CHAPTER 4

Algebra: Quadratic polynomials and Viète's Theorem

4.1 Polynomials

A **polynomial** in x **over** $\mathbb{Z}$ (or **over** $\mathbb{Q}$, or **over** $\mathbb{R}$, or …) is an *expression* of the form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0,$$

where $a_0, a_1, \ldots, a_n$ are fixed numbers called **coefficient**s, that are elements of $\mathbb{Z}$ (or $\mathbb{Q}$, or $\mathbb{R}$, or …).
For convenience, we usually like to give such expressions some sort of label; so that we will usually write something like:

Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$.

(Here $p(x)$ is said: p *of* x).
If $p(x)$ is identically 0, $p(x)$ is called the **zero polynomial**.
If $p(x)$ is not the *zero polynomial*, we insist that $a_n \neq 0$; then

n is the **degree** of $p(x)$,
a_n is the **leading coefficient** of $p(x)$, and
$a_n x^n$ is the **leading term** of $p(x)$.

Note that we haven't yet defined the *degree* of the *zero polynomial*. More generally,

a_k is the k^{th} *coefficient* of $p(x)$,
$a_k x^k$ is the k^{th} *term* of $p(x)$; and
a_0 is both the **constant coefficient** and **constant term** of $p(x)$.

Writing $p(3)$ is a shorthand way of writing:

$$a_n \cdot 3^n + a_{n-1} \cdot 3^{n-1} + \cdots + a_2 \cdot 3^2 + a_1 \cdot 3 + a_0$$
(the expression $p(x)$ with 3 substituted for each occurrence of x).

In words, we say for $p(3)$, *the value of the polynomial* $p(x)$ *at* $x = 3$ or $p(x)$ *evaluated at* $x = 3$ or just simply, p *of 3*.
If the leading coefficient $a_n = 1$ then the polynomial $p(x)$ is said to be **monic**.
An **equation** is something of the form

expression = *expression*.

So a **polynomial equation** is something of the form

polynomial = *expression*,

where the *expression* on the right-hand side is usually just a *value* (i.e. a number) and that *value* is usually 0. A *polynomial equation* (in x) usually only holds true for a small number of x values. For example,

$$x^2 - 1 = 0$$

only holds true for the x-values, 1 and -1. We say, the *polynomial equation* $x^2 - 1$ *is satisfied by 1 and* -1; or we say, it has **roots** 1 and -1; or we say, it has **solutions** 1 and -1.

On the other hand, a *polynomial* $p(x)$ is simply an expression in x. It makes sense, (i.e. has a *value*) for *any* choice of x. Sometimes this value is 0. For this reason, a choice of x such that $p(x)$ evaluates to 0, is called a **zero** of $p(x)$.

Example 4.1.1. *(a) The* ***polynomial*** $x^2 - 3x + 2$ *has two* ***zeros****, namely 1 and 2.*

(b) The ***polynomial equation*** $x^2 - 3x + 2 = 0$ *has two* ***roots****, namely 1 and 2.*
(In this context, the term ***root*** *can be used interchangeably with* ***solution****.)*

So we see that the terms *zero* and *root* (or *solution*) generally amount to the same thing but from different viewpoints!

Two polynomials $p(x), q(x)$ are said to be **equal** if they have the same value for every value of x. This occurs *if and only if* $p(x)$ and $q(x)$ have the same degree and identical coefficients. *Note that two polynomials can have the same value at several x-values without being* equal *polynomials.*

Example 4.1.2. *(a) The polynomials* $p(x) = x^2 + 1$ *and* $q(x) = x^4 + 1$ *are equal at* $x = 0$*, i.e.*

$$p(0) = q(0),$$

but $p(x), q(x)$ *are* not *equal polynomials.*

(b) The polynomials $p(x) = (x - 1)^2$ *and* $q(x) = x^2 - 2x + 1$ are *equal polynomials, and often this is written:* $p(x) = q(x)$*. Usually, the context makes it clear what is meant, but to avoid any ambiguity it is a good idea to get into the practice of writing:*

$$p(x) = q(x) \quad \textit{for all } x.$$

4.2 Degree of a polynomial

We will use the notation $\partial(p)$ for the **degree** of polynomial $p(x)$, which we effectively defined to be n, if the highest power of x occurring in $p(x)$ is n. As yet we haven't defined the *degree* of the *zero polynomial.* Considering, sums and products of polynomials, it would seem ∂ has the following properties:

Properties of ∂. For polynomials $p(x)$ and $q(x)$,

1. $\partial\big(p(x) + q(x)\big) \leqslant \max\big(\partial(p), \partial(q)\big)$.
2. $\partial\big(p(x) \cdot q(x)\big) = \partial(p) + \partial(q)$.

