difference lies in the induction hypothesis: we assume the statement holds for *all* previous cases, giving us more information to work with in the inductive step.

Example 6.6.8. Prove that any amount of postage of 12 pence or more can be formed using only 4-pence and 5-pence stamps. Let $P(n)$ be the statement "n pence can be formed using 4p and 5p stamps". We use strong induction with a starting value of $b = 12$.

- **(BC)** The inductive step will require us to look back 4 steps, so we must establish four consecutive base cases.
  - $P(12) : 12 = 3 \times 4$. True.
  - $P(13) : 13 = 2 \times 4 + 1 \times 5$. True.
  - $P(14) : 14 = 1 \times 4 + 2 \times 5$. True.
  - $P(15) : 15 = 3 \times 5$. True.
- **(IS)** Assume for some $n \geq 15$ that $P(k)$ is true for all integers k with $12 \leq k \leq n$ (IH). We must show that $P(n+1)$ is true.

  Consider the amount $n+1$. Our strategy is to use one 4p stamp and then form the remaining amount. The remaining amount is $(n+1)-4 = n-3$. Since we have assumed $n \geq 15$, it follows that $n-3 \geq 12$. Also, $n-3 \leq n$. Thus, the amount $n-3$ is within the range covered by our induction hypothesis.

  By the (IH), $P(n-3)$ is true, which means we can form $n-3$ pence using 4p and 5p stamps. By adding one more 4p stamp to that combination, we successfully form $(n-3)+4 = n+1$ pence. Thus, $P(n+1)$ is true.

By the principle of strong induction, the statement holds for all $n \geq 12$.

Example 6.6.9. Every integer $n > 1$ is either a prime number or can be expressed as a product of prime numbers. Let $P(n)$ be the statement "n is a prime or a product of primes". We use strong induction with base case $b = 2$.

- **(BC)** The number 2 is a prime number. So $P(2)$ is true.
- **(IS)** Assume for some $n \geq 2$ that $P(k)$ is true for all integers k with $2 \leq k \leq n$. This means every integer from 2 to n is either prime or a product of primes (IH). We must show $P(n+1)$ is true. Consider the integer $n+1$. There are two possibilities:
  1. $n+1$ is a prime number. In this case, $P(n+1)$ is true.
  2. $n+1$ is a composite number. By definition, this means $n+1 = a \times b$ for some integers a, b where $1 < a, b < n+1$. This means both a and b fall into the range covered by our induction hypothesis, so $2 \leq a, b \leq n$.

  By the (IH), both a and b must be either prime or a product of primes. Therefore, their product, $a \times b = n+1$, is also a product of primes. In this case also, $P(n+1)$ is true.

Since $P(n+1)$ holds in both cases, by the principle of strong induction, the statement is true for all $n > 1$.

Example 6.6.10. A sequence is defined by $a_0 = 0$, $a_1 = 1$, and $a_n = 3a_{n-1} - 2a_{n-2}$ for all $n \geq 2$. Prove that $a_n = 2^n - 1$ for all $n \in \mathbb{N}$. Here, the formula for a_n depends on two previous terms, so strong induction is a natural choice. Let $P(n)$ be "$a_n = 2^n - 1$".

- **(BC)** We need to check enough base cases to ensure the recurrence is always well-defined. Since the rule for a_n looks back two steps, we should check $n = 0$ and $n = 1$.
  - $P(0) : a_0 = 0$. Formula gives $2^0 - 1 = 1 - 1 = 0$. True.
  - $P(1) : a_1 = 1$. Formula gives $2^1 - 1 = 2 - 1 = 1$. True.
- **(IS)** Assume for some $n \geq 1$ that $P(k)$ is true for all $0 \leq k \leq n$. This means $a_k = 2^k - 1$ for all k in this range (IH). We want to prove $P(n+1)$, which is $a_{n+1} = 2^{n+1} - 1$. Since $n \geq 1$, we have $n+1 \geq 2$, so we can use the recurrence relation for a_{n+1}.

$$\begin{aligned}
a_{n+1} &= 3a_n - 2a_{n-1} && \text{By definition of the sequence} \\
&= 3(2^n - 1) - 2(2^{n-1} - 1) && \text{By (IH), since } n \text{ and } n-1 \text{ are in range} \\
&= 3 \cdot 2^n - 3 - 2 \cdot 2^{n-1} + 2 && \text{Distribute} \\
&= 3 \cdot 2^n - 2^1 \cdot 2^{n-1} - 1 && \text{Combine constants} \\
&= 3 \cdot 2^n - 2^n - 1 && \text{By laws of indices} \\
&= 2 \cdot 2^n - 1 \\
&= 2^{n+1} - 1
\end{aligned}$$

  This is precisely the formula for $P(n+1)$.

By the principle of strong induction, the formula is true for all $n \in \mathbb{N}$.

6.7 Exercises

Part I: Logic and Proof Techniques

1. For each statement below, state its negation in clear English, without simply prefixing "It is not the case that...".

(a) All cats are black.

(b) There exists a prime number that is even.

(c) For every integer x, if x is odd then x^2 is odd.

(d) If it is raining, then I will take my umbrella.

2. Let P be the statement "It is cold" and Q be "It is snowing". Write the following propositions using P, Q and logical connectives.

(a) It is cold and it is snowing.

(b) It is cold, but it is not snowing.

(c) It is not cold, nor is it snowing.

(d) If it is snowing, then it is cold.

3. Construct a truth table for each of the following logical expressions.

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

(b) $(P \implies Q) \iff (\neg P \vee Q)$

(c) $(P \wedge (P \implies Q)) \implies Q$ (This is the rule of *modus ponens*).

4. Prove the following statements about integers using a direct proof.

(a) If a and b are odd integers, then their product ab is odd.

(b) If n is an even integer, then n^2 is divisible by 4.

(c) If $a \mid b$ and $b \mid c$, then $a \mid c$.

5. Prove the following using proof by cases.

(a) For any integer n, the number $n^2 + n$ is always even.

(b) For any integer n, $n^3 - n$ is divisible by 3. (This was proven by induction in the text; prove it here without induction).

6. Prove the following using proof by contrapositive.

(a) For an integer n, if n^2 is odd, then n is odd.

(b) If x and y are two integers whose product is even, then at least one of them must be even.

7. Prove the following using proof by contradiction.

(a) There is no largest integer.

(b) The sum of a rational number and an irrational number is irrational.

Part II: Set Theory

8. Use the roster notation to designate the following sets of real numbers.

(a) $A = \{x \mid x^2 - 1 = 0\}$.

(b) $B = \{x \mid x^3 - x = 0\}$.

(c) $C = \{x \mid x^4 - 1 = 0\}$.

(d) $D = \{x \mid (x-1)^2 = 0\}$.

(e) $E = \{x \mid (x+1)^3 = 0\}$.

(f) $F = \{x \mid x^2 + 1 = 0\}$.

9. For the sets in the previous exercise, list all inclusion relations that hold (e.g. $A \subseteq B$).

10. Let $A = \{1, \{1\}\}$. Discuss the validity of the following statements.

(a) $1 \in A$.

(b) $1 \subseteq A$.

(c) $\{1\} \in A$.

(d) $\{1\} \subseteq A$.

(e) $\{\{1\}\} \subseteq A$.

11. Given the set $S = \{1, 2, 3, 4\}$. Display all 16 subsets of S.

12. Let $A = \{1, 2, 3\}$, $B = \{x \in \mathbb{Z} \mid 0 < x < 4\}$, $C = \{3, 2, 1\}$, and $D = \{1, 2, 2, 3, 3, 3\}$. Discuss the validity of the following statements.

(a) $A = B$.

(b) $A \subseteq C$.

(c) $C \subseteq A$.

(d) $A = C$.

(e) $A = D$.

(f) $B \subseteq D$.

13. Let $A = \{1, 2, 3\}$, $B = \{3, 4, 5\}$ and the universe $\mathcal{U} = \{1, 2, 3, 4, 5, 6, 7\}$. Find the following sets.

(a) $A \cup B$.

(b) $A \cap B$.

(c) $A \setminus B$.

(d) $B \setminus A$.

(e) A^c.

(f) $(A \cup B)^c$.

(g) $A^c \cap B^c$.

14. Let $X = \{a, b\}$. Write out the elements of $\mathcal{P}(X)$ and $X \times X$.

15. Prove the following properties of set equality.

(a) $A = A$.

(b) If $A = B$, then $B = A$.

(c) If $A = B$ and $B = C$, then $A = C$.

16. Prove the following fundamental set relations.

(a) **Commutative Laws:** $A \cup B = B \cup A$, $A \cap B = B \cap A$.

(b) **Associative Laws:** $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$.

(c) **Distributive Laws:** $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

(d) **Identity Laws:** $A \cup \emptyset = A$, $A \cap \mathcal{U} = A$.

(e) **Domination Laws:** $A \cup \mathcal{U} = \mathcal{U}$, $A \cap \emptyset = \emptyset$.

(f) **Idempotent Laws:** $A \cup A = A$, $A \cap A = A$.

(g) **Absorption Laws:** $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$.

(h) **Complementation:** $A \cup A^c = \mathcal{U}$, $A \cap A^c = \emptyset$.

Remark. Sample Proof of the Commutative Law $A \cup B = B \cup A$.

Proof. To prove that two sets X and Y are equal, we must prove that $X \subseteq Y$ and $Y \subseteq X$. First, let $x \in A \cup B$. By the definition of union, this means $x \in A$ or $x \in B$. This is logically equivalent to $x \in B$ or $x \in A$. Therefore, by the definition of union, $x \in B \cup A$. Since any element of $A \cup B$ is also in $B \cup A$, we have $A \cup B \subseteq B \cup A$. The argument for the reverse inclusion $B \cup A \subseteq A \cup B$ is identical. Therefore, $A \cup B = B \cup A$. ■

17. $A \subseteq A \cup B$, $A \cap B \subseteq A$.

18. If $C \subseteq A$ and $C \subseteq B$, then $C \subseteq A \cap B$.

19. If $A \subseteq B$, prove that $A \cup C \subseteq B \cup C$ and $A \cap C \subseteq B \cap C$.

20. Prove that $A \setminus B = A \cap B^c$.

21. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

22. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

23. Let X be a set. Prove that $X \times \emptyset = \emptyset$.

24. Let X, Y and Z be sets. Is it true that $X \times Y = Y \times X$? Is it true that $(X \times Y) \times Z = X \times (Y \times Z)$? Justify your answers.

25. ⋆ One of the following two formulae is always right and the other is sometimes wrong. Identify which is which, prove the correct one, and provide a counterexample for the wrong one.

(i) $A \setminus (B \setminus C) = (A \setminus B) \cup C$

(ii) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$

Part III: Families of Sets

The familiar operations of union and intersection can be extended from pairs of sets to large, even infinite, collections of sets. To do this formally, we first define what we mean by a collection of sets.

Definition 6.7.1. ***(Family of Sets)***. A family of sets is a collection of sets, often denoted by a calligraphic letter such as $\mathcal{A}$ or $\mathcal{F}$. We will assume all families of sets mentioned are non-empty.

With this terminology, we can now define the union and intersection over an entire family.

Definition 6.7.2. ***(Union over a Family)***. If $\mathcal{F}$ is a non-empty family of sets, its union is the set of all elements that belong to at least one member of the family. Formally:

$$\bigcup_{A\in\mathcal{F}} A := \{x : (\exists A \in \mathcal{F})\, x \in A\}$$

Definition 6.7.3. ***(Intersection over a Family)***. If $\mathcal{F}$ is a non-empty family of sets, its intersection is the set of all elements that belong to every member of the family. Formally:

$$\bigcap_{A\in\mathcal{F}} A := \{x : (\forall A \in \mathcal{F})\, x \in A\}$$

It is common for a family of sets to be indexed by another set I. For example, if we have a set A_i for each integer $i \in \mathbb{Z}$, the family is $\mathcal{F} = \{A_i : i \in \mathbb{Z}\}$. In such cases, we adopt a more convenient notation.

If $\mathcal{F} = \{A_i : i \in I\}$ is an indexed family of sets, we write the union and intersection as:

$$\bigcup_{i\in I} A_i \quad \text{and} \quad \bigcap_{i\in I} A_i$$

For a finite family, such as $\mathcal{F} = \{A_1, A_2, \ldots, A_n\}$, this notation becomes:

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

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

Remark. Due to the associative laws for $\cup$ and $\cap$, expressions like $A_1 \cup A_2 \cup \cdots \cup A_n$ are unambiguous. A valuable exercise for the reader is to carry out the proofs of the generalized laws for these operations (such as De Morgan's laws), as this is one of the best ways to become familiar with the terminology and notation.

26. For each integer $n \geq 1$, let $A_n = \{k \in \mathbb{Z} \mid -n \leq k \leq n\}$. Describe the following sets.

(a) $\bigcup_{n=1}^{5} A_n$
(b) $\bigcap_{n=1}^{5} A_n$
(c) $\bigcup_{n=1}^{\infty} A_n$
(d) $\bigcap_{n=1}^{\infty} A_n$

27. For each real number $r > 0$, let $B_r = (-r, r)$, which is the open interval of real numbers between $-r$ and r. Describe the following sets.

(a) $\bigcup_{r\in\{1,2,3\}} B_r$
(b) $\bigcap_{r\in\{1,2,3\}} B_r$
(c) $\bigcup_{r\in(0,\infty)} B_r$

(d) $\bigcap_{r\in(0,\infty)} B_r$

28. Let $\mathcal{F}$ be a collection of sets and let B be a set. Prove the generalised distributive laws:

(a) $B \cap \left(\bigcup_{A\in\mathcal{F}} A\right) = \bigcup_{A\in\mathcal{F}} (B \cap A)$

(b) $B \cup \left(\bigcap_{A\in\mathcal{F}} A\right) = \bigcap_{A\in\mathcal{F}} (B \cup A)$

29. Prove the generalised De Morgan's laws:

(a) $\left(\bigcup_{A\in\mathcal{F}} A\right)^c = \bigcap_{A\in\mathcal{F}} A^c$

(b) $\left(\bigcap_{A\in\mathcal{F}} A\right)^c = \bigcup_{A\in\mathcal{F}} A^c$

Part IV: Mathematical Induction

30. Prove the following summation formulae for all integers $n \geq 1$.

(a) $\sum_{k=1}^{n}(2k-1) = n^2$ (Sum of the first n odd numbers).

(b) $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

(c) $\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2 = (\sum_{k=1}^{n} k)^2$.

(d) $\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$.

31. Prove the following product formulae for all integers $n \geq 2$.

(a) $\prod_{k=2}^{n} \left(1 - \frac{1}{k}\right) = \frac{1}{n}$.

(b) $\prod_{k=2}^{n} \left(1 - \frac{1}{k^2}\right) = \frac{n+1}{2n}$.

32. Prove the following divisibility statements for all integers $n \geq 1$ (unless stated otherwise).

(a) $n^3 + 2n$ is divisible by 3.

(b) $8^n - 3^n$ is divisible by 5.

(c) $x^n - y^n$ is divisible by $x - y$ for any integers x, y with $x \neq y$.

(d) For $n \geq 0$, $11^{n+2} + 12^{2n+1}$ is divisible by 133.

33. Prove the following inequalities.

(a) For $n \geq 4$, $2^n < n!$.

(b) For $n \geq 5$, $n^2 < 2^n$.

(c) For any real number $h > -1$ and any non-negative integer n, $(1+h)^n \geq 1+nh$. (This is Bernoulli's Inequality).

34. Find the error in the following 'proof' that $a^n = 1$ for all non-negative integers n, whenever a is a non-zero real number.

- **(BC)** For $n = 0$, $a^0 = 1$. This is true by definition.
- **(IS)** Assume $a^k = 1$ for all integers k with $0 \leq k \leq n$. We must prove $a^{n+1} = 1$. We can write $a^{n+1} = \frac{a^n \cdot a^n}{a^{n-1}}$. By the induction hypothesis, since n and $n-1$ are less than or equal to n, we have $a^n = 1$ and $a^{n-1} = 1$. Substituting these values gives $a^{n+1} = \frac{1\cdot 1}{1} = 1$.
- By the principle of strong induction, the statement is true.

35. The Fibonacci numbers are defined by $F_0 = 0, F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. Use strong induction to prove the following properties.

(a) $F_n < 2^n$ for all $n \geq 0$.

(b) $\sum_{k=1}^{n} F_k = F_{n+2} - 1$.

(c) $\star$ $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$ for $n \geq 1$. (Cassini's Identity).

36. Any integer $n \geq 1$ can be written as a sum of distinct powers of 2. (This is the basis of the binary number system). Prove this using strong induction.

37. Consider a game where two players take turns removing 1, 2, or 3 stones from a pile that initially contains n stones. The player who takes the last stone wins. Prove that the second player has a winning strategy if and only if the initial number of stones n is a multiple of 4.

Chapter 7

Binomial Theorem

It may seem peculiar that a text on algebra should have a chapter on counting. At its most basic, counting is a process of enumeration. We seek to introduce mathematical techniques that bypass this process, allowing us to answer the question "How many?" in a more sophisticated manner. To do this, we must first establish a rigorous foundation for the objects we intend to count. Sets and the concept of order are central to this endeavour.

7.1 Cardinality of Sets

In our study of sets, we are often concerned with their size. The size of a set is the number of distinct elements it contains. This concept is formalised as cardinality.

Definition 7.1.1. ***(Cardinality)***. The cardinality of a finite set A is the number of elements in A. It is denoted by $\text{card}(A)$ or, more commonly, by $|A|$.

For example, if $A = \{a, b, c, d\}$, then $|A| = 4$. If E is the set of even integers between 1 and 10, then $E = \{2, 4, 6, 8\}$ and $|E| = 4$. The cardinality of the empty set is $|\emptyset| = 0$. For our purposes, we will only consider finite sets.

7.1.1 From Unordered Sets to Ordered Lists

A set is an unordered collection. The sets $\{a, b\}$ and $\{b, a\}$ are identical. However, in many counting problems, the order of objects is crucial. A phone number is not merely a set of digits; their sequence matters. To handle order, we must construct the idea of a list from the more primitive idea of a set.

We begin with the most basic ordered structure: a pair of objects.

Definition 7.1.2. ***(Ordered Pair)***. An ordered pair (a, b) is a collection of two objects in which a is designated as the first element and b as the second. Unlike a set, the order matters: if $a \neq b$, then $(a, b) \neq (b, a)$.

Remark. It is a remarkable fact of mathematics that even this concept of order can be built from the unordered world of sets. The standard construction, due to Kuratowski, defines the ordered pair (a, b) as the set $\{\{a\}, \{a, b\}\}$. The first element can be uniquely identified as the one present in both member sets. We shall not delve further into this, but it serves to show how fundamental the idea of a set is.

With the ordered pair established, we can define a list of any length.

Definition 7.1.3. ***(List)***. A list is an ordered sequence of objects. A list is denoted by an opening parenthesis, followed by the objects, separated by commas, followed by a closing parenthesis. The objects are called the **entries** of the list.

For instance, (a, b, c, d, e) is a list of the first five letters of the alphabet, in order. The length of a list is its number of entries. Unlike sets, lists can have repeated entries; $(5, 3, 5, 4, 3, 3)$ is a valid list of length six. Two lists are equal if and only if they have the same entries in exactly the same positions. There is one special list, the **empty list** $()$, which has length zero.

The outcome of tossing a coin ten times can be modelled by a list of length ten, such as

$$(H, H, T, H, T, T, T, H, H, T).$$

The outcome of rolling a die five times can be modelled by a list such as $(3, 5, 3, 1, 6)$. Information technology is built upon the byte, which is simply a list of length eight whose entries are drawn from the set $\{0, 1\}$. We now explore methods for counting such lists.

7.1.2 The Multiplication Principle

Many counting problems can be reduced to finding the number of possible lists that satisfy certain conditions.

Consider making a list of length three, where the first entry must be from the set $\{a, b, c\}$, the second from $\{5, 7\}$, and the third from $\{a, x\}$. How many such lists are possible? We can visualise the construction of such a list as a sequence of choices, represented by a tree diagram as shown in Figure 7.1.

There are $3 \times 2 \times 2 = 12$ distinct paths, each corresponding to a unique list.

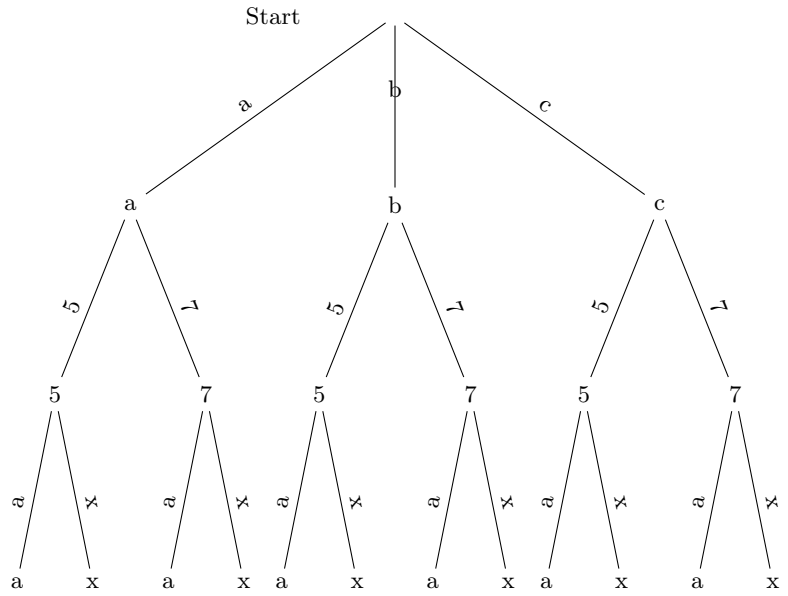


Figure 7.1: Constructing lists of length three. The number of choices at each stage multiplies.

There are 3 choices for the first entry. For each of these, there are 2 choices for the second entry. For each of these 3×2 partial lists, there are 2 choices for the third entry. The total number of lists is the product $3 \times 2 \times 2 = 12$. This illustrates a fundamental principle.

***Theorem* 7.1.1. (The Multiplication Principle).** Suppose a list of length n is to be made. If there are a_1 possible choices for the first entry, a_2 possible choices for the second entry, and so on, up to a_n choices for the n-th entry, then the total number of different lists that can be made is the product $a_1 \cdot a_2 \cdot a_3 \cdots a_n$.

Example 7.1.1. (Standard Licence Plates). A standard licence plate consists of three letters followed by four digits. How many are possible?

Well a licence plate corresponds to a list of length 7. There are 26 choices for each of the first three entries, and 10 choices for each of the last four. By the Multiplication Principle, the total number of possible plates is

$$26 \times 26 \times 26 \times 10 \times 10 \times 10 \times 10 = 26^3 \cdot 10^4 = 175,760,000.$$

There are two main types of list-counting problems. In some, entries may be repeated, as with licence plates. In others, repetition is not allowed.

Example 7.1.2. Consider lists of length 4 made from the symbols $\{A, B, C, D, E, F, G\}$..

(a) **How many lists are possible if repetition is allowed?**
There are 7 choices for each of the four positions. The total number of lists is $7 \times 7 \times 7 \times 7 = 7^4 = 2401$.

(b) **How many lists are possible if repetition is not allowed?**
There are 7 choices for the first entry. Once chosen, that symbol cannot be used again, leaving 6 choices for the second entry. This continues, leaving 5 choices for the third and 4 for the fourth. The total number is $7 \times 6 \times 5 \times 4 = 840$.

(c) **How many lists are there if repetition is not allowed and the list must contain an E?**
This is more complex. We can partition the problem into four disjoint cases depending on the position of the E. Let X be the set of all such lists. Let X_i be the set of lists where E is in the i-th position. Then $X = X_1 \cup X_2 \cup X_3 \cup X_4$. To count the lists in X_1, the first entry is fixed as E. The remaining three entries must be filled without repetition from the other 6 available symbols. By the multiplication principle, there are $6 \times 5 \times 4 = 120$ ways to do this. So, $|X_1| = 120$. Similarly, $|X_2| = |X_3| = |X_4| = 120$. Since the sets X_i are disjoint (a list cannot have E in two different positions), we can use add them together to find the total:

$$|X| = |X_1| + |X_2| + |X_3| + |X_4| = 120 + 120 + 120 + 120 = 480.$$

(d) **How many lists are there if repetition is allowed and the list must contain at least one E?**
A direct approach to this problem is surprisingly complicated. If we try to count the lists with exactly one E, then exactly two E's, and so on, we quickly run into issues of overcounting. For example, a list like (E, E, A, B) would be counted when we consider lists with an E in the first position, and counted again when we consider lists with an E in the second position.

Instead of counting what we *want*, a much simpler strategy is to count what we *don't want* and remove it from the total.

First, let's recall the total number of possible lists of length 4 with repetition allowed. As calculated in (a), with 7 choices for each of the 4 positions, there is a universe of $7^4 = 2401$ possible lists.

Now, let's consider the lists that we want to exclude: the ones that fail the condition. The condition is "the list must contain at least one E." The only lists that fail this condition are those that contain no E's at all. To form such a list, we can only choose from the remaining 6 letters (from $\{A, B, C, D, F, G\}$) for each of the four positions. The number of such lists is:

$$6 \times 6 \times 6 \times 6 = 6^4 = 1296.$$

Every list in our universe of 2401 lists either has at least one E or it has no E's. Therefore, to find the number of lists we want, we can simply take the total and subtract the number of lists we don't want:

$$\text{(Total possible lists)} - \text{(Lists with no E's)} = 2401 - 1296 = 1105.$$

Thus there are 1105 lists that contain at least one E.

The reasoning in the last two examples hints at two other fundamental principles, which we now formalise.

7.1.3 The Addition and Subtraction Principles

These principles formalise common-sense strategies for counting by relating them to set operations.

***Theorem* 7.1.2. (The Addition Principle)**. Suppose a finite set X can be decomposed into a union of n mutually disjoint subsets, $X = X_1 \cup X_2 \cup \ldots \cup X_n$, where $X_i \cap X_j = \emptyset$ whenever $i \neq j$. Then the cardinality of X is the sum of the cardinalities of the subsets:

$$|X| = |X_1| + |X_2| + \cdots + |X_n| = \sum_{i=1}^{n} |X_i|.$$

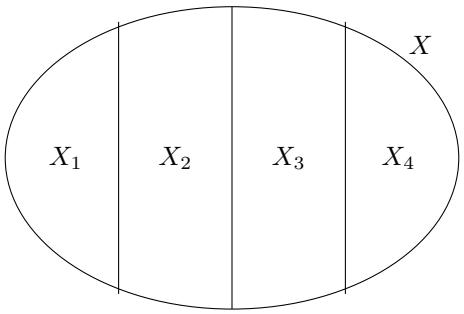


Figure 7.2: A set X partitioned into disjoint subsets. $|X|= |X_1|+|X_2|+|X_3|+|X_4|$.

We implicitly used this in part (c) of the previous example, where the set of all lists containing an E was partitioned into four disjoint sets based on the position of the E.

***Theorem* 7.1.3. (The Subtraction Principle)**. If X is a subset of a finite universal set $\mathcal{U}$, then the number of elements in the complement of X, denoted $\mathcal{U} \setminus X$ or X^c, is given by

$$|X^c|= |\mathcal{U}|-|X|.$$

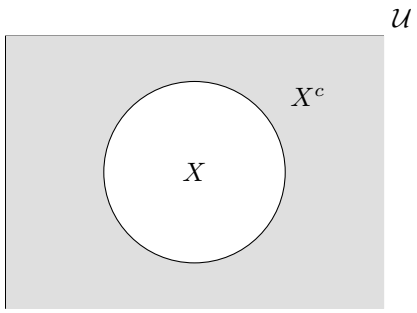


Figure 7.3: The subtraction principle: $|X^c|= |\mathcal{U}|-|X|$.

This principle is useful when it is easier to count the items we wish to exclude than those we wish to include. Part (d) of the previous example demonstrated this by counting all possible lists and then subtracting the number of lists that failed to meet the condition.

7.2 Exercises

Part I: Direct Applications

1. A restaurant menu has 5 starters, 10 main courses, and 6 desserts. How many different three-course meals can be ordered?

2. A standard six-sided die is rolled three times. How many possible outcomes are there (e.g., $(4, 1, 5)$ is one outcome)?

3. A local telephone number consists of 7 digits. The first digit cannot be 0 or 1. How many such telephone numbers are possible?

4. How many different lists of length 5 can be formed from the letters A, B, C, D, E, F if:

(a) Repetition of letters is allowed?

(b) Repetition of letters is not allowed?

5. In a race with 10 competitors, how many different ways can the first, second, and third place medals be awarded?

6. A computer password must be 8 characters long. The first 4 characters must be uppercase letters and the last 4 characters must be digits (0-9). How many different passwords can be created?

Part II: Addition and Subtraction Principles

7. (Justifying the Addition Principle) The principle states that if sets A and B are disjoint ($A \cap B = \emptyset$), then $|A \cup B| = |A| + |B|$. Prove this geometrically.

8. (Deriving the Subtraction Principle) Use the Addition Principle to prove the Subtraction Principle.

Remark. Consider a set X and its complement X^c within a universal set $\mathcal{U}$. Are X and X^c disjoint? What is their union? Apply the Addition Principle to this union.

9. Consider all positive integers with three distinct digits. (Note: the first digit cannot be 0).

(a) How many such integers are there?

(b) How many of them are odd?

(c) How many of them are even?

(d) How many are greater than 500?

10. From a standard deck of 52 playing cards, a hand of 5 cards is dealt. How many hands contain at least one Ace? (For this problem, consider the hand to be an ordered list of cards).

Remark. It is much easier to count the number of hands with no Aces and subtract from the total.

11. How many lists of length 4, made from the letters A, B, C, D, E, F, with repetition allowed, contain at least one A?

12. In a class of 30 students, a president, vice-president, and secretary are to be chosen. How many different ways can these offices be filled if Alice must be an officer?

Part III: Challenge Problems

13. How many positive integers between 100 and 999 inclusive are divisible by 7?

14. (Deriving the Principle of Inclusion-Exclusion) We wish to count the number of positive integers less than or equal to 1000 that are divisible by either 3 or 5. Let's build a general formula.

(a) Let A be the set of integers ≤ 1000 divisible by 3. What is $|A|$?

(b) Let B be the set of integers ≤ 1000 divisible by 5. What is $|B|$?

(c) If we calculate $|A| + |B|$, have we overcounted or undercounted the desired total? Which specific numbers have been counted incorrectly?

(d) Let $A \cap B$ be the set of integers ≤ 1000 divisible by both 3 and 5. Describe this set in a simpler way, and find its cardinality, $|A \cap B|$.

(e) Use your answers from (a), (b), and (d) to find the correct number of integers ≤ 1000 divisible by either 3 or 5.

(f) Propose and justify a general formula for $|A \cup B|$ in terms of $|A|$, $|B|$, and $|A \cap B|$.

15. $\star$ (Justifying the Multiplication Principle) Let's prove the Multiplication Principle by building up from a simple case.

(a) Consider making a list of length 2. If there are a_1 choices for the first entry and a_2 choices for the second, explain why there are $a_1 \cdot a_2$ total lists.

Remark. For each of the a_1 first choices, how many second choices can be paired with it?

(b) Now consider a list of length 3 with a_1, a_2, a_3 choices for each position. Think of a 3-entry list (x, y, z) as being formed by taking a 2-entry list (x, y) and appending a third entry z. Use your result from part (a) to show that the total number of lists is $(a_1 \cdot a_2) \cdot a_3$.

(c) Generalise your reasoning from part (b) to explain why the total number of lists of length n is $a_1 \cdot a_2 \cdots a_n$.

16. ⋆ A bit string is a list whose entries are from the set $\{0, 1\}$. How many bit strings of length 8 begin with a 1 or end with 00?

Remark. Let A be the set of strings that begin with 1 and B be the set of strings that end with 00. Are these sets disjoint? Use the principle you discovered in problem 14.

17. ⋆ A palindrome is a word or number that reads the same forwards and backwards (e.g., `MADAM`, 12321). How many five-letter palindromes can be formed using the 26 letters of the alphabet?

18. ⋆ Prove that the number of lists of length k from a set of n elements is n^k if repetition is allowed, and $n(n-1)\cdots(n-k+1)$ if repetition is not allowed (assuming $k \leq n$).

7.3 Factorials and Permutations

In our study of lists, we frequently encounter the problem of counting non-repetitive lists of length n made from n distinct symbols. This specific calculation occurs so often that it is given a special name and notation.

Definition 7.3.1. ***(Factorial)***. If n is a non-negative integer, then the factorial of n, denoted $n!$, is the number of non-repetitive lists of length n that can be made from a set of n symbols.

- By definition, there is one list of length 0 that can be made from 0 symbols: the empty list. Thus, $0! = 1$.
- For $n > 0$, the number of such lists can be found by the Multiplication Principle. There are n choices for the first entry, $n-1$ for the second, and so on, down to 1 choice for the last. Thus, for $n > 0$,

$$n! = n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1 = \prod_{i=1}^{n} i.$$

It follows that $1! = 1$, $2! = 2 \times 1 = 2$, $3! = 3 \times 2 \times 1 = 6$, $4! = 24$, and so on. The definition gives the recursive relationship $n! = n \cdot (n-1)!$ for $n \geq 1$. If we set $n = 1$, this gives $1! = 1 \cdot (0!)$, which implies $1 = 1 \cdot 0!$. This is consistent with our definition that $0! = 1$.

A non-repetitive list of length n using every element from a set of size n is simply an arrangement of the elements of that set in a row. This has a formal name.

Definition 7.3.2. ***(Permutation)***. A permutation of a set is an arrangement of all of the set's elements in a row. For a set with n elements, there are $n!$ distinct permutations.

For example, there are $3! = 6$ permutations of the set $\{a, b, c\}$:

$$(a,b,c), (a,c,b), (b,a,c), (b,c,a), (c,a,b), (c,b,a).$$

We now consider a variation: arranging only some of the elements from a set.

Definition 7.3.3. ***(k-Permutation)***. A k-permutation of an n-element set is a non-repetitive list of length k made from elements of the set. The number of k-permutations of an n-element set is denoted $P(n, k)$.

The value of $P(n,k)$ can be computed directly with the Multiplication Principle. We have n choices for the first entry, $n-1$ for the second, and so on. For the k-th entry, we will have used $k-1$ symbols, leaving $n-(k-1) = n-k+1$ choices.

$$P(n,k) = \underbrace{n(n-1)(n-2)\cdots(n-k+1)}_{k \text{ factors}}$$

This product can be expressed more compactly using factorials.

$$\begin{aligned} P(n,k) &= n(n-1)\cdots(n-k+1) \\ &= \frac{n(n-1)\cdots(n-k+1)\times(n-k)(n-k-1)\cdots 1}{(n-k)(n-k-1)\cdots 1} \\ &= \frac{n!}{(n-k)!} \end{aligned}$$

***Theorem* 7.3.1. (Number of k-Permutations)**. The number of k-permutations of an n-element set, for $0 \leq k \leq n$, is given by

$$P(n,k) = \frac{n!}{(n-k)!}.$$

Note that $P(n,n) = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!$, which is consistent, as an n-permutation is simply a permutation. Also, $P(n,0) = \frac{n!}{(n-0)!} = 1$, which is correct as there is only one list of length 0, the empty list.

