MA1006 ALGEBRA

MARK GRANT

University of Aberdeen

Contents

1. Introduction

The term *algebra* (derived from the Arabic word *al-jebr* meaning “reunion of broken parts") is used to describe a wide variety of mathematical techniques and disciplines. In its most elementary form, algebra involves the manipulation of symbols. It is characterised by the use of letters (such as x or y) to denote numbers whose value is not yet known, or *variables*. However algebra is a far-reaching and important current area of research in modern mathematics. In *abstract algebra*, sets with additional structure (such as groups, rings or fields) are studied and classified.

In this course we will focus on the parts of elementary algebra which are useful in solving equations. These techniques are vital for doing Mathematics and most branches of Science or Engineering.

E-mail address: mark.grant@abdn.ac.uk.

We will be naturally led to consider complex numbers, matrices and vectors, and their associated geometry.

1.1. **What is a number?** If you catch someone off guard with this question, they might answer "something like $1, 2, 3, \ldots$". This is a natural response, and indeed these positive whole numbers are called *natural numbers*. However, you might respond, there are also the negative whole numbers $-1, -2, -3, \ldots$ and 0. A whole number (whether positive, negative or zero) is called an *integer*. There are other numbers of course; we have fractions or *rational numbers* such as $\frac{1}{2}$ and $-\frac{3}{4}$, and real numbers which can't be expressed as fractions, such as $\sqrt{2}$ and π. Mathematicians have developed special notation for these different types of number. We use the symbols $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ to denote the sets of natural numbers, integers, rational and real numbers respectively. Note that there are containments between these sets of numbers—every natural number is an integer, every integer n is a rational $\frac{n}{1}$, and so on. In symbols, we write

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}.$$

A further piece of notation we will use is that for *set membership*. The notation

$$x \in A$$

means that x is in the set A. So for example, $\sqrt{2} \in \mathbb{R}$ but $\sqrt{2} \notin \mathbb{Q}$ (the square root of two is in the real numbers but not in the rational numbers).

Are there any other types of number? As we shall see, the answer is an emphatic yes. The complex numbers form a number system which contains the real numbers and is in many ways nicer for doing algebra (and in particular for solving equations). Many other types of generalized number exist (such as the quaternions and octonions) but few of these share all the good properties of the complex numbers.

1.2. **What is an equation?** An *equation* is a mathematical formula of the form $A = B$, asserting the equality of two mathematical expressions A and B. The expressions on the left and right hand side of the equals sign may involve variables, in which case the equation is neither true nor false. An equation can only be assigned a truth value once all the variables have been assigned a value.

Example 1.3. The following are all equations:

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

(4) $y = mx + c$, where m and c are real numbers.

In (4) the letters m and c are *constants* (to be treated as fixed, unlike variables). Note that while equation (3) is true and equation (2) is false, equations (1) and (4) are neither true nor false.

The following are not equations:

(5) $x^2 + 3x$
(6) $2x \leq 6$ (this is an example of an *inequality*).

♣

1.4. **Solving equations.** To *solve* an equation means to find all the values of the variables for which the equation is true, these values being called the *solutions* of the equation. This can often be achieved by applying a sequence of operations to the equation. Each operation (such as adding or subtracting a quantity, multiplying by a quantity, or dividing by a nonzero quantity) must be applied to both sides of the equation at the same time, so that equality is preserved. The goal is to rearrange the equation to the point where one of the variables appears on its own (with coefficient 1) on either the left- or right-hand side.

Example 1.5. Solve $2x + 4 = 0$.

$$\begin{aligned} \text{Subtracting } 4 \text{ from both sides:} \quad & 2x = -4 \\ \text{Dividing both sides by } 2\text{:} \quad & x = -2 \end{aligned}$$

So the only solution is $x = -2$. ♣

Example 1.6. Solve $x^2 = x$.

The temptation is to divide both sides by x, giving $x = 1$. However, x is a variable, and in particular *may be zero* (and division by zero is forbidden)! A better approach:

$$\begin{aligned} \text{Subtract } x \text{ from both sides:} \quad & x^2 - x = 0 \\ \text{Factorise the left-hand side:} \quad & x(x-1) = 0 \end{aligned}$$

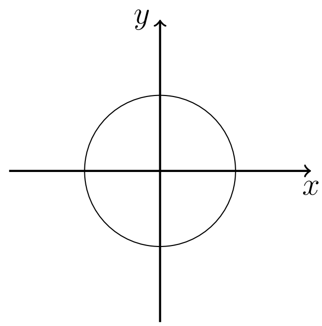
Now we use the following fact: multiplying two nonzero numbers gives a nonzero number. Put another way, if the product of two number is zero, then one or the other (or both) of them must be zero. It follows that $x = 0$ and $x = 1$ are the only solutions. ♣

Example 1.7. Solve $x^2 + 1 = 0$.

This can be rearranged to give $x^2 = -1$. We know that the square of any *real number* is non-negative. Hence this equation has no real solutions. However, in the next topic we will see that this equation *does* have solutions in the complex numbers! We must specify what kind of numbers we are prepared to accept as solutions. ♣

Example 1.8. Find all solutions of $x^2 + y^2 = 1$ with $x, y \in \mathbb{R}$.

Here there are two variables. We could rearrange to give $y = \pm\sqrt{x^2 - 1}$ or $x = \pm\sqrt{y^2 - 1}$. Here it is better to describe the solutions geometrically. Thinking of x and y as coordinates in the plane, we see (using Pythagoras' Theorem) that the solutions are the points on a circle of radius 1, centred at the origin $(0, 0)$.



Thinking of variables as coordinates in this way can be very useful. It sets up a correspondence between geometry and algebra, allowing us to use geometric techniques to solve algebraic problems, and vice versa. (The modern research field of *algebraic geometry* explores the far-reaching consequences of this idea.) ♣

Suggestions for further reading:

- http://en.wikipedia.org/wiki/Algebra
- http://en.wikipedia.org/wiki/Number
- http://en.wikipedia.org/wiki/Equation_solving
- P. J. Cameron, *Introduction to algebra*, Chapter 1, pp.10–13.

2. Polynomial equations

A polynomial is a mathematical expression formed from a single variable using only the operations of addition, exponentiation (taking powers), and scalar multiplication (multiplication by a real number). The *degree* of a polynomial is the largest power of the variable which occurs with a nonzero coefficient.

Example 2.1. The following are polynomials:

(1) $2x + 4$
(2) $4x^2 - 3x + 1$
(3) $x^7 + x^6 + \cdots + x^2 + x + 1$

Their degrees are 1, 2 and 7 respectively.

The following are not polynomials:

(4) $x \cos x$
(5) $\sqrt{x} + x$
(6) $\dfrac{x^2 + 1}{x^2 - 1}$

♣

Here is a formal definition.

Definition 2.2. Let n be a non-negative integer. A *polynomial of degree* n is an expression of the form

$$P(x) := a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_1 x + a_0,$$

where $a_0, a_1, \ldots, a_n \in \mathbb{R}$ and $a_n \neq 0$. Here x is a variable, and the number a_i is the *coefficient* of x^i. The number a_n is the *leading coefficient* and a_0 (the coefficient of $x^0 = 1$) is the *constant coefficient*.

A polynomial equation of degree n is an equation of the form

$$P(x) = 0$$

where $P(x)$ is a polynomial of degree n. A solution of the polynomial equation $P(x) = 0$ is also called a *root* of the polynomial $P(x)$.

Remark 2.3. The above definition of polynomial can be generalised in (at least) two ways:

(1) Here we are taking the coefficients a_i to be real numbers. We could also consider polynomials with coefficients in other number systems (such as the complex numbers; see the next section).
(2) We could also consider *multi-variable* polynomials, such as $P(x, y) := y^3 - 3x^2 + x$.

2.4. **Quadratic equations.** We'll now work our way up through the degrees. A degree zero polynomial is just a nonzero real number. A degree one polynomial is called a *linear polynomial.* Linear polynomial equations are easy to solve: the equation

$$a_1x + a_0 = 0 \qquad \text{where } a_1 \neq 0$$

has the unique solution $x = -\dfrac{a_0}{a_1}$.

The first interesting case is in degree 2, where we get *quadratic equations.* Renaming the coefficients in a standard way, the general quadratic equation is

$$ax^2 + bx + c = 0 \qquad \text{where } a \neq 0.$$

There are a couple of ways to solve quadratic equations. You could either try and factorise the polynomial into two linear factors, or use the standard formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

The formula is derived by the method of *completing the square.* The quantity $\Delta = b^2 - 4ac$ inside the square root is called the *discriminant* of the polynomial. It determines the number of roots of the polynomial:

- If $\Delta > 0$ there are two roots.
- If $\Delta = 0$ there is one *repeated root.*
- If $\Delta < 0$ there are no real roots (but there will be complex roots; see next section).

Example 2.5. Check that you can solve the following quadratic equations:

(1) $x^2 - 2x - 3 = 0$
(2) $x^2 + x - 1 = 0$
(3) $x^2 + 14x + 49 = 0$
(4) $x^2 + 7 = 0$.

♣

2.6. **Cubic and higher degree polynomials.** Polynomials of degree 3 are called *cubic polynomials.* The general cubic equation is of the form

$$ax^3 + bx^2 + cx + d = 0 \qquad \text{where } a \neq 0.$$

There is a general formula for the roots of a cubic polynomial (discovered by Italian mathematicians in the 16^{th} century). Although it is messier to write down than the quadratic formula (and we shall not do so here), it is expressed in terms of the coefficients of the cubic using only the basic operations of addition, subtraction, division, multiplication and taking roots (operations such as $\sqrt{}$ or $\sqrt[3]{}$, otherwise known as *radicals*). The general problem of solving an equation in terms of its coefficients using only the above operations is called *solution in radicals*.

The general quartic equation (polynomial equation of degree 4) has a solution in radicals, but it is far too long and unwieldy to be useful (see `http://planetmath.org/quarticformula`). A beautiful and surprising theorem (which you can learn about in a Level 4 course *Galois Theory*) states that the general polynomial equation of degree 5 or higher does not admit any solution in radicals.

2.7. **Long division of polynomials.** In the absence of a useable formula for solving polynomial equations of higher degree, we usually proceed as follows:

(1) Find a root c of $P(x)$ by trial and error;
(2) Use long division to write $P(x) = Q(x)(x - c)$, where $Q(x)$ is a polynomial of one degree lower than $P(x)$;
(3) Repeat the above steps for $Q(x)$.

In this section we will give details of each of these steps.

The long division algorithm can be also applied to polynomials. It proves the following fact.

Proposition 2.8. *Let* $P(x)$ *and* $D(x)$ *be polynomials with* $D(x) \neq 0$. *Then there exist unique polynomials* $Q(x)$ *and* $R(x)$ *such that*

$$P(x) = Q(x)D(x) + R(x),$$

and $\deg R(x) < \deg D(x)$.

In the above expression $D(x)$ is called the *divisor*, $Q(x)$ the *quotient* and $R(x)$ the *remainder*. We will adopt the convention that 0 is a polynomial of negative degree, so that $R(x) = 0$ is allowed.

Long division of polynomials works in exactly the same way as long division of numbers. It is easiest to see how using an example.

Example 2.9. We divide $P(x) = x^2 + x + 6$ by $D(x) = x - 2$ using long division:

$$\begin{array}{r r}
 & x+3 \\ \cline{2-2}
x-2\big) & x^2 \quad + x + 6 \\
 & -x^2 + 2x \qquad \\ \cline{2-2}
 & 3x + 6 \\
 & -3x + 6 \\ \cline{2-2}
 & 12
\end{array}$$

In the picture above, the $x + 3$ on the top line is the quotient and the 12 on the bottom line is the remainder. Notice that the remainder is a polynomial of degree zero, strictly smaller than the degree of $D(x)$. They are computed as follows: we divide the x of $D(x)$ into the leading x^2 of $P(x)$ to obtain the x which is written on top of the division brackets. Now multiply this x by $D(x)$ to obtain $x^2 - 2x$. This is subtracted from the first two terms under the bracket to produce the next line, $3x$. Now "bring down" the 6 from the line above, to produce $3x + 6$ and repeat the process: first divide the x from $D(x)$ into the $3x$ giving the answer 3, which is added to the quotient. Now multiply this 3 by $D(x)$ to give $3x - 6$ and write the result underneath (in the correct columns). Subtract this from the $3x + 6$ on the line above, to give the answer 12. Since this is a polynomial of degree smaller than the degree of D, we stop here.