Note that in 1., the "$\leqslant$" is necessary for the case where the leading terms of $p(x)$ and $q(x)$ cancel.

It would seem useful that these properties be generally true. So this brings into question what the *degree* of the *zero polynomial* should be. To make the properties above work with the *zero polynomial*, we *invent* a special integer $-\infty$ which is smaller than any genuine integer and has the property that:

$$-\infty + k = -\infty$$

for any integer k. The zero polynomial is then said to have degree $-\infty$ (rather than 0). All other **constant polynomial**s (i.e. *polynomial*s consisting of only a nonzero *constant* term) have degree 0.

Division Algorithm for polynomials.
*For polynomials $p(x), u(x)$ with $u(x) \neq 0$ there exist polynomials $q(x)$ (the **quotient**) and $r(x)$ (the **remainder**) such that*

$$p(x) = u(x)\,q(x) + r(x) \text{ where } \partial(r) < \partial(u).$$

Essentially $q(x), r(x)$ are the polynomials that make the following division work:

$$\begin{array}{r l} & \underline{\;q(x) \;\; \textit{rem.} \;\; r(x)\;} \\ u(x)\,) & p(x) \end{array}$$

(Compare the above with the corresponding Division Algorithm *for* integers *in Chapter 6.)*

Often $u(x) = x - a$ for some fixed number a, in which case $\partial(u) = 1$ so that $r(x)$, being necessarily of lower degree, is a **constant polynomial**. If $r(x)$ is the zero polynomial then $u(x)$ (and also $q(x)$) is a **factor** of $p(x)$. Now that we have a concrete idea of what polynomial division is, we are in a position to make sense of the following theorems.

Theorem (Remainder Theorem). *If the polynomial $p(x)$ is divided by the polynomial $x - a$ then the remainder is $p(a)$.*

Proof. Write $p(x) = (x - a)q(x) + r(x)$. Then $r(x)$ is a *constant* polynomial (and so we may as well drop the x and simply write r). Substituting a for x gives

$$\begin{aligned} p(a) &= (a - a)q(a) + r \\ &= r, \end{aligned}$$

i.e. the remainder is $p(a)$. □

An immediate consequence of the Remainder Theorem is the following.

Theorem (Factor Theorem). *Let $p(x)$ be a polynomial.*
Then a is a zero *of $p(x)$ $\iff$ $x - a$ is a factor of $p(x)$.*

Proof. Let $p(x)$ be a polynomial.

($\Longrightarrow$) First assume a is a zero of $p(x)$.
Then $p(a) = 0$, and so by the Remainder Theorem, for some polynomial $q(x)$,

$$\begin{aligned} p(x) &= (x - a)q(x) + p(a) \\ &= (x - a)q(x), \end{aligned}$$

and so $x - a$ is a factor of $p(x)$.

($\Longleftarrow$) Now assume $x - a$ is a factor of $p(x)$.

$$\begin{aligned} \Longrightarrow\; p(x) &= (x - a)q(x) \text{ for some polynomial } q(x) \\ \Longrightarrow\; p(a) &= (a - a)q(a) \\ &= 0 \end{aligned}$$

and so a is a zero of $p(x)$. □

Definition. A polynomial $p(x)$ is said to **factor over** $\mathbb{Z}$ (resp. *over* $\mathbb{Q}$, or *over* $\mathbb{R}$, or ...) if $p(x) = u(x)\,q(x)$ for some non-constant polynomials $u(x), q(x)$ that are both *polynomials over* $\mathbb{Z}$ (resp. *over* $\mathbb{Q}$, or *over* $\mathbb{R}$, or ...).

The next result shows that finding rational zeros of monic polynomials over $\mathbb{Z}$ is relatively easy.

Theorem (Rational Zero Theorem). *If* $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0$ *is a* monic *polynomial over* $\mathbb{Z}$, *and* α *is a rational zero of* $p(x)$, *then* $\alpha \in \mathbb{Z}$.