Example 7.3.1. A race has 10 contestants. How many different rankings for first, second, and third place are possible?

This is a problem of arranging 3 contestants chosen from a set of 10. The number of 3-permutations of a 10-element set is

$$P(10,3) = \frac{10!}{(10-3)!} = \frac{10!}{7!} = 10\times 9\times 8 = 720.$$

There are 720 possible rankings for the top three positions.

7.3.1 Counting Subsets

The previous section dealt with counting ordered lists. We now turn to a related but distinct question: how many unordered subsets of a certain size can be chosen from a larger set?

Let $A = \{a,b,c,d,e\}$. From this set of 5 elements, we can form $P(5,2) = 20$ distinct 2-permutations. However, there are only 10 subsets of size two:

$$\{a,b\},\{a,c\},\{a,d\},\{a,e\},\{b,c\},\{b,d\},\{b,e\},\{c,d\},\{c,e\},\{d,e\}.$$

The number of lists is greater because for any pair of distinct elements, say a and b, we can form two lists, (a,b) and (b,a), but only one subset, $\{a,b\}$. Each 2-element subset gives rise to $2! = 2$ different 2-permutations. This suggests a relationship between counting subsets and counting permutations.

Definition 7.3.4. ***(n choose k)***. If n and k are integers with $0 \leq k \leq n$, then the symbol $\binom{n}{k}$, read "n choose k", denotes the number of subsets of size k that can be formed from an n-element set.

To find a formula for $\binom{n}{k}$, we can reason as follows. Consider the task of creating a k-permutation from an n-element set. We can conceptualise this as a two-step process:

1. First, choose a subset of k elements from the n-element set. By definition, there are $\binom{n}{k}$ ways to do this.
2. Second, arrange the chosen k elements into a list. There are $k!$ ways to do this.

By the Multiplication Principle, the total number of ways to perform this two-step process is $\binom{n}{k} \times k!$. But this process is just another way of describing the formation of a k-permutation. Therefore, this product must be equal to the number of k-permutations, $P(n,k)$.

$$\binom{n}{k} \times k! = P(n,k) = \frac{n!}{(n-k)!}$$

Dividing both sides by $k!$ yields the fundamental formula for counting combinations.

***Theorem* 7.3.2. (Number of Subsets).** The number of k-element subsets of an n-element set, for $0 \leq k \leq n$, is given by

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}.$$

Proof. A k-permutation of an n-element set can be constructed in two steps: first, choose a k-element subset, and second, arrange the elements of that subset in a list.

1. *The number of ways to choose a k-element subset from an n-element set is, by definition, $\binom{n}{k}$.*
2. *The number of ways to arrange the k chosen elements into a list is $k!$.*

By the Multiplication Principle, the total number of k-permutations is the product $\binom{n}{k} \times k!$.
From Theorem 7.3.1, we know the number of k-permutations of an n-element set is also given by $P(n,k) = \frac{n!}{(n-k)!}$. Equating the two expressions for the number of k-permutations gives

$$\binom{n}{k} \times k! = \frac{n!}{(n-k)!}.$$

Dividing both sides by $k!$ yields the desired formula. ■

Example 7.3.2. How many 5-card hands can be dealt from a standard 52-card deck?

A 5-card hand is a 5-element subset of the 52-card deck. The order in which the cards are received does not matter. The number of such subsets is

$$\binom{52}{5} = \frac{52!}{5!\,(52-5)!} = \frac{52!}{5!\,47!} = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 2,598,960.$$

Example 7.3.3. A committee of 3 men and 4 women is to be selected from a group of 8 men and 6 women. How many different committees can be formed?

This is a two-step process. First, we choose the men, then we choose the women.

- The number of ways to choose 3 men from 8 is $\binom{8}{3} = \frac{8!}{3!5!} = \frac{8 \cdot 7 \cdot 6}{3 \cdot 2 \cdot 1} = 56$.
- The number of ways to choose 4 women from 6 is $\binom{6}{4} = \frac{6!}{4!2!} = \frac{6 \cdot 5}{2 \cdot 1} = 15$.

By the Multiplication Principle, the total number of ways to form the committee is the product of these two numbers:

$$\binom{8}{3} \times \binom{6}{4} = 56 \times 15 = 840.$$

7.3.2 The Binomial Theorem

We have previously established identities for the expansion of expressions like $(a+b)^2$ and $(a+b)^3$. We now seek a general formula for $(a+b)^n$ for any non-negative integer n. We can derive this formula by thinking about the expansion from a combinatorial perspective.

Consider the product of n factors of $(a+b)$:

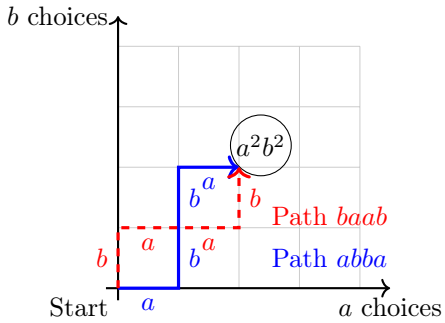
$$(a+b)^n = \underbrace{(a+b)(a+b)\cdots(a+b)}_{n \text{ brackets}}$$

By the Generalised Law of Distribution (Theorem 5.1.1), each term in the final expansion is formed by choosing either the term a or the term b from each of the n brackets and multiplying these choices together.

Let us consider what kind of terms can be formed. If we choose b from k of the brackets, we must necessarily choose a from the remaining $n-k$ brackets. The resulting product will be $a^{n-k}b^k$. All terms in the final expansion must be of this form for some k from 0 to n.

The crucial question is: for a given k, how many times will the term $a^{n-k}b^k$ appear in the expansion before like terms are collected? A specific term $a^{n-k}b^k$ arises every time we select b from exactly k of the n available brackets. The problem is therefore equivalent to counting the number of ways to choose a set of k brackets from the total collection of n brackets. This is precisely the definition of "n choose k". There are $\binom{n}{k}$ ways to do this.

A geometric interpretation provides another way to understand this result. Imagine a grid. To expand $(a+b)^n$, we must make n choices. Let each choice of 'a' correspond to a step to the right, and each choice of 'b' a step up. Any full expansion, such as $aba\cdots b$, corresponds to a path of n steps. A specific term $a^{n-k}b^k$ corresponds to a path that consists of exactly $n-k$ steps to the right and k steps up. The problem of finding the coefficient is thus equivalent to counting how many such distinct paths exist. Out of a total of n steps, we must choose which k of them are 'up' steps. The number of ways to make this choice is precisely $\binom{n}{k}$, as illustrated for $(a+b)^4$ in Figure 7.4.



Total paths from Start to $a^{n-k}b^k$ is $\binom{n}{k}$. Here, $\binom{4}{2} = 6$.

Figure 7.4: Path counting interpretation for the coefficient of a^2b^2 in $(a+b)^4$. Each path from $(0,0)$ to $(2,2)$ corresponds to a unique sequence of four choices with two a's and two b's.

Therefore, the coefficient of the term $a^{n-k}b^k$ in the expansion of $(a+b)^n$ must be $\binom{n}{k}$. Summing over all possible values of k gives the complete formula.

***Theorem* 7.3.3. (The Binomial Theorem).** For any numbers a, b and any non-negative integer n,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k. \tag{7.1}$$

In expanded form, this is:

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n.$$

The numbers $\binom{n}{k}$ are called the binomial coefficients because they appear in this expansion.

Example 7.3.4. Expand $(a+b)^4$ using the Binomial Theorem.

Here $n = 4$. We calculate the binomial coefficients:

- $\binom{4}{0} = \frac{4!}{0!4!} = 1$
- $\binom{4}{1} = \frac{4!}{1!3!} = 4$
- $\binom{4}{2} = \frac{4!}{2!2!} = \frac{24}{4} = 6$
- $\binom{4}{3} = \frac{4!}{3!1!} = 4$
- $\binom{4}{4} = \frac{4!}{4!0!} = 1$

Substituting these into the theorem:

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.$$

Example 7.3.5. Find the coefficient of the term $x^{10}y^3$ in the expansion of $(2x^2 - y)^8$.

We use the Binomial Theorem with $a = 2x^2$, $b = -y$, and $n = 8$. A general term in the expansion is of the form:

$$\binom{8}{k}(2x^2)^{8-k}(-y)^k = \binom{8}{k}2^{8-k}(x^2)^{8-k}(-1)^k y^k = \binom{8}{k}(-1)^k 2^{8-k}x^{16-2k}y^k.$$

We want the term where the power of y is 3, so we set $k = 3$. For $k = 3$, the power of x is $16 - 2(3) = 10$. This matches the term we are looking for. The coefficient is therefore:

$$\binom{8}{3}(-1)^3 2^{8-3} = \frac{8!}{3!\,5!} \cdot (-1) \cdot 2^5 = 56 \cdot (-1) \cdot 32 = -1792.$$

7.4 Exercises

Part I: Factorials, Permutations, and Combinations

1. Calculate the following values by hand.

(a) $6!$
(b) $\frac{9!}{6!}$
(c) $\frac{10!}{7!3!}$
(d) $P(7,3)$
(e) $\binom{8}{3}$
(f) $\binom{10}{8}$

2. Simplify the following expressions involving factorials, where $n \geq k \geq 2$.

(a) $\frac{(n+1)!}{(n-1)!}$
(b) $\frac{n!}{(n-k)!} \div \frac{(n-1)!}{(n-k-1)!}$
(c) $\frac{1}{(k-1)!} - \frac{1}{k!}$

3. From a group of 12 people, a committee of 4 is to be chosen. How many distinct committees can be formed?

4. A debating team consists of 3 speakers. There are 10 candidates. How many ways can the team be chosen and then arranged in a speaking order (first, second, third)?

5. How many ways can the letters of the word `ALGEBRA` be arranged?

6. Seven people are to be seated in a row of seven chairs. How many arrangements are possible if three particular people insist on sitting together?

7. A standard 52-card deck has 4 suits and 13 ranks. How many 5-card hands are possible that consist of:

(a) A "four of a kind" (four cards of one rank, and one other card)?

(b) A "flush" (all five cards of the same suit), but not a "straight flush" (a flush with cards in sequence)?

(c) Two pairs (two cards of one rank, two cards of another rank, and one card of a third rank)?

8. A committee of 6 is to be formed from a group of 7 men and 8 women.

(a) How many committees are possible if it must contain an equal number of men and women?

(b) How many committees are possible if it must contain at least one man?

9. Prove the identity $\binom{n}{k} = \binom{n}{n-k}$ using two different methods:

(a) Algebraically, using the formula from Theorem 7.3.2.

(b) By a combinatorial argument.

Remark. Relate the act of choosing k items from n to the act of leaving $n-k$ items behind.

10. ⋆ **Circular Permutations.** The number of ways to arrange n distinct objects in a circle is $(n-1)!$.

(a) How many ways can 8 people be seated around a circular table?

(b) Justify the formula.

Remark. First, arrange the n objects in a line ($n!$ ways). How many of these linear arrangements correspond to the same circular arrangement?

11. ⋆ **Permutations with Repetition.** Justify the formula for the number of distinct arrangements of n objects with n_1 identical objects of type 1, n_2 of type 2, etc., given by

$$\frac{n!}{n_1!\, n_2! \cdots n_k!}.$$

Remark. Imagine the n_1 identical objects are temporarily made distinct (e.g., $A_1, A_2, \dots$). How many new arrangements does this create from a single original arrangement? Generalise this idea for all repeated types.

Part II: The Binomial Theorem

13. Expand $(a+b)^n$ for $n = 2, 3, 4$. For each expansion, express the coefficients using the notation $\binom{n}{k}$. Observe the pattern.

14. Use the Binomial Theorem to expand the following expressions.

(a) $(x+y)^5$

(b) $(a-2b)^4$

(c) $(x^2+1)^6$

15. Find the coefficient of the specified term in the expansion of the given expression.

(a) The a^5b^7 term in $(a+b)^{12}$.

(b) The x^8y^3 term in $(x-3y)^{11}$.

(c) The constant term in $\left(x^2 + \frac{1}{x}\right)^9$.

16. Use the Binomial Theorem to calculate the exact value of $(99)^4$.

Remark. Write 99 as $(100-1)$.

17. ⋆ Let $P(n)$ be the statement of Theorem 7.3.3.

Remark. This problem guides you through an inductive proof of the Binomial Theorem, if you don't want a guide try proving it yourself first.

(a) Verify the base case, $P(1)$.

(b) Assume $P(n)$ holds for some $n \geq 1$. Write the expression for $(a+b)^{n+1}$ as $(a+b)(a+b)^n$ and substitute the assumed expansion for $(a+b)^n$.

(c) Distribute the $(a+b)$ factor. This will result in two separate summations.

(d) In the second summation, perform a change of index (e.g., let $j = k+1$) so that the power of b is the same in both sums.

(e) Combine the two summations. You will need to handle the first and last terms separately. The coefficient of a general term will be a sum of two binomial coefficients.

(f) Apply an identity you have proven in a previous exercise to simplify this coefficient and show that the final expression is precisely the statement $P(n+1)$.

18. By selecting appropriate values for a and b in the Binomial Theorem, prove the following identities for any integer $n \geq 1$.

(a) $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

(b) $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$.

(c) $\sum_{k=0}^{n} \binom{n}{k} 2^k = 3^n$.

19. Sum of Even and Odd Coefficients.

(a) Using the results from the previous problem, prove that for $n \geq 1$, the sum of the binomial coefficients with even indices equals the sum of those with odd indices. That is:

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \dots$$

(b) Prove that each of these sums is equal to 2^{n-1}.

Part III: Combinatorial Identities

20. Pascal's Identity. Prove that for integers $1 \leq k \leq n$,

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

(a) Provide an algebraic proof using the factorial formula.

(b) Provide a combinatorial proof by considering a set of n elements. Single out a specific element, X. How many k-element subsets contain X? How many do not?

21. Using Pascal's Identity, explain the construction of Pascal's Triangle and why its n-th row consists of the coefficients $\binom{n}{k}$.

22. The Chairperson Identity. Prove $k\binom{n}{k} = n\binom{n-1}{k-1}$ for $1 \leq k \leq n$.

(a) Provide an algebraic proof.

(b) Provide a combinatorial proof by counting, in two different ways, the number of ways to form a committee of k people from a group of n, with one member designated as chairperson.

23. Use the Chairperson Identity and other known results to prove that $\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$.

24. The Subcommittee Identity. Prove $\binom{n}{k}\binom{k}{\ell} = \binom{n}{\ell}\binom{n-\ell}{k-\ell}$ for $0 \leq \ell \leq k \leq n$.

Remark. Count, in two different ways, the number of ways to choose a committee of k people from n, and from that committee, a subcommittee of ℓ leaders.

25. The Hockey-Stick Identity. Prove $\sum_{i=r}^{n} \binom{i}{r} = \binom{n+1}{r+1}$ for $r \leq n$.

Remark. Consider the set of subsets of size $r+1$ from $\{1, 2, \ldots, n+1\}$. Classify these subsets based on their largest element.

26. ⋆ Sum of Squares. Prove the identity $\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$.

Remark. Consider the identity $(1+x)^{2n} = (1+x)^n(1+x)^n$. Find the coefficient of x^n on both sides of the equation. You may need the identity from problem 10.

27. ⋆ Vandermonde's Identity. For non-negative integers m, n, l,

$$\sum_{k=0}^{l} \binom{n}{k}\binom{m}{l-k} = \binom{n+m}{l}.$$

(a) Provide a combinatorial proof.

Remark. Consider a group of n men and m women. How many ways can one form a committee of l people?

(b) Provide an algebraic proof by generalising the technique from the previous problem.

Part IV: Advanced Topics

28. ⋆ Multinomial Coefficients. The number of ways to partition a set of n distinct objects into m distinct groups of sizes $k_1, k_2, \ldots, k_m$ (where $\sum k_i = n$) is given by the multinomial coefficient:

$$\binom{n}{k_1, k_2, \ldots, k_m} = \frac{n!}{k_1!\, k_2! \cdots k_m!}.$$

(a) Justify this formula using a combinatorial argument.

(b) The **Multinomial Theorem** states that the coefficient of the term $x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m}$ in the expansion of $(x_1 + x_2 + \cdots + x_m)^n$ is this coefficient. Explain why this is true based on the combinatorial interpretation of polynomial expansion.

(c) Find the coefficient of a^2b^3c in the expansion of $(a+b+c)^6$.

29. ⋆ Let $D_{n,k}$ be the number of permutations of $\{1, 2, \ldots, n\}$ that have exactly k fixed points (a fixed point is an element i such that the permutation maps i to itself). Prove that $\sum_{k=0}^{n} k \cdot D_{n,k} = n!$.

Remark. Consider the sum over all $n!$ permutations. For each permutation, count its fixed points. Instead of summing by permutation, sum by element. For each element $i \in \{1, \ldots, n\}$, how many permutations have i as a fixed point?

30. ⋆⋆ The Elementary Symmetric Polynomial Identity. Recall from the previous chapter that $P_k(S)$ denotes the elementary symmetric polynomial of degree k in the variables of set S (the sum of all products of k distinct variables from S). Let $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_m\}$ be two disjoint sets of variables. We wish to prove the identity:

$$P_k(A \cup B) = \sum_{j=0}^{k} P_j(A) P_{k-j}(B).$$

(a) Consider a typical product term in the expansion of $P_k(A \cup B)$. This term is formed by choosing k distinct variables from the set $A \cup B$.

(b) Suppose that in such a product, exactly j variables are chosen from set A. How many variables must be chosen from set B?

(c) The sum of all such products (with j variables from A and $k-j$ from B) can be expressed as the product of two other symmetric polynomials. What are they?

(d) By summing over all possible values for j, construct the final identity.

7.5 Special Cases of Polynomial Products

The general formula for the product of n linear factors, Equation 5.10, includes many important identities as special cases.

Factors with Negative Terms

A particularly important case involves factors of the form $(x-a_i)$. The expansion of $(x-a_1)(x-a_2)\cdots(x-a_n)$ can be derived from Equation 5.10 by substituting each a_i with $-a_i$. The resulting coefficients are determined by the elementary symmetric polynomials in the quantities $-a_1, \ldots, -a_n$.

Let P_k now denote the sum of all products of the positive quantities $a_1, a_2, \ldots, a_n$ taken k at a time. When forming the coefficient of x^{n-k}, we are summing products of k terms, each of which is a $-a_i$. The product of k such terms is $(-1)^k$ times the product of the corresponding positive terms. Therefore, the coefficient of x^{n-k} becomes $(-1)^k P_k$. This gives the expansion:

$$(x-a_1)(x-a_2)\cdots(x-a_n) = x^n - P_1 x^{n-1} + P_2 x^{n-2} - \cdots + (-1)^n P_n. \tag{7.2}$$

Example 7.5.1. Expand $(x-a)(x-2a)(x-3a)(x-4a)$. Here, $n=4$ and the constants are $a_1 = a, a_2 = 2a, a_3 = 3a, a_4 = 4a$. We calculate the symmetric sums P_k for these positive constants:

- $P_1 = a + 2a + 3a + 4a = 10a$.
- $P_2 = (a)(2a) + (a)(3a) + (a)(4a) + (2a)(3a) + (2a)(4a) + (3a)(4a)$
  $= (2+3+4+6+8+12)a^2 = 35a^2$.
- $P_3 = (a)(2a)(3a) + (a)(2a)(4a) + (a)(3a)(4a) + (2a)(3a)(4a)$
  $= (6+8+12+24)a^3 = 50a^3$.
- $P_4 = (a)(2a)(3a)(4a) = 24a^4$.

Using Equation 7.2, the expansion is:

$$x^4 - (10a)x^3 + (35a^2)x^2 - (50a^3)x + (24a^4).$$

Connection to the Binomial Theorem

This special case provides an algebraic derivation of the Binomial Theorem, which we previously established using combinatorial arguments in Theorem 7.3.3. When all constants in the product $(x+a_1)(x+a_2)\cdots(x+a_n)$ are made equal, say $a_1 = a_2 = \cdots = a_n = a$, the product becomes $(x+a)^n$. The coefficients on the right-hand side, P_r, become the elementary symmetric polynomials in n variables that are all equal to a.

A general coefficient, P_r, is the sum of all possible products of r distinct constants. In this case, each such product is simply a^r. The number of such products is the number of ways to choose which r of the n factors to take the constant a from. From combinatorics, we know this quantity is given by the binomial coefficient $\binom{n}{r}$.

Remark. The notation $\binom{n}{r}$ is standard in modern mathematics. An older, but still common, notation for this quantity is ${}_nC_r$ or ${}^nC_r$, representing the number of 'Combinations' of r items from n. We shall adopt the ${}_nC_r$ notation henceforth.

Therefore, in this specialisation, $P_r = {}_nC_r a^r$.

Substituting this back into the general formula from Equation 5.10 gives:

$$(x+a)^n = x^n + {}_nC_1 a x^{n-1} + {}_nC_2 a^2 x^{n-2} + \cdots + {}_nC_n a^n.$$

This confirms the Binomial Theorem from an algebraic standpoint. By convention ${}_nC_0 = 1$, so we may write the theorem symmetrically as:

$$(x+a)^n = \sum_{r=0}^{n} {}_nC_r a^r x^{n-r}.$$

From this, a number of useful identities can be derived by substitution.

$$(x-a)^n = x^n - {}_nC_1 a x^{n-1} + {}_nC_2 a^2 x^{n-2} - \cdots + (-1)^n {}_nC_n a^n \tag{7.3}$$

$$(x+1)^n = x^n + {}_nC_1 x^{n-1} + {}_nC_2 x^{n-2} + \cdots + {}_nC_n \tag{7.4}$$

$$(x-1)^n = x^n - {}_nC_1 x^{n-1} + {}_nC_2 x^{n-2} - \cdots + (-1)^n {}_nC_n \tag{7.5}$$

While the distributive law is the foundation of multiplication, certain schemes can help organise the calculation for complex polynomials.

7.5.1 Long Multiplication

This method consists of multiplying one polynomial by each term of the other, starting from the lowest power and proceeding to the highest, arranging the partial products so that like powers of the variable are aligned in the same vertical column.

Example 7.5.2. To distribute $(x^3 + 2x^2 + 2x + 1)(x^2 - x + 1)$:

$$\begin{array}{rrrrrr}
 & & & x^3 & +2x^2 & +2x & +1 \\
\times & & & x^2 & -x & +1 \\
\hline
 & & & x^3 & +2x^2 & +2x & +1 \\
 & & -x^4 & -2x^3 & -2x^2 & -x & \\
 & x^5 & +2x^4 & +2x^3 & +x^2 & & \\
\hline
 & x^5 & +x^4 & +x^3 & +x^2 & +x & +1
\end{array}$$

Example 7.5.3. To distribute $(px^2 + qx + r)(rx^2 + qx + p)$:

$$\begin{array}{rrrrrr}
 & & & px^2 & +qx & +r \\
 & & \times & rx^2 & +qx & +p \\
\hline
 & & & p^2x^2 & +pqx & +pr \\
 & & pqx^3 & +q^2x^2 & +qrx & \\
 & prx^4 & +qrx^3 & +r^2x^2 & & \\
\hline
 & prx^4 & +(pq+qr)x^3 & +(p^2+q^2+r^2)x^2 & +(pq+qr)x & +pr
\end{array}$$

Method of Detached Coefficients

When multiplying two polynomials in a single variable where all powers are present, labour can be saved by writing only the coefficients. The powers of the variable can be inserted at the end, as the highest power in the product is the product of the highest powers in the factors. Missing terms must be included with a zero coefficient.

Example 7.5.4. For $(x^3 + 2x^2 + 2x + 1)(x^2 - x + 1)$:

$$\begin{array}{rrrrrr}
 & & 1 & +2 & +2 & +1 \\
\times & & 1 & -1 & +1 & \\
\hline
 & & 1 & +2 & +2 & +1 \\
 & -1 & -2 & -2 & -1 & \\
 & 1 & +2 & +2 & +1 & \\
\hline
 & 1 & +1 & +1 & +1 & +1
\end{array}$$

The product starts with $x^{3+2} = x^5$. Thus the result is $x^5 + x^4 + x^3 + x^2 + x + 1$.

For $(px^2 + qx + r)(rx^2 + qx + p)$:

$$\begin{array}{rrrrr}
 & & p & +q & +r \\
 & \times & r & +q & +p \\
\hline
 & & p^2 & +pq & +pr \\
 & pq & +q^2 & +qr & \\
pr & +qr & +r^2 & & \\
\hline
pr & +(pq+qr) & +(p^2+q^2+r^2) & +(pq+qr) & +pr
\end{array}$$

The brackets in the sum are essential to group the coefficients of like powers. The highest power is $x^{2+2} = x^4$, yielding the same result as before.

Example 7.5.5. To calculate $(x^4-2x^2+1)(x^4+2x^2+1)$ by detached coefficients: We write the polynomials as having coefficients $(1, 0, -2, 0, 1)$ and $(1, 0, 2, 0, 1)$.

$$\begin{array}{rrrrrrrrr}
 & & & & 1 & 0 & -2 & 0 & 1 \\
\times & & & & 1 & 0 & 2 & 0 & 1 \\
\hline
 & & & & 1 & 0 & -2 & 0 & 1 \\
 & & & 0 & 0 & 0 & 0 & 0 & \\
 & & 2 & 0 & -4 & 0 & 2 & & \\
 & 0 & 0 & 0 & 0 & 0 & & & \\
1 & 0 & -2 & 0 & 1 & & & & \\
\hline
1 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 1
\end{array}$$

The highest power is x^8, so the result is $x^8 - 2x^4 + 1$. While correct, this method is less efficient here than using the difference of squares identity:

$$\begin{aligned}((x^4+1)-2x^2)((x^4+1)+2x^2) &= (x^4+1)^2 - (2x^2)^2 \\ &= (x^8+2x^4+1) - 4x^4 \\ &= x^8 - 2x^4 + 1.\end{aligned}$$

The method is also effective for homogeneous polynomials in two variables.

Note. A polynomial is called **homogeneous** if all its terms are of the same degree. The degree of a term is the sum of the exponents of all its variables. For example, $x^2 + 3xy + y^2$ is homogeneous of degree 2. The polynomial $ax^3 + bxy^2 + cyz^2$ is homogeneous of degree 3 in variables x, y, z (assuming a, b, c are constants). Conversely, $x^3 + y^2$ is not homogeneous as its terms have different degrees.

Example 7.5.6. For $(x^2 - xy + y^2)(x^3 - 2x^2y + 2xy^2 - y^3)$:

$$\begin{array}{rrrrrr}
 & & 1 & -2 & 2 & -1 \\
\times & & & 1 & -1 & 1 \\
\hline
 & & 1 & -2 & 2 & -1 \\
 & -1 & 2 & -2 & 1 & \\
1 & -2 & 2 & -1 & & \\
\hline
1 & -3 & 5 & -5 & 3 & -1
\end{array}$$

The highest power of x is x^5 and the terms follow a pattern of decreasing powers of x and increasing powers of y. Result: $x^5 - 3x^4y + 5x^3y^2 - 5x^2y^3 + 3xy^4 - y^5$.

An Addition Rule for Calculating Binomial Coefficients

The method of detached coefficients provides an elegant way to generate the binomial coefficients of successive orders. We compute the coefficients of $(x + 1)^n$ for $n = 2, 3, 4, \ldots$ by repeated multiplication by $(x + 1)$,

whose coefficients are $1, 1$. The coefficients of $(x+1)^1$ are $1, 1$. To find $(x+1)^2$:

$$\begin{array}{cccc} & & 1 & 1 \\ + & 1 & 1 & \\ \hline & 1 & 2 & 1 \end{array}$$

To find $(x+1)^3$:

$$\begin{array}{cccc} & & 1 & 2 & 1 \\ + & 1 & 2 & 1 & \\ \hline & 1 & 3 & 3 & 1 \end{array}$$

The rule that emerges is that to obtain the coefficients of order $n+1$ from those of order n, one writes down the coefficients of order n and then below them, shifted one place to the right, writes them down again, and adds the columns. This forms a triangular array known as Pascal's Triangle, shown in Figure 7.5.

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & 1 & & 1 & & & \\ & & 1 & & 2 & & 2 & & \\ & 1 & & 3 & & 3 & & 1 & \\ 1 & & 4 & & 6 & & 4 & & 1 \end{array}$$

$$_3C_0 +_3 C_1 =_4 C_1 \implies 1+3=4$$

Figure 7.5: Pascal's Triangle, showing how each entry is the sum of the two entries directly above it.

This can be used to reconfirms Pascal's Identity.

***Theorem* 7.5.1. (Pascal's Rule)**. The binomial coefficients satisfy the relation

$$_{n+1}C_r = {}_nC_{r-1} + {}_nC_r.$$

Proof. *We prove this law is general by induction. Suppose we have the expansion for* $(x+1)^n$ *from Equation 7.4:*

$$(x+1)^n = x^n + {}_nC_1x^{n-1} + {}_nC_2x^{n-2} + \cdots + {}_nC_n.$$

Then $(x+1)^{n+1} = (x+1)^n(x+1)$. *Using detached coefficients:*

$$\begin{array}{ccccccc} & & 1 & +{}_nC_1 & +\ldots & +{}_nC_{n-1} & +{}_nC_n \\ + & 1 & +{}_nC_1 & +{}_nC_2 & +\ldots & +{}_nC_n & \\ \hline & 1 & +(1+{}_nC_1) & +({}_nC_1+{}_nC_2) & +\ldots & +({}_nC_{n-1}+{}_nC_n) & +{}_nC_n \end{array}$$

The coefficients for $(x+1)^{n+1}$ *are therefore* $1, 1+{}_nC_1, {}_nC_1+{}_nC_2, \ldots$.
Let the coefficients of $(x+1)^{n+1}$ *be denoted by* $_{n+1}C_r$. *Comparing the terms, we see that:*

- $_{n+1}C_0 = 1 = {}_nC_0$
- $_{n+1}C_1 = 1 + {}_nC_1 = {}_nC_0 + {}_nC_1$
- $_{n+1}C_2 = {}_nC_1 + {}_nC_2$
- $\ldots$
- $_{n+1}C_r = {}_nC_{r-1} + {}_nC_r$ *for* $r > 0$
- $_{n+1}C_{n+1} = {}_nC_n$

This confirms that the coefficients follow the general rule derived from Pascal's triangle, proving the formula by induction. ■

Remark. It should be easy to see that $(x+1)^0$ exists.

7.5.2 Generalised Addition Rule

We saw how Pascal's Triangle offers a shortcut for calculating the coefficients of $(x+1)^n$. This is a specific instance of a broader principle for finding the powers of polynomials like $(x^k + x^{k-1} + \cdots + 1)$. This method is not for multiplying two different polynomials; it is a fast way to find the coefficients of $(x^k + \cdots + 1)^p$ by building upon the coefficients of $(x^k + \cdots + 1)^{p-1}$.

The rule arises directly from the process of long multiplication with detached coefficients. Let's see how the coefficients of $(x^3 + x^2 + x + 1)^2$ are formed. The coefficients of $(x^3 + x^2 + x + 1)^1$ are $(1, 1, 1, 1)$. The square is thus:

$$\begin{array}{cccccccc}
 & & & 1 & 1 & 1 & 1 \\
 & \times & & 1 & 1 & 1 & 1 \\
\hline
 & & & 1 & 1 & 1 & 1 \\
 & & 1 & 1 & 1 & 1 & \\
 & 1 & 1 & 1 & 1 & & \\
1 & 1 & 1 & 1 & & & \\
\hline
1 & 2 & 3 & 4 & 3 & 2 & 1
\end{array}$$

Look at how the final coefficients are formed by summing the columns. For example, the fourth coefficient of the result (the number 4) is the sum of the four 1s aligned in that column. Each of these 1s comes from one of the four shifted rows. This gives us the shortcut: because our multiplier polynomial, $x^3 + x^2 + x + 1$, has four terms, each new coefficient is the sum of a "window" of four consecutive coefficients from the previous power.

The Figure 7.6 illustrates this process for generating the coefficients of the 3rd power from those of the 2nd power.

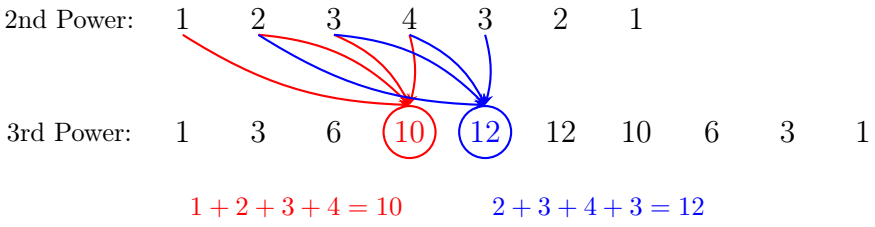


Figure 7.6: Generating coefficients for $(x^3 + x^2 + x + 1)^3$. Each new coefficient is the sum of the four coefficients ending at that position in the row above.

Example 7.5.7. To calculate the coefficients for powers of $F(x) = x^3 + x^2 + x + 1$:

Power												
1st	1	1	1	1								
2nd	1	2	3	4	3	2	1					
3rd	1	3	6	10	12	12	10	6	3	1		
4th	1	4	10	20	31	40	44	40	31	20	10	4	1

Thus $F(x)^4 = x^{12} + 4x^{11} + 10x^{10} + 20x^9 + 31x^8 + 40x^7 + 44x^6 + 40x^5 + 31x^4 + 20x^3 + 10x^2 + 4x + 1$.

The rule is general: to find the coefficients of the powers of $x^k + x^{k-1} + \cdots + 1$, you sum a sliding window of $k+1$ coefficients from the previous power.

Example 7.5.8. To calculate the coefficients for powers of $2x^2 + 3x + 1$: When the polynomial's coefficients are not all 1, the rule becomes a weighted sum. The weights are simply the coefficients of the polynomial itself. For $2x^2 + 3x + 1$, the coefficients are $(2, 3, 1)$.

To find the coefficients of the next power, the r-th new coefficient is calculated by multiplying the old coefficients by the weights $(2, 3, 1)$ in a sliding window, as shown in the long multiplication process. The r-th new coefficient is:

$$(\mathbf{1} \times \text{old coeff at pos } r) + (\mathbf{3} \times \text{old coeff at pos } r-1) + (\mathbf{2} \times \text{old coeff at pos } r-2)$$

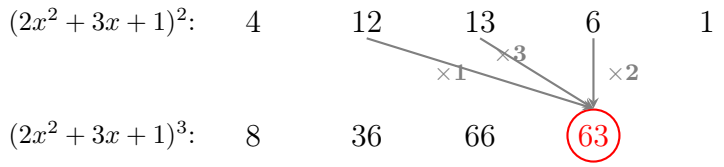


Figure 7.7: Generating coefficients for $(2x^2+3x+1)^3$.

This is visualised in Figure 7.7.