Our conclusion is that $x^2 + x + 6 = (x - 2)(x + 3) + 12$. ♣

Definition 2.10. We say that a polynomial $D(x)$ *divides* a polynomial $P(x)$ (or that $P(x)$ *is divisible by* $D(x)$) if the remainder in the above expression is equal to zero, $R(x) = 0$.

Example 2.11. The following calculation (using long division) shows that $x + 4$ divides $x^3 + 2x^2 - 5x + 12$.

$$\begin{array}{r r}
 & x^2 - 2x \quad + 3 \\ \cline{2-2}
x+4\big) & x^3 + 2x^2 - 5x + 12 \\
 & -x^3 - 4x^2 \qquad\qquad\quad \\ \cline{2-2}
 & -2x^2 - 5x \qquad \\
 & 2x^2 + 8x \qquad \\ \cline{2-2}
 & 3x + 12 \\
 & -3x - 12 \\ \cline{2-2}
 & 0
\end{array}$$

We can now solve the equation $x^3 + 2x^2 - 5x + 12 = 0$. The above shows this is equivalent to $(x+4)(x^2-2x+3) = 0$. Since the quadratic

$x^2 - 2x + 3$ has no real roots, we conclude that $x = -4$ is the only real solution. ♣

The method used to solve the cubic equation above involves guessing a linear polynomial dividing the given cubic. The next result explains how to choose such a linear polynomial.

Theorem 2.12. *A number s is a solution of a polynomial equation $P(x) = 0$ if and only if the polynomial $x-s$ divides the polynomial $P(x)$.*

Proof. If the polynomial $x - s$ divides $P(x)$ then there exists a polynomial $Q(x)$ such that

$$P(x) = (x - s)Q(x).$$

Thus we get that $P(s) = (s - s)Q(s) = 0 \cdot Q(s) = 0$, that is, s is a root of $P(x)$.

Conversely, suppose that s is a root of the polynomial $P(x)$. Write

$$P(x) = Q(x)(x - s) + R(x),$$

where $\deg R(x) < 1$, that is, $R(x)$ is a number. Since s is a root we have

$$0 = P(s) = Q(s)(s - s) + R(s) = R(s).$$

Thus $R(x) = 0$ and hence $x - s$ divides $P(x)$. □

The above theorem tells us that if s_1 is a root of a polynomial $P(x)$ then we can simplify it

$$P(x) = (x - s_1)Q_1(x),$$

where $Q_1(X)$ is a polynomial one degree lower that $P(x)$. If s_2 is a root of $Q_1(x)$ (and hence also a root of $P(x)$) then we can simplify it further

$$P(x) = (x - s_1)(x - s_2)Q_2(x).$$

If we can continue this process then we end up in the simplest possible form

$$P(x) = (x - s_1)(x - s_2) \dots (x - s_n).$$

This is however not always the case if we are dealing with real roots only. It will turn out that such a factorisation is always possible over the complex numbers (we will encounter them soon).

The following result is useful in finding roots by trial and error. To state it we introduce some terminology. If a and b are integers, we say that b *divides* a, and write $b \mid a$, if there exists some integer n such that $a = nb$. The *greatest common divisor* of integers p and q, denoted $\gcd(p, q)$, is the largest positive integer which divides both p and q. For example, $\gcd(4, 6) = 2$ and $\gcd(-1, 7) = 1$.

Theorem 2.13 (Rational root theorem). *Let $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial of degree n with integer coefficients, i.e. $a_i \in \mathbb{Z}$. If the equation $P(x) = 0$ has a rational solution $x = \frac{p}{q}$ where $\gcd(p, q) = 1$, then p divides a_0 and q divides a_n.*

Proof. Since $\frac{p}{q}$ is a solution we have that

$$a_n \frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0 = 0.$$

Multiplying the equation by q^n we obtain

$$\begin{aligned} a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 p q^{n-1} + a_0 q^n &= 0 \\ p(a_n p^{n-1} + a_{n-1}p^{n-2}q + \cdots + a_1 q^{n-1}) &= -a_0 q^n \end{aligned}$$

which means that p divides $a_0 q^n$. Since the greatest common divisor of p and q is one, this implies that p divides a_0 as claimed.

Similarly we have that

$$\begin{aligned} a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 p q^{n-1} + a_0 q^n &= 0 \\ q(a_{n-1}p^{n-1} + \cdots + a_1 p q^{n-2} + a_0 q^{n-1}) &= -a_n p^n \end{aligned}$$

which means that q divides $a_n p^n$ and hence q divides a_n as claimed. □

Example 2.14. Solve the following equation

$$x^3 - x^2 + x - 1 = 0.$$

To do this without knowing a general formula we can apply the rational root theorem 2.13. It tells us that if $\frac{p}{q}$ is a rational root in lowest terms, then $p \mid -1$ and $q \mid 1$. Hence (since p and q are integers) we have $p = \pm 1$ and $q = \pm 1$. The only possible rational roots are ± 1. We check that 1 is indeed a root and we divide the above polynomial by $x - 1$ and obtain

$$x^3 - x^2 + x - 1 = (x - 1)(x^2 + 1)$$

We can solve the remaining quadratic equation $x^2 + 1 = 0$; it has no real solutions. ♣

Example 2.15. Find all rational solutions of the equation

$$x^4 + 3x^3 + x^2 + 2x - 2 = 0.$$

If $\frac{p}{q}$ is a rational root then $p \mid -2$ and $q \mid 1$, so the only possible rational roots are $\pm 1, \pm 2$. One checks easily that none of these are roots. Hence this equation has no rational solutions.

Example 2.16. Consider the equation
$$2x^5 + 3x^4 - 7x^3 + x^2 - 10x + 6 = 0.$$
We know that there is no general solution for polynomial equations of degree 5. However, the rational root theorem tells us that the only possible rational solutions can be $\pm 1, \pm\frac{1}{2}, \pm 2, \pm 3, \pm\frac{3}{2}, \pm 6$. We can check by inspection that only $\frac{3}{2}$ is a rational solution. Dividing the above polynomial by $x - \frac{3}{2}$ we obtain that
$$2x^5 + 3x^4 - 7x^3 + x^2 - 10x + 6 = (2x - 3)(x^4 + 3x^3 + x^2 + 2x - 2).$$
We know that the quotient $x^4 + 3x^3 + x^2 + 2x - 2$ has no rational roots. ♣

Example 2.17. Solve the equation
$$x^5 - 2x^4 - 3x^3 + 6x^2 + 2x - 4 = 0.$$
The rational root theorem says that $\pm 1, \pm 2, \pm 4$ are the only possible rational roots. Indeed, we can check that ± 1 and 2 are the actual solutions. We do the long division and we obtain
$$x^5 - 2x^4 - 3x^3 + 6x^2 + 2x - 4 = (x - 1)(x + 1)(x - 2)(x^2 - 2).$$
We can now solve easily the equation $x^2 - 2 = 0$ and we finally get that
$$x^5 - 2x^4 - 3x^3 + 6x^2 + 2x - 4 = (x - 1)(x + 1)(x - 2)(x - \sqrt{2})(x + \sqrt{2}).$$
That is, the solutions of our equation are $\pm 1, 2, \pm\sqrt{2}$. ♣

Suggestions for further reading:

- http://en.wikipedia.org/wiki/Polynomial
- http://en.wikipedia.org/wiki/Rational_root_theorem
- http://en.wikipedia.org/wiki/Polynomial_long_division
- http://www.purplemath.com/modules/polydiv2.htm
- Work through the interactive tutorials at http://www.zweigmedia.com/RealWorld/tut_alg_review/framesA_5.html and http://www.zweigmedia.com/RealWorld/tut_alg_review/framesA_5B.html

3. Introduction to complex numbers

As we have seen in the last section, polynomial equations with real coefficients do not always have real solutions. For example, consider the equation $x^2 + 1 = 0$. A solution for this equation would be a "square root of -1", and there are no real numbers with this property. At the moment we just want to have a number which is the square root of -1 so we artificially add it to our number system and we would like to see what happens. We denote this new number by $\sqrt{-1}$, or more commonly by i (the notation probably comes from *imaginary number*, but this is unnecessarily whimsical). It has the property that $i^2 = -1$.

We want to multiply i by real numbers. So, if b is a real number then what we get is bi and we observe that this has the property that $(bi)^2 = b^2 i^2 = b^2(-1) = -b^2$ because we want the commutativity of the multiplication to hold in our new setting. Observe that bi is not a real number (unless $b = 0$) because its square is negative.

We also want to add together real numbers and these new 'imaginary' numbers. This leads to the following definition.

Definition 3.1. A pair of real numbers (a, b) is called a *complex number* and it is denoted by $z = a + bi$. The set of complex numbers is denoted by $\mathbb{C}$. The real number a is called the *real part* of z, and is denoted by $\mathrm{Re}(z)$. Similarly, the real number b is called the *imaginary part* of z and is denoted by $\mathrm{Im}(z)$.

Example 3.2.
(1) If $z = 1$, then $\mathrm{Re}(z) = 1$ and $\mathrm{Im}(z) = 0$.
(2) If $z = 1+i$, then $\mathrm{Re}(z) = 1$ and $\mathrm{Im}(z) = 1$. (Note that $\mathrm{Im}(z) = i$ is incorrect: the imaginary part is always a *real* number!)

♣

How can we do this? Remember, this is Mathematics, not real life. We can make any definition we wish (although admittedly some definitions are more useful than others).

Why do we do this? The simple answer is that even if we are only interested in real solutions to equations, having complex numbers around often simplifies things considerably. For instance, the formula for the real roots of cubic equations involves complex numbers (see http://en.wikipedia.org/wiki/Cubic_function). Remarkably, complex numbers turn out to be hugely useful outside of Mathematics, in fields such as Electrical Engineering and Quantum Physics.

3.3. **The arithmetic of complex numbers.** To define *addition*, *subtraction* and *multiplication* on $\mathbb{C}$, we just follow the ordinary rules of arithmetic, treating i as a variable and replacing all instances of i^2 with -1. To be explicit, let $z = a + bi$ and $w = c + di$ be complex numbers. Then addition and subtraction are defined by

$$z + w = (a + bi) + (c + di) = (a + c) + (b + d)i,$$
$$z - w = (a + bi) - (c + di) = (a - c) + (b - d)i,$$

and multiplication is defined by

$$\begin{aligned} zw &= (a + bi)(c + di) \\ &= ac + bic + adi + bidi \\ &= ac + bdi^2 + (ad + bc)i \\ &= (ac - bd) + (ad + bc)i. \end{aligned}$$

Example 3.4. Let $z = 3 + 2i$ and $w = 1 - 4i$. Then:

(1) $z + w = 4 - 2i$;
(2) $z - w = 2 + 6i$;
(3) $zw = (3 + 8) + (-12 + 2)i = 11 - 10i$.

♣

In order to perform division of complex numbers, we will first introduce the important notions of *conjugation* and *modulus*, and give a few of their basic properties.

Definition 3.5. Let $z = a + bi \in \mathbb{C}$. The *conjugate* of z is

$$\bar{z} = a - bi.$$

The *modulus* of z is the non-negative real number

$$|z| = \sqrt{a^2 + b^2}.$$

Proposition 3.6. *Let $z = a + bi$ be a complex number. Then*

(1) $z\bar{z} = |z|^2$,
(2) $|\bar{z}| = |z|$,
(3) $|z| = 0$ *if and only if* $z = 0$.

Proof. Each of the properties follows from a simple computation.

(1) $z\bar{z} = (a + bi)(a - bi) = a^2 + b^2 = |z|^2$.
(2) Since $\bar{z} = a - bi$ we have $|\bar{z}| = \sqrt{a^2 + (-b)^2} = \sqrt{a^2 + b^2} = |z|$.
(3) The modulus equals zero if and only if $a^2 + b^2 = 0$. Since a^2 and b^2 are both non-negative, this is true if and only if both a and b are zero, which means exactly that $z = 0$.

