CHAPTER 5

Combinatorics, Factorisation Background

Note that in this chapter, $n, k, r \in \mathbb{N}$.

5.1 Factorisation of $a^n \pm b^n$

Let us start with something familiar, summing

$$1 + r + r^2 + \cdots + r^{n-1}.$$

This is a *geometric series* with *common ratio* r (with 1 as the first term). It's useful to give the series a name. Lets call it S_n (the sum to n terms). Then

$$\begin{aligned} S_n &= 1 + r + r^2 + \cdots + r^{n-1} && (5.1.1)\\ rS_n &= \phantom{1 + {}} r + r^2 + \cdots + r^{n-1} + r^n && (5.1.2)\\ (1-r)S_n &= 1 - r^n, \qquad \text{subtracting (5.1.2) from (5.1.1).} && (5.1.3) \end{aligned}$$

In the context of *geometric series,* we would then proceed to isolate S_n, but in the current context, substituting (5.1.1) back in (5.1.3) and swapping the lefthand and righthand sides, gives us the factorisation

$$1 - r^n = (1-r)(1 + r + r^2 + \cdots + r^{n-1}).$$

Now replace r by b/a, and then multiply through both sides by a^n:

$$\begin{aligned} 1 - \left(\frac{b}{a}\right)^n &= \left(1 - \left(\frac{b}{a}\right)\right)\left(1 + \left(\frac{b}{a}\right) + \left(\frac{b}{a}\right)^2 + \cdots + \left(\frac{b}{a}\right)^{n-1}\right)\\ a^n - b^n &= (a-b)(a^{n-1} + a^{n-2}b + \cdots + a^{n-k}b^{k-1} + \cdots + b^{n-1}). && (5.1.4) \end{aligned}$$

In multiplying the righthand side by a^n, we multiply the first bracket by a and the second bracket by a^{n-1}, and note that that means the sum of the indices appearing in each term in the second bracket is $n-1$. We now have a factorisation of $a^n - b^n$.

To get a similar factorisation of $a^n + b^n$, we replace b by $-b$ in (5.1.4). Note that, in order for this to actually give us a factorisation of $a^n + b^n$, we need $-(-b)^n = b^n$, i.e. n must be *odd.* Thus,

$$\begin{aligned} a^n - (-b)^n &= \big(a - (-b)\big)\big(a^{n-1} + a^{n-2}(-b) + \cdots + a^{n-k}(-b)^{k-1} + \cdots + (-b)^{n-1}\big)\\ &= \big(a - (-b)\big)\big(a^{n-1} + a^{n-2}(-b) + \cdots + a^{n-k}(-b)^{k-1} + \cdots + (-b)^{n-1}\big)\\ a^n + b^n &= (a+b)(a^{n-1} - a^{n-2}b + \cdots + (-1)^{k-1}a^{n-k}b^{k-1} + \cdots + b^{n-1}), \quad \text{for } n \text{ odd.} && (5.1.5) \end{aligned}$$

Observe that $(-b)^{n-1} = b^{n-1}$ in (5.1.5), since $n-1$ is even.

Summarising, we have

$$\boxed{\begin{aligned} a^n - b^n &= (a-b)(a^{n-1} + a^{n-2}b + \cdots + a^{n-k}b^{k-1} + \cdots + b^{n-1})\\ a^n + b^n &= (a+b)(a^{n-1} - a^{n-2}b + \cdots + (-1)^{k-1}a^{n-k}b^{k-1} + \cdots + b^{n-1}), \quad \text{for } n \text{ odd.} \end{aligned}}$$