Power							
1st	2	3	1				
2nd	4	12	13	6	1		
3rd	8	36	66	63	33	9	1

Example 7.5.9. To calculate the coefficients for powers of x^2-x+1: The coefficients are $(1,-1,1)$. The rule for the r-th new coefficient is a weighted sum with weights $(1,-1,1)$:

$$(\mathbf{1}\times \text{old}_r) + (-\mathbf{1}\times \text{old}_{r-1}) + (\mathbf{1}\times \text{old}_{r-2})$$

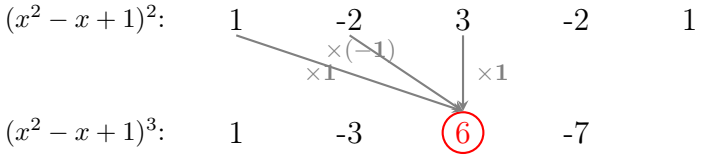


Figure 7.8: Generating coefficients for $(x^2-x+1)^3$ with alternating weights.

Power							
1st	1	−1	1				
2nd	1	−2	3	−2	1		
3rd	1	−3	6	−7	6	−3	1

7.5.3 Standard Product Formulae

Certain product forms appear frequently in algebra. The student may have already verified some of the following identities for specific cases. We can use the method of detached coefficients to provide a concise proof that these patterns hold for a general integer exponent n.

For any integer $n \geq 1$,

$$(x-y)(x^{n-1}+x^{n-2}y+\cdots+xy^{n-2}+y^{n-1}) = x^n - y^n. \tag{7.6}$$

Proof. *The coefficients of the second factor are all 1. The multiplier is $x-y$, with detached coefficients $1,-1$. We multiply by -1, then by 1 shifted left.*

	1	1	…	1	1
×				1	−1
	−1	−1	…	−1	−1
1	1	1	…	1	
1	0	0	…	0	−1

The product has a leading term x^n and a final term $-y^n$, with all intermediate terms cancelling to zero. ■

If n is an odd integer,

$$(x+y)(x^{n-1}-x^{n-2}y+x^{n-3}y^2-\cdots+y^{n-1})=x^n+y^n. \tag{7.7}$$

Proof. The coefficients of the second factor alternate $1,-1,1,\ldots$. Since n is odd, $n-1$ is even, so there is an odd number of terms, starting and ending with $+1$. The multiplier has coefficients $1,1$.

$$\begin{array}{rccccc} & 1 & -1 & \ldots & -1 & 1 \\ \times & & & & 1 & 1 \\ \hline & 1 & -1 & \ldots & -1 & 1 \\ 1 & -1 & 1 & \ldots & -1 & \\ \hline 1 & 0 & 0 & \ldots & 0 & 1 \end{array}$$

The result is x^n+y^n. ■

If n is an even integer,

$$(x+y)(x^{n-1}-x^{n-2}y+x^{n-3}y^2-\cdots-y^{n-1})=x^n-y^n. \tag{7.8}$$

Proof. Since n is even, $n-1$ is odd, so there is an even number of terms in the second factor. The coefficients are $1,-1,1,\ldots,1,-1$.

$$\begin{array}{rccccc} & 1 & -1 & \ldots & 1 & -1 \\ \times & & & & 1 & 1 \\ \hline & 1 & -1 & \ldots & 1 & -1 \\ 1 & -1 & 1 & \ldots & -1 & \\ \hline 1 & 0 & 0 & \ldots & 0 & -1 \end{array}$$

The result is x^n-y^n. ■

7.6 Exercises

Part I: Mechanical Multiplication

Remark. Practise the methods of long multiplication and detached coefficients until they become second nature. Pay close attention to signs and the placement of terms with missing powers.

1. Use the method of long multiplication to find the following products.

(a) $(x^2-3x+2)(x-4)$

(b) $(2a^2+5ab-b^2)(3a-2b)$

(c) $(y^3+2y^2-y+5)(y^2-3y-1)$

(d) $(p^4+p^2q^2+q^4)(p^2-q^2)$

2. Use the method of detached coefficients to find the products from the previous question. Remember to insert a zero for any missing powers.

3. Use detached coefficients to compute the following products.

(a) $(x^4-2x^3+x^2-5x+6)(x+2)$

(b) $(3z^5+2z^3-z^2-4)(z^2-z+3)$

(c) $(a^3-3a^2b+3ab^2-b^3)(a^2-2ab+b^2)$

(d) $(x^3 - 2x^2y + 4xy^2 - 8y^3)(x + 2y)$

4. Find the square of the polynomial $1 - 2x + 3x^2 - 4x^3$.

5. Find the cube of the polynomial $x^2 - x + 1$.

6. Use the addition rule demonstrated in Figure 7.5 to write out the first 8 rows of Pascal's Triangle. Use it to find the expansion of $(x + 1)^7$.

7. Use the generalised addition rule from Figure 7.6 to find the coefficients for the powers of $F(x) = x^2 + x + 1$.

(a) Find the coefficients for $F(x)^2$.

(b) Use the result from (a) to find the coefficients for $F(x)^3$.

(c) Use the result from (b) to find the coefficients for $F(x)^4$.

8. Use the weighted addition rule from Figure 7.7 to find the coefficients for the square and cube of the polynomial $2x^2 - x + 3$.

Part II: Application of Standard Formulae

Remark. These problems rely on recognising patterns that match the standard product formulae for $x^n \pm y^n$. Direct expansion is inefficient; the goal is to see the structure.

9. Write down the product of the following expressions without performing the full multiplication.

(a) $(a - 2b)(a^2 + 2ab + 4b^2)$

(b) $(x + 3)(x^4 - 3x^3 + 9x^2 - 27x + 81)$

(c) $(p^2 + q^2)(p^8 - p^6q^2 + p^4q^4 - p^2q^6 + q^8)$

(d) $(2x - y)(16x^4 + 8x^3y + 4x^2y^2 + 2xy^3 + y^4)$

10. Find the quotient of the following divisions by recognising the dividend as a standard form.

(a) $(x^5 - y^5) \div (x - y)$

(b) $(a^7 + 128) \div (a + 2)$

(c) $(x^6 - y^6) \div (x + y)$

(d) $(8p^3 + 27q^3) \div (2p + 3q)$

11. Let $P(x) = (x - a)(x - b)(x - c)$. Use the formula in Equation 7.2 to write the expansion. The coefficients should be written using the elementary symmetric polynomials in a, b, c. For example, the sum $a + b + c$ can be written as P_1 or Σa.

12. Use the result from the previous question to expand $(x - 1)(x - 2)(x - 5)$.

13. Expand $(x + 1)(x + 2)(x + 3)(x - 6)$.

Remark. It may be helpful to group the factors as $((x + 1)(x + 2)) \times ((x + 3)(x - 6))$ first.

14. Find the coefficient of x^3 in the product $(x-1)(x-2)(x-3)(x-4)(x-5)$ without computing the full expansion.

15. Show that $(a + b + c)(a + b - c)(a - b + c)(-a + b + c) = 2a^2b^2 + 2b^2c^2 + 2c^2a^2 - a^4 - b^4 - c^4$.

Part III: Proofs and Generalisations

16. Prove the identity $(a-b)^3+(b-c)^3+(c-a)^3 = 3(a-b)(b-c)(c-a)$.

Remark. Let $x = a-b, y = b-c, z = c-a$. What is the value of $x+y+z$? Recall the identity for $x^3+y^3+z^3-3xyz$.

17. Prove that $(x+y+z)^3-(x^3+y^3+z^3) = 3(x+y)(y+z)(z+x)$.

Remark. Expand the left-hand side. The result must be a homogeneous, symmetrical polynomial of degree 3. Find the coefficients of Σx^2y and xyz.

Note. Remember that $\Sigma x^2y = x^2y+x^2z+y^2x+y^2z+z^2x+z^2y$.

18. Prove that for any integer n, the expression $(n-1)n(n+1)$ is divisible by 6.

19. For the polynomial $F(x) = x^2+x+1$, we found the coefficients of its powers in question 7. Let $C(p,k)$ be the coefficient of x^k in the expansion of $F(x)^p$.

(a) Verify that the sum of the coefficients for $F(x)^p$ is 3^p.

(b) Prove that the sequence of coefficients is palindromic, i.e., $C(p,k) = C(p,2p-k)$.

20. If $x+y+z=0$, prove that $x^4+y^4+z^4 = 2(x^2y^2+y^2z^2+z^2x^2) = \frac{1}{2}(x^2+y^2+z^2)^2$.

21. ⋆ Use the method of detached coefficients to find the product of $P(x) = x^5-2x^4+x^3-3x+1$ and $Q(x) = 2x^4+3x^3-x^2+4x-5$.

22. ⋆ Prove the identity

$$(a^2+b^2+c^2)(x^2+y^2+z^2)-(ax+by+cz)^2 = (ay-bx)^2+(bz-cy)^2+(cx-az)^2.$$

Remark. This is Lagrange's Identity for $n=3$. Direct expansion is laborious. Consider using symmetry or a more structured approach.

23. ⋆ Let $P_k(n)$ be the sum of the products of the first n integers taken k at a time. For instance, for $n=3$, the integers are $\{1,2,3\}$ and $P_2(3) = 1\cdot2+1\cdot3+2\cdot3 = 11$. These are the coefficients in the expansion of $(x+1)(x+2)\cdots(x+n)$. Prove that

$$P_2(n) = \frac{n(n-1)(n+1)(3n+2)}{24}.$$

24. ⋆ The coefficients of $(x-1)^n$ alternate in sign. Use this fact and Equation 7.4 to prove that for any $n>0$, the sum of the binomial coefficients ${}_nC_r$ with r even is equal to the sum of the coefficients with r odd. That is,

$$\sum_{r \text{ even}} {}_nC_r = \sum_{r \text{ odd}} {}_nC_r.$$

Further, show that each of these sums is equal to 2^{n-1}.

25. ⋆ **(Exploration)** Let $S_n = (x+1)(x+2)\cdots(x+n)$.

(a) Write out the full expansions for S_1, S_2, S_3.

(b) The coefficients of these polynomials are known as the (unsigned) Stirling Numbers of the First Kind, denoted $\begin{bmatrix} n \\ k \end{bmatrix}$, the coefficient of x^{k-1} in S_{n-1}. Let us verify a recurrence relation. Show by direct computation from your expansions that

$$\begin{bmatrix} 4 \\ 3 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \end{bmatrix} + 3\begin{bmatrix} 3 \\ 3 \end{bmatrix}.$$

(c) Prove the general recurrence relation: $\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1)\begin{bmatrix} n-1 \\ k \end{bmatrix}$.

Remark. Consider how S_n is formed from S_{n-1}.

7.7 ⋆⋆ Homogeneity and Symmetry

Note. A-levels can ignore this topic once again, it does help understanding but it isn't necessary and thus a waste of your time studying for Alevel.

Remark. This has been introduced earlier but this section is more like a formal introduction to both.

As said earlier a polynomial is said to be homogeneous when the degree of every term in it is the same. The degree of the homogeneous polynomial is then the common degree of its terms. For example, the most general homogeneous polynomials of one, two, and three variables are as follows.

For two variables, x and y:

- 1st Degree: $Ax + By$
- 2nd Degree: $Ax^2 + Bxy + Cy^2$
- 3rd Degree: $Ax^3 + Bx^2y + Cxy^2 + Dy^3$

For three variables, x, y, and z:

- 1st Degree: $Ax + By + Cz$
- 2nd Degree: $Ax^2 + By^2 + Cz^2 + Dyz + Ezx + Fxy$
- 3rd Degree: $Ax^3 + By^3 + Cz^3 + Dy^2z + Eyz^2 + Fz^2x + Gzx^2 + Hx^2y + Ixy^2 + Jxyz$

Remark. Homogeneous polynomials are classified by the number of variables and their degree. A polynomial in two variables is binary, in three is ternary, etc. A polynomial of the second degree is quadric, of the third is cubic, and so on. Thus, $Ax^2 + Bxy + Cy^2$ is a binary quadric, and the third example for three variables above is a ternary cubic.

***Theorem* 7.7.1.** The number of terms in the most general homogeneous polynomial of degree n in three variables is

$$\frac{(n+1)(n+2)}{2}.$$

Proof. We may classify the terms of the polynomial according to the power of one variable, say x.

- *The terms that do not contain x are homogeneous of degree n in the variables y and z. There are $n+1$ such terms (of the form $y^n, y^{n-1}z, \ldots, z^n$).*
- *The terms that contain x to the first power are of the form $x \times$ (a term of degree $n-1$ in y, z). There are n such terms.*
- *The terms that contain x^2 are of the form $x^2 \times$ (a term of degree $n-2$ in y, z). There are $n-1$ such terms.*
- *This continues until we reach the term containing x^n, which is of the form $x^n \times$ (a term of degree 0 in y, z), of which there is only one.*

If N denotes the total number of terms, then

$$N = (n+1) + n + (n-1) + \cdots + 2 + 1 = \sum_{k=1}^{n+1} k = \sum_{k=1}^{n} k + (n+1) = \frac{(n+1)(n+2)}{2}.$$

■

Remark. We look at arithmetic series and such properly in the next notes (there is a reason for this).

Example 7.7.1. For $n = 3$, the formula gives $N = \frac{(3+1)(3+2)}{2} = \frac{4\times5}{2} = 10$. This matches the number of terms in the ternary cubic listed above.

Properties of Homogeneous Polynomials

Homogeneous polynomials possess a fundamental scaling property.

***Theorem* 7.7.2.** If $F(x, y, z, \dots)$ is a homogeneous polynomial of the n-th degree, and each variable is multiplied by a quantity ρ, the result is equivalent to multiplying the original polynomial by ρ^n.

Proof. Let a general term of the polynomial F be $Ax^p y^q z^r \dots$, where the sum of the powers is $p+q+r+\dots = n$. If we substitute $\rho x, \rho y, \rho z, \dots$ for the variables, this term becomes:

$$\begin{aligned} A(\rho x)^p(\rho y)^q(\rho z)^r \dots &= A(\rho^p x^p)(\rho^q y^q)(\rho^r z^r)\dots \\ &= A(\rho^p\rho^q\rho^r\dots)(x^p y^q z^r \dots) \\ &= A\rho^{p+q+r+\cdots}(x^p y^q z^r \dots) \\ &= A\rho^n(x^p y^q z^r \dots) \end{aligned}$$

Since this is true for every term in the polynomial, we can factor out the common ρ^n. The new polynomial F' is therefore

$$F'(\rho x, \rho y, \dots) = \rho^n F(x, y, \dots).$$

■

Example 7.7.2. . Consider the homogeneous polynomial $F(x, y) = 3x^2 - 2xy + y^2$ of degree 2. Substituting ρx and ρy:

$$\begin{aligned} 3(\rho x)^2 - 2(\rho x)(\rho y) + (\rho y)^2 &= 3\rho^2 x^2 - 2\rho^2 xy + \rho^2 y^2 \\ &= \rho^2(3x^2 - 2xy + y^2) = \rho^2 F(x, y). \end{aligned}$$

Remark. This scaling property is so fundamental that it can be used as the definition of a homogeneous function. The classification of functions by homogeneity was systematically introduced by Euler (1748). While we focus on polynomials, the concept can be extended to fractional functions, such as $\frac{x^3-y^3}{x+y}$, which is homogeneous of degree 2.

Homogeneous polynomials of the first degree have a special property related to linearity.

***Theorem* 7.7.3.** If $F(x, y, z)$ is a homogeneous polynomial of the first degree, then for any numbers $\lambda, \mu, x_1, y_1, z_1, x_2, y_2, z_2$,

$$F(\lambda x_1 + \mu x_2, \lambda y_1 + \mu y_2, \lambda z_1 + \mu z_2) = \lambda F(x_1, y_1, z_1) + \mu F(x_2, y_2, z_2).$$

Proof. A general homogeneous polynomial of the first degree is $F(x, y, z) = Ax + By + Cz$. Substituting the new expressions for the variables:

$$\begin{aligned} &A(\lambda x_1 + \mu x_2) + B(\lambda y_1 + \mu y_2) + C(\lambda z_1 + \mu z_2) && \\ &= A\lambda x_1 + A\mu x_2 + B\lambda y_1 + B\mu y_2 + C\lambda z_1 + C\mu z_2 && \textit{Distributive Law} \\ &= (A\lambda x_1 + B\lambda y_1 + C\lambda z_1) + (A\mu x_2 + B\mu y_2 + C\mu z_2) && \textit{Commutative Law} \\ &= \lambda(Ax_1 + By_1 + Cz_1) + \mu(Ax_2 + By_2 + Cz_2) && \textit{Factorisation} \\ &= \lambda F(x_1, y_1, z_1) + \mu F(x_2, y_2, z_2) && \end{aligned}$$

■

Law of Homogeneity for Products

There is an important law governing the multiplication of homogeneous polynomials.

***Theorem* 7.7.4. (Law of Homogeneity)**. The product of two homogeneous polynomials, of the m-th and n-th degrees respectively, is a homogeneous polynomial of the $(m + n)$-th degree.

Proof. Let P_1 be a homogeneous polynomial of degree m and P_2 be one of degree n. Any term in the product $P_1 \times P_2$ is formed by multiplying a term from P_1 by a term from P_2. Let a term from P_1 have degree m and a term from P_2 have degree n. The degree of their product is the sum of their degrees, which is $m+n$. Since every term in the distributed product is formed in this way, every term has degree $m+n$. The product is therefore a homogeneous polynomial of degree $m+n$. ■

This rule provides a valuable check on algebraic multiplication. If any term in the result of multiplying two homogeneous polynomials has a degree other than the sum of the factors' degrees, a mistake has been made.

General Polynomials

The concept of homogeneity allows us to precisely define the most general type of polynomial. A general polynomial of the n-th degree is not required to be homogeneous. It may contain terms of any degree up to and including n.

The most general polynomial of the n-th degree in a set of variables is the sum of the most general homogeneous polynomials of degrees $0, 1, 2, \ldots, n$ in those variables.

Example 7.7.3. . The most general polynomial of the third degree in x and y is the sum of the general homogeneous polynomials of degrees 0, 1, 2, and 3:

$$\underbrace{A}_{\text{deg 0}} + \underbrace{(Bx + Cy)}_{\text{deg 1}} + \underbrace{(Dx^2 + Exy + Fy^2)}_{\text{deg 2}} + \underbrace{(Gx^3 + Hx^2y + Ixy^2 + Jy^3)}_{\text{deg 3}}.$$

The number of terms in a general polynomial of degree n in two variables is the sum of the number of terms in the constituent homogeneous polynomials. The number of terms in a homogeneous polynomial of degree k in two variables is $k+1$. Therefore, the total number of terms is:

$$\sum_{k=0}^{n}(k+1) = (0+1) + (1+1) + \ldots + (n+1) = 1 + 2 + \ldots + n + 1 = \frac{(n+1)(n+2)}{2}.$$

Note. For the above sum we can also shift indices. Suppose we want to start at 1 instead of 0 in our sum above. First we make a new index j such that $j = k+1$. This is just a relabelling, so the sum's value doesn't change—only the name of the counter and its limits do. Track the bounds:

k	0	1	$\cdots$	n
$j = k+1$	1	2	$\cdots$	$n+1$

Inside the summand, $k+1$ becomes j. The limits move exactly as the table shows. So

$$\sum_{k=0}^{n}(k+1) \xrightarrow{j=k+1} \sum_{j=1}^{n+1} j,$$

which now starts at 1. (If you like, rename j back to k at the end).

If you're fussy about the upper limit staying n, peel off the first (or last) term:

$$\begin{aligned}\sum_{k=0}^{n}(k+1) &= \underbrace{1}_{k=0} + \sum_{k=1}^{n}(k+1) \\ &= 1 + \left(\sum_{k=1}^{n} k + \sum_{k=1}^{n} 1\right) \\ &= \left(\frac{n(n+1)}{2} + n\right) + 1 = \frac{(n+1)(n+2)}{2}.\end{aligned}$$

7.7.1 Symmetry

We have previously introduced the concept of a symmetrical polynomial, one which remains unaltered by the interchange of any two of its variables. We now explore the consequences of this property, its structure, and its application in simplifying algebraic work.

Forms and Properties of Symmetrical Polynomials

A polynomial may be symmetrical with respect to some, but not all, of its variables. For example, $2a+3b+3c$ is symmetrical with respect to b and c, but not with respect to a and b. Our primary focus, however, is on polynomials that are symmetrical with respect to all their variables.

The condition of symmetry imposes strict constraints on the coefficients of a polynomial. Any terms that can be transformed into one another by interchanging variables must have the same coefficient. Such terms form a symmetrical group, or type, which can be expressed compactly using the Σ notation.

For the general symmetrical homogeneous polynomials in two variables, x and y:

- 1st Degree: $A(x+y)$, or $A\Sigma x$.
- 2nd Degree: $A(x^2+y^2)+Bxy$, or $A\Sigma x^2+Bxy$.
- 3rd Degree: $A(x^3+y^3)+B(x^2y+xy^2)$, or $A\Sigma x^3+B\Sigma x^2y$.

For three variables, x, y, z:

- 1st Degree: $A(x+y+z)$, or $A\Sigma x$.
- 2nd Degree: $A(x^2+y^2+z^2)+B(xy+yz+zx)$, or $A\Sigma x^2+B\Sigma xy$.
- 3rd Degree: $A\Sigma x^3+B\Sigma x^2y+Cxyz$.

The most general symmetrical polynomial of a given degree is thus the sum of the general symmetrical homogeneous polynomials of all degrees up to and including that degree, plus a constant.

Remark. A related class of polynomials are alternating polynomials, which change their sign but are otherwise unaltered when any two variables are interchanged. A classic example is $(x-y)(y-z)(z-x)$. The product or quotient of two alternating polynomials is a symmetrical polynomial.

The Rule of Symmetry

From the definition of symmetry, a simple but powerful rule follows.

***Theorem* 7.7.5. (Rule of Symmetry)**. The algebraic sum, product, or quotient of two symmetrical polynomials is a symmetrical polynomial.

Proof. Let P_1 and P_2 be two symmetrical polynomials in the same variables. Let the result of interchanging any two variables be denoted by a prime (e.g., P_1'). By definition, $P_1' = P_1$ and $P_2' = P_2$. The sum is (P_1+P_2). After interchange, it becomes $P_1'+P_2' = P_1+P_2$. The product is (P_1P_2). After interchange, it becomes $P_1'P_2' = P_1P_2$. Thus, the sum and product are also symmetrical. The same logic applies to the quotient. ■

Remark. The product of two asymmetrical polynomials is not necessarily asymmetrical. For instance, a^2bc and ab^2c^2 are both asymmetrical in $\{a,b,c\}$, but their product, $a^3b^3c^3$, is symmetrical.

Application in Shortening Calculations

The rule of symmetry is an excellent tool for abbreviating algebraic work. If we know the product of two symmetrical polynomials must be symmetrical, we need not calculate every term in the expansion. We need only find the coefficient of one term from each symmetrical group; the coefficients of all other terms in that group are then known.

Example 7.7.4. Expand the product $(a+b+c)(a^2+b^2+c^2-ab-bc-ca)$. Both factors are symmetrical in $\{a,b,c\}$, so the product must also be symmetrical. We can determine the entire expansion by finding the coefficients of just a few representative terms. The types of terms that can appear in the product are a^3, a^2b, and abc.

1. *Terms of the type a^3:* The term a^3 can only be formed by multiplying a from the first factor by a^2 from the second. The coefficient is $1 \times 1 = 1$. Since the product is symmetrical, the terms b^3 and c^3 must also appear with a coefficient of 1. This gives the part of the result: $a^3+b^3+c^3$.
2. *Terms of the type a^2b:* The term a^2b can be formed in two ways: by multiplying a from the first factor with the term containing ab from the second, or by multiplying b from the first factor with a^2 from the second.
   - $(a) \times (-ab) = -a^2b$
   - $(b) \times (a^2) = +a^2b$

   The sum of the coefficients is $-1+1=0$. Therefore, the term a^2b does not appear in the final product. By symmetry, none of the other terms in its group (Σa^2b) will appear either.
3. *Terms of the type abc:* This term can be formed in three ways:
   - $(a) \times (-bc) = -abc$
   - $(b) \times (-ca) = -abc$
   - $(c) \times (-ab) = -abc$

   The sum of the coefficients is $-1-1-1=-3$.

Combining these results, we find the complete product without performing the full nine-term multiplication:

$$(a+b+c)(a^2+b^2+c^2-ab-bc-ca) = a^3+b^3+c^3-3abc.$$

The Principle of Indeterminate Coefficients

The coefficients of a polynomial are, by definition, independent of the variables. If an algebraic identity involving polynomials holds true for all values of the variables, it must hold for any specific values we choose to substitute. This fact allows for a powerful method for determining unknown coefficients in an expansion.

Remark. This technique is often called the principle of indeterminate coefficients, though the name is not entirely descriptive. The coefficients are unknown, but they are fixed constants which we seek to determine.

The method involves first assuming the general form of the result, guided by principles like homogeneity and symmetry. This general form will contain unknown, or 'indeterminate', coefficients. By substituting judiciously chosen values for the variables, we create a system of equations that can be solved to find these coefficients once for all.

Example 7.7.5. We seek to expand $(x+y)^2$.

By the laws of homogeneity and symmetry, the product must be a symmetrical, homogeneous polynomial of the second degree in x and y. The most general form for such a polynomial is $Ax^2+Bxy+Ay^2$. We thus have the identity:

$$(x+y)^2 = Ax^2+Bxy+Ay^2.$$

This identity must hold for any values of x and y.

- To find A, we select values that eliminate the other term. Let $x = 1$ and $y = 0$:

$$(1+0)^2 = A(1)^2 + B(1)(0) + A(0)^2$$
$$1 = A.$$

- The identity is now $(x+y)^2 = x^2 + Bxy + y^2$. To find B, we can use any other pair of values. Let $x = 1$ and $y = 1$:

$$(1+1)^2 = (1)^2 + B(1)(1) + (1)^2$$
$$4 = 1 + B + 1$$
$$B = 2.$$

Thus, the expansion is $(x+y)^2 = x^2 + 2xy + y^2$.

The choice of particular cases is a matter of convenience; any set of values will work, provided enough are taken to determine all coefficients. Strategic choices, such as using 0 or 1, can isolate coefficients one at a time and simplify the calculation.

Example 7.7.6. Let us re-establish the identity for the product $(x+y+z)(x^2+y^2+z^2-yz-zx-xy)$. Both factors are homogeneous and symmetrical. The first is of degree 1, the second of degree 2. Their product must be a homogeneous, symmetrical polynomial of degree 3. Using the shorthand from our earlier discussion on symmetry, the most general form is $A\Sigma x^3 + B\Sigma x^2 y + Cxyz$.

$$(x+y+z)(\Sigma x^2 - \Sigma xy) = A\Sigma x^3 + B\Sigma x^2 y + Cxyz.$$

- Let $x = 1, y = 0, z = 0$. The identity becomes:

$$(1)(1^2 - 0 - 0) = A(1^3) + B(0) + C(0)$$
$$1 = A.$$

- Now with $A = 1$, let $x = 1, y = 1, z = 0$:

$$(1+1)(1^2+1^2-1-0-0) = (1^3+1^3) + B(1^2 \cdot 1 + 1 \cdot 1^2) + C(0)$$
$$(2)(1) = 2 + B(2)$$
$$2 = 2 + 2B \implies B = 0.$$

- Finally, with $A = 1$ and $B = 0$, let $x = 1, y = 1, z = 1$:

$$(1+1+1)(1+1+1-1-1-1) = (1+1+1) + B(\dots) + C(1)$$
$$(3)(0) = 3 + 0 + C$$
$$0 = 3 + C \implies C = -3.$$

The product is $\Sigma x^3 - 3xyz$, which is $x^3 + y^3 + z^3 - 3xyz$, confirming our earlier result derived by tracking term types.

7.8 Exercises

Note. These Exercises are for those who want to do them, if you are Alevel you may skip them.

Part I: Definitions and Identification

Remark. These questions are designed to test your understanding of the core definitions. Focus on precision: what is the degree? What are the variables? Is it homogeneous, symmetrical, or both?

1. For each of the following polynomials, state whether it is homogeneous. If it is, provide its degree. The variables are x, y, z.

(a) $5x^3 - 2x^2y + 7xy^2 - y^3$

(b) $a^2x^2 + b^2y^2 + c^2z^2$

(c) $4x^2y + 3xy - 2y^2$

(d) $x + y + z + 1$

(e) $xyz + x^2y + y^2z + z^2x$

2. For each of the following polynomials, state whether it is symmetrical with respect to the variables a, b, c.

(a) $a^2 + b^2 + c^2 - abc$

(b) $a^3 + b^3 - c^3$

(c) $(a - b)^2 + (b - c)^2 + (c - a)^2$

(d) $a^2b + b^2c + c^2a$

(e) $(a + b)(b + c)$

3. Write down the most general homogeneous polynomial of the fourth degree in two variables, x and y. How many terms does it contain?

4. Write down the most general *symmetrical* homogeneous polynomial of the fourth degree in two variables, x and y.

5. Use the formula from the text to determine the number of terms in the most general homogeneous polynomial of degree 5 in three variables.

6. How many terms are there in the most general (non-homogeneous) polynomial of degree 4 in two variables?

7. Classify the following polynomials using the terminology from the text (e.g., binary cubic).

(a) $Ax^4 + Bx^3y + Cx^2y^2 + Dxy^3 + Ey^4$

(b) $Ax^2 + By^2 + Cz^2 + Dyz + Ezx + Fxy$

8. Express the polynomial $(a + b + c)(ab + bc + ca)$ using the Σ notation for symmetrical groups.

9. Expand the expression $\Sigma a^2(b - c)$ for the variables $\{a, b, c\}$. Is the resulting polynomial symmetrical?

10. A polynomial is called *cyclic* if it remains unchanged after replacing $x \to y$, $y \to z$, and $z \to x$. Is the polynomial $x^2(y - z) + y^2(z - x) + z^2(x - y)$ symmetrical or cyclic? Justify your answer.

Part II: Applying the Rules of Homogeneity and Symmetry

11. Let $F(x, y) = 2x^3 - 5x^2y + 3y^3$.

(a) Verify by direct calculation that $F(10x, 10y) = 10^3F(x, y)$.

(b) If you know $F(1, 2) = -16$, what is the value of $F(3, 6)$?

12. Let P_1 be a homogeneous polynomial of degree 3 and P_2 be a homogeneous polynomial of degree 4. What is the degree of their product, P_1P_2? If P_1 is also symmetrical, and P_2 is also symmetrical, what can you say about their product?

13. Decompose the polynomial $F(x, y) = x^3 + 2x^2 - 3xy + 4y^2 + 5x - 6y + 7$ into its homogeneous parts.

14. Is the rational function $F(x, y, z) = \frac{x^4+y^4}{x^2+z^2}$ homogeneous? If so, what is its degree?

15. If $F(x, y, z)$ and $G(x, y, z)$ are both homogeneous polynomials, is their sum $F + G$ necessarily homogeneous? Provide a proof or a counterexample.

16. An alternating polynomial is one that changes sign when any two variables are interchanged. Let $A(x, y) = x - y$ and $S(x, y) = x^2 + y^2$. Show that $A(x, y)$ is alternating and $S(x, y)$ is symmetrical. Is their product $A \cdot S$ alternating, symmetrical, or neither?

17. If A_1 and A_2 are two alternating polynomials, what can you say about their product A_1A_2? Justify your answer.

18. The polynomial $x^3 + y^3 + z^3 - 3xyz$ is symmetrical. What is the sum of its coefficients?

19. For the variables $\{x, y, z\}$, write the symmetrical polynomial represented by $A\Sigma x^3 + B\Sigma x^2y + Cxyz$ for $A = 2, B = -1, C = 5$.

20. What is the degree of the polynomial $(\Sigma a)^3$ for variables $\{a, b, c\}$?

Part III: Techniques for Expansion and Simplification

Remark. For these problems, avoid brute-force multiplication. Use the principles of symmetry and indeterminate coefficients to find the answer efficiently.

21. Use the rule of symmetry (tracking term types) to expand $(x + y + z)(xy + yz + zx)$.

22. Use the rule of symmetry to expand $(a + b + c)^2 - (a^2 + b^2 + c^2)$.

23. Find the product $(a - b + c)(a + b - c)$ using symmetry.

Remark. The polynomial is not fully symmetrical in $\{a, b, c\}$, but it is symmetrical in $\{b, c\}$.

24. Expand $(x + y)(y + z)(z + x)$.

25. Use the principle of indeterminate coefficients to find the expansion of $(x + y)^3$. Assume the result is of the form $A(x^3 + y^3) + B(x^2y + xy^2)$.

26. Use indeterminate coefficients to find the expansion of $(x + y + z)^2$. Assume the result is of the form $A\Sigma x^2 + B\Sigma xy$.

27. Find the expansion of $(x - y - z)^2$.

Remark. Let $a = x, b = -y, c = -z$ and use the known result for $(a + b + c)^2$.

28. Find the values of A, B, C in the identity:

$$(x + y)(y + z)(z + x) = A(x + y + z)(xy + yz + zx) + Bxyz.$$

29. Determine the coefficients A and B in the identity

$$(a^2 + b^2)(x^2 + y^2) = (ax - by)^2 + (Ay + Bx)^2.$$

30. Find the sum of the coefficients in the expansion of $(a + b - 2c)^3$.

Part IV: Proofs and Challenge Problems

31. Prove that the number of terms in the most general homogeneous polynomial of degree n in two variables is $n + 1$.

32. Prove that any polynomial $P(x, y)$ can be written as the sum of a symmetrical polynomial and an alternating polynomial.

Remark. Consider the expressions $P(x,y)+P(y,x)$ and $P(x,y)-P(y,x)$.

33. Use the rule of symmetry to prove the identity:

$$(a+b)^2+(b+c)^2+(c+a)^2-(a+b+c)^2=a^2+b^2+c^2.$$

34. If $F(x,y,z)$ is a homogeneous polynomial, prove that the polynomial obtained by substituting $x=u+v$, $y=u-v$, $z=w$ is also homogeneous. What is its degree?

35. Prove that for variables $\{x,y,z\}$, $\Sigma x\cdot\Sigma x^2=\Sigma x^3+\Sigma x^2y$.

36. ⋆ Prove that the number of terms in the most general symmetrical homogeneous polynomial of degree n in three variables is equal to the number of ways to partition the integer n into at most three parts.

37. ⋆ Let $s_1=x+y+z$, $s_2=xy+yz+zx$, $s_3=xyz$. Prove the identity:

$$x^3+y^3+z^3=s_1^3-3s_1s_2+3s_3.$$

Remark. Use indeterminate coefficients. Assume $x^3+y^3+z^3=As_1^3+Bs_1s_2+Cs_3$. Substitute values for x,y,z to find A,B,C.

38. ⋆ Prove Euler's identity for four variables:

$$(a+b+c+d)^3=\Sigma a^3+3\Sigma a^2b+6\Sigma abc.$$

Remark. Do not expand fully. Use symmetry to identify the term types $(\Sigma a^3,\Sigma a^2b,\Sigma a^2bc,\Sigma abcd)$ and find their coefficients by tracking how they can be formed.

39. ⋆ The polynomial $F(x,y,z)=x^3+y^3+z^3-3xyz$ has a special property. Show that it can be factored into

$$(x+y+z)(x^2+y^2+z^2-xy-yz-zx).$$

Use this result to find the factors of $G(a,b,c)=a^6+b^6+c^6-3a^2b^2c^2$ by setting $x=a^2,y=b^2,z=c^2$. Verify that $G(a,b,c)$ is a homogeneous polynomial of degree 6, and check if its factors are also homogeneous.