Proof. Assume $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0$ where $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$, and suppose $\alpha \in \mathbb{Q}$ is a zero of $p(x)$. Then $\alpha = s/t$ for some $s, t \in \mathbb{Z}$ with $t \neq 0$.
We may assume s/t is reduced to lowest terms so that $(s,t) = 1$.
For a contradiction, suppose $t > 1$, and hence has a prime divisor q.

$$
\begin{aligned}
\implies \quad 0 &= p(\alpha) \\
&= \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \\
&= \frac{s^n}{t^n} + a_{n-1}\frac{s^{n-1}}{t^{n-1}} + \cdots + a_1\frac{s}{t} + a_0 \\
\implies \quad 0 &= s^n + a_{n-1}s^{n-1}t + \cdots + a_1st^{n-1} + a_0t^n, \text{ multiplying through by } t^n \\
\implies \quad -s^n &= (a_{n-1}s^{n-1} + \cdots + a_1st^{n-2} + a_0t^{n-1})t \\
\implies \quad t &\mid s^n \\
\implies \quad q &\mid s^n \\
\implies \quad q &\mid s \\
\implies \quad (s,t) &\geqslant q > 1 \text{ (contradiction)}
\end{aligned}
$$

So, in fact, $t = 1$ and hence $\alpha \in \mathbb{Z}$. □

Remark. By the Rational Zero Theorem, to find the rational zeros of a *monic* polynomial with integer coefficients we only need to check all integer divisors of the *constant* coefficient a_0.

4.3 Quadratic polynomials

Definition. A **quadratic polynomial** is simply a *polynomial* of *degree* 2, i.e. a polynomial of form

$$ax^2 + bx + c$$

where a, b, c are fixed numbers and $a \neq 0$. Let $p(x) = ax^2 + bx + c$. Below, we will show many key properties of $p(x)$ are associated with the value of its **discriminant** $\Delta := b^2 - 4ac$.

Theorem 4.3.1. *Let* $p(x) = ax^2 + bx + c$ *be a quadratic polynomial over* $\mathbb{R}$ *with discriminant* $\Delta = b^2 - 4ac$. *Then*

$$p(x) \text{ has real zeros } \frac{-b \pm \sqrt{\Delta}}{2a} \iff \Delta \geqslant 0.$$

Proof. First using the identity

$$(A+B)^2 = A^2 + 2AB + B^2$$

we rewrite $p(x)$ to put "x in one place" (this process is called **completing the square**)

$$\begin{aligned} p(x) &= ax^2 + bx + c \\ &= a\Big(x^2 + \frac{b}{a}x + \frac{c}{a}\Big) \\ &= a\Big(x^2 + \frac{b}{a}x + \Big(\frac{b}{2a}\Big)^2 + \frac{c}{a} - \Big(\frac{b}{2a}\Big)^2\Big) \\ &= a\Big(\Big(x + \frac{b}{2a}\Big)^2 + \frac{4ac - b^2}{4a^2}\Big) \\ &= a\Big(\Big(x + \frac{b}{2a}\Big)^2 - \frac{b^2 - 4ac}{4a^2}\Big) \\ &= a\Big(\Big(x + \frac{b}{2a}\Big)^2 - \frac{\Delta}{4a^2}\Big) \end{aligned}$$

Since the square $\big(x + b/(2a)\big)^2$ is non-negative, the expression

$$\Big(x + \frac{b}{2a}\Big)^2 - \frac{\Delta}{4a^2}$$

is strictly positive, if Δ is negative, and hence for $p(x)$ to have zeros, it is necessary that $\Delta \geqslant 0$. Thus, assuming $\Delta \geqslant 0$, by using (in reverse) the identity

$$(A + B)(A - B) = A^2 - B^2,$$

we proceed further

$$\begin{aligned} p(x) &= a\Big(\Big(x + \frac{b}{2a}\Big)^2 - \frac{\Delta}{4a^2}\Big) \\ &= a\Big(\Big(x + \frac{b}{2a}\Big)^2 - \Big(\frac{\sqrt{\Delta}}{2a}\Big)^2\Big) \\ &= a\Big(x + \frac{b}{2a} + \frac{\sqrt{\Delta}}{2a}\Big)\Big(x + \frac{b}{2a} - \frac{\sqrt{\Delta}}{2a}\Big) \\ &= a\Big(x - \frac{-b - \sqrt{\Delta}}{2a}\Big)\Big(x - \frac{-b + \sqrt{\Delta}}{2a}\Big). \end{aligned}$$

Thus, $p(x)$ has real zeros $(-b - \sqrt{\Delta})/(2a)$ and $(-b + \sqrt{\Delta})/(2a)$ if and only if $\Delta \geqslant 0$. □

Remark 4.3.2. Observe that the quadratic polynomial $p(x) = ax^2 + bx + c$ (whose discriminant is $\Delta = b^2 - 4ac$), has

- two *distinct* real zeros, if $\Delta > 0$;
- two *equal* real zeros, if $\Delta = 0$;
- no real zeros, if $\Delta < 0$.