5.2 Expansion of the binomial $(a+b)^n$

Now consider the expansion of $(a+b)^n$. For completeness (it gives the first line of Pascal's Triangle), also consider $n=0$:

$$\begin{aligned}(a+b)^0 &= 1\\ (a+b)^1 &= a+b\\ (a+b)^2 &= a^2+2ab+b^2\\ (a+b)^3 &= a^3+3a^2b+3ab^2+b^3\end{aligned}$$

and in general,

Theorem 5.2.1 (Binomial Theorem). *For $n \in \mathbb{N} \cup \{0\}$,*

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{r}a^{n-r}b^r + \cdots + \binom{n}{n}b^n,$$

where

$$\binom{n}{r} = \frac{n(n-1)(n-2)\cdots(n-r+1)}{r(r-1)(r-2)\cdots 1}.$$

Proof. In expanding $(a+b)^n$ we note that there are 2^n terms, since there are 2 terms in each of n brackets, where each term is a product of some number of as and some number of bs. Since the number of brackets is n, and in forming a particular term we take either an a or a b from each bracket, the sum of the numbers of as and bs making up the term is n, i.e. each term of $(a+b)^n$ is of form

$$a^{n-r}b^r,$$

for some $r \in \{0,1,2,\ldots,n\}$. Evidently, a term of form $a^{n-r}b^r$ occurs many times, and we will see that this number is dependent on both n and r; we call this number a **binomial coefficient**, and write it as follows:

$$\binom{n}{r}.$$

Thus,

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{r}a^{n-r}b^r + \cdots + \binom{n}{n}b^n.$$

Now we do must establish a value for $\binom{n}{r}$; in forming $a^{n-r}b^r$ we may choose a b from r of the n brackets, then the brackets we take the as from are determined.

The first b can come from any of n brackets, leaving $n-1$ brackets from which to choose the second b, and so on, until the r^{th} b can be taken from $n-(r-1) = n-r+1$ brackets.

It would appear then that there are

$$n(n-1)(n-2)\cdots(n-r+1)$$

ways of choosing which of the r brackets we take a b from. However, we can choose the same r brackets in

$$r(r-1)(r-2)\cdots 1 = r!$$

different orders. Thus counting in the above way, overcounts every possible way by a factor of $r!$. Thus we have

$$\binom{n}{r} = \frac{n(n-1)(n-2)\cdots(n-r+1)}{r!}.$$

□

Note that there are r factors in both the numerator and denominator of the expression

$$\frac{n(n-1)(n-2)\cdots(n-r+1)}{r(r-1)(r-2)\cdots 1},$$

for $\binom{n}{r}$. The formula above doesn't appear to given an expression for $r = 0$. Just know that empty products are 1 (we will revisit this idea in a later chapter); so that $\binom{n}{0} = 1$.

Properties of binomial coefficients. Binomial coefficients have the following properties. You are asked to prove the fourth of these in Exercise 11.

$$\begin{aligned}
\binom{n}{0} &= 1 \\
\binom{n}{1} &= n \\
\binom{n}{r} &= \binom{n}{n-r}, \quad \text{(the symmetry property)} \\
\binom{n+1}{r+1} &= \binom{n}{r} + \binom{n}{r+1}
\end{aligned}$$

Pascal's Triangle. The *binomial coefficients* form a triangle known as **Pascal's triangle**, where n is the row number, starting at the 0^{th} row, and r is fixed along diagonals.

$$\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1 \\
 & & & & & & & & \\
\binom{n}{0} & \binom{n}{1} & \cdots & \binom{n}{r} & \binom{n}{r+1} & \cdots & \binom{n}{n-1} & \binom{n}{n} &
\end{array}$$

5.3 Counting

Fundamental Counting Principle. If one event can occur in m ways and another event in n ways, then:

FC1: *one* of the events can occur in $m + n$ ways. **(addition principle)**
In this case, the events are said to be **mutually exclusive**.

FC2: *both* events can occur in mn ways. **(multiplication principle)**
In this case, the events are said to be **independent**.

Definition 5.3.1. An r**-sequence** is a sequence of r elements, represented by enclosing the r elements separated by commas within parentheses, e.g. $(a_1, a_2, \ldots, a_r)$.

An r**-set** is a set of r (distinct) elements; it differs from an r*-sequence* in that it an r*-sequence* is ordered, whereas an r-set is not, in the sense, that if one rearranges the elements of an r-set, it is the same r-set, e.g. the 3-set, $\{1, 2, 3\} = \{1, 3, 2\}$.