40. ⋆ Let ω be a number such that $\omega^2+\omega+1=0$. Prove that

$$(x+y+z)(x+\omega y+\omega^2z)(x+\omega^2y+\omega z)=x^3+y^3+z^3-3xyz.$$

Remark. Expand the second and third factors first. The properties of ω will cause many terms to vanish.

Chapter 8

Division

The operations of this chapter are, for the most part, inverse to those of the last. Just as division is the inverse of multiplication for numbers, we can define a similar operation for polynomials.

8.1 Quotients of Polynomials

Let A and D be any polynomials in a single variable x, with D not being the zero polynomial. If there exists a polynomial Q such that $D \times Q = A$, then Q is called the quotient of A by D. We may symbolise this relationship using the notations $A \div D$ or $\frac{A}{D}$. In such an expression, A is the dividend and D is the divisor. The operation of finding Q is known as division, though we prefer to frame the operations of this chapter under the title of transformation of quotients.

When both A and D are polynomials, the quotient $\frac{A}{D}$ is a rational function of x, but it is not necessarily a polynomial.

- When the quotient $\frac{A}{D}$ can be transformed into a polynomial, we say that A is exactly divisible by D.
- When the quotient cannot be so transformed, it is called an essentially fractional function.

Properties of Degree in Division

***Theorem* 8.1.1.** When the quotient of two polynomials is itself a polynomial, its degree is the excess of the degree of the dividend over the degree of the divisor.

Proof. Exactly the same as Theorem 4.4.2 just instead of monomials its polynomials. ■

***Theorem* 8.1.2.** If the degree of the dividend is less than that of the divisor, the quotient is essentially fractional.

Proof. Let the degree of the dividend A be d_A and the degree of the divisor D be d_D, with $d_A < d_D$. Suppose, for the sake of contradiction, that the quotient $\frac{A}{D}$ is a polynomial, say Q, of degree d_Q. By definition, $A = Q \times D$. Taking the degrees of both sides, we have $d_A = d_Q + d_D$. By the definition of a polynomial, its degree must be a non-negative integer, so $d_Q \geq 0$. However, we are given that $d_A < d_D$, which makes the equation $d_A = d_Q + d_D$ impossible for any $d_Q \geq 0$. Our initial supposition must therefore be false. The quotient cannot be a polynomial; it must be fractional. ■

8.1.1 The Division Transformation

The following is the fundamental theorem in the transformation of quotients. It is often called the Division Algorithm for Polynomials.

***Theorem* 8.1.3.** Let A and D be polynomials of degrees d_A and d_D respectively, where D is not the zero polynomial. The quotient $\frac{A}{D}$ can always be transformed as follows:

$$\frac{A}{D} = P + \frac{R}{D},$$

where P is a polynomial of degree $d_A - d_D$ (if $d_A \geq d_D$) and R is a polynomial whose degree is less than d_D.

The polynomial P is called the integral quotient and R is the remainder. This transformation is effected by a series of steps. We shall first work through a particular case to build intuition, and then give the general proof.

Example 8.1.1. Let $A_6 = 8x^6 + 8x^5 - 20x^4 + 40x^3 - 50x^2 + 30x - 10$ and $D_4 = 2x^4 + 3x^3 - 4x^2 + 6x - 8$. Our goal is to eliminate the highest power of the dividend, $8x^6$, by subtracting a suitable multiple of the divisor. The highest term of A_6 is $8x^6$ and the highest term of D_4 is $2x^4$. Their quotient is $\frac{8x^6}{2x^4} = 4x^2$. We multiply D_4 by this term and subtract the result from A_6.

$$\begin{aligned} A_6 &= 8x^6 + 8x^5 - 20x^4 + 40x^3 - 50x^2 + 30x - 10 \\ 4x^2 D_4 &= 8x^6 + 12x^5 - 16x^4 + 24x^3 - 32x^2 \\ A_6 - 4x^2 D_4 &= \quad - 4x^5 - 4x^4 + 16x^3 - 18x^2 + 30x - 10 \end{aligned}$$

Let this new polynomial be A_5. We have found that $A_6 = 4x^2 D_4 + A_5$. Notice that the degree of the new dividend, A_5, is less than the degree of the original, A_6. We repeat the process with A_5. The quotient of the highest terms is now $\frac{-4x^5}{2x^4} = -2x$.

$$\begin{aligned} A_5 &= -4x^5 - 4x^4 + 16x^3 - 18x^2 + 30x - 10 \\ -2xD_4 &= -4x^5 - 6x^4 + 8x^3 - 12x^2 + 16x \\ A_5 - (-2xD_4) &= \quad + 2x^4 + 8x^3 - 6x^2 + 14x - 10 \end{aligned}$$

Let this new polynomial be A_4. We now have $A_5 = -2xD_4 + A_4$. We repeat the process one final time with A_4. The quotient of highest terms is $\frac{2x^4}{2x^4} = 1$.

$$\begin{aligned} A_4 &= 2x^4 + 8x^3 - 6x^2 + 14x - 10 \\ 1 \times D_4 &= 2x^4 + 3x^3 - 4x^2 + 6x - 8 \\ A_4 - D_4 &= \quad + 5x^3 - 2x^2 + 8x - 2 \end{aligned}$$

Let this final polynomial be A_3. We have $A_4 = 1 \times D_4 + A_3$. The process must now stop, as the degree of the residue A_3 (which is 3) is less than the degree of the divisor D_4 (which is 4).

We now combine our results.

$$\begin{aligned} A_6 &= 4x^2 D_4 + A_5 \\ &= 4x^2 D_4 + (-2xD_4 + A_4) \\ &= 4x^2 D_4 - 2xD_4 + (1 \times D_4 + A_3) \\ &= (4x^2 - 2x + 1)D_4 + A_3 \end{aligned}$$

Dividing the entire equation by D_4 gives the final transformation:

$$\frac{A_6}{D_4} = (4x^2 - 2x + 1) + \frac{A_3}{D_4}.$$

Here, $P = 4x^2 - 2x + 1$ is the integral quotient, and $R = A_3 = 5x^3 - 2x^2 + 8x - 2$ is the remainder. The degree of P is 2, which is $d_A - d_D = 6 - 4$. The degree of R is 3, which is less than the degree of D.

Proof.

(i) ***Existence.*** *Let $A_m = p_0x^m + p_1x^{m-1} + \dots$ and $D_n = q_0x^n + q_1x^{n-1} + \dots$, with $p_0, q_0 \neq 0$ and $m \geq n$. The first term of the integral quotient is formed by dividing the leading terms: $Q_1 = (\frac{p_0}{q_0})x^{m-n}$. We subtract the product Q_1D_n from A_m:*

$$A'_m = A_m - Q_1D_n = (p_0x^m + \dots) - \left(\frac{p_0}{q_0}x^{m-n}\right)(q_0x^n + \dots).$$

The highest term of Q_1D_n is $(\frac{p_0}{q_0}x^{m-n})(q_0x^n) = p_0x^m$. This is designed to cancel the highest term of A_m. Therefore, the degree of the residue A'_m is at most $m-1$. We can write $A_m = Q_1D_n + A'_m$. We can repeat this process with A'_m as the new dividend. We generate a sequence of quotients $Q_2, Q_3, \dots$ and residues $A''_m, A'''_m, \dots$ whose degrees are strictly decreasing. The process terminates when we obtain a residue R whose degree is less than n. At each step i, we have an equation of the form $A^{(i-1)} = Q_iD_n + A^{(i)}$. Combining these steps, we find:

$$\begin{aligned} A_m &= Q_1D_n + A'_m \\ &= Q_1D_n + (Q_2D_n + A''_m) \\ &= \dots \\ &= (Q_1 + Q_2 + \dots + Q_k)D_n + R \end{aligned}$$

The sum of the partial quotients $P = Q_1 + Q_2 + \dots + Q_k$ is a polynomial, and the final residue R has a degree less than n. This establishes the existence of P and R.

(ii) ***Uniqueness of the Quotient and Remainder.*** *Suppose, for the sake of contradiction, that the transformation can be done in two different ways.*

$$\frac{A}{D} = P + \frac{R}{D}$$
$$\text{and} \quad \frac{A}{D} = P' + \frac{R'}{D}$$

where both pairs (P, R) and (P', R') satisfy the conditions of the theorem. Since both expressions are equal to $\frac{A}{D}$, they must be equal to each other:

$$P + \frac{R}{D} = P' + \frac{R'}{D}.$$

Rearranging the terms to isolate the polynomials and the fractional parts gives:

$$P - P' = \frac{R'}{D} - \frac{R}{D} = \frac{R' - R}{D}.$$

The left-hand side, $P - P'$, is a polynomial. On the right-hand side, since the degrees of both R and R' are less than the degree of D, the degree of their difference, $R' - R$, must also be less than the degree of D. By the theorem we proved earlier, if the degree of the numerator is less than the degree of the denominator, the quotient is essentially fractional. The only way an essentially fractional function can be equal to a polynomial is if both are identically zero. Therefore, we must have $R' - R = 0$, which implies $R = R'$. It immediately follows that $P - P' = 0$, which implies $P = P'$. The two representations must be identical, proving that the integral quotient and remainder are unique.

■

8.1.2 The Long Division Algorithm

The process of repeated subtraction used to prove the division transformation can be arranged into a convenient algorithm, commonly known as polynomial long division. It is best illustrated with the example we have already worked through.

Arrange both dividend and divisor in descending powers of x.

$$\begin{array}{r} 4x^2 - 2x + 1 \\ 2x^4 + 3x^3 - 4x^2 + 6x - 8 \overline{)\, 8x^6 + 8x^5 - 20x^4 + 40x^3 - 50x^2 + 30x - 10} \\ \underline{-(8x^6 + 12x^5 - 16x^4 + 24x^3 - 32x^2)} \\ -4x^5 - 4x^4 + 16x^3 - 18x^2 + 30x \\ \underline{-(-4x^5 - 6x^4 + 8x^3 - 12x^2 + 16x)} \\ 2x^4 + 8x^3 - 6x^2 + 14x - 10 \\ \underline{-(2x^4 + 3x^3 - 4x^2 + 6x - 8)} \\ 5x^3 - 2x^2 + 8x - 2 \end{array}$$

The integral quotient is $4x^2 - 2x + 1$ and the remainder is $5x^3 - 2x^2 + 8x - 2$.

Method of Detached Coefficients

When the polynomials are written with all powers of x present (using zero coefficients for any missing terms), we may omit the powers of x during the calculation to save labour. Using our example:

$$\begin{array}{r} 4 - 2 + 1 \\ 2 + 3 - 4 + 6 - 8 \overline{)\, 8 + 8 - 20 + 40 - 50 + 30 - 10} \\ \underline{-(8 + 12 - 16 + 24 - 32)} \\ -4 - 4 + 16 - 18 + 30 \\ \underline{-(-4 - 6 + 8 - 12 + 16)} \\ 2 + 8 - 6 + 14 - 10 \\ \underline{-(2 + 3 - 4 + 6 - 8)} \\ 5 - 2 + 8 - 2 \end{array}$$

Since the dividend began with x^6 and the divisor with x^4, the quotient must begin with $x^{6-4} = x^2$. We can then fill in the powers, integral quotient as $4x^2 - 2x + 1$, and remainder as $5x^3 - 2x^2 + 8x - 2$.

A Geometric Interpretation

The division of polynomials can be viewed geometrically as finding the missing side of a rectangle. Suppose we have a rectangle with area $A = x^2 + 5x + 6$ and we know one side has length $D = x + 2$. The other side must have length $P = A/D$. We can construct the rectangle as shown in Figure 8.1.

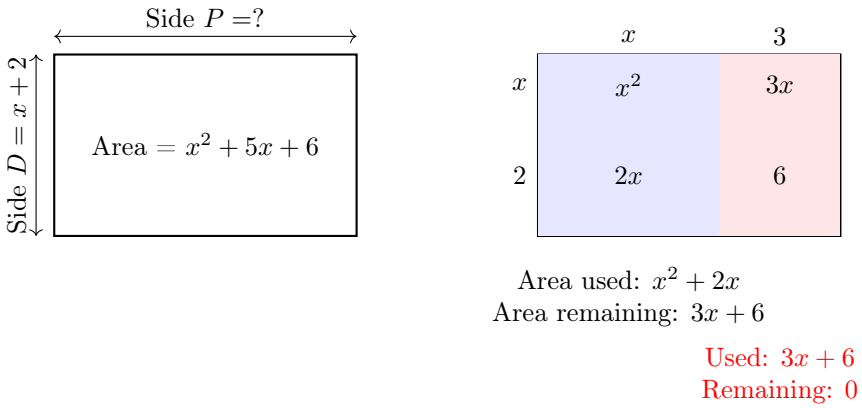


Figure 8.1: Geometric construction of $(x^2 + 5x + 6) \div (x + 2)$. The unknown side is found to be $x + 3$.

The process mirrors long division.

1. To account for the x^2 term in the area, the unknown side must have a term of x. This creates an area of $x(x + 2) = x^2 + 2x$.

2. The remaining area to be accounted for is $(x^2 + 5x + 6) - (x^2 + 2x) = 3x + 6$.
3. To account for this remaining area, the unknown side must have a constant term of $+3$. This creates an area of $3(x + 2) = 3x + 6$.
4. The total area is now accounted for, and the unknown side is determined to be $x + 3$. The remainder is zero.

8.1.3 The Remainder and Factor Theorems

The special case of dividing a polynomial by a linear factor of the form $(x - a)$ is particularly important and leads to two powerful theorems.

Example 8.1.2. . Let us divide the polynomial $A(x) = x^3 + px^2 + qx + r$ by $D(x) = x - a$.

$$\begin{array}{r} x^2 + (a+p)x + (a^2+ap+q) \\ \hline x-a\,)\,x^3 + px^2 + qx + r \\ \underline{-(x^3 - ax^2)} \\ (a+p)x^2 + qx \\ \underline{-((a+p)x^2 - (a^2+ap)x)} \\ (a^2+ap+q)x + r \\ \underline{-((a^2+ap+q)x - (a^3+a^2p+aq))} \\ a^3 + a^2p + aq + r \end{array}$$

The remainder is $a^3 + a^2p + aq + r$. Notice that this is precisely the original polynomial $A(x)$ with x replaced by a. This is not a coincidence.

***Theorem* 8.1.4. (The Remainder Theorem)**. When a polynomial $A(x)$ is divided by a linear factor $(x - a)$, the remainder is the constant value $A(a)$.

Proof. From the Division Transformation theorem, we can write

$$A(x) = P(x)(x - a) + R(x)$$

where $P(x)$ is the integral quotient and $R(x)$ is the remainder. The divisor, $(x - a)$, has degree 1. Therefore, the degree of the remainder $R(x)$ must be less than 1, which means its degree is 0. A polynomial of degree 0 is simply a constant. Let us call this constant R.

$$A(x) = P(x)(x - a) + R$$

This equation holds true for all values of x. If we substitute the specific value $x = a$ into the equation, we get:

$$\begin{aligned} A(a) &= P(a)(a - a) + R \\ &= P(a) \cdot 0 + R \\ &= R \end{aligned}$$

Thus, the remainder R is equal to the value of the polynomial at $x = a$. ■

A direct and powerful consequence of this theorem relates the roots of a polynomial to its factors. A polynomial $A(x)$ is exactly divisible by $(x - a)$ if and only if the remainder of the division is zero. The Remainder Theorem states that this remainder is $A(a)$. Combining these two facts gives the Factor Theorem.

***Theorem* 8.1.5. (The Factor Theorem)**. The linear expression $(x - a)$ is a factor of the polynomial $A(x)$ if and only if $A(a) = 0$.

Proof.

$\Rightarrow$ *If $(x-a)$ is a factor of $A(x)$, then $A(x) = (x-a)P(x)$ for some polynomial P. Substituting $x = a$ gives $A(a) = (a-a)P(a) = 0$.*

$\Leftarrow$ *If $A(a) = 0$, divide A by $(x-a)$ using the Division Transformation:*

$$A(x) = Q(x)(x-a) + R,$$

where R has degree < 1, hence R is a constant. Evaluating at $x = a$ yields

$$0 = A(a) = Q(a)(a-a) + R = R,$$

so $R = 0$ and $A(x) = (x-a)Q(x)$. Thus $(x-a)$ is a factor of $A(x)$.

■

Remark. The condition $A(a) = 0$ means that a is a root or a zero of the polynomial $A(x)$. The Factor Theorem provides a crucial link between the roots of a polynomial equation and its algebraic factors.

Example 8.1.3. Is $(x-2)$ a factor of $A(x) = x^3 - 8$? By the Factor Theorem, we only need to evaluate $A(2)$.

$$A(2) = 2^3 - 8 = 8 - 8 = 0.$$

Since $A(2) = 0$, $(x-2)$ is a factor.

Is $(x+1)$ a factor of $B(x) = x^4 + 2x^3 - x - 2$? Here, the factor is $(x-(-1))$, so we must evaluate $B(-1)$.

$$B(-1) = (-1)^4 + 2(-1)^3 - (-1) - 2 = 1 + 2(-1) + 1 - 2 = 1 - 2 + 1 - 2 = -2.$$

Since $B(-1) \neq 0$, $(x+1)$ is not a factor.

8.1.4 Synthetic Division: A Shorthand for Linear Divisors

The case of a binomial divisor of the first degree is of special importance. Let the dividend be the polynomial $A(x) = p_0x^n + p_1x^{n-1} + \cdots + p_n$ and the divisor be $D(x) = x - a$. The long division process can be significantly abbreviated. Using detached coefficients, the calculation proceeds as follows:

	p_0	p_1	p_2	$\ldots$	p_n
a		p_0a	$(p_0a + p_1)a$	$\ldots$	
	p_0	$(p_0a + p_1)$	$(p_0a^2 + p_1a + p_2)$	$\ldots$	R

The integral quotient, $P(x)$, is therefore

$$P(x) = p_0x^{n-1} + (p_0a + p_1)x^{n-2} + (p_0a^2 + p_1a + p_2)x^{n-3} + \ldots$$

The law of formation for the coefficients of the quotient is as follows:

- The first coefficient is simply the first coefficient of the dividend, p_0.
- The second coefficient is obtained by multiplying its predecessor (p_0) by a and adding the next coefficient of the dividend (p_1).
- The third is found by multiplying the second coefficient just obtained by a and adding the third coefficient of the dividend (p_2), and so on.

The remainder, R, which is a constant, is obtained by multiplying the last coefficient of the quotient by a and adding the last coefficient of the dividend, p_n. The operations may be conveniently arranged in a table.

Example 8.1.4. Find the quotient and remainder for $(2x^4 - 3x^2 + 6x - 4) \div (x - 2)$. The dividend has coefficients $(2, 0, -3, 6, -4)$, including a zero for the missing x^3 term. The divisor is of the form $(x - a)$ with $a = 2$.

	2	0	-3	6	-4
2		4	8	10	32
	2	4	5	16	28

The numbers in the bottom row are the coefficients of the quotient and the final remainder. The quotient starts with a power of $x^{4-1} = x^3$.

- Integral quotient: $2x^3 + 4x^2 + 5x + 16$.
- Remainder: 28.

Example 8.1.5. Division by $(x + a)$. To divide by a term like $(x + 2)$, we note that this is equivalent to $(x - (-2))$. The process is identical, but we use $a = -2$ as the multiplier. For $(2x^4 - 3x^2 + 6x - 4) \div (x + 2)$:

	2	0	−3	6	−4
−2		−4	8	−10	8
	2	−4	5	−4	4

- Integral quotient: $2x^3 - 4x^2 + 5x - 4$.
- Remainder: 4.

Example 8.1.6. Division by $(ax + b)$. To handle a divisor such as $(3x + 2)$, we can use a simple transformation.

$$\frac{3x^4 - 2x^3 + 3x^2 - 2x + 3}{3x + 2} = \frac{1}{3}\left(\frac{3x^4 - 2x^3 + 3x^2 - 2x + 3}{x + \frac{2}{3}}\right)$$

We first perform synthetic division on the quotient inside the bracket, using $a = -2/3$.

	3	−2	3	−2	3
−2/3		−2	8/3	−34/9	104/27
	3	−4	17/3	−52/9	185/27

This gives an intermediate quotient $3x^3 - 4x^2 + \frac{17}{3}x - \frac{52}{9}$ and a remainder of $\frac{185}{27}$. To find the final result, we must multiply the quotient by the factor of $1/3$, but the remainder remains unchanged relative to the original divisor $3x + 2$:

$$\frac{A}{D} = \frac{1}{3}\left(P_{int} + \frac{R}{x + 2/3}\right) = \frac{P_{int}}{3} + \frac{R}{3(x + 2/3)} = \frac{P_{int}}{3} + \frac{R}{3x + 2}.$$

- Integral quotient: $\frac{1}{3}(3x^3 - 4x^2 + \frac{17}{3}x - \frac{52}{9}) = x^3 - \frac{4}{3}x^2 + \frac{17}{9}x - \frac{52}{27}$.
- Remainder: $\frac{185}{27}$.

8.1.5 Applications to Factorisation

***Theorem* 8.1.6.** If a polynomial of degree n, $A(x)$, vanishes for r different values of x, say $a_1, a_2, \ldots, a_r$ (where $r \leq n$), then $A(x)$ is exactly divisible by the product $(x - a_1)(x - a_2) \cdots (x - a_r)$.

Proof. By the Factor Theorem, since $A(a_1) = 0$, $(x - a_1)$ must be a factor of $A(x)$. We can therefore write

$$A(x) = (x - a_1)P_{n-1}(x)$$

where $P_{n-1}(x)$ is a polynomial of degree $n - 1$. Since this identity holds for all values of x, it must hold for $x = a_2$.

$$A(a_2) = (a_2 - a_1)P_{n-1}(a_2)$$

By hypothesis, $A(a_2) = 0$. Also by hypothesis, a_1 and a_2 are different, so $a_2 - a_1 \neq 0$. The only way for the equation to hold is if $P_{n-1}(a_2) = 0$. By the Factor Theorem again, this implies that $(x - a_2)$ is a factor of $P_{n-1}(x)$. So we can write $P_{n-1}(x) = (x - a_2)P_{n-2}(x)$. Substituting this back gives:

$$A(x) = (x - a_1)(x - a_2)P_{n-2}(x)$$

We can continue this process step-by-step for all r roots. After r steps, we will arrive at the conclusion

$$A(x) = (x - a_1)(x - a_2) \cdots (x - a_r)P_{n-r}(x),$$

where $P_{n-r}(x)$ is a polynomial of degree $n - r$. This proves the theorem. ■

***Corollary* 8.1.1.** If a polynomial is divisible by several distinct linear factors $(x-a_1),(x-a_2),\ldots$, then it is divisible by their product.

Proof. For each i, the assumption $(x-a_i) \mid A(x)$ implies, by the Factor Theorem, that $A(a_i)=0$. Thus A vanishes at the r distinct points $a_1,\ldots,a_r$. Applying the preceding theorem with these r zeros, we conclude that $A(x)$ is divisible by $(x-a_1),\ldots$. ■

***Corollary* 8.1.2.** If a polynomial of degree n, $A(x)=p_0x^n+p_1x^{n-1}+\cdots+p_n$, vanishes for n distinct values $a_1,\ldots,a_n$, then it can be completely resolved into n linear factors:

$$A(x)=p_0(x-a_1)(x-a_2)\cdots(x-a_n).$$

Proof. From the previous theorem with $r=n$, we have $A(x)=(x-a_1)\cdots(x-a_n)P_0(x)$. The remaining polynomial, $P_0(x)$, has degree $n-n=0$, which means it is a constant. Let this constant be C.

$$p_0x^n+p_1x^{n-1}+\cdots+p_n=C(x-a_1)(x-a_2)\cdots(x-a_n).$$

To find the value of C, we compare the coefficients of the highest power of x, which is x^n, on both sides. On the left, the coefficient is p_0. On the right, the x^n term is formed by multiplying the x from each of the n brackets, giving Cx^n. Equating the coefficients gives $p_0=C$. ■

This leads to a profound result about the identity of polynomials.

***Theorem* 8.1.7. (The Identity Theorem)**. If a polynomial of degree n vanishes for more than n different values of x, it must be the zero polynomial; that is, each of its coefficients must be zero.

Proof. Let $A(x)$ be a polynomial of degree n with leading coefficient p_0. Let $a_1,\ldots,a_n$ be n of the distinct values for which $A(x)$ vanishes. By the previous corollary, we can write

$$A(x)=p_0(x-a_1)(x-a_2)\cdots(x-a_n).$$

Now, let β be another value, different from all the a_i, for which $A(x)$ vanishes. Substituting $x=\beta$ into the identity gives:

$$A(\beta)=0=p_0(\beta-a_1)(\beta-a_2)\cdots(\beta-a_n).$$

Since β is different from all the a_i, none of the factors $(\beta-a_i)$ can be zero. Therefore, their product cannot be zero. The only way for the equation to hold is if $p_0=0$. If the leading coefficient p_0 is zero, then $A(x)$ is actually a polynomial of degree at most $n-1$. But it still vanishes for more than n (and thus more than $n-1$) values. We can repeat the same argument to show that its new leading coefficient, p_1, must also be zero. Proceeding in this way, we show step-by-step that all coefficients must be zero. ■

***Corollary* 8.1.3.** If two polynomials, whose degrees do not exceed n, are equal in value for more than n different values of x, then they must be identically equal; that is, the coefficients of like powers of x must be equal.

Proof. Let the two polynomials be $P(x)=p_nx^n+\cdots+p_0$ and $Q(x)=q_nx^n+\cdots+q_0$. Let the new polynomial $F(x)=P(x)-Q(x)=(p_n-q_n)x^n+\cdots+(p_0-q_0)$. By hypothesis, $P(x)=Q(x)$ for more than n values of x. For each of these values, $F(x)=0$. So, $F(x)$ is a polynomial of degree at most n that vanishes for more than n values. By the Identity Theorem, $F(x)$ must be the zero polynomial. This means all its coefficients are zero.

$$p_n-q_n=0,\quad p_{n-1}-q_{n-1}=0,\quad \ldots,\quad p_0-q_0=0.$$

This implies $p_i=q_i$ for all i. The polynomials are identical. ■

Example 8.1.7. Determine the value of the constant k so that x^3+6x^2+4x+k is exactly divisible by $x+2$. For the polynomial to be divisible by $(x+2)=(x-(-2))$, the remainder must be zero. By the Remainder Theorem, the remainder is the value of the polynomial at $x=-2$.

$$R=(-2)^3+6(-2)^2+4(-2)+k=-8+6(4)-8+k=-8+24-8+k=8+k.$$

For exact divisibility, we require $R=0$, so $8+k=0$, which gives $k=-8$.

Example 8.1.8. Prove the identity $a^3(b-c)+b^3(c-a)+c^3(a-b) = -(a+b+c)(a-b)(b-c)(c-a)$. Let

$$P(a,b,c) = a^3(b-c)+b^3(c-a)+c^3(a-b).$$

Regard P as a polynomial in a. Then notice that when $a=b$ and $a=c$

$$P(b,b,c) = 0, \qquad P(c,b,c) = 0,$$

so $(a-b)(a-c)$ divides P. By symmetry we know $P(a,b,b)=0$, hence $(b-c)$ divides P. Therefore

$$P = (a-b)(a-c)(b-c)Q,$$

where Q is some polynomial. Since P has degree 4 and the product of the factors $(a-b)(a-c)(b-c)$ has degree 3, Q must be a polynomial of degree 1.

Furthermore, P has a special symmetry. Swapping any two variables, say a and b, negates the polynomial:

$$P(b,a,c) = b^3(a-c)+a^3(c-b)+c^3(b-a) = -b^3(c-a)-a^3(b-c)-c^3(a-b) = -P(a,b,c).$$

A polynomial with this property is called alternating. The product of the factors, written cyclically as $(a-b)(b-c)(c-a)$, is also alternating. Because both P and this product of factors are alternating, their quotient Q must be symmetric (unaffected by swapping variables). Since Q is a symmetric polynomial of degree 1, it must have the form $Q = k(a+b+c)$ for some constant k.

Putting these pieces together, we can express P as:

$$a^3(b-c)+b^3(c-a)+c^3(a-b) = k(a+b+c)(a-b)(b-c)(c-a).$$

To find the constant k, we can compare the coefficients of any term on both sides. Let's find the coefficient of a^3b. On the left-hand side, this term comes only from the expression $a^3(b-c)$, and its coefficient is 1. On the right-hand side, we can expand the product to find the corresponding term:

$$\begin{aligned} Q(a-b)(b-c)(c-a) &= (ab-ac-b^2+bc)(c-a) \\ &= Q(a^2c-a^2b+\dots) \\ &= k(a+b+c)(a^2c-a^2b+\dots) \\ &= k(a(a^2c-a^2b)+\dots) \\ &= k(a^3c-a^3b+\dots) \end{aligned}$$

The coefficient of a^3b on the right is $-k$. Equating coefficients: $1=-k$, so $k=-1$.

8.2 Exercises

Part I: The Division Transformation

1. For each pair of polynomials A (dividend) and D (divisor), state the expected degree of the integral quotient P and the maximum possible degree of the remainder R. Do not perform the division.

(a) $A = 3x^5 - 2x^2 + 1$, $D = x^2 + x + 1$

(b) $A = x^4 + 1$, $D = x^3 + 1$

(c) $A = 2x^3 - 5x + 7$, $D = x^5 - 3x^2$

2. Find the integral quotient and remainder for the following divisions using polynomial long division.

(a) $(x^3 - 7x^2 + 11x - 5) \div (x - 5)$

(b) $(6a^3 + 7a^2 - 8a + 4) \div (2a - 1)$

(c) $(y^4 - 2y^3 - 7y^2 + 20y - 12) \div (y^2 + y - 6)$

(d) $(p^5 - 1) \div (p - 1)$

3. Repeat the calculations from the previous question using the method of detached coefficients. Be sure to include zeros for any missing terms.

4. Find the integral quotient and remainder for the following, where terms are missing.

(a) $(x^4 + 1) \div (x + 1)$
(b) $(a^5 - 2a^2 + 3) \div (a^2 - a + 1)$
(c) $(z^6 - z^3 + 1) \div (z^2 + z + 1)$

5. Find the result of the following divisions.

(a) $(x^3 - 6x^2 + 11x - 6) \div (x - 1)(x - 2)$
(b) $(a^4 - 5a^2 + 4) \div (a^2 - 3a + 2)$

6. Divide $x^4 + (p - 2)x^3 - (2p - q)x^2 + (p + 2q)x - q$ by $x^2 + px - q$.

7. Divide $x^3 - (a + b + c)x^2 + (ab + bc + ca)x - abc$ by $x - a$.

Remark. Alternatively, what does the Factor Theorem predict about this division?

8. Find the quotient of $prx^3 + (qr - ps)x^2 - (p^2 + qs)x + p$ by $px + q$.

9. The area of a rectangle is given by the polynomial $A(x) = 6x^3 - 5x^2 - 17x + 6$. If one side has a length of $D(x) = 2x + 3$, find the length of the other side.

Part II: The Remainder and Factor Theorems

10. Without performing division, find the remainder for each of the following.

(a) $(x^4 - 3x^3 + 5x^2 - 2x + 7) \div (x - 1)$
(b) $(2y^3 + 5y^2 - 6y - 9) \div (y + 3)$
(c) $(a^5 + a^4 - 2a^2 + 1) \div (a + 1)$
(d) $(x^n + 1) \div (x + 1)$, for any odd integer n.

11. Use the Factor Theorem to determine if the first polynomial is a factor of the second.

(a) $(x - 3)$, $x^3 - 2x^2 - 5x + 6$
(b) $(x + 2)$, $x^4 + 2x^3 - x^2 - x + 7$
(c) $(a - b)$, $a^7 - b^7$
(d) $(y + 2z)$, $y^5 + 32z^5$

12. For what value of k is the polynomial $2x^3 - x^2 - 7x + k$ exactly divisible by $(x - 2)$?

13. The polynomial $x^4 + px^2 + q$ is divisible by $(x - 1)$ and $(x + 2)$. Find the values of p and q.

14. Find the values of A and B if $(x - 2)$ and $(x + 3)$ are both factors of $2x^3 + Ax^2 + Bx - 30$.

15. The expression $ax^4 + bx^3 + cx^2 + dx + e$ is divisible by $x^2 - 1$. Show that $a + c + e = b + d = 0$.

Remark. $x^2 - 1 = (x - 1)(x + 1)$.

16. What is the remainder when the polynomial $A(x)$ is divided by $(ax - b)$?

17. If $(x - a)$ is a common factor of $x^2 + px + q$ and $x^2 + rx + s$, prove that $a = \frac{s-q}{p-r}$.

18. When a polynomial $P(x)$ is divided by $(x - a)$, the remainder is R_1. When divided by $(x - b)$, the remainder is R_2. What is the remainder when $P(x)$ is divided by $(x - a)(x - b)$?

Remark. The remainder will be a polynomial of degree at most 1. Let it be $Cx + D$ and solve for C and D.

19. Show that $x + y$ is a factor of $x^n + y^n$ if and only if n is an odd integer.

Part III: Synthetic Division

20. Use synthetic division to find the integral quotient and remainder for the following.

(a) $(x^4 - 4x^3 + 2x^2 + 7x - 1) \div (x - 2)$

(b) $(2y^5 + y^4 - 10y^3 - 15) \div (y + 3)$

(c) $(a^6 - 7a^3 + 10) \div (a - 1)$

21. Use synthetic division to find the value of the polynomial $P(x) = 3x^5 - 8x^4 - 5x^3 + 26x^2 - 33x + 20$ for $x = 2$.

22. Use synthetic division to perform the following divisions.

(a) $(2x^3 - 9x^2 + 10x - 7) \div (2x - 1)$

(b) $(6a^4 + a^3 - 20a^2 + 12) \div (3a + 2)$

23. The polynomial $P(x) = x^3 - 6x^2 + 11x - 6$ has a root at $x = 1$. Use synthetic division to divide $P(x)$ by $(x - 1)$ and find the remaining quadratic factor. Use this to find all the roots of $P(x)$.

24. Given that $x = 1$ and $x = -2$ are roots of $x^4 - x^3 - 7x^2 + x + 6 = 0$, find the other two roots.

Part IV: Applications to Factorisation

25. Factorise the following polynomials completely.

(a) $x^3 + x^2 - 10x + 8$, given that $(x - 2)$ is a factor.

(b) $a^3 - 7ab^2 - 6b^3$, given that $(a + b)$ is a factor.

(c) $y^4 + 4y^3 - y^2 - 16y - 12$, given that $(y + 1)$ and $(y - 2)$ are factors.

26. Show that $(a-b)$, $(b-c)$, and $(c-a)$ are all factors of the polynomial $a(b^2-c^2)+b(c^2-a^2)+c(a^2-b^2)$. What must the fourth factor be?

27. Prove that $(x + y + z)$ is a factor of $x^n + y^n + z^n$ for all odd integers n, provided $x + y + z = 0$.

Remark. If $x + y + z = 0$, then $z = -(x + y)$. Substitute this into the expression.