Further, a *real* square is always either positive or zero. So

$$\Big(x + \frac{b}{2a}\Big)^2 - \frac{\Delta}{4a^2} \geqslant -\frac{\Delta}{4a^2} \quad \text{for all } x.$$

Hence, $p(x)$ is **bounded below** (resp. **bounded above**) by $-\Delta/(4a)$, if $a > 0$ (resp. if $a < 0$), and since this value is attained at $x = -b/(2a)$, $-\Delta/(4a)$ is the **minimum value** (resp. **maximum value**) of $p(x)$.

Over $\mathbb{Z}$, we can say a little more, but in order to prove, we need some results that follow easily.

Definition 4.3.3. A **perfect square** is the square of an integer.

Definition 4.3.4. The **parity** of an integer is its *oddness/evenness*. Let $m, n \in \mathbb{Z}$. If m, n are both even or both odd, we say m and n *have the same parity*. On the other hand, if one of m or n is odd and the other is even, we say m and n *have opposite parity*.

Lemma 4.3.5. *Let $m, n \in \mathbb{Z}$. Then m, n have the same parity (resp. opposite parity) if and only if $m - n$ and $m + n$ are even (resp. odd).*

Proof. If $m, n \in \mathbb{Z}$ have the same parity then $m = 2k + \varepsilon$ and $n = 2\ell + \varepsilon$ for some $k, \ell \in \mathbb{Z}$ and $\varepsilon \in \{0, 1\}$, in which case, $m - n = 2(k - \ell)$ is even.
If $m, n \in \mathbb{Z}$ have opposite parity then without loss of generality $m = 2k + 1$ (odd) and $n = 2\ell$ (even) for some $k, \ell \in \mathbb{Z}$ and $m - n = 2(k - \ell) + 1$ is odd.
Observe that $-n$ has the same parity as n; so the corresponding result for $m + n$ follows. □

Lemma 4.3.6. *An integer and its square have the same parity.*

Proof. Let $n \in \mathbb{Z}$. Then $n^2 - n = n(n - 1)$ which is even, since it is the product of two consecutive integers, one of which is even and the other odd. □

Theorem 4.3.7. *Let $p(x) = x^2 + bx + c$ be a monic quadratic polynomial over $\mathbb{Z}$. Then*

$$p(x) \text{ has integer zeros} \iff \Delta = b^2 - 4c \text{ is a perfect square.}$$

Proof. Let $p(x) = x^2 + bx + c$ be a monic polynomial over $\mathbb{Z}$.

($\Longrightarrow$) First assume $p(x)$ has integer zeros.

$$\begin{aligned}
&\Longrightarrow \frac{-b \pm \sqrt{\Delta}}{2} \in \mathbb{Z} \\
&\Longrightarrow -b \pm \sqrt{\Delta} \in 2\mathbb{Z} \subset \mathbb{Z}, \text{ where } 2\mathbb{Z} \text{ is the set of even integers} \\
&\Longrightarrow \sqrt{\Delta} \in \mathbb{Z} \\
&\Longrightarrow \Delta \text{ is a perfect square.}
\end{aligned}$$

($\Longleftarrow$) Now assume $\Delta = b^2 - 4c$ is a perfect square, and hence $\sqrt{\Delta} \in \mathbb{Z}$.

$$\begin{aligned}
&\Longrightarrow -b, b^2, \Delta = b^2 - 4c, \sqrt{\Delta} \text{ have the same parity by Lemmas 4.3.5, 4.3.6} \\
&\Longrightarrow -b \pm \sqrt{\Delta} \text{ is even, by Lemma 4.3.5} \\
&\Longrightarrow \frac{-b \pm \sqrt{\Delta}}{2} \in \mathbb{Z}.
\end{aligned}$$

□

Theorem (Viète's Theorem). *Let $p(x) = x^2 + bx + c$ be a* monic quadratic polynomial *with* zeros α, β. *Then*

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

Proof. First observe that $(x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta$.
Now α, β are the zeros of $p(x)$, and $p(x)$ is monic; so $p(x)$ must factor as per the left-hand side of the above equation. The result now follows by comparison of coefficients of $p(x)$ with the right-hand side of the above equation. □