A **permutation** of an n-set, is an n-sequence of that n-set. From a given n-set, one can form $n!$ permutations of that n-set.

Remark 5.3.2. From a given r-set, one can form $r!$ distinct r-sequences, e.g. from the 3-set $\{a, b, c\}$ one can form $3! = 6$ 3-sequences,

$$(a, b, c),\ (a, c, b),\ (b, a, c),\ (b, c, a),\ (c, a, b),\ (c, b, a).$$

Notation 5.3.3. We will use # followed by a quoted string, to denote **number of** ways of forming the thing represented by the quoted string. In particular,

$$\begin{aligned}
\#\text{“}r\text{-sequences formed from an }n\text{-set”} &= n(n-1)\cdots(n-r+1)\\
&= \frac{n!}{(n-r)!}\\
\#\text{“}r\text{-sets formed from an }n\text{-set”} &= \frac{n(n-1)\dots(n-r+1)}{r!}\\
&= \frac{n!}{r!(n-r)!}\\
&= \binom{n}{r}.
\end{aligned}$$

Remark 5.3.4. In the literature, #“r-sequences formed from an n-set” is denoted by ${}^nP_r$, and is vaguely referred to as the “number of permutations”, but this is an abbreviation of “number of permutations of r of n objects”. Without these last five words it's gibberish.

Also, in the literature, #“r-sets formed from an n-set” is commonly denoted by ${}^nC_r$, and is vaguely referred to as the “number of combinations”. However, ${}^nC_r = \binom{n}{r}$, and *mathematicians* read both notations as *“n choose r”*, which is beautifully succinct and precise, and mnemonically uses the C.

Exercise Set 5.

1. Expand:
   - (a) $(1 + a)(1 + b)(1 + c)$.
   - (b) $(1 + x)^3$.
   - (c) $(a + b + c)^3$.
   - (d) $(a + b)^4$.
2. Factor:
   - (a) $a - b$ as the difference of two squares.
   - (b) $x + 2\sqrt{xy} + y$, where $x, y \geqslant 0$.
3. (i) Factor $a^6 - b^6$ as the difference of two squares.
   - (ii) Factor $a^6 - b^6$ as the difference of two cubes.
   - (iii) Factor $a^6 - b^6$ as the difference of two sixth powers.
   - (iv) Fully factor $a^6 - b^6$.

4. Factor fully (over $\mathbb{Q}$):
   (a) $(a+b)^2 - c^2$.
   (b) $a^4 + 2a^2b^2 + b^4$.
   (c) $a^4 + a^2b^2 + b^4$.
   (d) $x^4 + 3x^2 + 4$.
   (e) $x^4 - 15x^2y^2 + 9y^4$.
   (f) $a^2 - 2a - b^2 + 1$.

5. Find all possible integers solutions to the equation,

$$x^2 + y^2 + z^2 = 10(x+y+z).$$

   Prove that there are no other integer solutions.

6. Express

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

   as the sum of three squares.

7. If $x+3$ divides $3x^2 + x + k$ without remainder, find the value of k.

8. Factor $n^4 + 4$ as the product of two quadratics.
   For what positive integer values of n is $n^4 + 4$ a prime number?

9. Factor:
   (a) $1 + y(1+x)^2(1+xy)$.
   (b) $1 - b - a^2 + a^3b + a^2b^3 - a^3b^3$.

10. Given that

$$\binom{n}{r} = \frac{n(n-1)(n-2)\cdots(n-r+1)}{r(r-1)(r-2)\cdots 1},$$

   (a) find $\binom{21}{3}$ and $\binom{12}{5}$.
   (b) Show that $\displaystyle\binom{n}{r} = \frac{n!}{r!(n-r)!}$.