28. Show that $a^2 + b^2 + c^2 - ab - bc - ca$ is a factor of $a^3 + b^3 + c^3 - 3abc$.

29. Factorise the symmetrical expression $(x + y + z)^5 - x^5 - y^5 - z^5$.

30. Prove the identity $a^4(b^2 - c^2) + b^4(c^2 - a^2) + c^4(a^2 - b^2) = -(a^2 - b^2)(b^2 - c^2)(c^2 - a^2)$.

31. Resolve into factors: $(x^2 + 5x + 6)(x^2 + 7x + 6) - 24x^2$.

32. Factorise $\Sigma a^2(b - c)$ over variables $\{a, b, c\}$. The sum is $a^2(b - c) + b^2(c - a) + c^2(a - b)$.

33. Prove that for any positive integer n, $(x - 1)^2$ is a factor of $nx^{n+1} - (n + 1)x^n + 1$.

Part V: The Identity Theorem and Advanced Problems

34. A polynomial $P(x)$ of degree 3 satisfies $P(0) = P(1) = P(2) = 1$. If $P(3) = 7$, find the polynomial.

Remark. Consider the polynomial $Q(x) = P(x) - 1$. What are the roots of $Q(x)$?

35. If two polynomials $P(x)$ and $Q(x)$ of degree n are equal for $n + 1$ distinct values of x, does it follow that they are equal for all values of x? Justify your answer using the theorems from this chapter.

36. Find the conditions that must be satisfied by the coefficients of $A(x) = x^3 + px + q$ for it to be divisible by a factor of the form $(x - a)^2$.

37. Find a polynomial $P(x)$ of degree 4 such that $P(x) = P(-x)$ for all x, and $P(0) = 1, P(1) = 0, P(2) = 9$.

38. Prove that if $A(x)$ is a polynomial in x, then $A(x) - A(y)$ is exactly divisible by $(x - y)$.

39. $\star$ When the polynomial $P(x)$ is divided by $(x-1)^2$, the remainder is $2x+1$. What is the remainder when $P(x)$ is divided by $(x-1)$?

40. $\star$ A polynomial $P(x)$ leaves a remainder of 3 when divided by $(x-1)$ and a remainder of 5 when divided by $(x-3)$. Find the remainder when $P(x)$ is divided by $(x-1)(x-3)$.

41. $\star$ Prove that $(a+b+c)^3 - (a^3+b^3+c^3)$ is divisible by $(a+b)$, $(b+c)$, and $(c+a)$.

42. $\star$ If the polynomial $P(x) = x^4 + ax^3 + bx^2 + cx + 1$ is a perfect square, find the relations between the coefficients a, b, c.

Remark. Assume $P(x) = (x^2 + px + q)^2$. Expand and compare coefficients.

43. $\star\star$ **The Formal Derivative and Double Roots.**

Remark. We have not defined derivatives using limits as in calculus. Here, we define a purely algebraic object and uncover one of its most important properties.

(a) **Definition of the Formal Derivative.** For any polynomial $f(x) = \sum_{k=0}^{n} p_k x^k$, we define a new polynomial, called its formal derivative, denoted $f'(x)$, as

$$f'(x) \coloneqq \sum_{k=1}^{n} k p_k x^{k-1}.$$

For example, if $f(x) = x^3 - 2x^2 + 5$, its formal derivative is $f'(x) = 3x^2 - 4x$.

Using this definition, prove that for any two polynomials $f(x)$ and $g(x)$, the derivative of their sum is the sum of their derivatives: $(f+g)'(x) = f'(x) + g'(x)$.

(b) **A Fundamental Quotient.** We know from the Factor Theorem that if a is a root of $f(x)$, then $(x-a)$ is a factor. Let us generalise this. For any polynomial $f(x)$ and any number a, prove that the polynomial $f(x) - f(a)$ is always exactly divisible by $(x-a)$.

Remark. Write $f(x) - f(a)$ as a sum of terms of the form $p_k(x^k - a^k)$ and recall the standard factorisation of $x^k - a^k$.

As a consequence, the expression $Q(x) = \frac{f(x)-f(a)}{x-a}$ is always a polynomial.

(c) **Connecting the Quotient and the Derivative.** The goal of this part is to prove the remarkable result that $Q(a) = f'(a)$.

i. First, consider the simple case $f(x) = x^k$. Show that the corresponding quotient polynomial is $Q(x) = \frac{x^k - a^k}{x-a} = x^{k-1} + ax^{k-2} + \cdots + a^{k-2}x + a^{k-1}$.

ii. Evaluate this quotient at $x = a$ to show that $Q(a) = ka^{k-1}$, which is precisely $f'(a)$ for this simple case.

iii. Now, for a general polynomial $f(x) = \sum p_k x^k$, use the result from part (i) and the additive property from part (a) to prove that $Q(a) = f'(a)$.

(d) **The Condition for a Double Root.** A polynomial $f(x)$ is said to have a double root at $x = a$ if it is divisible by $(x-a)^2$. Use the results from the previous parts to prove the following theorem:

A polynomial $f(x)$ has a double root at $x = a$ if and only if both $f(a) = 0$ and $f'(a) = 0$.

Remark. Structure your proof in two parts. First, assume $f(x)$ has a double root. What does this imply about $f(a)$ and the polynomial $Q(x)$ from part (b)? Then, assume $f(a) = 0$ and $f'(a) = 0$. What does this tell you about $Q(a)$ and its divisibility?

8.3 Infinite Series from Division

The process of long division gives rise to an algebraic identity at each step. If we stop the division of A by D after finding some partial quotient P', the polynomial A can be expressed as $A = P'D + R'$, where R' is the current residue. This gives the identity:

$$\frac{A}{D} = P' + \frac{R'}{D}.$$

8.3.1 Descending Series

If we continue the division process beyond the point where a remainder with degree less than the divisor is found, we begin to generate terms with negative powers of x. This process, which can be continued indefinitely, is called descending continued division. At any stage, we obtain an identity of the form:

$$\frac{A}{D} = (c_p x^p + \cdots + c_0 + c_{-1}x^{-1} + \cdots + c_{-q}x^{-q}) + \frac{R'}{D}$$

where the remainder R' will contain even lower powers of x.

Example 8.3.1. Expand $\frac{x^3+2x^2+3x+4}{x^2+x+1}$ as a descending series.. Using the contracted form of long division:

	x^3	$+2x^2$	$+3x$	$+4$		
x^2+x+1	x	$+1$	$+1/x$	$+2/x^2$	$-3/x^3$	$\ldots$
Residues	x^2	$+2x$	$+4$			
	x	$+3$				
	2	$-1/x$				
		$-3/x$	$-1/x^2$			
			$2/x^2$	$+3/x^3$		

The process yields the series expansion:

$$\frac{x^3+2x^2+3x+4}{x^2+x+1} = x + 1 + \frac{1}{x} + \frac{2}{x^2} - \frac{3}{x^3} + \ldots$$

At any point, we can form an exact identity. For instance, after three terms:

$$\frac{x^3+2x^2+3x+4}{x^2+x+1} = x + 1 + \frac{1}{x} + \frac{2 - 1/x}{x^2+x+1}.$$

8.3.2 Ascending Series

Alternatively, we can arrange both dividend and divisor according to ascending powers of x. This produces a series in ascending powers, a process called ascending continued division.

Example 8.3.2. Expand $\frac{x^3+2x^2+3x+4}{x^2+x+1}$ as an ascending series.. First, we reorder the polynomials: $4+3x+2x^2+x^3$ and $1+x+x^2$.

	4	$+3x$	$+2x^2$	$+x^3$		
$1+x+x^2$	4	$-x$	$-x^2$	$+3x^3$	$-2x^4$	$\ldots$
Residues	$-x$	$-2x^2$	$+x^3$			
		$-x^2$	$+2x^3$			
			$3x^3$	$-x^4$		
				$-2x^4$	$-3x^5$	

This gives the series expansion:

$$\frac{4+3x+2x^2+x^3}{1+x+x^2} = 4 - x - x^2 + 3x^3 - 2x^4 + \ldots$$

These expansions are unique for a given number of terms. The resulting series are examples of a broader class known as **recurring series**.

8.3.3 Standard Expansions

(i) Division of 1 by $1 - x$ gives the geometric series:

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots + x^n + \frac{x^{n+1}}{1-x}.$$

(ii) Similarly,

$$\frac{1}{1+x} = 1 - x + x^2 - \cdots + (-1)^n x^n + \frac{(-1)^{n+1} x^{n+1}}{1+x}.$$

8.4 Expressing a Polynomial in Powers of Another

It is often useful to express a polynomial not in powers of x, but in powers of another polynomial, say $Q(x)$.

***Theorem* 8.4.1.** Let P and Q be polynomials of degrees m and n respectively ($m \geq n$). Then P can always be expressed in the form

$$P = R_0 + R_1 Q + R_2 Q^2 + \cdots + R_p Q^p,$$

where $R_0, R_1, \ldots, R_p$ are polynomials, each of degree at most $n - 1$, and p is an integer not exceeding m/n.

Proof. We apply the Division Transformation repeatedly. First, divide P by Q:

$$P = Q_0 Q + R_0, \quad \textit{where } \deg(R_0) < n.$$

If $\deg(Q_0) \geq n$, we divide Q_0 by Q:

$$Q_0 = Q_1 Q + R_1, \quad \textit{where } \deg(R_1) < n.$$

We continue this process, generating a sequence of quotients Q_i and remainders R_i.

$$Q_1 = Q_2 Q + R_2, \quad \ldots, \quad Q_{p-1} = R_p Q + R_{p-1}.$$

The process terminates when the degree of a quotient Q_{p-1} is less than the degree of Q. We rename this final quotient R_p. Substituting these equations back into one another:

$$\begin{aligned} P &= (Q_1 Q + R_1)Q + R_0 = R_1 Q + Q_1 Q^2 + R_0 \\ &= R_0 + R_1 Q + (Q_2 Q + R_2)Q^2 = R_0 + R_1 Q + R_2 Q^2 + Q_2 Q^3 \\ &\cdots \\ &= R_0 + R_1 Q + R_2 Q^2 + \cdots + R_p Q^p. \end{aligned}$$

The degrees of the successive quotients $Q_0, Q_1, \ldots$ are $m - n, m - 2n, \ldots$. The process must terminate, and the number of steps p cannot exceed m/n. Each remainder R_i has a degree less than n. ■

A particularly important case is expressing a polynomial in powers of a linear factor $(x - a)$.

***Corollary* 8.4.1.** Any polynomial $P(x)$ of degree n can be written in the form

$$P(x) = c_0 + c_1(x - a) + c_2(x - a)^2 + \cdots + c_n(x - a)^n,$$

where $c_0, \ldots, c_n$ are constants.

Proof. This follows from the general theorem with $Q(x) = x - a$, which has degree $n = 1$. The remainders R_i must have degree less than 1, making them constants. ■

The coefficients c_i in this expansion are the successive remainders from the division process. They can be calculated efficiently using repeated synthetic division.

Example 8.4.1. Express $P(x) = 5x^3 - 11x^2 + 10x - 2$ in powers of $(x-1)$. We divide $P(x)$ by $(x-1)$. The remainder is c_0 and the quotient is $Q_0(x)$. Then we divide $Q_0(x)$ by $(x-1)$. The remainder is c_1 and the quotient is $Q_1(x)$. We repeat this until the quotient is a constant. This is best arranged in a tableau of synthetic divisions.

	5	−11	10	−2
1		5	−6	4
	5	−6	4	**2**
1		5	−1	
	5	−1	**3**	
1		5		
	5	**4**		

The remainders are read from bottom to top: $c_3 = 5, c_2 = 4, c_1 = 3, c_0 = 2$. Thus, $5x^3 - 11x^2 + 10x - 2 = 5(x-1)^3 + 4(x-1)^2 + 3(x-1) + 2$.

8.4.1 Newton's Interpolation Formula

A related expansion expresses a polynomial using a sequence of different linear factors.

***Theorem* 8.4.2.** Any polynomial $P_n(x)$ of degree n may be put into the form

$$P_n(x) = A_0 + A_1(x-a_1) + A_2(x-a_1)(x-a_2) + \cdots + A_n(x-a_1)\cdots(x-a_n),$$

where $A_0, \ldots, A_n$ are constants.

Proof. Divide $P_n(x)$ by $(x-a_1)$ to get a quotient $P_{n-1}(x)$ and a constant remainder A_0. Divide $P_{n-1}(x)$ by $(x-a_2)$ to get a quotient $P_{n-2}(x)$ and a constant remainder A_1. Continue this process. The constants A_i are the successive remainders. ■

Example 8.4.2. Express $x^3 - 1$ in the form $A_0 + A_1(x-1) + A_2(x-1)(x-2) + A_3(x-1)(x-2)(x-3)$. We perform successive divisions by $(x-1), (x-2), (x-3)$.

1. Divide $x^3 - 1$ by $(x-1)$. Using synthetic division with $a = 1$:

	1	0	0	−1
1		1	1	1
	1	1	1	**0**

   The quotient is $x^2 + x + 1$ and the remainder is $A_0 = 0$.

2. Divide $x^2 + x + 1$ by $(x-2)$. Using synthetic division with $a = 2$:

	1	1	1
2		2	6
	1	3	**7**

   The quotient is $x + 3$ and the remainder is $A_1 = 7$.

3. Divide $x + 3$ by $(x-3)$. The remainder is $A_2 = 3 + 3 = 6$. The quotient is 1, which is A_3.

So, $x^3 - 1 = 0 + 7(x-1) + 6(x-1)(x-2) + 1(x-1)(x-2)(x-3)$.

8.5 Exercises

Part I: Infinite Series from Division

1. Find the first four terms in the descending series expansion of $\frac{x^3-3x^2+1}{x^2+x+1}$.

2. Find the first four terms in the ascending series expansion of $\frac{1-3x^2+x^3}{1+x+x^2}$.

3. Find the first five terms of the ascending series for $\frac{1+x}{1-x+x^2}$.

4. Find the first four terms of the descending series for $\frac{x^4+x^2-1}{x^3-x}$.

5. For the division of 1 by $1-2x$, find the first four terms of the ascending series and state the remainder term at that point, in the form of the identity $\frac{A}{D} = P + \frac{R}{D}$.

6. By division, show that the first three terms of the ascending series for $\frac{1}{(1-x)^2}$ are $1 + 2x + 3x^2$.

Remark. First, expand $(1-x)^2$.

7. Find the first three terms and the remainder term when x^n is divided by $x-1$ (assuming n is a large positive integer).

8. Find the first three terms in the ascending series for $\frac{2-3x}{1+x-2x^2}$.

Part II: Expansion in Powers of a Polynomial

Remark. The key computational skill in this section is repeated division. For the special case of linear factors $(x-a)$, the tableau method of repeated synthetic division is the most efficient.

9. Use repeated synthetic division to express the polynomial $P(x) = x^4 - 5x^3 + 7x^2 - 3x + 1$ in powers of $(x-1)$.

10. Express $P(y) = 2y^4 + 3y^2 - 8y + 5$ in powers of $(y+2)$.

11. Express $P(a) = a^3 + a + 1$ in powers of $(a+4)$.

12. Let $P(x) = 4x^3 - 6x^2 + 8x - 5$. Find the expansion of this polynomial in powers of $(2x-1)$.

Remark. First, express the polynomial in powers of $(x - \frac{1}{2})$. Then substitute $(x - \frac{1}{2}) = \frac{1}{2}(2x-1)$.

13. Let $P(x) = c_0 + c_1(x-a) + c_2(x-a)^2 + \ldots$. Explain, using the Remainder Theorem, why the coefficient c_0 must be equal to $P(a)$.

14. Express the polynomial $P(x) = x^5 - 2x^4 + x^2 - 1$ in the form $R_0 + R_1(x^2-1) + R_2(x^2-1)^2$.

Remark. This requires repeated long division by the quadratic factor $x^2 - 1$.

15. Express $P(x) = x^6$ in powers of $(x^2 - x)$.

16. Verify your answer from question 9 by expanding the result and showing that it simplifies back to the original polynomial.

17. If $P(x) = 2(x-3)^4 + 5(x-3)^3 - (x-3)^2 + 7(x-3) - 4$, what is the remainder when $P(x)$ is divided by $(x-3)$? What is the remainder when the resulting quotient is divided by $(x-3)$?

18. Express $1 + x + x^2 + x^3$ in powers of $1 + x$.

Part III: Newton's Interpolation Formula

19. Use Newton's formula to express $P(x) = x^3 + x^2 + x + 1$ in the form $A_0 + A_1(x-1) + A_2(x-1)(x-2) + A_3(x-1)(x-2)(x-3)$.

20. Express $P(y) = 2y^3 - 5y^2 + 3y + 1$ in the form $A_0 + A_1(y+1) + A_2(y+1)y + A_3(y+1)y(y-1)$.

21. Find the polynomial of the second degree whose values are $3, 7, 13$ when $x = 1, 2, 3$ respectively.

22. Find the cubic polynomial which takes the values $1, 0, 1, 10$ when $x = 0, 1, 2, 3$ respectively.

23. Let $P(x)$ be a polynomial written in Newton's form with base points $a_1, a_2, \ldots$.

$$P(x) = A_0 + A_1(x - a_1) + A_2(x - a_1)(x - a_2) + \ldots$$

Show that $A_0 = P(a_1)$ and $A_1 = \frac{P(a_2) - P(a_1)}{a_2 - a_1}$.

24. Express x^4 in the form $A_0 + A_1(x+2) + A_2(x+2)(x+1) + A_3(x+2)(x+1)x + A_4(x+2)(x+1)x(x-1)$.

Part IV: Proofs and Challenge Problems

25. Prove that the expansion of a polynomial in powers of $(x - a)$ is unique.

26. Let $S(x) = \frac{1+x}{1-x-x^2}$. By assuming it can be written as an ascending series $S(x) = \sum_{n=0}^{\infty} c_n x^n$, prove that the coefficients satisfy the recurrence relation $c_n = c_{n-1} + c_{n-2}$ for $n \geq 2$, with $c_0 = 1, c_1 = 2$.

Remark. Start from the identity $1 + x = (1 - x - x^2)(c_0 + c_1 x + c_2 x^2 + \ldots)$. Expand the right-hand side and equate the coefficients of like powers of x.

27. Let $P(x)$ be expressed in powers of $(x - a)$ as $P(x) = \sum_{k=0}^{n} c_k (x - a)^k$. Now express $P(x)$ in powers of $(x - b)$. Let the new coefficients be d_k. Find a formula for d_k in terms of the coefficients c_j and the quantity $(b - a)$.

Remark. Write $(x - a) = (x - b) + (b - a)$ and substitute this into the first expansion.

28. Prove the general form of Newton's interpolation formula stated in the text.

29. $\star$ Let $f(x)$ be a polynomial. Let $f_h(x) = \frac{f(x+h) - f(x)}{h}$ be the difference quotient.

(a) If $f(x) = x^n$, show that $f_h(x)$ is a polynomial in x and h of degree $n - 1$ in x.

(b) Express $f(x) = \sum c_k (x - a)^k$. Use this form to compute $f(a + h)$ and show that $f_h(a) = c_1 + c_2 h + c_3 h^2 + \ldots$.

(c) As h becomes very small, what value does $f_h(a)$ approach? This provides a link between the algebraic expansion and the calculus concept of a derivative.

30. $\star\star$ **Taylor's Expansion for Polynomials.** This problem develops a direct formula for the coefficients in the expansion of a polynomial in powers of $(x - a)$, generalising the idea from the previous starred problem.

(a) **The Formal Derivative.** For a polynomial $f(x) = \sum_{k=0}^{n} p_k x^k$, its formal derivative is $f'(x) := \sum_{k=1}^{n} k p_k x^{k-1}$. The second derivative, $f''(x)$, is the derivative of $f'(x)$, and so on. Let $f^{(j)}(x)$ denote the j-th derivative.

Calculate the first, second, and third derivatives of $f(x) = x^4 - 3x^3 + 5x^2 - x + 2$.

(b) **Derivatives of the Expansion.** Let $f(x)$ be expressed as $f(x) = c_0 + c_1(x - a) + c_2(x - a)^2 + c_3(x - a)^3 + \cdots + c_n(x - a)^n$. Prove that the derivative of $(x - a)^k$ is $k(x - a)^{k-1}$. Use this to find expressions for $f'(x), f''(x), f'''(x), \ldots$

(c) **Finding the Coefficients.** By evaluating the expressions from part (b) at the specific point $x = a$, prove the following sequence of results:

i. $f(a) = c_0$
ii. $f'(a) = c_1$
iii. $f''(a) = 2c_2$
iv. $f'''(a) = 6c_3 = 3!\, c_3$

(d) **The General Formula.** Generalise your findings to prove that the coefficient c_k in the expansion is given by the formula

$$c_k = \frac{f^{(k)}(a)}{k!}.$$

This gives the full Taylor expansion for a polynomial about the point a.

(e) **Application.** Use this formula to find the expansion of $f(x) = x^4 - 2x^2 + x - 1$ in powers of $(x - 2)$ without using repeated synthetic division.

Chapter 9

GCM and LCM

Having seen how to test for divisibility, we are naturally led to the problem of finding what two polynomials may have in common as a divisor.

9.1 G.C.D.

Remark. The term "measure" (G.C.M.) is an older, though perfectly valid, term for "divisor". In modern usage, "Greatest Common Divisor" (G.C.D.) is standard. We will adopt the modern G.C.D. notation throughout this text.

Definition 9.1.1. ***(Common Divisor)***. A common divisor of two or more polynomials is any polynomial that divides each of them exactly.

Definition 9.1.2. ***(Greatest Common Divisor)***. The greatest common divisor (G.C.D.) is the common divisor of the highest possible degree. Any constant multiple of a G.C.D. is also a G.C.D. In practice, we typically select the one with the simplest integer coefficients, often with a positive leading coefficient, known as the monic G.C.D.

G.C.D. by Inspection of Factors

When polynomials are presented in their factorised form, their G.C.D. can be found by a simple inspection, analogous to finding the greatest common factor of integers from their prime factorisations.

***Theorem* 9.1.1.** The G.C.D. of several factorised polynomials is the product of all factors that are common to every polynomial, where each common factor is raised to the lowest power in which it appears in any of the polynomials.

Proof. Let the polynomials be $P, P', P'', \ldots$. Any common divisor can only contain factors that are present in all of the polynomials. To be the common divisor of the highest degree, it must include every common factor. For any such common factor, say $(x-a)$, if it is raised to a power higher than its lowest exponent in the set of polynomials, it would fail to be a divisor of at least one of them. Therefore, to remain a divisor of all, each common factor must be taken with its lowest occurring exponent. ■

Example 9.1.1. Let $P = 2x^2 - 6x + 4 = 2(x-1)(x-2)$ and $P' = 6x^2 - 6x - 12 = 6(x+1)(x-2)$. The only factor common to both is $(x-2)$. It appears to the power of 1 in both. Hence, the G.C.D. is $(x-2)$.

Example 9.1.2. Consider the three polynomials:

$$P = x^5 - 5x^4 + 7x^3 + x^2 - 8x + 4 = (x-1)^2(x+1)(x-2)^2$$
$$P' = x^6 - 7x^5 + 17x^4 - 13x^3 - 10x^2 + 20x - 8 = (x-1)^2(x+1)(x-2)^3$$
$$P'' = x^5 - x^4 - 3x^3 + x^2 + 2x = x(x-1)(x+1)^2(x-2)$$

The common factors are $(x-1)$, $(x+1)$, and $(x-2)$.

- The lowest power of $(x-1)$ is 1 (from P'').
- The lowest power of $(x+1)$ is 1 (from P and P').
- The lowest power of $(x-2)$ is 1 (from P'').

The factor x is not common to all three. The G.C.D. is therefore $(x-1)(x+1)(x-2) = x^3 - 2x^2 - x + 2$.

The Case of Monomials

The rule for factorised polynomials simplifies neatly for monomials.

***Theorem* 9.1.2.** The G.C.D. of several monomials is the product of all variables common to each, where each variable is raised to the lowest power it holds in any of the monomials.

Example 9.1.3. Consider the monomials $12x^5y^2z^3$ and $18x^3y^4z$.

- The common variables are x, y, z.
- The lowest power of x is x^3.
- The lowest power of y is y^2.
- The lowest power of z is z^1.

Ignoring the numerical coefficients, the algebraical G.C.D. is x^3y^2z.

A Cautionary Note: Algebraical versus Arithmetical G.C.D.

It is crucial to distinguish the algebraical G.C.D. from its arithmetical counterpart. The term 'greatest' in algebra refers exclusively to the degree of the polynomial, not its numerical value for a given x. The two concepts do not, in general, align.

Example 9.1.4. Consider the polynomials $A(x) = x^2 - 3x + 2 = (x-1)(x-2)$ and $B(x) = x^2 - x - 2 = (x+1)(x-2)$. Their algebraical G.C.D. is clearly $G(x) = x - 2$.

Let us now substitute a particular value, for instance $x = 31$.

- The numerical value of $A(31)$ is $31^2 - 3(31) + 2 = 961 - 93 + 2 = 870$.
- The numerical value of $B(31)$ is $31^2 - 31 - 2 = 961 - 33 = 928$.
- The numerical value of the algebraical G.C.D. is $G(31) = 31 - 2 = 29$.

However, the arithmetical G.C.D. of the numbers 870 and 928 is 58. Clearly, $58 \neq 29$. No definition of the algebraical G.C.D. can be framed such that its numerical evaluation will always yield the arithmetical G.C.D. of the evaluated functions.

9.1.1 The G.C.D. Algorithm (The Long Rule)

The method of finding the G.C.D. by inspecting factors is only practical when the polynomials are already factorised. Since we lack a general method for factorising high-degree polynomials, we need a systematic process that works for any pair of polynomials. This process is analogous to the Euclidean algorithm for finding the G.C.D. of two integers and is based on a single, powerful proposition.

***Theorem* 9.1.3.** If A, B, Q, R are polynomials such that $A = BQ + R$, then the G.C.D. of A and B is the same as the G.C.D. of B and R.

Proof. Let $G_1 = G.C.D.(A, B)$ and $G_2 = G.C.D.(B, R)$. We must show that G_1 and G_2 divide each other, which implies they are the same (up to a constant multiple).

1. *First, we show that any common divisor of B and R also divides A. Let C be a common divisor of B and R. Then $B = C \cdot P_1$ and $R = C \cdot P_2$ for some polynomials P_1, P_2. Substituting into the given equation:*
$$A = (C \cdot P_1)Q + (C \cdot P_2) = C(P_1Q + P_2).$$
This shows that C also divides A. Thus, every common divisor of B and R is also a common divisor of A and B.

2. *Second, we show that any common divisor of A and B also divides R. Let C' be a common divisor of A and B. We can rearrange the given equation to $R = A - BQ$. Since C' divides both A and B, it must divide their combination, $A - BQ$. Thus, C' also divides R. This means every common divisor of A and B is also a common divisor of B and R.*

Since the set of common divisors for the pair (A, B) is identical to the set for the pair (B, R), their greatest common divisors must be the same. ■

This theorem allows us to replace the problem of finding G.C.D.(A, B) with the simpler problem of finding G.C.D.(B, R), where R is the remainder of A divided by B and has a lower degree than A. We can repeat this process, generating a sequence of polynomials of decreasing degree. This is the Euclidean Algorithm for polynomials.

The Algorithm

Let A and B be two polynomials, with $\deg(A) \geq \deg(B)$.

1. Divide A by B to find quotient Q_1 and remainder R_1.
2. Divide B by R_1 to find quotient Q_2 and remainder R_2.
3. Divide R_1 by R_2 to find quotient Q_3 and remainder R_3.
4. Continue this process until a remainder of zero is obtained.

The degrees of the remainders are strictly decreasing, so the process must terminate.

$$\begin{aligned} A &= BQ_1 + R_1 \\ B &= R_1Q_2 + R_2 \\ R_1 &= R_2Q_3 + R_3 \\ &\vdots \\ R_{n-2} &= R_{n-1}Q_n + R_n \\ R_{n-1} &= R_nQ_{n+1} + 0 \end{aligned}$$

By the fundamental theorem, we have the chain of equalities:

$$\text{G.C.D.}(A, B) = \text{G.C.D.}(B, R_1) = \text{G.C.D.}(R_1, R_2) = \cdots = \text{G.C.D.}(R_{n-1}, R_n) = \text{G.C.D.}(R_n, 0).$$

The greatest polynomial that divides both R_n and 0 is simply R_n itself.

- **Conclusion I:** The last non-zero remainder in the algorithm is the G.C.D. of A and B.
- **Conclusion II:** If the last non-zero remainder is a constant, the polynomials have no common divisor other than a constant. We say they are relatively prime, and their G.C.D. is taken to be 1.

Practical Simplifications

The algorithm can produce complicated fractions. To simplify the arithmetic, we are permitted to make the following modification at any step:

- We may multiply or divide any divisor or remainder by any non-zero constant.

This is permissible because we are concerned with the degree and factors of the G.C.D., not its specific numerical coefficient. Multiplying by a constant does not introduce a new polynomial factor, so it does not alter the final G.C.D. This allows us to clear fractions or reduce the size of coefficients at every stage.

Example 9.1.5. Find the G.C.D. of $A(x) = x^5 - 2x^4 - 2x^3 + 8x^2 - 7x + 2$ and $B(x) = x^4 - 4x + 3$. We use detached coefficients.

1. **Divide A by B:** The quotient is $(x - 2)$, and the remainder is $R_1 = -2x^3 + 12x^2 - 18x + 8$. To simplify, we can divide R_1 by -2 to get $R_1' = x^3 - 6x^2 + 9x - 4$. We now find G.C.D.$(B, R_1')$.
2. **Divide B by R_1':** $B = x^4 - 4x + 3$ and $R_1' = x^3 - 6x^2 + 9x - 4$. The quotient is $(x + 6)$, and the remainder is $R_2 = 27x^2 - 54x + 27$. Simplify R_2 by dividing by 27 to get $R_2' = x^2 - 2x + 1$. We now find G.C.D.(R_1', R_2').
3. **Divide R_1' by R_2':** $R_1' = x^3 - 6x^2 + 9x - 4$ and $R_2' = x^2 - 2x + 1$. The quotient is $(x - 4)$, and the remainder is $R_3 = 0$.

The process terminates. The last non-zero remainder (in its simplified form) was $R_2' = x^2 - 2x + 1$. Therefore, the G.C.D. is $x^2 - 2x + 1$.

The calculation using detached coefficients can be arranged compactly:

A	1	-2	-2	8	-7	2
B	1	0	0	-4	3	
R_1		-2	12	-18	8	(Remainder of A/B)
R_1'		1	-6	9	-4	(Divide by -2)
R_2			27	-54	27	(Remainder of B/R_1')
R_2'			1	-2	1	(Divide by 27)
R_3				0	0	(Remainder of R_1'/R_2')

9.1.2 Alternative Methods for the G.C.D.

Method of Alternate Elimination of Terms

This method is based on the following general principle.

***Theorem* 9.1.4.** Let A, B be two polynomials. If two new polynomials, P and Q, are formed by the linear combinations

$$P = lA + mB$$
$$Q = pA + qB$$

where l, m, p, q are constants such that $lq - mp \neq 0$, then the G.C.D. of the new pair (P, Q) is the same as the G.C.D. of the original pair (A, B).

Proof. First, any common divisor of A and B must also divide any linear combination of them. Thus, G.C.D.(A, B) divides both P and Q. Conversely, we can express A and B in terms of P and Q. Solving the system of equations for A and B, we find:

$$qP - mQ = q(lA + mB) - m(pA + qB) = (lq - mp)A$$
$$-pP + lQ = -p(lA + mB) + l(pA + qB) = (lq - mp)B$$

Since $lq - mp$ is a non-zero constant, this shows that any common divisor of P and Q must also divide A and B. As the pairs (A, B) and (P, Q) have the same set of common divisors, their G.C.D. must be the same. ■

In practice, we choose the constants to eliminate either the highest or lowest degree terms.

- To eliminate the highest degree terms, we form a new polynomial $A' = lA + mB$.
- To eliminate the lowest degree terms (the constants), we form another new polynomial $B' = pA + qB$.

We then find the G.C.D. of the new, lower-degree pair (A', B').

Example 9.1.6. Find the G.C.D. of $A = 4x^4 + 26x^3 + 41x^2 - 2x - 24$ and $B = 3x^4 + 20x^3 + 32x^2 - 8x - 32$.

The leading coefficients are 4 and 3. To eliminate the x^4 term, we can form $P = 3A - 4B$. The constant terms are -24 and -32. To eliminate them, we can form $Q = 4A - 3B$.

$$P = 3(4x^4 + \dots) - 4(3x^4 + \dots) = (78 - 80)x^3 + \cdots = -2x^3 - 5x^2 + 26x + 56$$
$$Q = 4(4x^4 + \dots) - 3(3x^4 + \dots) = (104 - 60)x^3 + \cdots = 7x^4 + 44x^3 + 68x^2 + 16x$$

We can simplify P to $P' = 2x^3 + 5x^2 - 26x - 56$ and Q to $Q' = x(7x^3 + 44x^2 + 68x + 16)$. Since x is not a factor of A or B, it cannot be part of the G.C.D., so we find the G.C.D. of P' and $Q'' = 7x^3 + 44x^2 + 68x + 16$. We can repeat the process with P' and Q'':

$$7P' - 2Q'' = 7(2x^3 + \dots) - 2(7x^3 + \dots) = (35 - 88)x^2 + \cdots = -53x^2 - 318x - 424$$
$$\to x^2 + 6x + 8 \text{ (dividing by -53)}$$

We can now test if $x^2 + 6x + 8 = (x + 2)(x + 4)$ is the G.C.D. by dividing it into one of the original polynomials. Division of A by $x^2 + 6x + 8$ gives a remainder of zero. Thus, $x^2 + 6x + 8$ is the G.C.D.

Semi-Tentative Method

This approach relies on a simple observation and can often be the fastest method.

***Theorem* 9.1.5.** Every common divisor of two polynomials A and B must also divide their difference, $A - B$.

Proof. If C divides A and C divides B, then $A = CP_1$ and $B = CP_2$. Then $A - B = C(P_1 - P_2)$, so C must also divide $A - B$. ■

The strategy is to compute the difference $A - B$, which will have a lower degree. We then find all the factors of this simpler polynomial. The G.C.D. of A and B must be among these factors. We can then test each factor using the Remainder Theorem.

Example 9.1.7. Find the G.C.D. of $A = 2x^4 - 3x^3 - 3x^2 + 4$ and $B = 2x^4 - x^3 - 9x^2 + 4x + 4$.

The G.C.D. must divide their difference:

$$\begin{aligned} B - A &= (2x^4 - x^3 - 9x^2 + 4x + 4) - (2x^4 - 3x^3 - 3x^2 + 4) \\ &= 2x^3 - 6x^2 + 4x \\ &= 2x(x^2 - 3x + 2) \\ &= 2x(x-1)(x-2) \end{aligned}$$

The G.C.D. must be a product of some of the factors $\{x, (x-1), (x-2)\}$.

- Is x a factor? $A(0) = 4 \neq 0$. No.
- Is $(x-1)$ a factor? $A(1) = 2 - 3 - 3 + 4 = 0$. Yes. $B(1) = 2 - 1 - 9 + 4 + 4 = 0$. Yes.
- Is $(x-2)$ a factor? $A(2) = 2(16) - 3(8) - 3(4) + 4 = 32 - 24 - 12 + 4 = 0$. Yes. $B(2) = 2(16) - 8 - 9(4) + 4(2) + 4 = 32 - 8 - 36 + 8 + 4 = 0$. Yes.