□

Now let $z = a + bi$ and $w = c + di$. We wish to write

$$\frac{z}{w} = \frac{a+bi}{c+di}$$

in the form $x + yi$, where x and y are real numbers. In order to do this we apply a simple trick: we multiply top and bottom by $\bar{w}$. This of course doesn't change the fraction, and we end up with a real number on the bottom, since

$$\frac{z}{w} = \frac{z}{w}\frac{\bar{w}}{\bar{w}} = \frac{z\bar{w}}{w\bar{w}} = \frac{z\bar{w}}{|w|^2}.$$

Let's see an example.

Example 3.7. Divide $z = 3+4i$ by $w = 2-i$, expressing your answer in the form $a + bi$ with $a, b \in \mathbb{R}$.

$$\begin{aligned} \frac{3+4i}{2-i} &= \frac{3+4i}{2-i} \cdot \frac{2+i}{2+i} \\ &= \frac{2+11i}{2^2+1^1} \\ &= \frac{2}{5} + \frac{11}{5}i. \end{aligned}$$

♣

3.8. **The complex numbers form a field.** The complex number system shares many good properties with the real or rational numbers. We can formalise these properties as follows.

Proposition 3.9. *The addition and multiplication on $\mathbb{C}$ satisfy the following properties.*

(1) The addition of complex numbers is commutative:

$$x + y = y + x \quad \textit{for all } x, y \in \mathbb{C}.$$

(2) The addition of complex numbers is associative:

$$x + (y + z) = (x + y) + z \quad \textit{for all } x, y, z \in \mathbb{C}.$$

(3) $0 \in \mathbb{C}$ is the identity for addition:

$$x + 0 = x = 0 + x \quad \textit{for all } x \in \mathbb{C}.$$

(4) Every complex number has an additive inverse:

$$\textit{For all } x \in \mathbb{C}, \ \textit{there exists } -x \in \mathbb{C} \textit{ such that } x + (-x) = 0.$$

(5) The multiplication of complex numbers is commutative:

$$xy = yx \quad \textit{for all } x, y \in \mathbb{C}.$$

(6) *The multiplication of complex numbers is associative:*

$$x(yz) = (xy)z \quad \textit{for all } x, y, z \in \mathbb{C}.$$

(7) $1 \in \mathbb{C}$ *is the identity for multiplication:*

$$x1 = x = 1x \quad \textit{for all } x \in \mathbb{C}.$$

(8) *Every nonzero complex number has a multiplicative inverse:*

$$\textit{For all } x \in \mathbb{C} \textit{ such that } x \neq 0, \textit{ there exists } x^{-1} \in \mathbb{C} \textit{ such that } \quad xx^{-1} = 1.$$

(9) *The multiplication is distributive over the addition:*

$$x(y+z) = xy + xz \quad \textit{for all } x, y, z \in \mathbb{C}.$$

Proof. As an exercise, you can prove (1) - (7) and (9) using the corresponding facts about real numbers (although you may well wonder about how those facts you are using could be proved!). Here we will only prove (8). So let $x \in \mathbb{C}$, $x \neq 0$. By Proposition 3.6,

$$x\bar{x} = |x|^2 \neq 0$$

and we can define $x^{-1} = \dfrac{\bar{x}}{|x|^2}$. Then,

$$xx^{-1} = x\frac{\bar{x}}{|x|^2} = \frac{x\bar{x}}{|x|^2} = 1.$$

□

Remark 3.10. Let X be a set of numbers with addition and multiplication. Depending on which of the properties from Proposition 3.9 are satisfied, the set X has different names. For instance, if X only satisfies (1), (2) and (3) then it is called a *monoid*; if it also satisfies (4), then it is called a *group*. If X satisfies all the properties except (8), then X is a *ring*, and if it satisfies all of the properties (1)-(9) then it is called a *field*.

Actually, you already know some examples of these notions. So far we know the following sequence of inclusions

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

The set of natural numbers $\mathbb{N}$ is a monoid, the set of integers $\mathbb{Z}$ is a ring, and the sets of rational, real and complex numbers $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields. Not all fields are like these three, some of them are finite. The algebra of finite fields has powerful applications in cryptography. All your electronic devices use this abstract algebra.

3.11. Further properties of the modulus and conjugate.

Proposition 3.12. *Let z and w be complex numbers. Then*

(1) $\overline{z+w} = \bar{z} + \bar{w}$,
(2) $\overline{zw} = \bar{z}\bar{w}$,
(3) $\overline{\left(\frac{z}{w}\right)} = \frac{\bar{z}}{\bar{w}}$ *when* $w \neq 0$.

All of these statements are easy enough to check directly (just let $z = a + bi$ and $w = c + di$ and evaluate both sides). They say that the usual arithmetic operations of addition, multiplication and division are preserved under conjugation.

Proposition 3.13. *Let z and w be complex numbers. Then*

(1) $|zw| = |z||w|$,
(2) $\left|\frac{z}{w}\right| = \frac{|z|}{|w|}$ *when* $w \neq 0$.

The modulus preserves multiplication and division. Note, however, that for addition the equality corresponding to Proposition 3.12(1) is not true for the modulus; instead it must be replaced by an inequality.

Proposition 3.14 (The triangle inequality in $\mathbb{C}$)**.** *Let z and w be complex numbers. Then*

$$|z+w| \leq |z| + |w|.$$

Proof. Let us first observe that for every complex number $z = a + bi$ we have:

- $z + \bar{z} = a + bi + a - bi = 2a = 2\,\mathrm{Re}(z)$,
- $\mathrm{Re}(z) = a \leq |a| = \sqrt{a^2} \leq \sqrt{a^2 + b^2} = |z|$.

These facts will be used in the following computation.

$$\begin{aligned}
|z+w|^2 &= (z+w)\overline{(z+w)} \\
&= (z+w)(\bar{z}+\bar{w}) \\
&= z\bar{z} + w\bar{w} + w\bar{z} + z\bar{w} \\
&= |z|^2 + |w|^2 + (w\bar{z} + \overline{w\bar{z}}) \\
&= |z|^2 + |w|^2 + 2\,\mathrm{Re}(w\bar{z}) \\
&\leq |z|^2 + |w|^2 + 2|w\bar{z}| \\
&= |z|^2 + |w|^2 + 2|w||z| \\
&= (|z| + |w|)^2
\end{aligned}$$

Since both $|z+w|$ and $|z|+|w|$ are non-negative, taking square roots preserves the inequality and gives the result. $\square$

The statement of the triangle inequality (and the reason for it's name) will become intuitively obvious in the next section, once we have interpreted complex numbers geometrically as points in the plane.

3.15. **Solving equations over $\mathbb{C}$.** In what follows we will discuss a sequence of miraculous facts and properties about complex numbers. Let's start with an easy one.

Lemma 3.16. *Every complex number has a square root.*

Proof. Let $a+bi \in \mathbb{C}$. We will assume $b \neq 0$ (otherwise we know the roots are $\pm\sqrt{a}$ or $\pm i\sqrt{-a}$). We want to find $x+yi \in \mathbb{C}$ such that $(x+yi)^2 = a+bi$. Note that

$$\begin{aligned}(x+yi)^2 &= x^2 + 2xyi + (yi)^2 \\ &= (x^2 - y^2) + 2xyi\end{aligned}$$

and so we have to solve the system of equations

$$\begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases}$$

Keep in mind that we want to find x and y *real numbers* satisfying the above system!

Since $b \neq 0$ we have $x, y \neq 0$. Then, from the second equation we obtain

$$y = \frac{b}{2x}.$$

We can substitute this in first equation:

$$x^2 - \left(\frac{b}{2x}\right)^2 = a.$$

Rearranging everything, we get a quartic equation

$$x^4 - ax^2 - \frac{b^2}{4} = 0.$$

Treating this as a quadratic equation in x^2, we get

$$x^2 = \frac{a \pm \sqrt{a^2+b^2}}{2}.$$

Since x has to be a real number, we get

$$x = \pm \frac{\sqrt{a + \sqrt{a^2 + b^2}}}{\sqrt{2}}.$$

Also, we deduce then that

$$y = \pm \frac{\sqrt{\sqrt{a^2 + b^2} - a}}{\sqrt{2}}.$$

To finish the proof we have to say which combinations $x + yi$ satisfy $(x + yi)^2 = a + bi$. The equation $2xy = b$ shows that x and y will be of the same sign if $b > 0$ and of different signs when $b < 0$. Hence the two roots are z and $-z$, where

$$z = \frac{\sqrt{a + \sqrt{a^2 + b^2}}}{\sqrt{2}} + \frac{|b|}{b}\left(\frac{\sqrt{\sqrt{a^2 + b^2} - a}}{\sqrt{2}}\right)i.$$

□

The following (obvious) result shows that the complex numbers simplify dealing with quadratic equations.

Theorem 3.17. *Every quadratic equation*

$$ax^2 + bx + c = 0$$

with complex coefficients has complex solutions given by the formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

□

In fact, more is true. The following result is called *The Fundamental Theorem of Algebra*.

Theorem 3.18. *Every polynomial of positive degree with complex coefficients has at least one root in the field of complex numbers.*

We will not give a proof here, but simply mention that there are many beautiful proofs which use a variety of different branches of Mathematics. Perhaps the most elementary proof can be found in Chapter 19 of *Proofs from the Book* by Aigner and Ziegler. It uses only very basic facts from calculus. Notice that the theorem does not tell how to find a solution, it only proves that it exists.

By applying Theorem 2.12 we immediately obtain the following result.

Corollary 3.19. *Every polynomial $P(x)$ of degree $n \geq 1$ with complex coefficients is equal to a product of n polynomials of degree one*

$$P(x) = a_n(x - c_1)(x - c_2)\dots(x - c_n),$$

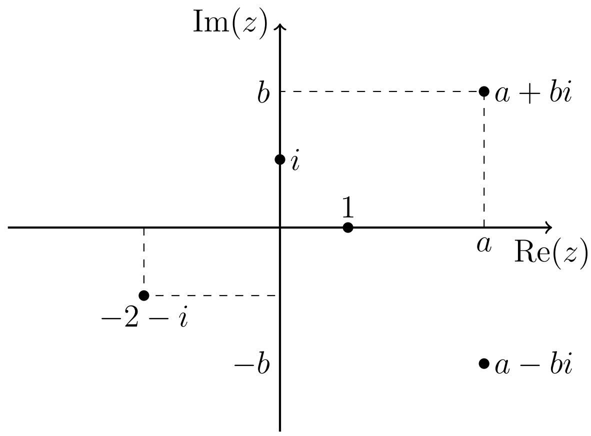
where $a_n \in \mathbb{C}$ is the leading coefficient and $c_i \in \mathbb{C}$ are the roots of $P(x)$. □

Suggestions for further reading:

- http://en.wikipedia.org/wiki/Complex_number
- http://en.wikipedia.org/wiki/Fundamental_theorem_of_algebra
- P. J. Cameron, *Introduction to algebra*, Chapter 1, pp.13–15.
- H. Anton, *Elementary Linear Algebra* (10^{th} ed.), Appendix B.

4. The geometry of complex numbers

We defined complex numbers as ordered pairs (a, b) where a and b are real numbers. We can then visualize the complex number $z = a + bi$ as the point in a plane with horizontal coordinate a and vertical coordinate b. Such a pictorial representation of the complex numbers is sometimes called an *Argand diagram*, sometimes just the *complex plane*. The following figure shows an Argand diagram with a few complex numbers plotted as black dots.

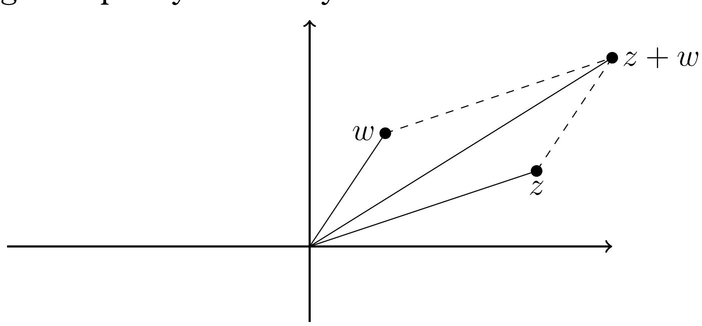


If we imagine complex numbers this way, then (by Pythagoras' Theorem) the modulus of z is simply the distance of z to the point $(0, 0)$, and the conjugate $\bar{z}$ is the point that we obtain when we reflect or 'flip' the plane along the horizontal axis.