4.4 Horner's Method and Synthetic Division

A quick method for evaluating a polynomial at a point x_0 is given by **Horner's Method**, which is based on writing the polynomial in "nested form":

$$\begin{aligned} p(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0 \\ &= ((\cdots(a_n x + a_{n-1})x + \cdots + a_2)x + a_1)x + a_0 \end{aligned}$$

To evaluate $p(x_0)$ then, we evaluate a sequence of numbers as follows

$$\begin{aligned} b_n &= a_n \\ b_{n-1} &= b_n x_0 + a_{n-1} \\ &\vdots \\ b_0 &= b_1 x_0 + a_0. \end{aligned}$$

Then the final number b_0 is $p(x_0)$, since

$$\begin{aligned} p(x_0) &= ((\cdots(a_n x_0 + a_{n-1})x_0 + \cdots + a_2)x_0 + a_1)x_0 + a_0 \\ &= ((\cdots(b_n x_0 + a_{n-1})x_0 + \cdots + a_2)x_0 + a_1)x_0 + a_0 \\ &= ((\cdots b_{n-1}x_0 + \cdots + a_2)x_0 + a_1)x_0 + a_0 \\ &\vdots \\ &= b_1 x_0 + a_0 \\ &= b_0. \end{aligned}$$

Of course, from above we saw that $p(x_0)$ is the *remainder* when $p(x)$ is divided by $x - x_0$. The way the above process is usually performed is via a tableau as below:

	a_n	a_{n-1}	a_{n-2}	$\cdots$	a_0
x_0		$b_n x_0$	$b_{n-1}x_0$	$\cdots$	b_1
	b_n	b_{n-1}	b_{n-2}	$\cdots$	b_0

As a by-product, $b_n, b_{n-1}, \ldots, b_1$ are the coefficients of the *quotient* when $p(x)$ is divided by $x - x_0$, i.e.

$$p(x) = (x - x_0)(b_n x^{n-1} + b_{n-1}x^{n-2} + \cdots + b_1) + b_0.$$

Example 4.4.1. Find $p(3)$ by Horner's Method/Synthetic Division for $p(x) = x^3 + 2x^2 - 13x + 10$, and hence find the *quotient* and *remainder* when $p(x)$ is divided by $x - 3$.

Exercise Set 4.

1. The *quadratic equation* $x^2 - 3x - 5 = 0$ has *roots* α, β. Determine $\alpha^2 + \beta^2$ and $\alpha^{-2} + \beta^{-2}$.
2. The *quadratic polynomial* $x^2 + 4x - 1$ has *zeros* α, β. Determine $\alpha^3 + \beta^3$ and $\alpha^{-3} + \beta^{-3}$.
   Hint. $(\alpha + \beta)^3 = \alpha^3 + \beta^3 + 3\alpha^2\beta + 3\alpha\beta^2 = \alpha^3 + \beta^3 + 3\alpha\beta(\alpha + \beta)$.
3. Solve $2\big(x + \dfrac{1}{x}\big)^2 - \big(x + \dfrac{1}{x}\big) = 10$.
4. Use the Remainder and Factor Theorems to factorise

   (i) $x^3 - 2x^2 - 5x + 6$ (ii) $x^3 - 5x^2 + 3x + 1$
5. The *quadratic polynomial* $ax^2 + bx - 4$ leaves remainder 12 on division by $x - 1$ and has $x + 2$ as a factor. Find a, b and the *zeros* of the polynomial.
6. Find a *quadratic equation* with *roots* $2 + \sqrt{3}$ and $2 - \sqrt{3}$.
7. June solved a *quadratic equation* of the form:
$$ax^2 + bx + c = 0$$
   and got 2 as a root. Kay switched the b and the c and got 3 as a root. What was June's equation?
8. The equation $x^2 + ax + (b + 2) = 0$ has real roots. What is the least value that $a^2 + b^2$ could be?

∗9. If a, b are odd integers, prove that the equation
$$x^2 + 2ax + 2b = 0$$
   has no *rational* roots.

10. Find $p(1)$ and $p(-2)$ via Horner's method, given $p(x) = 2x^4 - 3x^3 - 2x^2 + x - 4$.
11. Find the quotient and remainder when

    (i) $3x^5 + 2x^4 - 3x^2 + 2x - 7$ is divided by $x + 2$;

    (ii) $x^3 + 3x^2 - 5x + 6$ is divided by $(x - 1)(x + 2)$;

    (iii) $x^4 - 2x^3 + x^2 - 5x + 11$ is divided by $x^2 + 3x + 2$.