The common factors are $(x-1)$ and $(x-2)$. Therefore, the G.C.D. is $(x-1)(x-2) = x^2 - 3x + 2$.

G.C.D. of Three or More Polynomials

The G.C.D. of a set of polynomials can be found by a successive application of the algorithm for two.

***Theorem* 9.1.6.** Every common divisor of two polynomials A and B is also a divisor of their G.C.D.

To find the G.C.D. of three polynomials A, B, C:

1. Find $G_1 = \text{G.C.D.}(A, B)$.
2. Find $G_2 = \text{G.C.D.}(G_1, C)$.

Then G_2 is the G.C.D. of A, B, and C. This process extends to any number of polynomials.

9.1.3 Properties of Relatively Prime Polynomials

Definition 9.1.3. ***(Relatively Prime)***. Two polynomials are said to be relatively prime (or prime to each other) if their only common divisors are constants.

The properties of relatively prime polynomials are analogous to those of relatively prime integers. The cornerstone of these properties is Bézout's Identity for polynomials.

***Theorem* 9.1.7. (Bézout's Identity for Polynomials)**. If A and B are two polynomials, there exist polynomials L and M such that

$$LA + MB = \text{G.C.D.}(A, B).$$

In particular, if A and B are relatively prime, there exist polynomials L and M such that

$$LA + MB = 1.$$

Proof. This identity is a direct consequence of the Euclidean Algorithm. Each remainder in the process can be expressed as a linear combination of the previous two.

$$R_1 = A - Q_1 B$$
$$R_2 = B - Q_2 R_1 = B - Q_2(A - Q_1 B) = (-Q_2)A + (1 + Q_1 Q_2)B$$
$$\vdots$$

By working backwards through the steps of the algorithm (a process known as the Extended Euclidean Algorithm), we can express the final non-zero remainder, which is the G.C.D., as a linear combination of the original polynomials A and B. ■

This identity leads to several important corollaries, which are the polynomial analogues of Euclid's Lemma.

***Corollary* 9.1.1.** If a polynomial B divides the product AH and is relatively prime to A, then B must divide H.

Proof. Since A and B are relatively prime, there exist polynomials L, M such that $LA+MB = 1$. Multiplying by H gives $LAH+MBH = H$. By hypothesis, B divides AH, so we can write $AH = BK$ for some polynomial K. Substituting this in gives $L(BK)+MBH = H$, which simplifies to $B(LK+MH) = H$. This shows that B divides H. ■

***Corollary* 9.1.2.** If a polynomial is prime to several other polynomials, it is prime to their product or in other words if $\gcd(A, B_i) = 1$ for $i = 1, \dots, k$, then

$$\gcd\left(A, \prod_{i=1}^{k} B_i\right) = 1.$$

Proof. Proof based by Induction.

(i) Base $k = 2$. Suppose D divides A and D divides BC. Because $\gcd(A, B) = 1$ and $D \mid A$ any common divisor of D and B would also divide A, hence $\gcd(D, B) = 1$. By corollary 9.1.1 from $D \mid BC$ and $\gcd(D, B) = 1$ then D divides C. But $\gcd(A, C) = 1$ and D divides A force D to be constant, hence $\gcd(A, BC) = 1$.

(ii) Inductive step. If $\gcd(A, \prod_{i=1}^{k-1} B_i) = 1$ and $\gcd(A, B_k) = 1$, apply the base case to $B = \prod_{i=1}^{k-1} B_i$ and $C = B_k$.

■

***Corollary* 9.1.3.** If a set of polynomials $\{A, B, \dots\}$ are each resolved into factors that are relatively prime to each other, the G.C.D. of the set is found by taking the product of all common factors, each raised to the lowest power in which it appears.

Proof. Let the set of polynomials be $\{P_1, P_2, \dots\}$. Let the set of all unique factors appearing in any of these polynomials be $\{F_1, F_2, \dots, F_k\}$, which are by hypothesis relatively prime to one another. Each polynomial P_j can be written in the form:

$$P_j = F_1^{e_{j,1}} F_2^{e_{j,2}} \cdots F_k^{e_{j,k}}$$

where the exponent $e_{j,i}$ is zero if the factor F_i is not present in P_j.
Let G be the polynomial constructed according to the rule in Theorem 9.1.1. That is,

$$G = F_1^{m_1} F_2^{m_2} \cdots F_k^{m_k}, \quad \text{where } m_i = \min(e_{1,i}, e_{2,i}, \dots).$$

We must show that G is a common divisor, and that it is the greatest such divisor.

1. *G **is a common divisor.** For any polynomial P_j in the set, the exponent $e_{j,i}$ of each factor F_i is, by definition of the minimum, greater than or equal to m_i. Thus, we can write*

$$P_j = G \cdot (F_1^{e_{j,1}-m_1} F_2^{e_{j,2}-m_2} \cdots F_k^{e_{j,k}-m_k}).$$

Since all exponents in the second term are non-negative, this is a valid polynomial expression, which shows that G divides every P_j. Hence, G is a common divisor.

2. *G **is the greatest common divisor.** Let D be any other common divisor of the set. Any factor of D must also be a factor of each P_j. Since the factors $\{F_i\}$ are relatively prime, D can only be composed of products of these same factors. Let the highest power of F_i that divides D be F_i^s.*
Since D divides every P_j, it follows that F_i^s must divide every P_j. Let us write $P_j = F_i^{e_{j,i}} \cdot H_j$, where H_j is the product of all other factors of P_j. By hypothesis, F_i is relatively prime to every factor in H_j, and thus by the preceding corollary, it is relatively prime to their product H_j. That is, $G.C.D.(F_i, H_j) = 1$, which implies $G.C.D.(F_i^s, H_j) = 1$.
Now, since F_i^s divides the product $F_i^{e_{j,i}} H_j$ and is relatively prime to H_j, it follows from corollary 9.1.1 that F_i^s must divide $F_i^{e_{j,i}}$. This implies that $s \leq e_{j,i}$.
This inequality must hold for every polynomial P_j in the set. Therefore, s must be less than or equal to the minimum of all such exponents: $s \leq \min(e_{1,i}, e_{2,i}, \dots) = m_i$.
This argument applies to every factor F_i of D. Thus, every factor in D appears with a power no greater than its power in G. It follows that D must divide G.

Since G is a common divisor and any other common divisor D must divide G, G is, by definition, the greatest common divisor. ■

Remark. This provides a formal justification for the method of inspection we introduced at the start of the chapter.

9.2 The Least Common Multiple

Closely allied to the problem of finding the G.C.D. of a set of polynomials is the problem of finding the polynomial of least degree which is divisible by each of them.

Definition 9.2.1. ***(Least Common Multiple)***. The least common multiple (L.C.M.) of two or more polynomials is the polynomial of lowest degree that is exactly divisible by each of them.

L.C.M. of Monomials

For monomials, the L.C.M. is found by taking the product of all variables that appear in any of the monomials, each raised to the highest power in which it occurs.

Example 9.2.1. Consider the monomials $3x^3yz^2$, $6x^2y^3z^4$, and $8xyzu$.

- The variables present are x, y, z, u.
- The highest power of x is x^3.
- The highest power of y is y^3.
- The highest power of z is z^4.
- The highest power of u is u^1.

The algebraical L.C.M. is therefore $x^3y^3z^4u$. The L.C.M. of the numerical coefficients $(3, 6, 8)$ is 24.

9.2.1 Relationship between L.C.M. and G.C.D.

***Theorem* 9.2.1.** The L.C.M. of two polynomials, A and B, is their product divided by their G.C.D.

$$\text{L.C.M.}(A, B) = \frac{A \cdot B}{\text{G.C.D.}(A, B)}.$$

Proof. Let $G = G.C.D.(A, B)$. We can write $A = aG$ and $B = bG$, where a and b are two polynomials that are relatively prime. Let M be any common multiple of A and B. Since M is divisible by A, we can write $M = PA$ for some polynomial P. Substituting $A = aG$, we have $M = PaG$. Since M is also divisible by B, the quotient M/B must be a polynomial.

$$\frac{M}{B} = \frac{PaG}{bG} = \frac{Pa}{b}.$$

For this expression to be a polynomial, b must divide the product Pa. Since a and b are relatively prime, it follows that b must divide P. We can therefore write $P = Qb$ for some polynomial Q. Substituting this back into the expression for M, we get

$$M = (Qb)aG = Q(abG).$$

This shows that every common multiple of A and B is a multiple of the polynomial abG. To find the common multiple of the least *degree, we must choose the arbitrary polynomial Q to have the lowest possible degree, which is degree zero. Thus, we choose Q to be a constant, say* 1*. The L.C.M. is therefore abG. We can rewrite this expression as:*

$$L.C.M. = abG = \frac{(aG)(bG)}{G} = \frac{A \cdot B}{G}.$$

■

***Corollary* 9.2.1.** Every common multiple of two polynomials is a multiple of their least common multiple.

9.2.2 Finding the L.C.M.

The relationship between the L.C.M. and G.C.D. provides a method for finding the L.C.M. of any number of polynomials. To find the L.C.M. of a set of polynomials $A, B, C, \ldots$:

1. Find $L_1 = \text{L.C.M.}(A, B)$.
2. Find $L_2 = \text{L.C.M.}(L_1, C)$.
3. Continue this process until all polynomials have been included. The final result is the L.C.M. of the entire set.

L.C.M. by Inspection of Factors

When the polynomials are already factorised, a more direct method is available.

***Theorem* 9.2.2.** The L.C.M. of a set of factorised polynomials is the product of all distinct factors that appear in any of the polynomials, each raised to the highest power in which it occurs.

Example 9.2.2. . Let the functions be:

$$P_1 = (x-1)^2(x+2)^3(x^2+x+1)$$
$$P_2 = (x-2)^2(x-3)(x^2-x+1)^2$$
$$P_3 = (x-1)^5(x-2)^3(x-3)^4(x^2+x+1)^3$$

The distinct factors appearing across all polynomials are $(x-1), (x+2), (x^2+x+1), (x-2), (x-3)$, and (x^2-x+1). We take each factor raised to its highest observed power.

- Highest power of $(x-1)$ is 5 (from P_3).
- Highest power of $(x+2)$ is 3 (from P_1).
- Highest power of (x^2+x+1) is 3 (from P_3).
- Highest power of $(x-2)$ is 3 (from P_3).
- Highest power of $(x-3)$ is 4 (from P_3).
- Highest power of (x^2-x+1) is 2 (from P_2).

The L.C.M. is the product of these:

$$\text{L.C.M.} = (x-1)^5(x+2)^3(x-2)^3(x-3)^4(x^2+x+1)^3(x^2-x+1)^2.$$

9.3 Exercises

Part I: G.C.D. and L.C.M. by Inspection

1. Find the G.C.D. of the following monomials.

(a) $15x^3y^4z$ and $25x^2y^5z^2$

(b) $8a^2b^3c$, $12ab^4c^2$, and $20a^3bc^3$

2. Find the L.C.M. of the following monomials.

(a) $9p^4q^2r^3$ and $12p^2q^3r^5$

(b) $2x^2y$, $3xy^2z$, and $4y^3z^2$

3. Find the G.C.D. of the following factorised polynomials.

(a) $(x-1)^2(x+2)$ and $(x-1)(x-3)$

(b) $6a^2(a-b)^3(a+b)$ and $4a^3(a-b)^2(a+c)$

(c) $x(x-1)^2(x+1)^3$, $x^2(x-1)(x-2)^2$, and $3x(x-1)^3(x+1)$

4. Find the L.C.M. of the following factorised polynomials.

(a) $(x-a)^2(x-b)$ and $(x-a)(x-b)^3$

(b) x^2-1 and x^2-3x+2

(c) $(a-b)(b-c)$, $(b-c)(c-a)$, and $(c-a)(a-b)$

5. Find the G.C.D. and L.C.M. of $15(x+y)^2(x-y)$ and $20(x^2-y^2)$.

6. Find the G.C.D. of $(a^2-ab)^2$ and $ab(a^2-b^2)$.

7. Find the G.C.D. of x^2-y^2, x^3-y^3, and $x^2-7xy+6y^2$.

8. Find the L.C.M. of a^2-4b^2, a^3-8b^3, and $a^2-ab-2b^2$.

Part II: The Euclidean Algorithm

Remark. Use the method of long division with detached coefficients to find the G.C.D. Remember to simplify remainders at each step by removing any numerical factors to keep the calculations manageable.

9. Find the G.C.D. of x^3-x^2-x-2 and x^3-3x-2.

10. Find the G.C.D. of $x^4 - x^3 + 2x^2 + x + 3$ and $x^4 + 2x^3 - x - 2$.

11. Find the G.C.D. of $2x^3 + x^2 - x - 2$ and $x^3 - x^2 - x + 1$.

12. Find the G.C.D. of $6x^3 - 7x^2 - x + 2$ and $2x^3 - x^2 + 3x - 2$.

13. Find the G.C.D. of $3a^4 + a^3 - 2a^2 - a - 1$ and $2a^4 - a^3 - 3a^2 + 3a - 1$.

14. Find the G.C.D. of $x^3 - 1$ and $x^2 + x + 1$. What does the result imply?

15. Find the G.C.D. of $x^4 + x^2 + 1$ and $x^4 - x^3 - x - 1$.

16. Find the G.C.D. of $A = x^3 - 6x^2 + 11x - 6$, $B = x^3 - 9x^2 + 26x - 24$, and $C = x^3 - 8x^2 + 19x - 12$.

Part III: Alternative Methods and L.C.M. Calculation

17. Use the semi-tentative method (difference of polynomials) to find the G.C.D. of the following pairs.

(a) $x^3 + 2x^2 + 3x + 2$ and $x^3 + x^2 + x + 1$

(b) $2x^3 - 11x^2 + 12x + 9$ and $2x^3 - 7x^2 - 9$

(c) $x^4 - x^2 - 2x - 1$ and $x^4 - 2x^2 - 1$

18. Use the method of alternate elimination to find the G.C.D. of $x^3 - 5x^2 - 99x + 40$ and $x^3 - 6x^2 - 86x + 35$.

19. Find the L.C.M. of the following polynomials by first calculating their G.C.D.

(a) $x^2 - 1$ and $x^3 - 1$

(b) $x^2 + 5x + 6$ and $x^2 + 6x + 8$

(c) $x^3 - 3x^2 + 3x - 1$ and $x^3 - x^2 - x + 1$

20. The G.C.D. of two polynomials is $x + 3$ and their L.C.M. is $x^3 - 7x + 6$. If one of the polynomials is $x^2 + x - 6$, what is the other?

21. Find the L.C.M. of $x^4 + x^2 + 1$, $x^2 + x + 1$, and $x^2 - x + 1$.

22. Find the polynomial of lowest degree which has a remainder of 2 when divided by $x - 1$ and a remainder of 1 when divided by $x - 2$.

Part IV: Proofs and Theoretical Problems

23. Prove that if a polynomial P divides polynomials Q and R, then P must divide their sum $Q + R$ and their difference $Q - R$.

24. Use the result of the previous exercise to prove that G.C.D.(A, B) = G.C.D.$(A, A + B)$.

25. Prove that if two polynomials are relatively prime, their squares are also relatively prime.

26. If A and B are relatively prime, and A divides C and B divides C, prove that their product AB must also divide C.

27. Prove that if A and B are relatively prime, then L.C.M.$(A, B) = AB$.

28. Prove that every common multiple of two polynomials is a multiple of their least common multiple.

29. Let A and B be two polynomials and let G = G.C.D.(A, B). Show that the polynomials A/G and B/G are relatively prime.

30. Prove that L.C.M.$(kA, kB) = k \cdot$ L.C.M.(A, B) for any constant k.

31. Show that the process of finding the G.C.D. by eliminating the highest degree terms is equivalent to one step of the Euclidean algorithm.

32. Can the numerical value of the L.C.M. of two polynomials $A(x)$ and $B(x)$ for a specific value of x be different from the arithmetical L.C.M. of the numbers $A(x)$ and $B(x)$? Provide an example.

33. Prove that if A is prime to B and also to C, then it is prime to their product BC.

34. Let $G = \text{G.C.D.}(A, B)$ and $L = \text{L.C.M.}(A, B)$. Prove that $GL = AB$.

35. $\star$ Use the Euclidean Algorithm to find polynomials $L(x)$ and $M(x)$ such that $L(x)(x^2+1)+M(x)(x-1) = 1$.

36. $\star$ Prove that the polynomials $L(x)$ and $M(x)$ in Bézout's identity are not unique. If $LA + MB = G$ is one solution, find the general form of all other solutions.

37. $\star$ Let $A(x) = x^n - 1$ and $B(x) = x^m - 1$. Find the G.C.D. of $A(x)$ and $B(x)$.

Remark. Consider the Euclidean algorithm for the integers n, m. Let $n = mq + r$. Show that $x^n - 1 = (x^m - 1)(x^{n-m} + \cdots + x^r) + (x^r - 1)$. What does this imply about the relationship between $\text{G.C.D.}(x^n - 1, x^m - 1)$ and $\text{G.C.D.}(x^m - 1, x^r - 1)$?

38. $\star$ Let $G = \text{G.C.D.}(A, B, C)$. Prove that

$$\text{L.C.M.}(A, B, C) = \frac{ABC \cdot G}{\text{G.C.D.}(A, B)\text{G.C.D.}(B, C)\text{G.C.D.}(C, A)}.$$

Chapter 10

Factoring

Having seen how to determine whether a given polynomial is a factor of another, and how to find the factor of highest degree common to two polynomials, we are naturally led to the question: How can any given polynomial be resolved into its constituent factors?

10.1 Tentative Methods

We begin by considering cases where factors of the first degree, with rational coefficients, are suspected or known to exist. These can often be found through a process of educated trial.

Factorisation by Recognising Identities

Every known identity resulting from the distribution of a product, when read in reverse, provides a rule for factorisation. For example, the identity $(x+y)(x-y) = x^2 - y^2$ tells us that the difference of two squares, $x^2 - y^2$, may be resolved into the factors $(x+y)$ and $(x-y)$. The student should review the tables of identities from previous sections from this new perspective.

Factorisation by Trial

When first-degree factors with rational coefficients exist, they can often be found by a tentative process, as the number of possible trial factors is limited.

Example 10.1.1. Factorise $x^2 - 12x + 32$. Let us assume the polynomial is resolvable into a product of the form $(x-a)(x-b)$. Expanding this gives $x^2 - (a+b)x + ab$. By comparing the coefficients with the original polynomial, we must find two numbers, a and b, such that:

$$ab = 32 \quad \text{and} \quad a + b = 12.$$

Since their product is positive, a and b must have the same sign. Since their sum is positive, both must be positive. We need only consider pairs of positive integers whose product is 32: $(1, 32), (2, 16), (4, 8)$. Of these, only the pair $(4, 8)$ has a sum of 12. Thus, the factorisation is $(x-4)(x-8)$.

Example 10.1.2. Factorise $x^3 - 2x^2 - 23x + 60$. If this polynomial has a factor $(x-a)$ where a is an integer, then a must be a divisor of the constant term, 60. The possible integer values for a are therefore $\pm 1, \pm 2, \pm 3, \pm 4, \ldots$. We can test these potential roots using the Remainder Theorem, or more efficiently, with synthetic division. Let us test the factor $(x-3)$, which corresponds to a root of $a = 3$:

	1	−2	−23	60
3		3	3	−60
	1	1	−20	**0**

The remainder is 0, so $(x-3)$ is a factor. The quotient is the quadratic polynomial x^2+x-20. We can factor this by inspection, seeking two numbers that multiply to -20 and add to 1. The numbers are 5 and -4. So, $x^2+x-20=(x+5)(x-4)$. The complete factorisation is therefore $(x-3)(x-4)(x+5)$.

Example 10.1.3. Factorise $6x^2-19x+15$.. We assume a factorisation of the form $(ax+b)(cx+d)$. By comparing coefficients, we know that $ac=6$ and $bd=15$. This leads to a number of possibilities for the integer pairs (a,c) and (b,d). A few trials reveal the correct combination:

$$6x^2-19x+15=(2x-3)(3x-5).$$

Factorisation by Grouping

In many cases, a polynomial's factors can be revealed by a suitable grouping of its terms. If an expression can be arranged as a sum of groups where each group shares a common factor, then that common factor must be a factor of the entire expression.

Example 10.1.4. Factorise $x^3-2x^2-23x+60$ by grouping.. We can test for the factor $(x-3)$ by attempting to extract it from groups of terms.

$$\begin{aligned}x^3-2x^2-23x+60 &= x^2(x-3)+x^2-23x+60\\ &= x^2(x-3)+x(x-3)-20x+60\\ &= x^2(x-3)+x(x-3)-20(x-3)\\ &= (x^2+x-20)(x-3)\end{aligned}$$

This confirms that $(x-3)$ is a factor and recovers the quadratic quotient.

Example 10.1.5. Factorise $x^3+(m+n+1)x^2a+(m+n+mn)xa^2+mna^3$. We group terms strategically to reveal a common factor of $(x+a)$.

$$\begin{aligned}&x^3+x^2a+(m+n)x^2a+(m+n)xa^2+mnxa^2+mna^3\\ &=x^2(x+a)+(m+n)xa(x+a)+mna^2(x+a)\\ &=(x^2+(m+n)xa+mna^2)(x+a)\\ &=(x(x+ma)+na(x+ma))(x+a)\\ &=(x+na)(x+ma)(x+a)\end{aligned}$$

10.1.1 General Solution for a Quadratic Polynomial

While the methods above rely on some measure of trial and insight, there exists a systematic algorithm for factorising any quadratic polynomial of the form ax^2+bx+c. The method is known as **completing the square**.

First, we observe that an expression of the form x^2+px can be made into a perfect square by adding a specific constant. The expansion of $(x+\beta)^2=x^2+2\beta x+\beta^2$ shows that the linear term is $2\beta x$. To match this with px, we must have $2\beta=p$, or $\beta=p/2$. The required constant term is therefore $\beta^2=(p/2)^2$.

This process allows us to resolve any quadratic into the difference of two squares.

$$\begin{aligned}ax^2+bx+c &= a\left(x^2+\frac{b}{a}x+\frac{c}{a}\right)\\ &= a\left(\left(x^2+2\left(\frac{b}{2a}\right)x+\left(\frac{b}{2a}\right)^2\right)-\left(\frac{b}{2a}\right)^2+\frac{c}{a}\right)\\ &= a\left(\left(x+\frac{b}{2a}\right)^2-\left(\frac{b^2}{4a^2}-\frac{4ac}{4a^2}\right)\right)\\ &= a\left(\left(x+\frac{b}{2a}\right)^2-\frac{b^2-4ac}{4a^2}\right)\end{aligned}$$

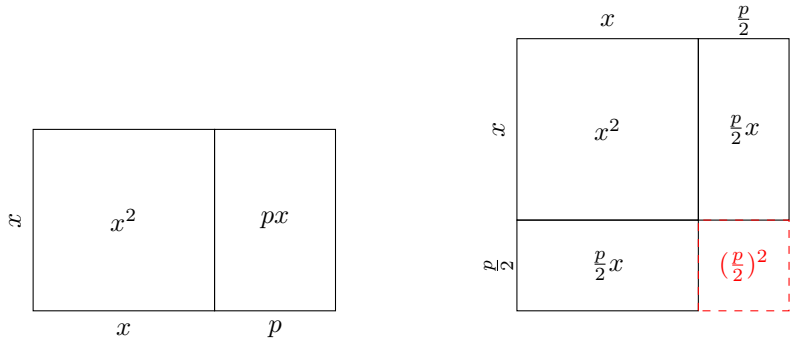


Figure 10.1: Geometric view of completing the square for $x^2 + px$. The missing corner required to form a larger square of side length $(x + p/2)$ has area $(p/2)^2$.

This is of the form $a(X^2 - M^2)$, which factorises as $a(X - M)(X + M)$. The factors are therefore:

$$a\left(\left(x + \frac{b}{2a}\right) - \frac{\sqrt{b^2 - 4ac}}{2a}\right)\left(\left(x + \frac{b}{2a}\right) + \frac{\sqrt{b^2 - 4ac}}{2a}\right).$$

This gives a complete, systematic method for factorising any quadratic polynomial.

Example 10.1.6. Factorise $6x^2 - 19x + 15$..

$$\begin{aligned}
6x^2 - 19x + 15 &= 6\left(x^2 - \frac{19}{6}x + \frac{15}{6}\right) \\
&= 6\left(\left(x - \frac{19}{12}\right)^2 - \left(\frac{19}{12}\right)^2 + \frac{15}{6}\right) \\
&= 6\left(\left(x - \frac{19}{12}\right)^2 - \frac{361}{144} + \frac{360}{144}\right) \\
&= 6\left(\left(x - \frac{19}{12}\right)^2 - \frac{1}{144}\right) \\
&= 6\left(\left(x - \frac{19}{12}\right)^2 - \left(\frac{1}{12}\right)^2\right) \\
&= 6\left(\left(x - \frac{19}{12} - \frac{1}{12}\right)\left(x - \frac{19}{12} + \frac{1}{12}\right)\right) \\
&= 6\left(x - \frac{20}{12}\right)\left(x - \frac{18}{12}\right) \\
&= 6\left(x - \frac{5}{3}\right)\left(x - \frac{3}{2}\right) \\
&= (2 \cdot 3)\left(\frac{3x - 5}{3}\right)\left(\frac{2x - 3}{2}\right) \\
&= (3x - 5)(2x - 3)
\end{aligned}$$

This method also applies to polynomials that are quadratic in form.

Example 10.1.7. Factorise $x^6 - 5x^3 + 6$. We can regard this as a quadratic polynomial in the variable x^3: $(x^3)^2 - 5(x^3) + 6$. By inspection, we seek two numbers that multiply to 6 and add to -5. These are -2 and -3. The factorisation in terms of x^3 is $(x^3 - 2)(x^3 - 3)$.

Manipulating Expressions with Surds

While an expression like $\frac{1}{\sqrt{2}}$ is perfectly valid, it is often desirable to transform a fraction so that the denominator contains only rational numbers. This process is called rationalising the denominator. A similar process, rationalising the numerator, is also a useful technique in certain contexts, particularly in calculus.

The key to these transformations is the identity for the difference of two squares, $(x-y)(x+y) = x^2 - y^2$. For an expression of the form $a \pm \sqrt{b}$, its conjugate is $a \mp \sqrt{b}$. Multiplying an expression by its conjugate eliminates the square root.

Example 10.1.8. (Rationalising the denominator). Transform the fraction $\frac{7}{3-\sqrt{2}}$ into an equivalent fraction with a rational denominator.

We multiply the numerator and denominator by the conjugate of the denominator, which is $3+\sqrt{2}$.

$$\begin{aligned}\frac{7}{3-\sqrt{2}} &= \frac{7}{3-\sqrt{2}} \times \frac{3+\sqrt{2}}{3+\sqrt{2}} \\ &= \frac{7(3+\sqrt{2})}{3^2-(\sqrt{2})^2} \\ &= \frac{21+7\sqrt{2}}{9-2} = \frac{21+7\sqrt{2}}{7} = 3+\sqrt{2}.\end{aligned}$$

Example 10.1.9. (Rationalising the numerator). Transform the fraction $\frac{\sqrt{x+h}-\sqrt{x-h}}{h}$ so that no surds appear in the numerator.

We multiply the numerator and denominator by the conjugate of the numerator, which is $\sqrt{x+h}+\sqrt{x-h}$.

$$\begin{aligned}\frac{\sqrt{x+h}-\sqrt{x-h}}{h} &= \frac{(\sqrt{x+h}-\sqrt{x-h})}{h} \times \frac{(\sqrt{x+h}+\sqrt{x-h})}{(\sqrt{x+h}+\sqrt{x-h})} \\ &= \frac{(\sqrt{x+h})^2-(\sqrt{x-h})^2}{h(\sqrt{x+h}+\sqrt{x-h})} \\ &= \frac{(x+h)-(x-h)}{h(\sqrt{x+h}+\sqrt{x-h})} \\ &= \frac{2h}{h(\sqrt{x+h}+\sqrt{x-h})} \\ &= \frac{2}{\sqrt{x+h}+\sqrt{x-h}} \quad \text{(cancelling } h, \text{ assuming } h \neq 0).\end{aligned}$$

These transformations are standard tools for simplifying expressions and preparing them for further analysis, such as in the study of limits or coordinate geometry.

10.2 Exercises

Part I: Tentative Methods

1. Use standard identities to factorise the following expressions.

(a) $9a^2 - 16b^2$

(b) $x^3 + 8y^3$

(c) $64p^6 - q^6$

(d) $(x+y)^2 - z^2$

2. Factorise the following quadratic polynomials by inspection.

(a) $x^2 + 8x + 15$
(b) $a^2 - 3a - 40$
(c) $y^2 - 13y + 36$
(d) $x^2 + 2xy - 35y^2$

3. Factorise the following quadratic polynomials by trial.

(a) $2x^2 + 11x + 12$
(b) $5a^2 - 17a + 6$
(c) $12y^2 - 23y - 24$

4. Use the Factor Theorem and synthetic division to factorise the following cubic polynomials.

(a) $x^3 - 6x^2 + 11x - 6$
(b) $a^3 + 2a^2 - 13a + 10$
(c) $2y^3 + y^2 - 13y + 6$

5. Find the rational roots of the polynomial $P(x) = x^4 - 2x^3 - 13x^2 + 14x + 24$ and hence factorise it completely.

6. Factorise the following expressions by grouping terms.

(a) $x^3 - 5x^2 + 3x - 15$
(b) $a^2 - b^2 - ac + bc$
(c) $y^3 + y^2 - y - 1$
(d) $x^2 - 4y^2 + x + 2y$

7. Factorise by grouping terms to form a difference of squares.

(a) $a^2 - 4b^2 + 12bc - 9c^2$
(b) $x^4 + x^2y^2 + y^4$

Remark. Add and subtract x^2y^2.

(c) $p^2 - 2p - q^2 - 4q - 3$

Remark. Group the p terms and q terms and complete the square for each.

8. Factorise the expression $(x^2 - 3x)^2 - 2(x^2 - 3x) - 8$ by treating $(x^2 - 3x)$ as a single variable.

Part II: The General Quadratic and Completing the Square

9. Use the method of completing the square to factorise the following quadratics.

(a) $x^2 + 8x + 12$
(b) $y^2 - 10y - 11$
(c) $a^2 + 3a - 10$

10. Use completing the square to factorise the following.

(a) $2x^2 + 7x + 3$
(b) $3a^2 - 10a - 8$

11. Use completing the square to find the factors of $x^2 + 2x - 5$. The factors will involve surds.

12. Factorise the following polynomials which are quadratic in form.

(a) $x^4 - 13x^2 + 36$
(b) $a^6 + 7a^3 - 8$
(c) $(x^2 + 2x)^2 - 11(x^2 + 2x) + 24$

Part III: Manipulating Expressions with Surds

13. Rationalise the denominator of the following expressions.

(a) $\dfrac{5}{\sqrt{10}}$

(b) $\dfrac{1}{2+\sqrt{3}}$

(c) $\dfrac{3\sqrt{2}}{\sqrt{5}-\sqrt{2}}$

(d) $\dfrac{x-a}{\sqrt{x}-\sqrt{a}}$

14. Simplify the expression $\dfrac{1}{1+\sqrt{2}}+\dfrac{1}{\sqrt{2}+\sqrt{3}}+\dfrac{1}{\sqrt{3}+2}$.

15. Rationalise the numerator of the following expressions.

(a) $\dfrac{\sqrt{7}-2}{3}$

(b) $\dfrac{\sqrt{a+h}-\sqrt{a}}{h}$

16. Find the value of x^2+3x-1 if $x=\sqrt{2}+1$.

17. Find the square root of $7+4\sqrt{3}$.

Remark. Assume the square root is of the form $\sqrt{a}+\sqrt{b}$. Square this expression and equate the rational and irrational parts.

18. Rationalise the denominator of $\dfrac{1}{1+\sqrt{2}+\sqrt{3}}$.

Remark. Group the terms as $(1+\sqrt{2})+\sqrt{3}$ and multiply by the conjugate.

Part IV: Comprehensive Problems and Proofs

19. Factorise the symmetrical polynomial $x^3+y^3+z^3-3xyz$.

Remark. Show that $(x+y+z)$ is a factor.

20. Factorise $a(b-c)^2+b(c-a)^2+c(a-b)^2+8abc$.

21. Show that $a^4(b-c)+b^4(c-a)+c^4(a-b)$ is divisible by $(a-b)(b-c)(c-a)$. What is the other factor?

22. Prove that for any positive integer n, the polynomial x^n-y^n is divisible by $x-y$.

23. Factorise $(a+b+c)^3-a^3-b^3-c^3$.

24. Factorise $(xy+yz+zx)^2-(x^2y^2+y^2z^2+z^2x^2)$.

25. Prove that the expression n^4-20n^2+4 is composite for any integer n.

26. $\star$ Factorise the expression $(x+y+z)^5-x^5-y^5-z^5$.

27. $\star$ Let $f(x)=ax^2+bx+c$. Show that the quantity b^2-4ac (known as the discriminant) determines the nature of the factors.

(a) If b^2-4ac is a perfect square of a rational number, prove the factors have rational coefficients.

(b) If $b^2-4ac=0$, prove that $f(x)$ is a perfect square.

(c) If $b^2 - 4ac < 0$, explain why the polynomial cannot be factorised into linear factors with real coefficients.

28. ⋆ Prove that if x, y, z are rational numbers such that $x^2 + y^2 + z^2 - xy - yz - zx = 0$, then it must be that $x = y = z$.

Remark. Multiply the expression by 2 and rearrange it into a sum of squares.

29. ⋆ Find all integer solutions to the equation $a^3 + b^3 + c^3 = (a + b + c)^3$.

10.3 Introduction of Imaginary Numbers

The method of completing the square reduces the problem of factorising a quadratic to finding the square root of the term $k = \frac{b^2-4ac}{4a^2}$. This forces us to consider the nature of square roots for any real number k. The square of any real number is non-negative, a fact illustrated by the graph of $y = x^2$ in Figure 10.2. This leads to three distinct cases for the nature of $m = \sqrt{k}$.

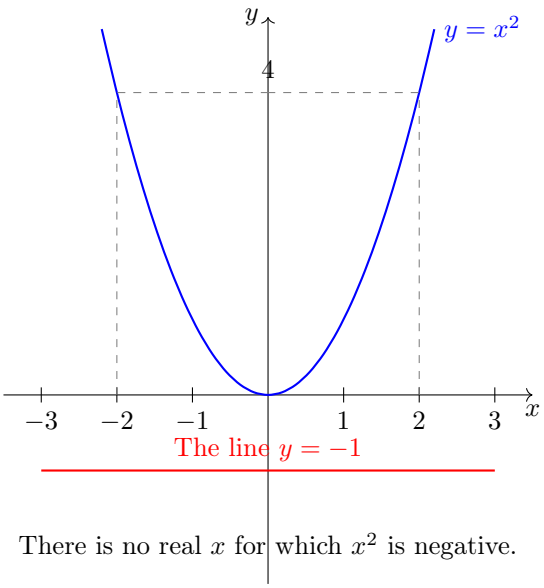


Figure 10.2: The graph of $y = x^2$. For any real input x, the output y is always non-negative. There is no real number whose square is negative.