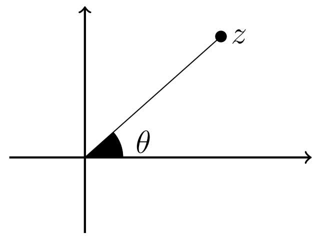
Many other properties of the modulus and the conjugate have an easy interpretation this way. For instance, given $z, w \in \mathbb{C}$, we know from Proposition 3.14 that

$$|z + w| \leq |z| + |w|.$$

The next figure shows how $z+w$ has a simple geometric interpretation as the diagonal of a parallelogram with sides z and w. This makes the triangle inequality intuitively obvious.



4.1. **The argument of a complex number.** Let $z \in \mathbb{C}$ with $z \neq 0$, and let θ be the angle from the positive real axis to the interval joining the origin with z, measured anti-clockwise in radians.



The angle θ is called the *argument* of z, written $\arg(z)$. Note that it is only defined when z is nonzero, and even then it is only defined up to integer multiples of 2π (that is, any of the angles $\theta + 2n\pi$ where $n \in \mathbb{Z}$ could equally well be called "the" argument). The unique argument in the interval $[0, 2\pi)$ (that is, with $0 \leq \theta < 2\pi$) is called the *principal argument* of z and it is denoted by $\operatorname{Arg}(z)$.

Remark 4.2. Some authors define the principal argument to be in the interval $(-\pi, \pi]$. It is a matter of convention.

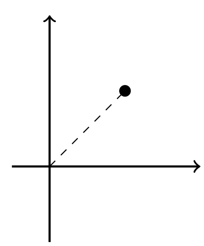
Computing the argument of the complex number $z = a + bi$ requires some care. Basic trigonometry tells us that $\tan\theta = b/a$. Calculating the inverse tangent $\arctan(b/a)$ gives a value in the interval $(-\pi/2, \pi/2)$. The correct value for the argument will be one of

$$\theta = \arctan(b/a) \qquad \text{or} \qquad \theta = \arctan(b/a) + \pi.$$

Example 4.3. For each of the following complex numbers, calculate its argument and principal argument:

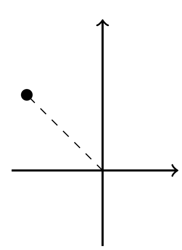
(1) $z = 1 + i$.

Here $\tan\theta = \frac{1}{1} = 1$, so $\arg(z) = \pi/4$ or $5\pi/4$. A quick glance at the Argand diagram tells us that $\arg(z) = \pi/4$. Since this is in the range $[0, 2\pi)$, it is also the principal argument.



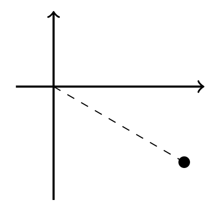
(2) $-1 + i$.

Here $\tan\theta = \frac{1}{-1} = -1$, so $\arg(z) = -\pi/4$ or $3\pi/4$. From the diagram, $\arg(z) = 3\pi/4$. The principal argument is $\operatorname{Arg}(z) = 3\pi/4$.



(3) $\sqrt{3} - i$.

Here $\tan\theta = \frac{-1}{\sqrt{3}}$, so $\arg(z) = -\pi/6$ or $5\pi/6$. From the diagram, $\arg(z) = -\pi/6$. Since this is *not* in the range $[0, 2\pi)$, we add 2π to get the principal argument $\operatorname{Arg}(z) = 11\pi/6$.



♣

4.4. **The polar form of a complex number.**

Lemma 4.5. *For each $z \in \mathbb{C}, z \neq 0$ there is an equality*

$$z = |z|(\cos\theta + i\,\sin\theta)$$

where $\theta = \arg(z)$.

The above expression of z is known as the *polar form* of z. To write the complex number $z = a + bi$ in polar form, we simply have to compute its modulus and argument and plug them into the above expression.

Example 4.6. (1) $1 + i = \sqrt{2}\,(\cos(\pi/4) + i\sin(\pi/4))$
(2) $-1 + i = \sqrt{2}\,(\cos(3\pi/4) + i\sin(3\pi/4))$
(3) $\sqrt{3} + i = 2\,(\cos(\pi/6) + i\sin(\pi/6))$
(4) $1 + i\sqrt{3} = 2\,(\cos(\pi/3) + i\sin(\pi/3))$ ♣

Converting a complex number given in polar form back to the form $z = a + bi$ (sometimes known as *Cartesian form*) is easy. We just evaluate $\cos\theta$ and $\sin\theta$ and expand out the brackets.

4.7. **Loci and regions in the complex plane.** The interpretation of complex numbers as points in the plane often allows us to give succinct formulas for planar figures. For example, the equations

$$x^2 + y^2 = 1, \quad x, y \in \mathbb{R} \qquad \text{and} \qquad |z| = 1, \quad z \in \mathbb{C}$$

both describe a circle of unit radius centered at the origin. The set of points satisfying a particular equation is sometimes called a *locus* (the plural is *loci*). Equations relating the modulus and argument of complex numbers define loci in the complex plane. By considering *inequalities* instead of equations, we can also describe *regions* in the complex plane. (Note however that there is no sensible interpretation of $z \leq w$ for $z, w \in \mathbb{C}$—the complex numbers are not ordered in the same way that the reals are.)

Let's look at some examples of loci first.

Example 4.8. Sketch the solutions to the equation

$$|z - (1+i)| = 2, \quad z \in \mathbb{C}.$$

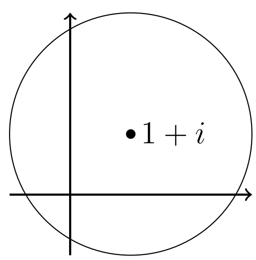
We write $z = a + bi$ and try to find an equation linking a and b. The left-hand side is

$$\begin{aligned} |z - (i+1)| &= |a + bi - (1+i)| \\ &= |(a-1) + (b-1)i| \\ &= \sqrt{(a-1)^2 + (b-1)^2}. \end{aligned}$$

Both sides of the equation are non-negative, so we can square both sides giving

$$(a-1)^2 + (b-1)^2 = 4,$$

which is the equation of a circle with centre $(1, 1)$ and radius 2. Hence the solutions form a circle in the complex plane centered at $1+i$ with radius 2.



In fact, we can see this with less work. Given $z, w \in \mathbb{C}$, the modulus $|z - w|$ is the distance between z and w in the complex plane. Hence solutions to our equation are all complex numbers at distance 2 from $1 + i$. ♣

Example 4.9. Now let's try and sketch the locus

$$|z| = \mathrm{Re}(z) + \mathrm{Im}(z).$$

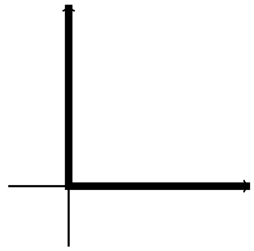
Again we write $z = a + bi$ and try to get an equation linking a and b. We get

$$\sqrt{a^2 + b^2} = a + b.$$

Since the left-hand side is non-negative, we get $a + b \geq 0$ and we can square both sides to give

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

Therefore $2ab = 0$ which implies that $a = 0$ or $b = 0$ (or both). If $a = 0$ then $a + b \geq 0$ gives $b \geq 0$. Similarly if $b = 0$ then $a \geq 0$. We see that the solution set is the union of the non-negative real and imaginary axes.

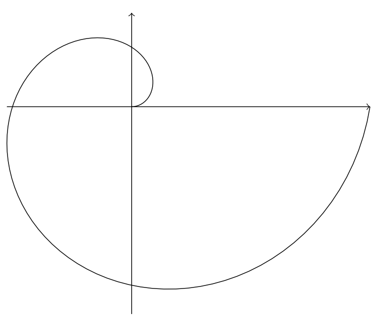


♣

Example 4.10. Sketch the solutions to $|z| = \mathrm{Arg}(z)$.

There is one solution for each value of $\theta = \mathrm{Arg}(z) \in (0, 2\pi)$. The origin $z = 0$ is not a solution because $\mathrm{Arg}(z)$ is not defined there. Using the polar form, we have solutions

$$z = \theta(\cos\theta + i\,\sin\theta), \qquad \theta \in (0, 2\pi).$$



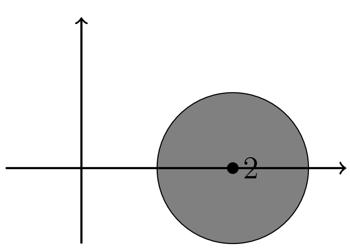
These form part of a spiral.

♣

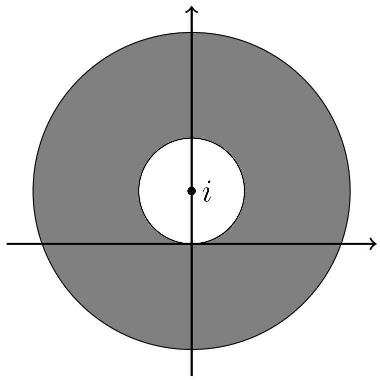
Now let's consider some regions.

Example 4.11. Sketch the regions of the complex plane given by the inequalities

(1) $|z - 2| \leq 1$
(2) $1 \leq |z - i| \leq 3$



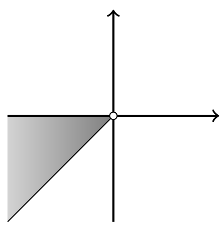
The first region is a disk of radius 1 centred at 2.



The second region is an *annulus*. It is the area enclosed between two concentric circles centred at i, of radii 1 and 3.

♣

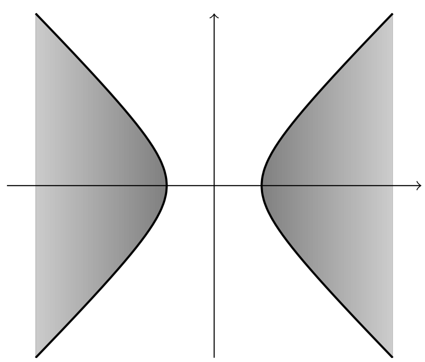
Example 4.12. Sketch the region $\pi \leq \mathrm{Arg}(z) \leq \frac{5\pi}{4}$.



This is the area enclosed between two *rays* (infinite half-lines). It does not include the origin, where $\mathrm{Arg}(z)$ is undefined.

♣

Example 4.13. Sketch the region $\mathrm{Re}(z^2) \geq 1$.



Writing $z = a + bi$, the following inequalities are equivalent:

$$\begin{aligned} \mathrm{Re}(z^2) &\geq 1 \\ \mathrm{Re}(a^2 - b^2 + 2abi) &\geq 1 \\ a^2 - b^2 &\geq 1. \end{aligned}$$

The required region $a^2 - b^2 \geq 1$ is bounded by a hyperbola as shown.

♣

Suggestions for further reading:

- http://en.wikipedia.org/wiki/Complex_plane
- http://en.wikipedia.org/wiki/Argument_(complex_analysis)
- H. Anton, *Elementary Linear Algebra* (10th ed.), Appendix B.
- T. Needham, *Visual Complex Analysis*, Chapter 1 (in particular the Exercises at the end).

5. De Moivre's Theorem

The next result, known as *De Moivre's theorem*, provides an intuition for the multiplication of complex numbers. It shows that the polar form of complex numbers is far more convenient than the Cartesian form for multiplication and taking powers.

Theorem 5.1 (De Moivre's theorem). *Let* $z = |z|(\cos\alpha + i\sin\alpha)$ *and* $w = |w|(\cos\beta + i\sin\beta)$. *Then*

$$zw = |z||w|(\cos(\alpha+\beta) + i\sin(\alpha+\beta)).$$

In other words, in order to multiply two complex numbers we multiply their moduli and add their arguments.