11. (i) Show that the sum of the coefficients of the r^{th} and $(r+1)^{\text{st}}$ term in the expansion of $(1+x)^n$ is equal to the $(r+1)^{\text{st}}$ term in the expansion of $(1+x)^{n+1}$. (To avoid awkward numbering of the terms, let us call the x^0 term, the *zeroth* term, so that the r^{th} term is the term involving x^r.)
   (ii) Prove the same result using the factorial expression of $\binom{n}{r}$.
   (iii) How is the result connected with Pascal's Triangle?
   (iv) Use the result of (i) (or equivalently, (ii)), to prove

$$\sum_{m=r}^{n} \binom{m}{r} = \binom{n+1}{r+1},$$

   for $r, n \in \mathbb{N}$ such that $n \geqslant r$.
   Hints. Use induction, with fixed r. Call the displayed equation $P(n)$. The *'base case'* is $P(r)$. It's easy!

12. Given the Binomial Theorem result:

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n,$$

prove each of the following.

(a) $\displaystyle\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n.$

(b) $\displaystyle\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n\binom{n}{n} = 0.$

(c) $\displaystyle\binom{n}{0} + 2\binom{n}{1} + 4\binom{n}{2} + 8\binom{n}{3} + \cdots + 2^n\binom{n}{n} = 3^n.$

(d) $\displaystyle\binom{n}{0} - 2\binom{n}{1} + 4\binom{n}{2} - 8\binom{n}{3} + \cdots + (-1)^n 2^n\binom{n}{n} = \begin{cases} 1, & \text{if } n \text{ is even;} \\ -1, & \text{if } n \text{ is odd.} \end{cases}$

13. Prove that

$$\binom{n}{r} = \frac{n-r+1}{r} \cdot \binom{n}{r-1},$$

and hence find the value of r that maximises $\binom{n}{r}$.

14. Observe that in any row of Pascal's Triangle that the sum of the odd-indexed elements is equal to the sum of the even-indexed elements, i.e.

$$\binom{n}{1} + \binom{n}{3} + \cdots = \binom{n}{0} + \binom{n}{2} + \cdots .$$

Prove this result.
Hint. You've already done it!

15. The relation *divides* (written: $|$) is defined and discussed in detail in the next chapter. For now, we say,

For $a, b \in \mathbb{Z}$, a **divides** b (written: $a \mid b$) if $b = aq$ for some $q \in \mathbb{Z}$.

In (a), we assume $a, b \in \mathbb{Z}$, so that $a+b, a-b \in \mathbb{Z}$.
However, the statements in (a) still make sense in a *polynomial* context, in which case, '$|$' should be interpreted to mean *is a factor of*, i.e. there is *zero remainder*.

(a) Show
  (i) $(a-b) \mid (a^n - b^n)$, for all $n \in \mathbb{N}$.
  (ii) $(a+b) \mid (a^n + b^n)$, for all odd $n \in \mathbb{N}$.

(b) Show
  (i) $3 \mid 5^{39} - 2^{39}$.
  (ii) $5 \mid 2^{99} + 3^{99}$.
  (iii) $5 \nmid 2^{98} + 3^{98}$.
  (iv) $7 \mid 2^{99} + 3^{99} + 4^{99} + 5^{99}$.
  (v) $10 \mid 2^{99} - 4^{99} - 7^{99} + 9^{99}$.

(c) Prove that $1991 \mid 3500^n - 728^n - 785^n + 4^n$ for all $n \in \mathbb{N}$.

16. Find a short expression for the following.
    (a) $1 + x + x^2 + \cdots + x^n$ for all positive integers n.
    (b) $1 - x + x^2 - \cdots + x^n$ for all even positive integers n.

17. Factor $a^2(b - c) + b^2(c - a) + c^2(a - b)$.

18. Find all positive integer pairs (x, y) that satisfy

$$x^2 - 871 = y^6.$$

19. If $\left(a - \frac{1}{a}\right)^2 = 3$ and $a - \frac{1}{a} > 0$, evaluate
    (i) $a^3 - \frac{1}{a^3}$.
    (ii) $a^4 + \frac{1}{a^4}$.

20. If a is the difference between any quantity and its reciprocal, and b is the difference between the square of the same quantity and the square of its reciprocal, show that

$$a^2(a^2 + 4) = b^2.$$