1. **Case 1: k is a positive rational square.** If $k = (p/q)^2$, the problem is solved by taking $m = \pm(p/q)$. The factors of the quadratic are rational.

2. **Case 2: k is positive, but not a rational square.** No exact rational number exists for $m = \sqrt{k}$. We can find rational approximations to any desired degree of accuracy, but the exact value is an irrational number (or surd). We denote the two algebraic values by $\pm\sqrt{k}$. These symbols obey all the ordinary laws of algebra.

3. **Case 3: k is negative.** Let $k = -k'$, where $k' > 0$. The square of any real number is non-negative, so no real number m exists such that $m^2 = -k'$. To maintain the generality of our operations, we must widen the field of quantity. We introduce the imaginary unit, i, defined by the property:

$$i^2 = -1.$$

This unit allows us to form a new series of purely imaginary numbers, such as qi where q is any real number. When combined with real numbers by addition, they form complex numbers of the form $p + qi$. With this extension, the problem of finding a square root is always solved. If $m^2 = -k'$, then $m = \pm i\sqrt{k'}$.

10.3.1 Types of Quadratic Factors

The nature of the factors of a quadratic polynomial $ax^2 + bx + c$ is determined entirely by the quantity $b^2 - 4ac$, known as the *discriminant*.

1. If $b^2 - 4ac > 0$ and is a perfect square of a rational number, the factors are linear with real, rational coefficients.
2. If $b^2 - 4ac > 0$ but is not a perfect square, the factors are linear with real, irrational coefficients.

   Example 10.3.1.
   $$x^2 + 2x - 1 = (x+1)^2 - 2 = (x + 1 - \sqrt{2})(x + 1 + \sqrt{2}).$$
3. If $b^2 - 4ac < 0$, the factors are linear with complex coefficients.

   Example 10.3.2.
   $$x^2 + 2x + 5 = (x+1)^2 + 4 = (x+1)^2 - (2i)^2 = (x + 1 - 2i)(x + 1 + 2i).$$
4. If $b^2 - 4ac = 0$, the quadratic is a complete square in x. The two factors are real but identical, resulting in a repeated root.

   Example 10.3.3.
   $$4x^2 - 12x + 9 = 4\left(x^2 - 3x + \frac{9}{4}\right) = 4\left(x - \frac{3}{2}\right)^2.$$

If the coefficients a, b, c are themselves functions of other variables, we may inquire under what circumstances the factors will be algebraically rational functions of those variables. This requires that the discriminant $b^2 - 4ac$ be a complete square of a rational function of the variables in question, say P^2. The factors are then $a\left(x + \frac{b \pm P}{2a}\right)$, which are rational.

10.3.2 Homogeneous Polynomials and Substitution

The factorisation of a quadratic $ax^2 + bx + c$ extends directly to the homogeneous quadratic $ax^2 + bxy + cy^2$.

$$ax^2 + bxy + cy^2 = y^2\left(a\left(\frac{x}{y}\right)^2 + b\left(\frac{x}{y}\right) + c\right).$$

The factors of the polynomial in (x/y) yield the factors of the original homogeneous polynomial. Any homogeneous function of two variables may be factorised, provided the corresponding non-homogeneous function of one variable can be factorised.

Example 10.3.4. From $x^2 + 2x + 3 = (x + 1 - i\sqrt{2})(x + 1 + i\sqrt{2})$, we deduce.
$$x^2 + 2xy + 3y^2 = (x + (1 - i\sqrt{2})y)(x + (1 + i\sqrt{2})y).$$

Example 10.3.5. From $x^3 - 2x^2 - 23x + 60 = (x-3)(x-4)(x+5)$, we deduce.
$$x^3 - 2x^2y - 23xy^2 + 60y^3 = (x - 3y)(x - 4y)(x + 5y).$$

Many factorisations can be simplified by substitution.

Example 10.3.6.
$$x^4 + x^2y^2 + y^4 = (x^2 + y^2)^2 - (xy)^2 = (x^2 - xy + y^2)(x^2 + xy + y^2).$$
$$\begin{aligned} a^4 + b^4 &= (a^2 + b^2)^2 - 2a^2b^2 = (a^2 + b^2)^2 - (\sqrt{2}ab)^2 \\ &= (a^2 - \sqrt{2}ab + b^2)(a^2 + \sqrt{2}ab + b^2). \end{aligned}$$

The factors can be further resolved into linear factors with complex coefficients:

$$a^4 + b^4 = \left(a - \frac{1+i}{\sqrt{2}}b\right)\left(a - \frac{1-i}{\sqrt{2}}b\right)\left(a + \frac{1-i}{\sqrt{2}}b\right)\left(a + \frac{1+i}{\sqrt{2}}b\right).$$

Example 10.3.7. $2b^2c^2 + 2c^2a^2 + 2a^2b^2 - a^4 - b^4 - c^4$.

$$\begin{aligned} 4b^2c^2 - (a^4 + b^4 + c^4 - 2b^2c^2 - 2c^2a^2 - 2a^2b^2) &= 4b^2c^2 - (a^2 - b^2 - c^2)^2 \\ &= (2bc - (a^2 - b^2 - c^2))(2bc + (a^2 - b^2 - c^2)) \\ &= ((b+c)^2 - a^2)(a^2 - (b-c)^2) \\ &= (b + c - a)(b + c + a)(a - b + c)(a + b - c). \end{aligned}$$

10.3.3 General Results on Factorisation

The Remainder Theorem provides the key principle: for every root a of a polynomial $P(x)$, there is a corresponding factor $(x - a)$. The Fundamental Theorem of Algebra states that a polynomial of degree n with complex coefficients has exactly n complex roots, counting multiplicity. This implies:

- Any polynomial of degree n can be resolved into n linear factors with complex coefficients.
- If the polynomial has real coefficients, its complex roots must occur in conjugate pairs $(\lambda \pm \mu i)$. The product of the corresponding factors, $(x - (\lambda + \mu i))(x - (\lambda - \mu i))$, is the irreducible real quadratic $x^2 - 2\lambda x + (\lambda^2 + \mu^2)$.
- Any polynomial with real coefficients can be resolved into a product of linear and irreducible quadratic factors, all of which have real coefficients.

The general problem of factorising an n-th degree polynomial is coextensive with that of solving an n-th degree equation.

10.4 Factorisation of Multivariable Polynomials

General Case and Irreducibility

When the number of variables exceeds one, the problem of factorisation of an integral function (excepting special cases, such as homogeneous functions) is not in general soluble. To establish this, it is sufficient to demonstrate the insolubility of a particular case. Consider the polynomial $x^2 + y^2 + 1$. If it is resolvable into a product of linear factors integral in x and y, we would have:

$$x^2 + y^2 + 1 = (px + qy + r)(p'x + q'y + r')$$

Expanding the right-hand side and equating coefficients gives a system of equations:

$$\begin{aligned} pp' &= 1 \quad (1) & pq' + p'q &= 0 \quad (4) \\ qq' &= 1 \quad (2) & pr' + p'r &= 0 \quad (5) \\ rr' &= 1 \quad (3) & qr' + q'r &= 0 \quad (6) \end{aligned}$$

From (1), (2), (3), none of p, q, r, p', q', r' can be zero. We have $p' = 1/p$, $q' = 1/q$, $r' = 1/r$. Substituting these into (4), (5), (6) yields:

$$\begin{aligned} p/q + q/p = 0 &\implies p^2 + q^2 = 0 \\ p/r + r/p = 0 &\implies p^2 + r^2 = 0 \\ q/r + r/q = 0 &\implies q^2 + r^2 = 0 \end{aligned}$$

From $p^2 + r^2 = 0$ and $q^2 + r^2 = 0$, we subtract to get $p^2 - q^2 = 0$. Adding this to $p^2 + q^2 = 0$ gives $2p^2 = 0$, which implies $p = 0$. This contradicts equation (1), so the initial assumption of factorisability is false.

The General Quadratic in Two Variables

Consider the general function of the second degree in two variables:

$$F = ax^2 + 2hxy + by^2 + 2gx + 2fy + c.$$

For F to be resolvable into two linear factors, it must be expressible in the form $L^2 - M^2$, where L is a linear function of x and y, and M is a linear function of y alone. Assuming $a \neq 0$, we complete the square with respect to x:

$$\begin{aligned} F &= a\left[x^2 + 2\frac{hy+g}{a}x + \frac{by^2+2fy+c}{a}\right] \\ &= a\left[\left(x + \frac{hy+g}{a}\right)^2 - \frac{(hy+g)^2}{a^2} + \frac{by^2+2fy+c}{a}\right] \\ &= a\left[\left(x + \frac{hy+g}{a}\right)^2 - \frac{(h^2-ab)y^2 + 2(gh-af)y + (g^2-ac)}{a^2}\right]. \end{aligned}$$

For this to be of the form $L^2 - M^2$, the term $(h^2-ab)y^2 + 2(gh-af)y + (g^2-ac)$ must be a complete square in y. The condition for this is that its discriminant is zero:

$$4(gh-af)^2 - 4(h^2-ab)(g^2-ac) = 0.$$

Expanding and simplifying, and assuming $a \neq 0$, this reduces to:

$$\Delta = abc + 2fgh - af^2 - bg^2 - ch^2 = 0.$$

This quantity, Δ, is the discriminant of the general quadratic in two variables. Its vanishing is the necessary and sufficient condition for the function to be resolvable into two linear factors. The same condition is found if we begin by assuming $b \neq 0$ and completing the square for y. If $a = b = 0$ but $h \neq 0$, $F = 2hxy + 2gx + 2fy + c$. For this to be factorisable, it must be of the form $2h(x+p)(y+q)$, which requires $c = 2fg/h$, or $2fgh - ch^2 = 0$. This is what the general condition $\Delta = 0$ reduces to when $a = b = 0$.

Example 10.4.1. To factorise $3x^2 + 2xy - y^2 + 2x - 2y - 1$. The homogeneous part of highest degree is $3x^2 + 2xy - y^2 = (3x - y)(x + y)$. If the full expression is factorisable, the factors must be of the form $(3x - y + n)(x + y + n')$. Expanding this and equating coefficients with the original expression gives a system of equations for n and n':

$$\begin{aligned} n + 3n' &= 2 \\ n - n' &= -2 \\ nn' &= -1 \end{aligned}$$

Solving the first two equations gives $n = -1$ and $n' = 1$. These values satisfy the third equation, so the factorisation is possible.

$$3x^2 + 2xy - y^2 + 2x - 2y - 1 = (3x - y - 1)(x + y + 1).$$

10.5 Exercises

Part I: Nature of Factors and Basic Identities

1. For each of the following quadratic polynomials, calculate the discriminant $(b^2 - 4ac)$ and describe the nature of its factors (real and rational, real and irrational, complex conjugates, or repeated real).

(a) $2x^2 + 5x - 3$

(b) $x^2 - 6x + 9$

(c) $3x^2 + 2x + 1$

(d) $x^2 - 4x - 1$

2. Create a quadratic polynomial $ax^2 + bx + c$ with integer coefficients that has:

(a) Two distinct, real, irrational factors.

(b) Two complex conjugate factors.

3. Use standard identities to factorise the following expressions over the complex numbers.

(a) $x^2 + 16$

(b) $4a^2 + 9b^2$

(c) $p^4 - 81$

(d) $y^3 + 5$

4. Factorise the following homogeneous quadratic polynomials.

(a) $x^2 - 5xy + 6y^2$

(b) $3a^2 + 10ab - 8b^2$

(c) $p^2 + 2pq + 5q^2$

5. If $(x - (2 + 3i))$ is a factor of a quadratic polynomial with real coefficients, what must the other factor be? What is the polynomial?

Part II: Factorisation of Polynomials

Remark. Apply the method of completing the square, or other appropriate techniques, to find the complete factorisation of each polynomial over the field of complex numbers.

6. Factorise the following quadratics, which have real, irrational roots.

(a) $x^2 - 4x + 2$

(b) $a^2 + 6a - 3$

(c) $2y^2 - 2y - 1$

7. Factorise the following quadratics, which have complex roots.

(a) $x^2 - 2x + 10$

(b) $p^2 + 8p + 25$

(c) $3y^2 - 4y + 2$

8. Find the complete factorisation for each of the following.

(a) $9x^2 + 30x + 25$

(b) $x^3 - x^2 - x - 2$

(c) $x^4 - 1$

9. Factorise the following polynomials by first completing the square to create a difference of squares.

(a) $x^4 + 4$

(b) $a^4 + 3a^2 + 4$

(c) $4p^4 + 1$

10. Factorise the following expressions using an appropriate substitution.

(a) $(x^2 + 3x - 2)^2 - 10(x^2 + 3x - 2) + 21$

(b) $x^6 - 9x^3 + 8$

11. Find all four roots of the equation $x^4 + 5x^2 - 36 = 0$.

12. Factorise $x^6 - y^6$ in two ways: first as a difference of squares, then as a difference of cubes. Show that both methods yield the same set of factors.

Part III: Rationalisation and Surds

13. Rationalise the denominator of the following expressions.

(a) $\dfrac{1}{3i}$

(b) $\dfrac{1}{2+i}$

(c) $\dfrac{\sqrt{3}+i\sqrt{2}}{\sqrt{3}-i\sqrt{2}}$

14. Find the value of $x^3 - 3x^2 - 8x + 15$ when $x = 3 + i$.

15. Find the square root of the complex number $5 + 12i$.

Remark. Assume the square root is of the form $a + bi$. Square this expression and equate the real and imaginary parts.

16. If $x = \frac{\sqrt{5}+1}{2}$, prove that $x^2 = x + 1$. Use this to show that $x^3 = 2x + 1$.

17. Simplify the expression $\frac{(\sqrt{a}+\sqrt{b})^2-(\sqrt{a}-\sqrt{b})^2}{(\sqrt{a}+\sqrt{b})(\sqrt{a}-\sqrt{b})}$.

Part IV: Proofs and Challenge Problems

18. Prove that if a polynomial with real coefficients has a complex root $z = p + qi$, then its conjugate $\bar{z} = p - qi$ must also be a root.

19. Use the result from the previous question to prove that any polynomial with real coefficients can be factorised into a product of linear and irreducible quadratic factors with real coefficients.

20. Factorise $x^4 + 1$ into a product of two irreducible quadratic factors with real coefficients.

21. Factorise $x^6 + 1$ completely into factors with real coefficients.

22. Resolve into factors: $(ab + cd)(a^2 - b^2 + c^2 - d^2) + (ac + bd)(a^2 + b^2 - c^2 - d^2)$.

23. Factorise $x^3 + y^3 + z^3 - 3xyz$.

24. Show that $(a - b)^3 + (b - c)^3 + (c - a)^3 = 3(a - b)(b - c)(c - a)$.

25. If a quadratic polynomial $ax^2 + bx + c$ is a perfect square, prove that its discriminant $b^2 - 4ac$ must be zero.

26. $\star$ Factorise the cyclotomic polynomial $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$.

Remark. Divide by x^2 and make the substitution $y = x + 1/x$.

27. $\star$ Resolve $x^8 + x^4 + 1$ into four factors.

28. $\star$ Prove that the expression $(x + y + z)^3 - (x^3 + y^3 + z^3)$ is divisible by $(x + y)$, $(y + z)$, and $(z + x)$. Find the complete factorisation.

29. $\star$ Factorise the polynomial $P(x) = x^5 + x + 1$.

Remark. Consider adding and subtracting x^2.

Chapter 11

Rational Fractions

A rational fraction is the quotient of any two polynomials. Unless otherwise stated, we will deal with functions of a single variable, x. Let the fraction be A/B.

- If $\deg(A) \geq \deg(B)$, the fraction is **improper**.
- If $\deg(A) < \deg(B)$, the fraction is **proper**.

11.1 General Propositions

***Theorem* 11.1.1.** Every improper fraction can be expressed as the sum of a polynomial and a proper fraction.

Proof. *Let the fraction be A_m/B_n, where $m \geq n$. By the Division Transformation, we have*

$$\frac{A_m}{B_n} = P_{m-n} + \frac{R}{B_n},$$

where P_{m-n} is a polynomial of degree $m-n$, and the remainder R is a polynomial with $\deg(R) < n$. This proves the statement. ■

***Corollary* 11.1.1.** The sum of a polynomial and a proper fraction can be exhibited as an improper fraction.

***Theorem* 11.1.2.** If two improper fractions are equal, then their polynomial parts and their proper fractional parts must be equal separately.

Proof. *Let $\frac{A}{B} = P + \frac{R}{B}$ and $\frac{A'}{B'} = P' + \frac{R'}{B'}$. If these two improper fractions are equal, then*

$$P + \frac{R}{B} = P' + \frac{R'}{B'}.$$

Rearranging gives

$$P - P' = \frac{R'}{B'} - \frac{R}{B} = \frac{R'B - RB'}{BB'}.$$

The left-hand side is a polynomial. On the right, since $\deg(R) < \deg(B)$ and $\deg(R') < \deg(B')$, the degree of the numerator is less than the degree of the denominator. The only way a polynomial can be equal to a proper fraction is if both are identically zero. Thus, we must have $P - P' = 0$ and $\frac{R'B-RB'}{BB'} = 0$. This implies $P = P'$ and $\frac{R}{B} = \frac{R'}{B'}$. ■

Remark. The sum of two proper algebraical fractions is a proper algebraical fraction. This highlights a difference from arithmetic, where $\frac{3}{4} + \frac{3}{4} = \frac{6}{4}$ is improper.

Simplification to Lowest Terms

If the numerator and denominator of a rational fraction share common factors, we can cancel them. When all common factors have been removed, the fraction is said to be in its **lowest terms**. The G.C.D. is the tool used to find these common factors.

Example 11.1.1. Simplify $\frac{x^3+5x^2+7x+3}{x^4+3x^3+4x^2+3x+1}$. The G.C.D. of the numerator and denominator is $x^2+2x+1 = (x+1)^2$. Dividing the numerator by $(x+1)^2$ gives $x+3$. Dividing the denominator by $(x+1)^2$ gives x^2+x+1. The simplified fraction is $\frac{x+3}{x^2+x+1}$.

***Theorem* 11.1.3.** If two rational fractions P/Q and P'/Q' are equal, and P/Q is in its lowest terms, then $P' = AP$ and $Q' = AQ$ for some polynomial A. If P'/Q' is also in lowest terms, then A must be a constant.

Proof. From $P/Q = P'/Q'$, we have $P' = Q'P/Q$. Since P' is a polynomial, $Q'P$ must be divisible by Q. As P and Q are relatively prime, it follows that Q must divide Q'. So $Q' = AQ$ for some polynomial A. Substituting back, we find $P' = AP$. ■

Operations with Rational Fractions

The application of the G.C.D. and L.C.M. facilitates operations with rational fractions. The student should cultivate the use of factorisation and general principles like symmetry to simplify the work.

Example 11.1.2.

$$\frac{x-y}{x+y}\frac{x^3-y^3}{x^3+y^3} = \frac{x-y}{x+y}\frac{(x-y)(x^2+xy+y^2)}{(x+y)(x^2-xy+y^2)} = \frac{(x-y)^2(x^2+xy+y^2)}{(x+y)^2(x^2-xy+y^2)}.$$

Example 11.1.3. Simplify $F = \frac{a^3}{(a-b)(a-c)} + \frac{b^3}{(b-c)(b-a)} + \frac{c^3}{(c-a)(c-b)}$. First, create a common denominator $(a-b)(b-c)(c-a)$.

$$F = \frac{-a^3(b-c) - b^3(c-a) - c^3(a-b)}{(a-b)(b-c)(c-a)}.$$

Let the numerator be $N(a,b,c)$. If we set $a = b$, the numerator becomes $-b^3(b-c) - b^3(c-b) = 0$. So $(a-b)$ is a factor of N. By symmetry, $(b-c)$ and $(c-a)$ are also factors. Since the numerator is a homogeneous polynomial of degree 4, the remaining factor must be a symmetric homogeneous polynomial of degree 1, which must be of the form $k(a+b+c)$ for some constant k.

$$N(a,b,c) = k(a+b+c)(a-b)(b-c)(c-a).$$

To find k, we compare the coefficient of a term, say a^3b. On the left side, the coefficient of a^3b comes from $-a^3(b-c)$, which gives -1. On the right side, the term a^3b comes from $k(a)(a)(-c)(-b) = ka^2bc$... this is incorrect. The a^3 term on the right comes from $k(a)(a)(c-a)(b-c)$ which gives $-ka^3(b-c)$. Let's trace the terms with highest power of a. $N(a,b,c) = -a^3(b-c) +$ terms of lower degree in a. $k(a+b+c)(a-b)(b-c)(c-a) = k(a)(a)(b-c)(-a) = -ka^3(b-c) + \ldots$. Comparing the coefficients of a^3, we have $-(b-c) = -k(b-c)$, which implies $k = 1$. So, $N = (a+b+c)(a-b)(b-c)(c-a)$. Therefore,

$$F = \frac{(a+b+c)(a-b)(b-c)(c-a)}{(a-b)(b-c)(c-a)} = a+b+c.$$

11.2 Decomposition into Partial Fractions

Since every improper fraction can be expressed as the sum of a polynomial and a proper fraction, we need only consider how to decompose a proper fraction into a sum of simpler proper fractions. These simpler fractions, called **partial fractions**, have denominators that are factors of the original denominator.

***Theorem* 11.2.1. (Fundamental Theorem)**. If A/PQ is a proper fraction, where P and Q are polynomials relatively prime to each other, then A/PQ can be decomposed into the sum of two proper fractions with denominators P and Q.

$$\frac{A}{PQ} = \frac{P'}{P} + \frac{Q'}{Q}$$

Proof. Since P and Q are relatively prime, by Bézout's Identity there exist polynomials L and M such that

$$LP + MQ = 1.$$

Multiplying this identity by the fraction A/PQ gives:

$$\frac{A}{PQ} = \frac{A(LP+MQ)}{PQ} = \frac{ALP}{PQ} + \frac{AMQ}{PQ} = \frac{AL}{Q} + \frac{AM}{P}.$$

The fractions AL/Q and AM/P may be improper. We transform them by division:

$$\frac{AL}{Q} = S + \frac{Q'}{Q}, \quad \textit{where } \deg(Q') < \deg(Q)$$
$$\frac{AM}{P} = T + \frac{P'}{P}, \quad \textit{where } \deg(P') < \deg(P)$$

Substituting these back:

$$\frac{A}{PQ} = (S+T) + \frac{P'}{P} + \frac{Q'}{Q}.$$

Since A/PQ is a proper fraction, and P'/P and Q'/Q are proper fractions, their sum must also be a proper fraction. Therefore, the polynomial part $(S+T)$ must be zero.

$$\frac{A}{PQ} = \frac{P'}{P} + \frac{Q'}{Q}.$$

■

***Corollary* 11.2.1.** By repeated application, if the denominator is a product of pairwise relatively prime factors, $D = P \cdot Q \cdot R \cdots$, then any proper fraction A/D can be decomposed into a sum of proper fractions

$$\frac{A}{D} = \frac{P'}{P} + \frac{Q'}{Q} + \frac{R'}{R} + \cdots$$

General Form of Partial Fractions

Any polynomial can be factorised over the real numbers into a product of linear factors $(x-a)$ and irreducible quadratic factors $(x^2+\beta x+\gamma)$, possibly repeated.

1. For a non-repeated linear factor $(x-a)$, the corresponding partial fraction is of the form $\frac{k}{x-a}$, where k is a constant.
2. For a repeated linear factor $(x-a)^r$, the decomposition yields a sum of r partial fractions:
$$\frac{k_1}{x-a} + \frac{k_2}{(x-a)^2} + \cdots + \frac{k_r}{(x-a)^r}.$$
3. For a non-repeated irreducible quadratic factor $(x^2+\beta x+\gamma)$, the partial fraction is $\frac{ax+b}{x^2+\beta x+\gamma}$.
4. For a repeated irreducible quadratic factor $(x^2+\beta x+\gamma)^s$, we get a sum of s fractions:
$$\frac{a_1x+b_1}{x^2+\beta x+\gamma} + \frac{a_2x+b_2}{(x^2+\beta x+\gamma)^2} + \cdots + \frac{a_sx+b_s}{(x^2+\beta x+\gamma)^s}.$$

Each constant can be determined independently.

11.2.1 Methods for Finding Coefficients

Several methods are available for finding the unknown constants.

Linear Factors: The Cover-Up Method

For a non-repeated linear factor $(x-a)$, the constant numerator is found by evaluating the rest of the expression at $x=a$. Consider $F(x)=\frac{N(x)}{(x-a)Q(x)}=\frac{k}{x-a}+\frac{R(x)}{Q(x)}$. Multiplying by $(x-a)$ gives:

$$\frac{N(x)}{Q(x)}=k+(x-a)\frac{R(x)}{Q(x)}.$$

Setting $x=a$ eliminates the second term, yielding $k=\frac{N(a)}{Q(a)}$. In practice, we "cover up" the factor $(x-a)$ in the original fraction and evaluate what remains at $x=a$.

Example 11.2.1. Decompose $\frac{x^2+px+q}{(x-a)(x-b)(x-c)}$ assuming a,b,c are distinct. Let the expression be

$$\frac{A}{x-a}+\frac{B}{x-b}+\frac{C}{x-c}.$$

To find A, cover $(x-a)$ and set $x=a$: $A=\frac{a^2+pa+q}{(a-b)(a-c)}$. By symmetry, $B=\frac{b^2+pb+q}{(b-a)(b-c)}$ and $C=\frac{c^2+pc+q}{(c-a)(c-b)}$.

Repeated Linear Factors

For a factor $(x-a)^r$, we can find the numerators $k_r,k_{r-1},\ldots,k_1$ by successive division. Let $F(x)=\frac{N(x)}{(x-a)^rQ(x)}$. The decomposition for this factor is

$$\frac{P(x)}{(x-a)^r}=\frac{k_1(x-a)^{r-1}+\cdots+k_r}{(x-a)^r}=\frac{k_1}{x-a}+\cdots+\frac{k_r}{(x-a)^r}.$$

Here, $P(x)$ is a polynomial derived from $N(x)/Q(x)$. Specifically, multiply the master identity by $(x-a)^r$:

$$\frac{N(x)}{Q(x)}=k_r+k_{r-1}(x-a)+\cdots+k_1(x-a)^{r-1}+(x-a)^r\frac{R(x)}{Q(x)}.$$

To find the coefficients k_i, we first express the rational function $\frac{N(x)}{Q(x)}$ as a series in powers of $(x-a)$. This can be done by substituting $x=y+a$ and performing ascending continued division by y.

Example 11.2.2. Find terms for $(x-2)^2$ in $\frac{4x^4-16x^3+17x^2-8x+7}{(x-1)(x-2)^2(x^2+1)}$. Let the form be $\frac{k_1}{x-2}+\frac{k_2}{(x-2)^2}$. Multiply original fraction by $(x-2)^2$:

$$\frac{4x^4-16x^3+17x^2-8x+7}{(x-1)(x^2+1)}=k_2+k_1(x-2)+(x-2)^2(\ldots)$$

Set $x=2$ to find k_2:

$$k_2=\frac{4(16)-16(8)+17(4)-8(2)+7}{(1)(5)}=\frac{64-128+68-16+7}{5}=\frac{-5}{5}=-1.$$

To find k_1, we can use ascending division. Put $x=y+2$ in the left side: Numerator: $4(y+2)^4-16(y+2)^3+17(y+2)^2-8(y+2)+7=-5-4y+\ldots$ Denominator: $(y+1)((y+2)^2+1)=(y+1)(y^2+4y+5)=5+9y+\ldots$ Quotient by ascending division:

$$\frac{-5-4y+\ldots}{5+9y+\ldots}=-1+y+\ldots$$

This expansion corresponds to $k_2+k_1y+\ldots$. Comparing terms, $k_2=-1$ and $k_1=1$. The partial fractions are $\frac{1}{x-2}-\frac{1}{(x-2)^2}$.

Quadratic Factors and Equating Coefficients

For quadratic factors, or as a general method, we can clear fractions to form a polynomial identity, then equate coefficients of like powers of x to form a system of linear equations.

Example 11.2.3. Find the term for (x^2+1) in the fraction from the previous example.

Form is $\frac{ax+b}{x^2+1}$. We assume other terms are found. Identity: $4x^4-16x^3+17x^2-8x+7 = (ax+b)(x-1)(x-2)^2 + Q'(x)(x^2+1)$. To isolate $ax+b$, setting $x^2=-1$ (or $x=i$) is a powerful shortcut. Substitute $x=i$: Left side: $4(1)-16(-i)+17(-1)-8i+7 = 4+16i-17-8i+7 = -6+8i$. Right side: $(ai+b)(i-1)(i-2)^2+0$. $(i-1)(i^2-4i+4) = (i-1)(3-4i) = 3i-4i^2-3+4i = 3i+4-3+4i = 1+7i$. So, $-6+8i = (ai+b)(1+7i) = ai-7a+b+7bi = (b-7a)+(a+7b)i$. Equating real and imaginary parts:

$$b-7a=-6$$
$$a+7b=8$$

Multiplying second eq by 7: $7a+49b=56$. Adding to first: $50b=50 \implies b=1$. Then $a+7=8 \implies a=1$. Partial fraction is $\frac{x+1}{x^2+1}$.

11.3 Exercises

Part I: Simplification and Basic Operations

1. Reduce the following rational fractions to their lowest terms.

(a) $\dfrac{x^3-6x^2+11x-6}{x^3-2x^2-x+2}$

(b) $\dfrac{a^4+a^2b^2+b^4}{a^6-b^6}$

(c) $\dfrac{2x^4+9x^3+14x^2+9x+2}{3x^4+13x^3+21x^2+13x+3}$

2. Perform the indicated operations and simplify the result to its lowest terms.

(a) $\dfrac{x^2-5x+6}{x^2-2x-15} \times \dfrac{x^2+x-12}{x^2-6x+8}$

(b) $\dfrac{a^2-b^2}{a^3-b^3} \div \dfrac{a^2+ab}{a^2+ab+b^2}$

3. Combine the following expressions into a single fraction.

(a) $\dfrac{1}{x-1} - \dfrac{1}{x} - \dfrac{1}{x(x+1)}$

(b) $\dfrac{a+b}{a-b} - \dfrac{a-b}{a+b} - \dfrac{4ab}{a^2+b^2}$

(c) $\dfrac{x+3}{x^2-3x+2} - \dfrac{x-1}{x^2-5x+6} + \dfrac{x-3}{x^2-4x+3}$

4. Prove the following identity using the methods for symmetrical expressions:

$$\sum_{\text{cyc}} \frac{a^2}{(a-b)(a-c)} = 1$$

Remark. The notation $\sum_{\text{cyc}}$ denotes a cyclic sum over variables a, b, c. The full expression is $\frac{a^2}{(a-b)(a-c)} + \frac{b^2}{(b-c)(b-a)} + \frac{c^2}{(c-a)(c-b)}$.

5. Simplify the expression $\dfrac{1}{(x-y)(x-z)} + \dfrac{1}{(y-z)(y-x)} + \dfrac{1}{(z-x)(z-y)}$.

Part II: Decomposition into Partial Fractions

6. Resolve the following into partial fractions. (Denominator with distinct linear factors)

(a) $\dfrac{7x-1}{x^2-x-6}$

(b) $\dfrac{x^2-10x+13}{(x-1)(x-2)(x-3)}$

(c) $\dfrac{1}{x(x^2-4)}$

7. Resolve the following into partial fractions. (Denominator with repeated linear factors)

(a) $\dfrac{2x+3}{(x+1)^2}$

(b) $\dfrac{x^2-3x-1}{x(x+1)^2}$

(c) $\dfrac{2x^3+x^2-x-1}{(x-2)^3}$

8. Resolve the following into partial fractions. (Denominator with irreducible quadratic factors)

(a) $\dfrac{x-2}{(x+1)(x^2+2)}$

(b) $\dfrac{5-2x}{(x^2+x+1)(x-2)}$

(c) $\dfrac{1}{(x^2+1)(x^2+4)}$

9. Resolve the following into partial fractions. (Denominator with repeated quadratic factors)

(a) $\dfrac{2x^3+x-1}{(x^2+1)^2}$

(b) $\dfrac{x^4+1}{x(x^2+x+1)^2}$

10. Resolve into partial fractions: $\dfrac{x^4}{(x-1)^2(x^2+1)}$.

11. Resolve the improper fraction $\dfrac{x^4+3x^3-x^2+5x+1}{x^2+3x-4}$ into a sum of a polynomial and partial fractions.

Part III: Proofs and Generalisations

12. Prove that the decomposition of a proper rational fraction into its partial fractions is unique.

Remark. Assume that $\frac{A}{D} = \frac{P_1}{D_1} + \frac{P_2}{D_2}$ and also $\frac{A}{D} = \frac{Q_1}{D_1} + \frac{Q_2}{D_2}$, where $D = D_1 D_2$. Show this implies $P_1 = Q_1$ and $P_2 = Q_2$.

13. Let a, b, c be distinct constants. Show that if we decompose $\dfrac{1}{(x-a)(x-b)(x-c)}$, the sum of the numerators of the partial fractions is zero.

14. Find the decomposition for $\dfrac{1}{(x+a)(x+b)}$ where $a \neq b$. Use this result to prove the identity:

$$\sum_{k=1}^{n} \frac{1}{(k+1)(k+2)} = \frac{n}{2(n+2)}$$

15. Prove that the sum of two proper rational fractions is itself a proper rational fraction.

16. Consider the fraction $F(x) = \dfrac{N(x)}{(x-a)Q(x)}$ where $Q(a) \neq 0$. The partial fraction corresponding to the factor $(x-a)$ is $\dfrac{k}{x-a}$. Prove the cover-up rule by showing that if we define a new function $f(x) = (x-a)F(x)$, then $k = f(a)$.

17. Let $P(x)$ be a polynomial of degree less than n. Show that

$$\frac{P(x)}{(x-a_1)(x-a_2)\cdots(x-a_n)} = \sum_{j=1}^{n} \frac{P(a_j)}{(a_j-a_1)\cdots(a_j-a_{j-1})(a_j-a_{j+1})\cdots(a_j-a_n)} \frac{1}{x-a_j}$$

assuming all a_j are distinct.

18. If $\dfrac{1-ax-bx^2}{(1-cx)(1-dx)} = 1 + px + qx^2 + \ldots$ is an ascending series expansion, show that $p = a+c+d$ and $q = b + ac + ad + c^2 + cd + d^2$.

19. ⋆ Let $F(x) = \dfrac{N(x)}{(x-a)^r Q(x)}$, where $Q(a) \neq 0$. The decomposition includes the terms $\dfrac{k_r}{(x-a)^r} + \dfrac{k_{r-1}}{(x-a)^{r-1}} + \ldots$. Define the function $f(x) = (x-a)^r F(x) = \dfrac{N(x)}{Q(x)}$.

(a) Show that $f(x)$ can be expanded in powers of $(x-a)$ as $f(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \ldots$, where $f^{(k)}(a)$ is the k-th formal derivative of $f(x)$ evaluated at $x = a$.

(b) By comparing this expansion with the partial fraction identity, prove that the coefficients are given by the formula

$$k_{r-j} = \frac{f^{(j)}(a)}{j!}.$$

(c) Use this result to find the partial fraction decomposition of $\dfrac{x^2}{(x-1)^3}$.