Proof. We have

$$\begin{aligned} zw &= |z||w|(\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) \\ &= |z||w|(\cos\alpha\cos\beta - \sin\alpha\sin\beta + i(\sin\alpha\cos\beta + \cos\alpha\sin\beta)) \\ &= |z||w|(\cos(\alpha+\beta) + i\sin(\alpha+\beta)) \end{aligned}$$

as claimed, where at the last step we have used the standard sum formulae for $\cos$ and $\sin$. (In Section 9 below we will justify these formulae using rotation matrices.) $\square$

Corollary 5.2. *If* $z = |z|(\cos\theta + i\sin\theta)$ *then for every integer* $n \in \mathbb{Z}$ *we have that*

$$z^n = |z|^n(\cos(n\theta) + i\sin(n\theta)).$$

Proof. This follows from De Moivre's theorem by the principle of mathematical induction, and the observation that if $z \neq 0$ then

$$z^{-1} = \frac{\bar{z}}{|z|^2} = \frac{|z|}{|z|^2}(\cos\theta - i\sin\theta) = |z|^{-1}(\cos(-\theta) + i\sin(-\theta)).$$

Here we have used the identities $\cos(-\theta) = \cos\theta$ and $\sin(-\theta) = -\sin\theta$. We omit the details. $\square$

Example 5.3. Let $z = 1 + i$. Calculate z^{10} and z^{-8} using De Moivre, giving your answers in Cartesian form.

We first write z in polar form as $z = \sqrt{2}(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})$. Then

$$\begin{aligned} z^{10} &= (\sqrt{2})^{10}\left(\cos\frac{10\pi}{4} + i\sin\frac{10\pi}{4}\right) \\ &= 2^5\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right) \\ &= 32i. \\ z^{-8} &= (\sqrt{2})^{-8}\left(\cos\frac{-8\pi}{4} + i\sin\frac{-8\pi}{4}\right) \\ &= 2^{-4}(\cos 0 + i\sin 0) \\ &= \frac{1}{16}. \end{aligned}$$

♣

We might ask if De Moivre's Theorem extends to non-integer powers. The answer is yes, almost. For example,

$$z^{1/2} = |z|^{1/2}\big(\cos(\theta/2) + i\sin(\theta/2)\big)$$

gives one value of the square root, but not the other. What about complex exponents? In what sense is the equation

$$z^w = |z|^w\big(\cos(w\theta) + i\sin(w\theta)\big), \qquad w \in \mathbb{C}$$

true? We will try to make sense of this in subsequent sections.

5.4. **Applications of De Moivre to root finding.** In this section we apply De Moivre's theorem to find the degree n roots of a complex number. In other words, we find all (complex) solutions of the equation

$$z^n - c = 0,$$

where $c \in \mathbb{C}$ is a complex number. Notice that, if $c = 0$ then the only solution is zero. The following result is an immediate consequence of De Moivre's theorem.

Corollary 5.5. *Let $n \in \mathbb{N}$ be a natural number. Every nonzero complex number $c \in \mathbb{C}$ has exactly n roots of degree n. Moreover, the roots $z_1, z_2, \dots, z_n$ are given by*

$$z_k = \sqrt[n]{|c|}\left(\cos\left(\frac{2\pi(k-1)+\theta}{n}\right) + i\sin\left(\frac{2\pi(k-1)+\theta}{n}\right)\right)$$

for $k = 1, 2, \dots, n$, where $\theta = \operatorname{Arg}(c)$.

Proof. It is easy to check, by making a quick computation using De Moivre's theorem, that each of the above numbers is a degree n root of c. On the other hand we know that the equation $z^n - c = 0$ has at most n solutions. Hence the above numbers (which are all distinct) are all of the degree n roots of c. □

On Figure 5.1 we show how to draw all degree n roots of a complex number $z = r(\cos\theta + i\sin\theta)$. We can quickly check that the number $z_1 = \sqrt[n]{r}(\cos(\theta/n) + i\sin(\theta/n))$ is a root of degree n of the number z. All of the other roots are obtained from this one by a rotation through $2\pi/n$ radians. In order to draw all of them we proceed as follows (see Figure 5.1).

(1) The number z is given and drawn on the plane;
(2) draw a ray from 0 to z;
(3) draw a circle of radius $\sqrt[n]{r}$ centered at the origin;
(4) on the circle draw the number whose argument is θ/n; this is z_1;
(5) draw a regular n-gon with vertices on the circle and such that z_1 is a vertex.

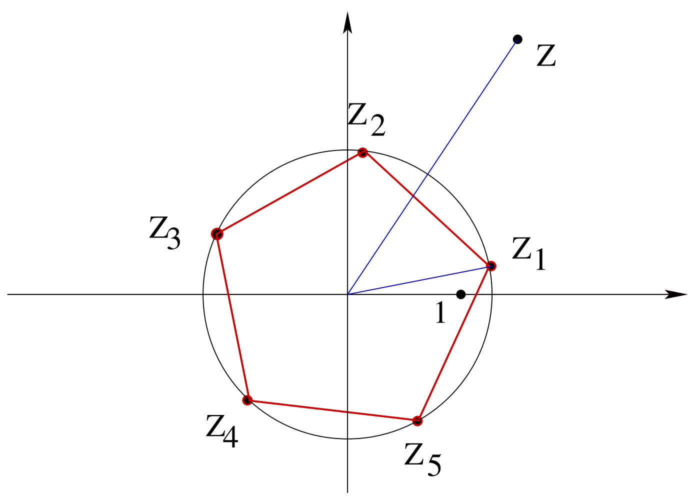


FIGURE 5.1. Degree n roots of a complex number

One special case is particularly interesting, namely when $c = 1$. We have the equation

$$z^n - 1 = 0$$

and its solution is called a degree n *root of unity*.

These are the numbers $\omega, \omega^2, \omega^3, \ldots, \omega^n = 1$ where

$$\omega = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right).$$

Let us consider several cases for small values of n.

(1) The only degree one root of unity is 1 itself.
(2) 1 and -1 are the square roots of unity.
(3) The numbers $1,\ -\frac{1}{2}+i\frac{\sqrt{3}}{2},\ -\frac{1}{2}-i\frac{\sqrt{3}}{2}$ are the degree three roots of unity.
(4) $1, i, -1$ and $-i$ are the degree four roots of unity.

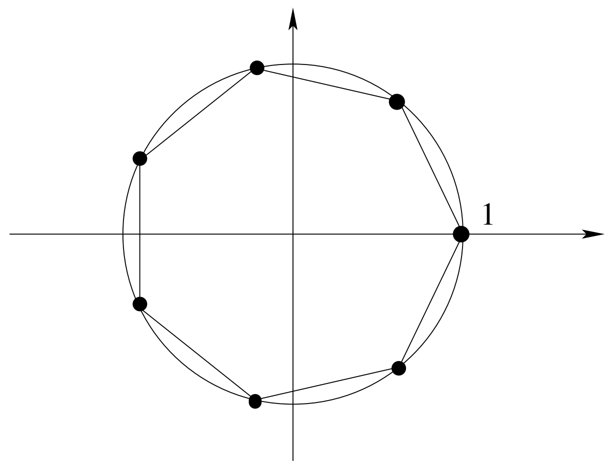


FIGURE 5.2. Degree seven roots of unity

In general, observe that the degree n roots of unity are the vertices of the regular n-gon inscribed in the unit circle so that 1 is a vertex (see Figure 5.2).

Since we know that one itself is a root of unity of any degree we can divide the polynomial $z^n - 1$ by $z - 1$. The quotient is equal to

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

Thus the degree n roots of unity different from one are the solutions of the equation

$$z^{n-1} + z^{n-2} + \cdots + z^2 + z + 1 = 0.$$

5.6. **Applications of De Moivre to trigonometry.** Although it is a result about complex numbers, De Moivre's Theorem can be used to deduce trigonometric identities, in particular multiple-angle formulae for sine and cosine. The general method is to take the identity

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$$

for some $n \in \mathbb{N}$, expand out the left-hand side, then equate real and imaginary parts.

Example 5.7. Use De Moivre's theorem to express $\cos(3\theta)$ as a polynomial in $\cos\theta$.

We have

$$\begin{aligned}(\cos\theta + i\sin\theta)^3 &= \cos^3\theta - 3\sin^2\theta\cos\theta + i(3\sin\theta\cos^2\theta - \sin^3\theta)\\ &= \cos(3\theta) + i\sin(3\theta),\end{aligned}$$

the last equality from De Moivre. Comparing real parts and using the identity $\sin^2\theta = 1 - \cos^2\theta$, we have

$$\begin{aligned}\cos(3\theta) &= \cos^3\theta - 3\sin^2\theta\cos\theta\\ &= \cos^3\theta - 3(1-\cos^2\theta)\cos\theta\\ &= 4\cos^3\theta - 3\cos\theta.\end{aligned}$$

♣

Example 5.8. Express $\sin(4\theta)$ as a polynomial in $\sin\theta$ and $\cos\theta$.

$$\begin{aligned}(\cos\theta + i\sin\theta)^4 &= \cos^4\theta - 6\cos^2\theta\sin^2\theta + \sin^4\theta\\ &\quad + i(4\cos^3\theta\sin\theta - 4\cos\theta\sin^3\theta)\\ &= \cos(4\theta) + i\sin(4\theta).\end{aligned}$$

Equating imaginary parts gives

$$\sin(4\theta) = 4\cos^3\theta\sin\theta - 4\cos\theta\sin^3\theta.$$

♣

5.9. **The complex exponential.** Suppose we wish to define the exponential e^z of a complex number $z = a + bi$, where $e = 2.71828\ldots$ is the base of the natural logarithm. The usual rules for exponentiation tell us that

$$e^{a+bi} = e^a e^{bi},$$

and since a is a real number e^a is already defined (as a real number). So we are left to define the exponential of purely imaginary numbers. For this, recall that the exponential function and sine and cosine can be defined by the following series:

$$\begin{aligned}e^x &= 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots = \sum_{k=0}^{\infty}\frac{x^k}{k!};\\ \cos(x) &= 1 - \frac{x^2}{2} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots = \sum_{k=0}^{\infty}(-1)^k\frac{x^{2k}}{(2k)!};\\ \sin(x) &= x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots = \sum_{k=0}^{\infty}(-1)^k\frac{x^{2k+1}}{(2k+1)!}.\end{aligned}$$

If we evaluate the first formula on bi we get that

$$\begin{aligned} e^{bi} &= 1 + bi + \frac{(bi)^2}{2} + \frac{(bi)^3}{3!} + \frac{(bi)^4}{4!} + \frac{(bi)^5}{5!} + \cdots \\ &= 1 + bi - \frac{b^2}{2} - \frac{b^3 i}{3!} + \frac{b^4}{4!} + \frac{b^5 i}{5!} + \cdots \\ &= \left(1 - \frac{b^2}{2} + \frac{b^4}{4!} + \cdots\right) + i\left(b - \frac{b^3}{3!} + \frac{b^5}{5!} + \cdots\right) \\ &= \cos b + i \sin b. \end{aligned}$$

Finally we arrive at the definition of the *complex exponential*:

$$e^z = e^{a+bi} = e^a(\cos b + i \sin b).$$

Note that $|e^z| = e^{\mathrm{Re}(z)}$ and $\arg(e^z) = \mathrm{Im}(z)$.

In particular, for any real number θ we have $e^{i\theta} = \cos\theta + i\sin\theta$, and so we can write a complex number in polar form as $z = |z|e^{i\theta}$ which simplifies the notation somewhat. De Moivre's Theorem in this form is equivalent to the identity

$$e^{i\alpha}e^{i\beta} = e^{i(\alpha+\beta)},$$

which is easier to remember as it is the usual rule for multiplying powers.

Example 5.10. Letting $z = i\pi$ we have $e^{i\pi} = \cos\pi + i\sin\pi = -1$. Written in the form

$$e^{i\pi} + 1 = 0$$

this is known as *Euler's identity*, and is regarded by many as the most beautiful equation in all of Mathematics. ♣

5.11. **The complex logarithm, sine and cosine.** Now that we have defined exponentiation of complex numbers, we should be able to define the inverse process of taking logarithms. Given a complex number z, its logarithm $\log(z)$ should be a complex number w such that $e^w = z$. This means that $|e^w| = e^{\mathrm{Re}(w)} = |z|$ and $\arg(e^w) = \mathrm{Im}(w) = \arg(z)$. We are led to the following definition:

Definition 5.12. Given a nonzero complex number $z \in \mathbb{C}$, its *complex logarithm* is any number of the form

$$\log(z) = \ln|z| + i\arg(z),$$

where $\ln$ denotes the ordinary (real) natural logarithm.

Remark 5.13. Due to the fact that $\arg(z)$ is only defined up to integer multiples of 2π, the complex logarithm is *multi-valued*, and so does not define a function in the usual sense. We could however choose the unique value

$$\operatorname{Log}(z) = \ln|z| + i\operatorname{Arg}(z)$$

and call this the *principal logarithm*. Note also that $\log(z)$ is defined for all $z \neq 0$, unlike the real logarithm $\ln(x)$ which is undefined for negative real numbers x.

You might wonder about extending other well-known functions to the complex numbers. This can be done, for example we can define *complex cosine* and *complex sine* using the complex exponential. First note that for a real number θ we have

$$e^{i\theta} + e^{-i\theta} = 2\cos\theta, \qquad e^{i\theta} - e^{-i\theta} = 2i\sin\theta.$$

Rearranging and replacing θ with an arbitrary *complex* number z, we arrive at the following.

Definition 5.14. The *complex cosine* and *complex sine* of a complex number z are given by

$$\cos z = \frac{e^{iz} + e^{-iz}}{2}, \qquad \sin z = \frac{e^{iz} - e^{-iz}}{2i}.$$

Example 5.15. We can calculate $\cos i$ and $\sin(\pi - i)$ as follows:

$$\begin{aligned} \cos i &= \frac{1}{2}\left(e^{i(i)} + e^{-i(i)}\right) \\ &= \frac{1}{2}(e^{-1} + e). \end{aligned}$$

$$\begin{aligned} \sin(\pi - i) &= \frac{1}{2i}\left(e^{i(\pi-i)} - e^{-i(\pi-i)}\right) \\ &= \frac{1}{2i}\left(e^{1+\pi i} - e^{-1-\pi i}\right) \\ &= \frac{1}{2i}(e(\cos\pi + i\sin\pi) - e^{-1}(\cos(-\pi) + i\sin(-\pi))) \\ &= -i\frac{(e^{-1} - e)}{2}. \end{aligned}$$

♣

We now return to the problem posed at the end of the last section, asking whether De Moivre's Theorem holds for complex powers. In order to make sense of complex powers of complex numbers, we use the exponential and logarithm functions. For $z, w \in \mathbb{C}$, we define

$$z^w = e^{w\log z}.$$

Recall that the logarithm is multi-valued, so z^w will be multi-valued in general. With this definition, De Moivre's formula

$$z^w = |z|^w \big(\cos(w\theta) + i \sin(w\theta) \big)$$

can be interpreted as giving one of the values.

Suggestions for further reading:

- http://en.wikipedia.org/wiki/De_Moivre's_formula
- http://en.wikipedia.org/wiki/Complex_logarithm
- R. A. Adams, *Calculus - A Complete Course*, Appendix 1.
- A. S. T. Lue, *Basic Pure Mathematics II*, Chapter 1.
- H. Anton, *Elementary Linear Algebra* (10$^{\text{th}}$ ed.), Appendix B.

6. Systems of linear equations

In the previous sections we saw that polynomial equations with one unknown can be difficult to solve in general. In this section we will look at *systems of equations* with many unknowns but the equations will be of a simpler form.

Example 6.1. Consider the following system of equations with two unknowns x_1 and x_2.

$$\begin{cases} x_1 & - & x_2 & = & 1 \\ 2x_1 & + & 3x_2 & = & 3 \end{cases}$$

To solve this system means to find all pairs (x_1, x_2) which solve both equations simultaneously. We proceed as follows.

First, to eliminate x_1 from the second equation, we multiply the first equation by two:

$$\begin{cases} 2x_1 - 2x_2 = 2 \\ 2x_1 + 3x_2 = 3 \end{cases}$$

and then we subtract the first equation from the second:

$$\begin{cases} 2x_1 - 2x_2 = 2 \\ \qquad\quad 5x_2 = 1 \end{cases}$$

Dividing the second equation by five we have:

$$\begin{cases} 2x_1 - 2x_2 = 2 \\ \qquad\quad x_2 = 1/5 \end{cases}$$

We have found that $x_2 = 1/5$. Substituting this into the first equation, we get

$$\begin{cases} 2x_1 - 2/5 = 2 \\ \qquad\quad x_2 = 1/5 \end{cases}$$

which on rearranging gives

$$\begin{cases} x_1 = 6/5 \\ x_2 = 1/5 \end{cases}$$

This system has the unique solution $(6/5, 1/5)$. ♣

Example 6.2. Consider the following system of 3 equations in 3 unknowns.

$$\begin{cases} x_1 & - & x_2 & + & x_3 = & -2 \\ 2x_1 & + & 3x_2 & + & x_3 = & 7 \\ x_1 & - & 2x_2 & - & x_3 = & -2 \end{cases}$$

Subtract the first equation from the third:

$$\begin{cases} x_1 & - & x_2 & + & x_3 = & -2 \\ 2x_1 & + & 3x_2 & + & x_3 = & 7 \\ 0 & - & x_2 & - & 2x_3 = & 0 \end{cases}$$

Now we multiply the first equation by two and subtract the result from the second equation:

$$\begin{cases} x_1 & - & x_2 & + & x_3 = & -2 \\ 0 & + & 5x_2 & - & x_3 = & 11 \\ 0 & - & x_2 & - & 2x_3 = & 0 \end{cases}$$

Swap the second equation with the third:

$$\begin{cases} x_1 & - & x_2 & + & x_3 = & -2 \\ 0 & - & x_2 & - & 2x_3 = & 0 \\ 0 & + & 5x_2 & - & x_3 = & 11 \end{cases}$$

Multiply the second equation by five and add to the third:

$$\begin{cases} x_1 & - & x_2 & + & x_3 = & -2 \\ 0 & - & x_2 & - & 2x_3 = & 0 \\ 0 & + & 0 & - & 11x_3 = & 11 \end{cases}$$

The last equation is now solved and we substitute the solution $x_3 = -1$ into the second and the first equation:

$$\begin{cases} x_1 & - & x_2 & - & 1 = & -2 \\ 0 & - & x_2 & + & 2 = & 0 \\ & & & & x_3 = & -1 \end{cases}$$

Now the second equation is solved and we substitute the solution $x_2 = 2$ to the first equation:

$$\begin{cases} x_1 & - & 2 & - & 1 = & -2 \\ & & x_2 & & = & 2 \\ & & & & x_3 = & 1 \end{cases}$$

Finally we get the full solution:

$$\begin{cases} x_1 & & & = & 1 \\ & & x_2 & = & 2 \\ & & & x_3 = & -1 \end{cases}$$

♣

In the above examples we manipulate with the system of equations so that the manipulation does not change the solution and that we get zeros in the bottom left corner of the system.

6.3. **A complex example.** The same procedure can be used to solve systems of linear equations with complex coefficients. Consider the system:

$$\begin{cases} ix_1 & - & x_2 & + & (1-i)x_3 = & i \\ 2x_1 & + & 3x_2 & + & ix_3 = & 2 \\ x_1 & - & (2+i)x_2 & - & ix_3 = & 1 \end{cases}$$

We play the same game as in the previous examples. To start we multiply the first equation by i and add to the third equation:

$$\begin{cases} ix_1 & - & x_2 & + & (1-i)x_3 = & i \\ 2x_1 & + & 3x_2 & + & ix_3 = & 2 \\ & - & (2+2i)x_2 & + & x_3 = & 0 \end{cases}$$

Next we multiply the first equation by $2/i = -2i$ and subtract from the second equation:

$$\begin{cases} ix_1 & - & x_2 & + & (1-i)x_3 = & i \\ & + & (3-2i)x_2 & + & (2+3i)x_3 = & 0 \\ & + & (-2-2i)x_2 & + & x_3 = & 0 \end{cases}$$

Multiply the second equation by $(2+2i)/(3-2i)$ and add to the third equation:

$$\begin{cases} ix_1 & - & x_2 & + & (1-i)x_3 = & i \\ & + & (3-2i)x_2 & + & (2+3i)x_3 = & 0 \\ & & & + & \dfrac{(2+2i)(2+3i)+(3-2i)}{3-2i}x_3 = & 0 \end{cases}$$

We obtain that $x_3 = 0$ and substitute this to the second and the first equation:

$$\begin{cases} ix_1 & - & x_2 & & = & i \\ & + & (3-2i)x_2 & & = & 0 \\ & & & x_3 = & & 0 \end{cases}$$

We get that $x_2 = 0$ and substitute it to the first equation and finally get the full solution:

$$\begin{cases} x_1 & & & = & 1 \\ & x_2 & & = & 0 \\ & & x_3 = & & 0 \end{cases}$$

Whether we are working over the real numbers or the complex numbers, the method is the same. In fact all we need to solve such a system of equations is that we can add/subtract and multiply/divide the coefficients. So this method works for linear systems with coefficients in any *field*.

6.4. **Matrices.** A *matrix* is a rectangular array of symbols. More precisely, an $(m \times n)$-matrix has the following form

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

It has m rows and n columns. Each a_{ij} is called an *entry* or a *coefficient* of the matrix. For example,

$$\begin{bmatrix} 2 & 3 & 7 \\ 1 & -1 & 2 \end{bmatrix}$$

is a (2×3)-matrix with integer coefficients. And

$$\begin{bmatrix} i & 3 \\ 1 & -1+i \\ -2-3i & 1-i \end{bmatrix}$$

is a (3×2)-matrix with complex entries.

Matrices are useful in many situations. First, let us apply them to solving linear systems of equations. Let us look again at the equation from Example 6.2

$$\begin{cases} x_1 & - & x_2 & + & x_3 = & -2 \\ 2x_1 & + & 3x_2 & + & x_3 = & 7 \\ x_1 & - & 2x_2 & - & x_3 = & -2 \end{cases}$$

All the manipulations we did in order to solve the system were applied to the coefficients. The following (3×4)-matrix collects all the coefficients of the system of equations.

$$\left[\begin{array}{ccc|c} 1 & -1 & 1 & -2 \\ 2 & 3 & 1 & 7 \\ 1 & -2 & -1 & -2 \end{array}\right]$$

This called the *augmented matrix* of the system (it is augmented by the vertical line which separates the coefficients of the left-hand sides from the right-hand sides).

Our task is to obtain a matrix with zeros in the bottom left corner and ones on the diagonal by applying the following operations which don't change the solutions of the system:

- swapping rows;
- multiplying a row by a number;
- adding one row to another.