20. ⋆ Resolve into partial fractions: $\dfrac{n!}{x(x-1)(x-2)\cdots(x-n)}$.

Remark. Use the cover-up method. The numerators will involve binomial coefficients.

Chapter 12

System of Equations

12.1 Systems of Linear Equations

We now consider the problem of finding a common solution to two or more linear equations.

Definition 12.1.1. ***(System of Linear Equations)***. A system of two linear equations in two variables, x and y, is a pair of equations of the form:

$$\begin{aligned} ax + by &= c \\ dx + ey &= f \end{aligned}$$

where a, b, c, d, e, f are constants. A solution to the system is an ordered pair of numbers (x_0, y_0) that simultaneously satisfies both equations.

The Method of Elimination

The fundamental strategy for solving such a system is the method of elimination. The objective is to transform the given system into an equivalent one from which a variable has been removed, thereby reducing the problem to a single equation in a single variable. This is achieved by taking a linear combination of the two equations.

Example 12.1.1. Solve the system of equations:.

$$15x + 12y = 4 \tag{12.1}$$
$$12x - 18y = 17 \tag{12.2}$$

Eliminating y: Our goal is to make the coefficients of y equal in magnitude but opposite in sign. The least common multiple of the coefficients 12 and 18 is 36. We multiply equation (1) by 3 and equation (2) by 2 to obtain an equivalent system:

$$\begin{aligned} 45x + 36y &= 12 \\ 24x - 36y &= 34 \end{aligned}$$

Adding the two new equations eliminates y:

$$\begin{aligned} (45x + 36y) + (24x - 36y) &= 12 + 34 \\ 69x &= 46 \\ x &= \frac{46}{69} = \frac{2}{3} \end{aligned}$$

We now substitute this value of x back into one of the original equations to find y. Using equation (1):

$$\begin{aligned} 15\left(\frac{2}{3}\right) + 12y &= 4 \\ 10 + 12y &= 4 \\ 12y &= -6 \\ y &= -\frac{6}{12} = -\frac{1}{2} \end{aligned}$$

The unique solution to the system is $(x, y) = (\frac{2}{3}, -\frac{1}{2})$.

Alternative (Eliminating x): The least common multiple of 15 and 12 is 60. We multiply equation (1) by 4 and equation (2) by 5:

$$\begin{aligned} 60x + 48y &= 16 \\ 60x - 90y &= 85 \end{aligned}$$

Subtracting the second new equation from the first eliminates x:

$$\begin{aligned} (60x + 48y) - (60x - 90y) &= 16 - 85 \\ 138y &= -69 \\ y &= -\frac{69}{138} = -\frac{1}{2} \end{aligned}$$

Substituting this value of y back into equation (1) yields $15x + 12(-\frac{1}{2}) = 4 \implies 15x - 6 = 4 \implies 15x = 10 \implies x = \frac{10}{15} = \frac{2}{3}$. Both approaches yield the same unique solution.

Inconsistent and Dependent Systems

Not all systems of linear equations possess a unique solution.

1. **Inconsistent Systems:** A system may have no solution. Consider the system:

$$\begin{aligned} 3x + 5y &= 2 \\ -12x - 20y &= 9 \end{aligned}$$

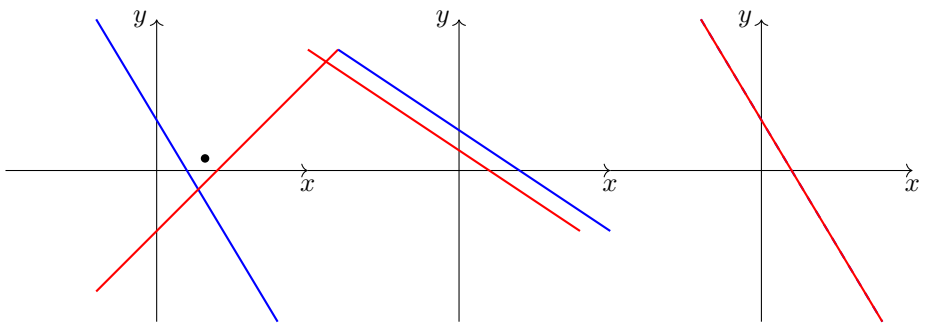
   If we multiply the first equation by -4, we obtain an equivalent equation: $-12x - 20y = -8$. This directly contradicts the second equation, which asserts that the same expression, $-12x - 20y$, equals 9. This contradiction implies that no pair (x, y) can simultaneously satisfy both equations. The system is inconsistent.

2. **Dependent Systems:** A system may have infinitely many solutions. If one equation is a multiple of the other, for example $3x + 5y = 2$ and $-12x - 20y = -8$, then the two equations are equivalent. Any pair (x, y) that satisfies the first equation will automatically satisfy the second. The system is dependent.

General Solution and Geometric Interpretation

The nature of the solution to a system of two linear equations corresponds to the geometric relationship between the two straight lines they represent in a Cartesian coordinate system.

As shown in Figure 12.1, a unique solution corresponds to the point of intersection of two lines. An inconsistent system corresponds to two distinct parallel lines, and a dependent system corresponds to two coincident lines.



(a) Unique Solution (b) No Solution (c) Infinite Solutions

Figure 12.1: Geometric interpretation of a 2x2 system of linear equations. (a) Intersecting lines give a unique solution. (b) Parallel lines give no solution. (c) Coincident lines give infinitely many solutions.

***Theorem* 12.1.1.** For the system $ax + by = c$ and $dx + ey = f$:

1. If $ae - bd \neq 0$, there is a unique solution.
2. If $ae - bd = 0$ and the equations are not multiples of each other, there is no solution.
3. If $ae - bd = 0$ and one equation is a multiple of the other, there are infinitely many solutions.

The quantity $ae - bd$ is the determinant of the system's coefficient matrix. Its non-vanishing is the condition for a unique solution.

Proof of the Elimination Method

The elimination procedure is valid because it transforms a given system into an **equivalent system**, one which has precisely the same solution set.

***Theorem* 12.1.2.** The operations of (i) multiplying an equation by a non-zero constant, and (ii) adding a multiple of one equation to another, transform a linear system into an equivalent one.

Proof. Let the original system be S, comprising equations $E_1 : ax+by = c$ and $E_2 : dx+ey = f$. Let (x_0, y_0) be any solution to S. Operation (i): Consider the new system S' with equations kE_1 (for $k \neq 0$) and E_2. Clearly, if (x_0, y_0) satisfies E_1, it also satisfies kE_1. It still satisfies E_2. So any solution of S is a solution of S'. Conversely, since $k \neq 0$, we can divide kE_1 by k to recover E_1. Thus any solution of S' is also a solution of S. The systems are equivalent. Operation (ii): Consider the system S'' with equations E_1 and $E_2 + kE_1$. If (x_0, y_0) solves S, it satisfies E_1 and E_2. It must therefore also satisfy $E_2 + kE_1$. Thus (x_0, y_0) is a solution to S''. Conversely, if (x_0, y_0) solves S'', it satisfies E_1 and $E_2 + kE_1$. Subtracting kE_1 from the second equation shows that it must also satisfy E_2. Thus (x_0, y_0) is a solution to S. The systems are equivalent. Since the elimination method consists of a sequence of these equivalence-preserving operations, the final values obtained for x and y are the only possible solutions to the original system. ■

Application

Systems of linear equations provide a natural framework for solving word problems.

Example 12.1.2. A metallurgist needs to create 200g of an alloy that is 52% gold by weight. She has two alloys available: Alloy A is 40% gold and 60% silver, and Alloy B is 70% gold and 30% silver. How many grams of each alloy should she mix?. Let x be the mass (in grams) of Alloy A used, and let y be the mass of Alloy B used. The total mass of the final mixture must be 200g, which gives our first equation:

$$x + y = 200.$$

The total mass of gold in the final mixture must be 52% of 200g, which is $0.52 \times 200 = 104$g. The amount of gold contributed by Alloy A is $0.40x$, and by Alloy B is $0.70y$. This gives our second equation:

$$0.4x + 0.7y = 104.$$

We now solve the system. It is convenient to clear the decimals from the second equation by multiplying it by 10:

$$4x + 7y = 1040.$$

From the first equation, we can express x in terms of y: $x = 200 - y$. Substituting this into our modified second equation:

$$\begin{aligned} 4(200 - y) + 7y &= 1040 \\ 800 - 4y + 7y &= 1040 \\ 3y &= 240 \\ y &= 80 \end{aligned}$$

Now, we find x using the first equation:

$$x = 200 - y = 200 - 80 = 120.$$

The metallurgist must mix 120g of Alloy A and 80g of Alloy B to achieve the desired result.

12.2 Systems of Linear Equations in Three Variables

The method of elimination extends naturally to systems with more variables. For a system of three linear equations in three variables, the strategy is to reduce the problem to a 2x2 system, which can then be solved as before.

Method of Successive Elimination

The process involves two main stages:

1. **Reduction to a 2x2 System:** Choose one variable to eliminate. Use two different pairs of the original equations to eliminate this chosen variable, resulting in a new system of two equations in the remaining two variables.
2. **Solution and Back-Substitution:** Solve the new 2x2 system. Substitute the two values found back into one of the original equations to find the value of the first variable that was eliminated.

Example 12.2.1. Solve the system for x, y, z:.

$$x + y + z = 4 \tag{12.3}$$
$$2x - y + 3z = 14 \tag{12.4}$$
$$3x + 2y - z = 1 \tag{12.5}$$

Stage 1: Reduction to a 2x2 System

We choose to eliminate the variable y, as its coefficients are convenient. First, we use equations (1) and (2). Adding them directly eliminates y:

$$\begin{aligned} (x + y + z) + (2x - y + 3z) &= 4 + 14 \\ 3x + 4z &= 18 \end{aligned} \tag{4}$$

Next, we use a different pair, say equations (1) and (3), to eliminate y again. We multiply equation (1) by -2 and add it to equation (3):

$$\begin{aligned} -2(x+y+z)+(3x+2y-z) &= -2(4)+1 \\ (-2x-2y-2z)+(3x+2y-z) &= -8+1 \\ x-3z &= -7 \end{aligned} \tag{5}$$

Equations (4) and (5) now form a 2x2 system in variables x and z.

Stage 2: Solution and Back-Substitution

We now solve the system:

$$\begin{aligned} 3x+4z &= 18 \\ x-3z &= -7 \end{aligned}$$

To eliminate x, we multiply equation (5) by -3 and add it to equation (4):

$$\begin{aligned} (3x+4z)-3(x-3z) &= 18-3(-7) \\ 3x+4z-3x+9z &= 18+21 \\ 13z &= 39 \\ z &= 3 \end{aligned}$$

Now, we substitute $z=3$ back into one of the 2x2 equations to find x. Using equation (5):

$$x-3(3)=-7 \implies x-9=-7 \implies x=2.$$

Finally, we substitute $x=2$ and $z=3$ back into one of the original equations to find y. Using equation (1):

$$2+y+3=4 \implies y+5=4 \implies y=-1.$$

The unique solution to the system is the ordered triple $(x,y,z)=(2,-1,3)$.

Geometric Interpretation

Just as a linear equation in two variables represents a line in a two-dimensional plane, a linear equation in three variables represents a plane in three-dimensional space. The solution to a 3x3 system is the set of all points that lie on all three planes simultaneously.

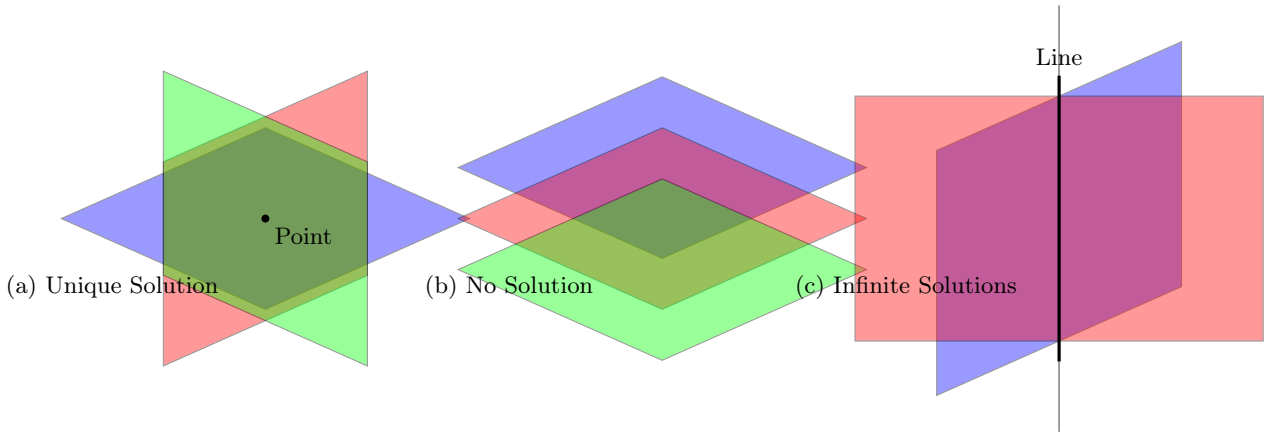


Figure 12.2: Geometric interpretation of a 3x3 system. (a) Three planes intersecting at a single point. (b) Three parallel planes with no common intersection. (c) Three planes intersecting along a common line.

As illustrated in Figure 12.2:

- **Unique Solution:** The three planes intersect at a single, unique point.
- **No Solution (Inconsistent):** The geometric configuration allows for no common point of intersection. This can occur if the planes are parallel, if two are parallel and the third intersects them, or if the planes intersect in pairs along three parallel lines.
- **Infinite Solutions (Dependent):** The three planes intersect along a common line, or all three planes are coincident (i.e., they are the same plane).

12.3 Exercises

Part I: Systems in Two Variables

1. Solve the following systems of equations for x and y.

(a) $2x + 5y = 19, \quad 3x - y = 3$

(b) $7x - 4y = 2, \quad 8x - 5y = 1$

(c) $\dfrac{x}{3} + \dfrac{y}{2} = 3, \quad \dfrac{x}{4} - \dfrac{y}{3} = -\dfrac{1}{12}$

2. Solve the following systems for x and y in terms of the other letters.

(a) $ax - by = a^2 + b^2, \quad bx + ay = 2ab$

(b) $\dfrac{x}{a} + \dfrac{y}{b} = 2, \quad \dfrac{x}{a-b} - \dfrac{y}{a+b} = \dfrac{4ab}{a^2 - b^2}$

3. Solve the system: $19x + 23y = 3, \quad 23x + 19y = 43.$

Remark. Instead of direct elimination, first add the two equations, then subtract one from the other. This will produce a much simpler equivalent system.

4. A person has £2550 to invest. They divide the money into two accounts, one paying 4% annual interest and the other 5.5% annual interest. After one year, the total interest earned from both accounts is £124.50. How much was invested in each account?

5. A boat travels 36 miles downstream in 3 hours. The return trip upstream takes 4 hours. Find the speed of the boat in still water and the speed of the current.

6. Investigate the solution sets of the following systems. If a unique solution exists, find it. If not, state whether the system is inconsistent or dependent, and describe the solution set.

(a) $3x - 6y = 9$ and $2y - x = -3$

(b) $2x + 5y = 7$ and $15y = 21 - 6x$

(c) $x - y = 4$ and $y = x - 5$

7. Without solving, determine the geometric relationship (intersecting, parallel, or coincident) between the pairs of lines represented by the equations in the previous question. Justify your answer by comparing the ratios of the coefficients.

8. Find the value of the constant k for which the system of equations $5x + 2y = 3$ and $10x + ky = 8$ is inconsistent (has no solution).

Part II: Systems in Three or More Variables

9. Solve the following system for x, y, z.

$$\begin{aligned} 3x - 2y + z &= 7 \\ x + 3y - 2z &= -3 \\ 2x - y - z &= 0 \end{aligned}$$

10. Solve the following systems, noting their symmetric structure.

(a) $x + y = 10, \quad y + z = 13, \quad z + x = 17$

(b) $\dfrac{1}{x} + \dfrac{1}{y} = 8, \quad \dfrac{1}{y} + \dfrac{1}{z} = 10, \quad \dfrac{1}{z} + \dfrac{1}{x} = 12$

11. Solve for x, y, z in terms of a, b, c.

$$\begin{aligned} -x + y + z &= a \\ x - y + z &= b \\ x + y - z &= c \end{aligned}$$

12. Investigate the system:

$$\begin{aligned} x + y - z &= 5 \\ 2x - y + 3z &= 1 \\ 4x + y + z &= 11 \end{aligned}$$

What happens during the elimination process? Interpret the result geometrically.

13. ⋆ The method of elimination generalises. Solve the following 4x4 system for w, x, y, z.

$$\begin{aligned} w + x + y &= 6 \\ x + y + z &= 7 \\ y + z + w &= 8 \\ z + w + x &= 9 \end{aligned}$$

Part III: Proofs and Advanced Problems

15. Solve the general system for x and y:

$$\begin{aligned} ax + by &= c \\ dx + ey &= f \end{aligned}$$

Use your result to prove that a unique solution exists if and only if the determinant, $ae - bd$, is not equal to zero.

16. A system of the form $ax + by = 0, dx + ey = 0$ is called a **homogeneous system**.

(a) Explain why such a system can never be inconsistent.

(b) What is the condition on the coefficients for the system to have a unique solution? What is this solution?

(c) Under what condition does the system have infinitely many solutions?

17. Find the constants A, B, C such that the following equation is an identity (true for all values of x):

$$5x^2 - 7x + 3 = A(x-1)^2 + B(x-1) + C$$

Remark. Expand the right-hand side, collect terms, and equate the coefficients of like powers of x. This will create a 3x3 system for A, B, C.

18. Three solutions to the equation $y = f(x)$ for a polynomial function f are given: $(1, -2), (2, 3), (3, 12)$.

(a) Find the unique quadratic polynomial $f(x) = ax^2 + bx + c$ that passes through these three points.

(b) Is there a unique linear polynomial $f(x) = mx + c$ that passes through these points? Explain.

19. Find the point of intersection of the three lines given by the equations:

$$\begin{aligned} x - y &= 6 \\ 3x + y &= 2 \\ \frac{x-1}{2} - \frac{y+2}{3} &= \frac{8}{3} \end{aligned}$$

20. ⋆ If the system of equations $x + ay = b$ and $cx + y = d$ has a unique solution, what condition must be satisfied by the constants a, b, c, d for the solution to be $x = y$?

21. ⋆ For a system of three linear equations in x, y, z, let the equations be $E_1 = 0, E_2 = 0, E_3 = 0$. Prove that if there exist three constants k_1, k_2, k_3, not all zero, such that $k_1E_1 + k_2E_2 + k_3E_3 = 0$ is an identity (i.e., it reduces to $0x + 0y + 0z = 0$), then the system is dependent and has infinitely many solutions. Interpret this geometrically.

Appendix A

Review of Core Algebraic Topics

A.1 Inequalities

We have thus far dealt with equations, which assert the equality of two quantities. We now consider inequalities, which concern their relative order. The fundamental properties of order for real numbers are based on the concept of positivity.

***Axiom* A.1.1. (Properties of Positive Numbers).**

1. If a and b are positive, then their sum $a + b$ is positive.
2. If a and b are positive, then their product ab is positive.

From these two axioms, all the rules for manipulating inequalities can be derived.

We define the order relations as follows:

- A number a is positive if we write $a > 0$.
- We write $a > b$ to mean that the difference $a - b$ is positive.
- We write $a < 0$ to mean that $-a$ is positive.
- We write $a < b$ to mean that $b > a$.

Geometrically, the relation $a > b$ means that the number a lies to the right of the number b on the number line, as shown in Figure A.1.

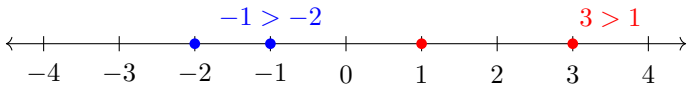


Figure A.1: Geometric representation of order on the number line.

We also use the symbols $\geq$ and $\leq$ to include the possibility of equality.

- $a \geq b$ means that a is greater than or equal to b.
- $a \leq b$ means that a is less than or equal to b.

Thus, $3 \geq 2$ and $3 \geq 3$ are both true statements.

A.1.1 Fundamental Rules for Inequalities

***Theorem* A.1.1.** Let a, b, c be real numbers. The following rules hold:

(i) **(Transitivity)** If $a > b$ and $b > c$, then $a > c$.

(ii) **(Preservation)** If $a > b$ and $c > 0$, then $ac > bc$.

(iii) **(Reversal)** If $a > b$ and $c < 0$, then $ac < bc$.

Rule (ii) states that an inequality is preserved when multiplied by a positive number. Rule (iii) states that an inequality is reversed when multiplied by a negative number. For instance, $3 > 1$, but multiplying by -2 gives $-6 < -2$.

Proof.

(i) By definition, $a > b$ means $a - b > 0$, and $b > c$ means $b - c > 0$. By the axiom of positive numbers, their sum must be positive:

$$(a - b) + (b - c) > 0 \implies a - c > 0.$$

By definition, this means $a > c$.

(ii) By definition, $a - b > 0$. We are given $c > 0$. By the axiom of positive numbers, their product must be positive:

$$(a - b)c > 0 \implies ac - bc > 0.$$

By definition, this means $ac > bc$.

The proof of (iii) is left as an exercise for the reader. ■

A.1.2 Solving Inequalities

To solve an inequality is to find the set of all numbers for which the inequality holds true.

Example A.1.1. Solve $3x - 5 > 7$.

$3x - 5 > 7$	
$3x > 12$	Add 5 to both sides
$x > 4$	Divide by 3 (a positive number)

The solution is the set of all real numbers greater than 4.

Example A.1.2. Solve $\frac{2x+1}{x-3} \leq 1$. The critical step here is multiplying by the denominator, $x - 3$. The sign of this term determines whether the inequality is preserved or reversed. We must therefore consider two separate cases. The expression is undefined for $x = 3$.

Case 1: $x - 3 > 0$, i.e., $x > 3$. In this case, we multiply by a positive number, preserving the inequality.

$$\begin{aligned} 2x + 1 &\leq 1(x - 3) \\ 2x + 1 &\leq x - 3 \\ x &\leq -4 \end{aligned}$$

We are seeking numbers x that satisfy both $x > 3$ and $x \leq -4$. There are no such numbers. Thus, there is no solution in this case.

Case 2: $x - 3 < 0$, i.e., $x < 3$. In this case, we multiply by a negative number, reversing the inequality.

$$\begin{aligned} 2x + 1 &\geq 1(x - 3) \\ 2x + 1 &\geq x - 3 \\ x &\geq -4 \end{aligned}$$

We are seeking numbers x that satisfy both $x < 3$ and $x \geq -4$. The solution set for this case consists of all numbers between -4 and 3, including -4. Combining the results from both cases, the final solution is $-4 \leq x < 3$.

A.1.3 Intervals

The solution sets of inequalities are often **intervals**.

Definition A.1.1. ***(Interval)***. An interval is a subset of the real numbers corresponding to a continuous segment of the number line. Let a, b be numbers with $a \leq b$.

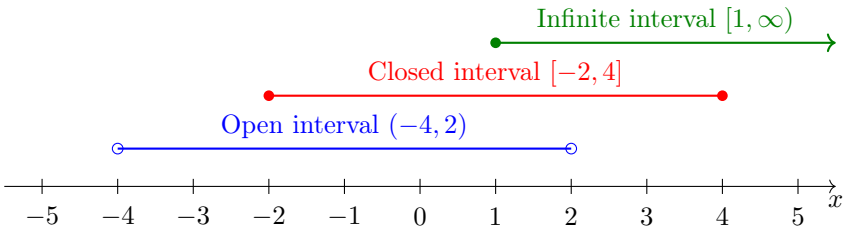


Figure A.2: Representation of various types of intervals on the number line. An open circle indicates an endpoint is not included; a filled circle indicates it is included.

- The open interval (a, b) is the set $\{x \mid a < x < b\}$.
- The closed interval $[a, b]$ is the set $\{x \mid a \leq x \leq b\}$.
- Half-open intervals are $[a, b) = \{x \mid a \leq x < b\}$ and $(a, b] = \{x \mid a < x \leq b\}$.
- Infinite intervals represent unbounded sets, such as $(a, \infty) = \{x \mid x > a\}$ or $(-\infty, b] = \{x \mid x \leq b\}$.

A.2 Exercises

Part I: Solving Basic Inequalities

1. Solve the following linear inequalities for x. Express your answer as an inequality and represent it on a number line.

(a) $5x + 3 > 28$

(b) $4 - 2x \geq 10$

(c) $\frac{x}{3} - 1 \leq \frac{x}{4} + 1$

(d) $2(x - 3) + 5 < 3(x + 1) - 2x$

2. Find the range of values for x that satisfy the following compound inequalities. Express your answer using interval notation as described in Figure A.2.

(a) $-2 \leq 3x + 1 < 7$

(b) $0 < 5 - 2x \leq 11$

(c) $x - 1 < 2x + 3 < 3x - 1$

3. Given that $a > b$ and $c > d$, determine which of the following statements are always true. Provide a proof or a counterexample for each.

(a) $a + c > b + d$

(b) $a - c > b - d$

(c) $ac > bd$

(d) $a/c > b/d$ (assuming all are positive)

4. A student has scores of 85, 91, 82, and 94 on four tests. What score must the student achieve on the fifth test to have an average of at least 90?

5. Prove part (iii) of the fundamental rules theorem: If $a > b$ and $c < 0$, then $ac < bc$.

Part II: Rational and Quadratic Inequalities

Remark. Solving inequalities where the variable appears in the denominator or in a quadratic expression requires a more careful analysis of signs. The critical points of an expression are the values where it is zero or undefined. These points divide the number line into intervals, within which the sign of the expression is constant.

6. Solve the following rational inequalities by considering cases based on the sign of the denominator.

(a) $\dfrac{x+4}{x-2} > 0$

(b) $\dfrac{1}{x+1} \geq 2$

(c) $\dfrac{3x-1}{x+5} \leq 1$

7. Solve the following quadratic inequalities. First, factorise the quadratic expression to find its roots. Then, test the sign of the expression in the intervals defined by these roots.

(a) $(x-3)(x+2) > 0$

(b) $x^2 - 7x + 10 \leq 0$

(c) $2x^2 + 5x - 3 \geq 0$

(d) $x^2 + 2x - 8 > 0$

8. Find the set of all real numbers x for which the expression $\sqrt{x^2 - 4}$ is a real number.

9. $\star$ Solve the inequality $\dfrac{x^2 - 3x - 4}{x - 1} \geq 0$.

Remark. Find the critical points from both the numerator and the denominator. Use these points to divide the number line and test the sign of the fraction in each interval.

Part III: Absolute Value and Fundamental Proofs

Definition A.2.1. ***(Absolute Value)***. The absolute value of a real number x, denoted $|x|$, is defined as:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

Geometrically, $|x|$ represents the distance of x from the origin on the number line. Similarly, $|a-b|$ represents the distance between a and b.

11. Solve the following inequalities involving absolute values. Interpret your solution both algebraically and geometrically in terms of distance.

(a) $|x| < 3$

(b) $|x-2| \geq 5$

(c) $|2x+1| \leq 7$

12. Let a be a positive number. Prove the following fundamental equivalences for absolute value.

(a) $|x| < a$ is equivalent to $-a < x < a$.

(b) $|x| > a$ is equivalent to $x > a$ or $x < -a$.

Remark. For each proof, consider the two cases based on the definition of $|x|$: $x \geq 0$ and $x < 0$.

13. Prove the Triangle Inequality: For any real numbers a and b,

$$|a+b| \leq |a| + |b|.$$

Remark. Begin by noting that $-|a| \leq a \leq |a|$ and $-|b| \leq b \leq |b|$. Add these two inequalities.

14. Prove that for any positive numbers a and b, if $a > b$, then $a^2 > b^2$. Is the converse true?

15. $\star$ **(Arithmetic Mean - Geometric Mean Inequality)** Prove that for any two non-negative real numbers a and b, their arithmetic mean is greater than or equal to their geometric mean:

$$\frac{a+b}{2} \geq \sqrt{ab}.$$

Remark. Start from the fact that the square of any real number is non-negative. Consider the expression $(\sqrt{a} - \sqrt{b})^2$.

When does equality hold?

16. Use the result of the previous problem to prove that among all rectangles with a fixed perimeter P, the square has the largest area.

Remark. Let the sides be l and w. The perimeter is $P = 2(l+w)$ and the area is $A = lw$. Relate the quantities $l + w$ and $\sqrt{lw}$.

17. $\star$ **(Cauchy-Schwarz Inequality)** For any real numbers a, b, c, d, prove that

$$(a^2 + b^2)(c^2 + d^2) \geq (ac + bd)^2.$$

Remark. Expand both sides of the inequality and rearrange the terms to form an expression that is clearly non-negative.

A.3 The Logarithmic Function

The logarithmic function is the inverse of the exponential function. Given the exponential relation $y = a^x$, where $a > 0$ and $a \neq 1$, the logarithm is defined as the exponent x to which the base a must be raised to yield the number y.

Definition A.3.1. ***(Logarithm)***. The expression $x = \log_a y$ is the logarithmic form of the equation $y = a^x$.

- a is the base of the logarithm.
- y is the argument of the logarithm, and must be positive.
- The two equations, $y = a^x$ and $x = \log_a y$, are equivalent statements.

From this definition, a logarithm is fundamentally an exponent. For instance, $\log_2 8 = 3$ because $2^3 = 8$. Similarly, $\log_{10} 100 = 2$ because $10^2 = 100$.

The relationship between the exponential function and its inverse, the logarithmic function, is shown in Figure A.3. The graph of $y = \log_a x$ is a reflection of the graph of $y = a^x$ across the line $y = x$.

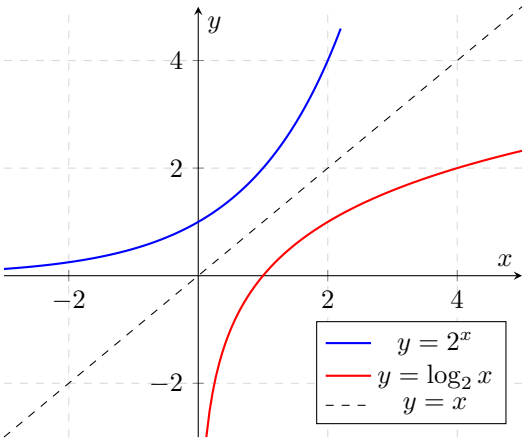


Figure A.3: The graphs of an exponential function ($y = 2^x$) and its corresponding logarithmic function ($y = \log_2 x$), illustrating their symmetry about the line $y = x$.

A.3.1 Fundamental Properties of Logarithms

The laws of logarithms are direct consequences of the laws of indices.

***Theorem* A.3.1. (Product Rule)**. The logarithm of a product is the sum of the logarithms of its factors.

$$\log_a(xy) = \log_a x + \log_a y$$

Proof. *Let* $m = \log_a x$ *and* $n = \log_a y$. *By definition,* $a^m = x$ *and* $a^n = y$. *Then,* $xy = a^m \cdot a^n = a^{m+n}$ *by the laws of indices. Converting back to logarithmic form, we have* $\log_a(xy) = m + n$. *Substituting the original expressions for* m *and* n *gives* $\log_a(xy) = \log_a x + \log_a y$. ■

***Theorem* A.3.2. (Quotient Rule)**. The logarithm of a quotient is the logarithm of the numerator minus the logarithm of the denominator.

$$\log_a\left(\frac{x}{y}\right) = \log_a x - \log_a y$$

Proof. *Let* $m = \log_a x$ *and* $n = \log_a y$. *Then* $a^m = x$ *and* $a^n = y$. *The quotient is* $\frac{x}{y} = \frac{a^m}{a^n} = a^{m-n}$. *In logarithmic form, this is* $\log_a\left(\frac{x}{y}\right) = m - n$. *Substituting for* m *and* n *yields* $\log_a\left(\frac{x}{y}\right) = \log_a x - \log_a y$. ■

***Theorem* A.3.3. (Power Rule)**. The logarithm of a number raised to a power is the power multiplied by the logarithm of the number.

$$\log_a(x^p) = p \log_a x$$

Proof. *Let* $m = \log_a x$, *so* $a^m = x$. *Then* $x^p = (a^m)^p = a^{mp}$. *In logarithmic form, this is* $\log_a(x^p) = mp$. *Substituting for* m *gives* $\log_a(x^p) = p \log_a x$. ■

A.3.2 Special Bases and the Change of Base Formula

While a logarithm can have any valid base, two bases are used so frequently they have special names and notation.

1. **Common Logarithm:** This is the logarithm with base 10, written as $\log x \equiv \log_{10} x$. It is particularly useful for calculations in our base-10 number system.
2. **Natural Logarithm:** This is the logarithm with base e, Euler's number ($e \approx 2.71828$), written as $\ln x \equiv \log_e x$. The natural logarithm is fundamental in calculus and many areas of science.

It is often necessary to convert a logarithm from one base to another. This is achieved with the change of base formula.

***Theorem* A.3.4. (Change of Base)**. For any valid bases $a, b \neq 1$, and any $x > 0$:

$$\log_a x = \frac{\log_b x}{\log_b a}$$

Proof. Let $y = \log_a x$. By definition, $a^y = x$. Take the logarithm with base b of both sides of the equation:

$$\log_b(a^y) = \log_b x$$

Using the power rule, we bring the exponent y to the front:

$$y \log_b a = \log_b x$$

Solving for y gives:

$$y = \frac{\log_b x}{\log_b a}$$

Substituting $y = \log_a x$ back gives the identity $\log_a x = \frac{\log_b x}{\log_b a}$. ■

This formula allows any logarithm to be calculated using only common or natural logarithms, which are standard on calculators. For example, $\log_3 35 = \frac{\ln 35}{\ln 3}$.

A.3.3 Exercises

1. Evaluate the following logarithms without using a calculator.

(a) $\log_4 64$
(b) $\log_5 \left(\frac{1}{25}\right)$
(c) $\log_9 3$
(d) $\ln(e^5)$

2. Use the laws of logarithms to expand the following expressions.

(a) $\log\left(\frac{x^2 y^3}{z}\right)$
(b) $\ln\left(\sqrt{\frac{a(b-c)^2}{d}}\right)$

3. Condense the following into a single logarithmic expression.

(a) $2\log x + 3\log y - \frac{1}{2}\log z$
(b) $\ln(x^2 - 1) - \ln(x + 1)$

4. Solve the following exponential equations for x.

(a) $5^x = 125$
(b) $3^{x-1} = 7$
(c) $e^{2x+1} = 10$

5. Use the change of base formula to evaluate $\log_7 50$ using natural logarithms.

6. Prove the following identity: $\log_b a \cdot \log_c b \cdot \log_a c = 1$.

7. If $\log_a x = p$ and $\log_a y = q$, express $\log_a \sqrt{x^3 y}$ in terms of p and q.

8. Solve the equation $\log_2(x) + \log_2(x - 2) = 3$.

9. Prove that $\log_{a^n}(x^n) = \log_a x$ for any integer $n \geq 1$.

10. ⋆ Given that $a^2 + b^2 = 7ab$, prove that $\log\left(\frac{a+b}{3}\right) = \frac{1}{2}(\log a + \log b)$.