In this concrete example we proceed as we did in Example 6.2, systematically reducing the entries of the matrix of coefficients until we obtain an equivalent system which can be solved easily. The idea is to obtain zeroes in all the positions under the diagonal of the matrix, using only the three rules mentioned above. Let us first get a zero in the position $(2,1)$ of the matrix. To do so, we subtract two times the first row from the second. This operation is codified as $r_2 - 2r_1$:

$$\left[\begin{array}{ccc|c} 1 & -1 & 1 & -2 \\ 2 & 3 & 1 & 7 \\ 1 & -2 & -1 & -2 \end{array}\right]_{r_2-2r_1} \sim \left[\begin{array}{ccc|c} 1 & -1 & 1 & -2 \\ 0 & 5 & -1 & 11 \\ 1 & -2 & -1 & -2 \end{array}\right]$$

Now we want to get a zero in the position $(3,1)$. To do so, we subtract the first row from the third, which we abbreviate by $r_3 - r_1$:

$$\left[\begin{array}{ccc|c} 1 & -1 & 1 & -2 \\ 0 & 5 & -1 & 11 \\ 1 & -2 & -1 & -2 \end{array}\right]_{r_3-r_1} \sim \left[\begin{array}{ccc|c} 1 & -1 & 1 & -2 \\ 0 & 5 & -1 & 11 \\ 0 & -1 & -2 & 0 \end{array}\right]$$

Next, we have to get a zero in the position $(3,2)$. To further simplify calculations, before doing so we can swap the second and the third rows, which we abbreviate by $r_2 \leftrightarrow r_3$:

$$\left[\begin{array}{ccc|c} 1 & -1 & 1 & -2 \\ 0 & 5 & -1 & 11 \\ 0 & -1 & -2 & 0 \end{array}\right]_{r_2\leftrightarrow r_3} \sim \left[\begin{array}{ccc|c} 1 & -1 & 1 & -2 \\ 0 & -1 & -2 & 0 \\ 0 & 5 & -1 & 11 \end{array}\right]$$

Now we can easily get a zero in the position $(3,2)$ by adding five times the second row to the third ($r_3 + 5r_2$):

$$\left[\begin{array}{ccc|c} 1 & -1 & 1 & -2 \\ 0 & -1 & -2 & 0 \\ 0 & 5 & -1 & 11 \end{array}\right]_{r_3+5r_2} \sim \left[\begin{array}{ccc|c} 1 & -1 & 1 & -2 \\ 0 & -1 & -2 & 0 \\ 0 & 0 & -11 & 11 \end{array}\right]$$

Finally, we can multiply the third row by $-\frac{1}{11}$ to get 1 on the left-hand side. We denote this simply by $-\frac{1}{11}r_3$:

$$\left[\begin{array}{ccc|c} 1 & -1 & 1 & -2 \\ 0 & -1 & -2 & 0 \\ 0 & 0 & -11 & 11 \end{array}\right]_{-\frac{1}{11}r_3} \sim \left[\begin{array}{ccc|c} 1 & -1 & 1 & -2 \\ 0 & -1 & -2 & 0 \\ 0 & 0 & 1 & -1 \end{array}\right]$$

The original system of equations is then equivalent to the system

$$\begin{cases} x_1 - x_2 + x_3 = -2 \\ \quad -x_2 - 2x_3 = 0 \\ \quad\quad x_3 = -1 \end{cases}$$

meaning that both have the same solutions. But the system above is very easy to solve: from the third equation we see that $x_3 = -1$. Substituting this in the second equation, we have $x_2 = 2$, and then substituting $x_2 = 2$ and $x_3 = -1$ in the first equation we deduce $x_1 = 1$.

It's actually possible to simplify the system even more by using further row operations: next, we use the third row to get a zero in position (2,3):

$$\left[\begin{array}{ccc|c} 1 & -1 & 1 & -2 \\ 0 & -1 & -2 & 0 \\ 0 & 0 & 1 & -1 \end{array}\right]_{r_2+2r_3} \sim \left[\begin{array}{ccc|c} 1 & -1 & 1 & -2 \\ 0 & -1 & 0 & -2 \\ 0 & 0 & 1 & -1 \end{array}\right]$$

Now use row 3 to get a 0 in position (1,3):

$$\left[\begin{array}{ccc|c} 1 & -1 & 1 & -2 \\ 0 & -1 & 0 & -2 \\ 0 & 0 & 1 & -1 \end{array}\right]_{r_1-r_3} \sim \left[\begin{array}{ccc|c} 1 & -1 & 0 & -1 \\ 0 & -1 & 0 & -2 \\ 0 & 0 & 1 & -1 \end{array}\right]$$

Finally, use row 2 to get a zero in position (1,2),

$$\left[\begin{array}{ccc|c} 1 & -1 & 0 & -1 \\ 0 & -1 & 0 & -2 \\ 0 & 0 & 1 & -1 \end{array}\right]_{r_1-r_2} \sim \left[\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & -1 & 0 & -2 \\ 0 & 0 & 1 & -1 \end{array}\right]$$

and multiply row 2 by -1:

$$\left[\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & -1 & 0 & -2 \\ 0 & 0 & 1 & -1 \end{array}\right]_{-r_2} \sim \left[\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & -1 \end{array}\right].$$

We can now simply read the solution from the matrix.

Remark 6.5. The method of solving systems of linear equations presented in the above examples is called *Gaussian elimination*. It is very efficient, and is the method used by computer algebra packages.

Example 6.6. Consider the following system where we have more equations than unknowns.

$$\begin{cases} x_1 - x_2 = -2 \\ 2x_1 + 3x_2 = 7 \\ x_1 - 2x_2 = -2 \end{cases}$$

The matrix of coefficients is

$$\left[\begin{array}{cc|c} 1 & -1 & -2 \\ 2 & 3 & 7 \\ 1 & -2 & -2 \end{array}\right]$$

Let us apply the Gaussian elimination algorithm. The operation that we do at each step is specified on the bottom right corner. For instance, in the first step we subtract two times the first row from the second, and this corresponds to $r_2 - 2r_1$:

$$\left[\begin{array}{cc|c} 1 & -1 & -2 \\ 2 & 3 & 7 \\ 1 & -2 & -2 \end{array}\right]_{r_2-2r_1} \sim \left[\begin{array}{cc|c} 1 & -1 & -2 \\ 0 & 5 & 11 \\ 1 & -2 & -2 \end{array}\right]_{r_3-r_1} \sim$$

$$\left[\begin{array}{cc|c} 1 & -1 & -2 \\ 0 & 5 & 11 \\ 0 & -1 & 0 \end{array}\right]_{-r_3} \sim \left[\begin{array}{cc|c} 1 & -1 & -2 \\ 0 & 5 & 11 \\ 0 & 1 & 0 \end{array}\right]_{r_2\leftrightarrow r_3} \sim$$

$$\left[\begin{array}{cc|c} 1 & -1 & -2 \\ 0 & 1 & 0 \\ 0 & 5 & 11 \end{array}\right]_{r_3-5r_1} \sim \left[\begin{array}{cc|c} 1 & -1 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 11 \end{array}\right]$$

The third row produces then the equation

$$0x_1 + 0x_2 = 11$$

which *has no solutions*. This means that the system has no solutions. ♣

Example 6.7. Now let us consider the system with two equations and three unknowns and let's find all real solutions.

$$\begin{cases} x_1 + x_2 - x_3 = -2 \\ 2x_1 + x_2 + 3x_3 = 7 \end{cases}$$

The associated matrix of coefficients is

$$\left[\begin{array}{ccc|c} 1 & 1 & -1 & -2 \\ 2 & 1 & 3 & 7 \end{array}\right]$$

Again, let us apply Gaussian elimination to solve the system.

$$\left[\begin{array}{ccc|c} 1 & 1 & -1 & -2 \\ 2 & 1 & 3 & 7 \end{array}\right]_{r_2-2r_1} \sim \left[\begin{array}{ccc|c} 1 & 1 & -1 & -2 \\ 0 & -1 & 5 & 11 \end{array}\right]_{r_1+r_2}$$

$$\sim \left[\begin{array}{ccc|c} 1 & 0 & 4 & 9 \\ 0 & -1 & 5 & 11 \end{array}\right]_{-r_2} \sim \left[\begin{array}{ccc|c} 1 & 0 & 4 & 9 \\ 0 & 1 & -5 & -11 \end{array}\right]$$

In this case, we cannot reduce the coefficient matrix any more. Notice that we have more variables than equations. We may then consider x_3 as a parameter, and we get then

$$x_2 = 5x_3 - 11 \qquad x_1 = -4x_3 + 9.$$

In other words, the solutions of the system form the (infinite) set

$$\{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 = -4t + 9,\ x_2 = 5t - 11,\ x_3 = t \text{ for some } t \in \mathbb{R}\}.$$

(Here we are using the standard notation $\mathbb{R}^3$ to denote the set of triples of real numbers.)

We can also write the solutions of the system as the set

$$\{(-4t + 9, 5t - 11, t) \in \mathbb{R}^3 \mid t \in \mathbb{R}\}.$$

♣

Remark 6.8. In both the previous examples, we solved the system by transforming the matrix into the simplest possible form. This is called *reduced row echelon form*. The formal definition is below:

Definition 6.9. A matrix is said to be in *row echelon form* if:

(1) The first nonzero entry in each row is 1.
(2) In two consecutive nonzero rows, the leading 1 in the lower row occurs farther to the right.
(3) Any rows consisting entirely of zeroes are grouped at the bottom.

It is said to be in *reduced row echelon form* if in addition

(4) All the entries above each leading 1 are zero.

Any matrix can be put into (reduced) row echelon form using Gaussian elimination.

Example 6.10. Let us see a longer example: consider the system

$$\begin{cases} \quad\;\; 2x_2 + x_3 + x_4 \qquad\;\; = 0 \\ x_1 \qquad\;\; + x_3 \qquad\;\; + x_5 = 6 \\ x_1 - x_2 \qquad\;\; - x_4 \qquad\;\; = 2 \\ 2x_1 + x_2 + 2x_3 \qquad\;\; + x_5 = 8 \\ 2x_1 \qquad\;\; + x_3 - x_4 \qquad\;\; = 4 \end{cases}$$

The matrix of coefficients is

$$A = \left[\begin{array}{ccccc|c} 0 & 2 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 6 \\ 1 & -1 & 0 & -1 & 0 & 2 \\ 2 & 1 & 2 & 0 & 1 & 8 \\ 2 & 0 & 1 & -1 & 0 & 4 \end{array}\right]$$

We can now start applying Gaussian elimination

$$\left[\begin{array}{ccccc|c} 0 & 2 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 6 \\ 1 & -1 & 0 & -1 & 0 & 2 \\ 2 & 1 & 2 & 0 & 1 & 8 \\ 2 & 0 & 1 & -1 & 0 & 4 \end{array}\right]_{r_1 \leftrightarrow r_3} \sim \left[\begin{array}{ccccc|c} 1 & -1 & 0 & -1 & 0 & 2 \\ 1 & 0 & 1 & 0 & 1 & 6 \\ 0 & 2 & 1 & 1 & 0 & 0 \\ 2 & 1 & 2 & 0 & 1 & 8 \\ 2 & 0 & 1 & -1 & 0 & 4 \end{array}\right]_{r_2 - r_1}$$

$$\left[\begin{array}{ccccc|c} 1 & -1 & 0 & -1 & 0 & 2 \\ 0 & 1 & 1 & 1 & 1 & 4 \\ 0 & 2 & 1 & 1 & 0 & 0 \\ 2 & 1 & 2 & 0 & 1 & 8 \\ 2 & 0 & 1 & -1 & 0 & 4 \end{array}\right]_{r_4 - 2r_1} \sim \left[\begin{array}{ccccc|c} 1 & -1 & 0 & -1 & 0 & 2 \\ 0 & 1 & 1 & 1 & 1 & 4 \\ 0 & 2 & 1 & 1 & 0 & 0 \\ 0 & 3 & 2 & 2 & 1 & 4 \\ 2 & 0 & 1 & -1 & 0 & 4 \end{array}\right]_{r_5 - 2r_1}$$

$$\left[\begin{array}{ccccc|c} 1 & -1 & 0 & -1 & 0 & 2 \\ 0 & 1 & 1 & 1 & 1 & 4 \\ 0 & 2 & 1 & 1 & 0 & 0 \\ 0 & 3 & 2 & 2 & 1 & 4 \\ 0 & 2 & 1 & 1 & 0 & 0 \end{array}\right]_{r_3 - 2r_1} \sim \left[\begin{array}{ccccc|c} 1 & -1 & 0 & -1 & 0 & 2 \\ 0 & 1 & 1 & 1 & 1 & 4 \\ 0 & 0 & -1 & -1 & -2 & -8 \\ 0 & 3 & 2 & 2 & 1 & 4 \\ 0 & 2 & 1 & 1 & 0 & 0 \end{array}\right]_{r_4 - 3r_2}$$

$$\left[\begin{array}{ccccc|c} 1 & -1 & 0 & -1 & 0 & 2 \\ 0 & 1 & 1 & 1 & 1 & 4 \\ 0 & 0 & -1 & -1 & -2 & -8 \\ 0 & 0 & -1 & -1 & -2 & -8 \\ 0 & 2 & 1 & 1 & 0 & 0 \end{array}\right]_{r_5 - 2r_2} \sim \left[\begin{array}{ccccc|c} 1 & -1 & 0 & -1 & 0 & 2 \\ 0 & 1 & 1 & 1 & 1 & 4 \\ 0 & 0 & -1 & -1 & -2 & -8 \\ 0 & 0 & -1 & -1 & -2 & -8 \\ 0 & 0 & -1 & -1 & -2 & -8 \end{array}\right]_{r_4 - r_3}$$

$$\left[\begin{array}{ccccc|c} 1 & -1 & 0 & -1 & 0 & 2 \\ 0 & 1 & 1 & 1 & 1 & 4 \\ 0 & 0 & -1 & -1 & -2 & -8 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & -2 & -8 \end{array}\right]_{r_5 - r_3} \sim \left[\begin{array}{ccccc|c} 1 & -1 & 0 & -1 & 0 & 2 \\ 0 & 1 & 1 & 1 & 1 & 4 \\ 0 & 0 & -1 & -1 & -2 & -8 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]_{-r_3}$$

$$\sim \left[\begin{array}{ccccc|c} 1 & -1 & 0 & -1 & 0 & 2 \\ 0 & 1 & 1 & 1 & 1 & 4 \\ 0 & 0 & 1 & 1 & 2 & 8 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

This matrix is in row echelon form. We could solve the system now, but it is easier and more instructive to continue until the matrix is in reduced row echelon form:

$$\left[\begin{array}{ccccc|c} 1 & -1 & 0 & -1 & 0 & 2 \\ 0 & 1 & 1 & 1 & 1 & 4 \\ 0 & 0 & 1 & 1 & 2 & 8 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]_{r_2 - r_3} \sim \left[\begin{array}{ccccc|c} 1 & -1 & 0 & -1 & 0 & 2 \\ 0 & 1 & 0 & 0 & -1 & -4 \\ 0 & 0 & 1 & 1 & 2 & 8 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]_{r_1 + r_2}$$

$$\sim \left[\begin{array}{ccccc|c} 1 & 0 & 0 & -1 & -1 & -2 \\ 0 & 1 & 0 & 0 & -1 & -4 \\ 0 & 0 & 1 & 1 & 2 & 8 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

We can ignore the last two rows, since they do not give any information about the system. Also, there is no row of the form

$$\left[\begin{array}{ccccc|c} 0 & 0 & 0 & 0 & 0 & * \end{array}\right]$$

and this means that the system has solutions.

However, once we discard the last two rows, the resulting system has five variables and three equations. This means that the system has infinitely many solutions, which depend on two parameters. In other words, the solutions of the system form the set

$$\{(z + t - 2, t - 4, 8 - z - 2t, z, t) \in \mathbb{R}^5 \mid z, t \in \mathbb{R}\}.$$

♣

Suggestions for further reading:

- http://en.wikipedia.org/wiki/Gaussian_elimination
- Type *Gaussian elimination* into a search engine. One set of online notes I like are at http://www.it.uom.gr/teaching/linearalgebra/chapt6.pdf/
- Almost any book with the words *Linear Algebra* in the title will have a chapter on Gaussian elimination. One such is H. Anton, *Elementary Linear Algebra*.

7. Determinants

In this section we will see how to associate a number to any square matrix (a *square matrix* is a matrix with the same number of rows as columns). This number is called the *determinant*, because it determines the nature of the solutions of a linear system having the given matrix as its coefficients.

To illustrate the idea, consider the general (2×2) system

$$\left\{ \begin{array}{ccccc} ax_1 & + & bx_2 & = & y_1 \\ cx_1 & + & dx_2 & = & y_2 \end{array} \right. \qquad \text{where } y_1, y_2 \text{ are constants.}$$

If we try to eliminate x_1 by subtracting c times the first equation from a times the second, we arrive at the equation

$$(ad - bc)x_2 = ay_2 - cy_1.$$

The nature of the solutions is then determined by the quantity $ad - bc$ associated to the matrix of coefficients.

- If $ad - bc \neq 0$, then the system has a unique solution.
- If $ad - bc = 0$, the system either has no solutions (if $ay_2 - cy_1 \neq 0$) or infinitely many solutions (if $ay_2 - cy_1 = 0$).

The quantity $ad - bc$ is called the *determinant* of the (2×2)-matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, and denoted $\det A$ or $|A|$.

More generally, if A is a square matrix we can associate to it a number, denoted $\det(A)$ or $|A|$ and called its *determinant*. This number determines the nature of the solutions of a linear system with coefficient matrix A. In particular, the system has a unique solution if and only if $\det A \neq 0$.

7.1. Definition of the determinant.

The formula for an $(n \times n)$ determinant is recursive in nature. To give it, we first make the following definition.

Definition 7.2. Let A be an $(n \times n)$-matrix. The matrix A_{ij} obtained by deleting the i-th row and j-th column of A is called the *(i, j)-th minor* of A.

Example 7.3. Let $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$. Then

$$A_{12} = \begin{bmatrix} 4 & 6 \\ 7 & 9 \end{bmatrix}, \qquad A_{31} = \begin{bmatrix} 2 & 3 \\ 5 & 6 \end{bmatrix}.$$

♣

The formula for the determinant of an $(n \times n)$ matrix is as follows:

- If $n = 1$ then $\det[a] = a$;
- If $n = 2$ then $\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc$;
- If $n \geq 3$ then

$$\det \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} = \sum_{k=1}^{n} (-1)^{1+k} a_{1k} \det A_{1k}.$$

Remark 7.4. For (1×1)-matrices there is a potential notational conflict with the modulus if we use vertical bars to denote determinants. In particular we have $|a| = a$, which isn't generally true for the modulus. We won't worry too much about this, as we won't have much to do with (1×1) determinants.

Example 7.5. Let's compute the determinant of the (3×3)-matrix

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$

from Example 7.3. The relevant minors are

$$A_{11} = \begin{bmatrix} 5 & 6 \\ 8 & 9 \end{bmatrix}, \qquad A_{12} = \begin{bmatrix} 4 & 6 \\ 7 & 9 \end{bmatrix}, \qquad A_{13} = \begin{bmatrix} 4 & 5 \\ 7 & 8 \end{bmatrix}.$$

Let's calculate their determinants:

$$\begin{aligned} \det A_{11} &= 5 \cdot 9 - 6 \cdot 8 \\ &= -3, \\ \det A_{12} &= 4 \cdot 9 - 6 \cdot 7 \\ &= -6, \\ \det A_{13} &= 4 \cdot 8 - 5 \cdot 7 \\ &= -3. \end{aligned}$$

Now expanding out the formula for the determinant given above, we have

$$\begin{aligned} \det A &= a_{11} \det A_{11} - a_{12} \det A_{12} + a_{13} \det A_{13} \\ &= 1 \cdot (-3) - 2 \cdot (-6) + 3 \cdot (-3) \\ &= 0. \end{aligned}$$

♣

The formula given above for an $(n \times n)$-determinant is called the *Laplace formula* or *Laplace expansion*. (There is another formula for determinants know as the *Leibniz formula* which will not be discussed here.) Notice that the first row of A played a special rôle in our formula. Indeed, $\det A$ is obtained by multiplying each entry a_{1k} of the first row by the determinant of its corresponding minor A_{1k}, and then taking an alternating sum. In fact, the first row is not so special; we could equally well expand around any other row or any column.

Theorem 7.6. *Let $A = [a_{ij}]$ be an $(n \times n)$-matrix. Then for all $1 \leq i, j, \leq n$, we have*

$$\det A = \sum_{k=1}^{n} (-1)^{i+k} a_{ik} \det A_{ik} = \sum_{k=1}^{n} (-1)^{k+j} a_{kj} \det A_{kj}.$$

Note the pattern of signs appearing in the Laplace expansion. Here we represent the $(n \times n)$-matrix $[(-1)^{i+j}]$ for some small values of n:

$$\begin{bmatrix} + & - \\ - & + \end{bmatrix}, \qquad \begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}, \qquad \begin{bmatrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ - & + & - & + \end{bmatrix}.$$

Example 7.7. Let's go back to the matrix

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$

from Example 7.3 and calculate $\det A$ by expanding around the second column instead. The relevant minors are

$$A_{12} = \begin{bmatrix} 4 & 6 \\ 7 & 9 \end{bmatrix}, \qquad A_{22} = \begin{bmatrix} 1 & 3 \\ 7 & 9 \end{bmatrix}, \qquad A_{32} = \begin{bmatrix} 1 & 3 \\ 4 & 6 \end{bmatrix},$$

and their determinants are

$$\det A_{12} = -6, \qquad \det A_{22} = -12 \quad \text{and} \quad \det A_{32} = -6.$$

Applying the $j = 2$ case of the formula from Theorem 7.6, we find

$$\begin{aligned} \det A &= -a_{12} \det A_{12} + a_{22} \det A_{22} - a_{32} \det A_{32} \\ &= -2 \cdot (-6) + 5 \cdot (-12) - 8 \cdot (-6) \\ &= 0, \end{aligned}$$

which is the same answer as before. ♣

Example 7.8. We can use Theorem 7.6 to reduce the number of computations needed to compute the determinant, by choosing to expand around rows or columns which are ‘sparse’, i.e. which contain lots of zeroes. Take for instance the matrix

$$B = \begin{bmatrix} 1 & 4 & 7 & -1 \\ 2 & 6 & 0 & 0 \\ -1 & 3 & 0 & 2 \\ 4 & 1 & 0 & 0 \end{bmatrix}.$$

If we were to expand around the first row we’d have to calculate four (3×3) determinants. However, note that

$$\begin{aligned} \det B &= 7 \begin{vmatrix} 2 & 6 & 0 \\ -1 & 3 & 2 \\ 4 & 1 & 0 \end{vmatrix} && \text{(expanding around 3}^{\text{rd}}\text{ column)} \\ &= 7(-2) \begin{vmatrix} 2 & 6 \\ 4 & 1 \end{vmatrix} && \text{(expanding around 3}^{\text{rd}}\text{ column)} \\ &= 7(-2)(-22) = 308. \end{aligned}$$

♣

7.9. **Properties of determinants.** In this section we will give some further useful properties of determinants, which will assist in their calculation. We begin by identifying some special types of matrices for which the determinant is particularly easy to compute.

Definition 7.10. A square matrix $A = [a_{ij}]$ is called:

- *diagonal* if all entries off the main diagonal are zero, that is, if $a_{ij} = 0$ for $i \neq j$;
- *upper-triangular* if all entries below the main diagonal are zero, that is, if $a_{ij} = 0$ for $i > j$;
- *lower-triangular* if all entries above the main diagonal are zero, that is, if $a_{ij} = 0$ for $i < j$.

Remark 7.11. Note that a matrix is diagonal if and only if it is both upper- and lower-triangular.

Example 7.12. Let

$$A = \begin{bmatrix} 1 & 4 & 0 \\ 0 & 7 & 8 \\ 0 & 0 & -1 \end{bmatrix}, \qquad B = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \quad \text{and} \quad C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The matrix A is upper-triangular. The matrix B is lower-triangular (but not upper-triangular). The matrix C is diagonal. ♣

Proposition 7.13. *The determinant of an upper-triangular or lower-triangular matrix is the product of its diagonal entries.*

Proof. We will prove the result for upper-triangular matrices by induction on the size of the matrix. The result is clearly true for (1×1)-matrices. Assume that the result holds for $(n \times n)$-matrices, and let A be a $\big((n+1) \times (n+1)\big)$-matrix with diagonal entries $a_{11}, \dots, a_{nn}, a_{(n+1)(n+1)}$. Expanding around the first column, we have

$$\det A = \sum_{k=1}^{n+1} (-1)^{k+1} a_{k1} \det A_{k1}.$$

Since A is upper triangular, $a_{k1} = 0$ for $k > 1$, and so the sum reduces to

$$\det A = a_{11} \det A_{11}.$$

Now, by our inductive hypothesis, since the minor A_{11} is $(n \times n)$ upper-triangular, its determinant is the product of its diagonal entries $a_{22}, \dots, a_{(n+1)(n+1)}$. Therefore

$$\det A = a_{11} a_{22} \cdots a_{(n+1)(n+1)}$$

is the product of the diagonal entries of A. This completes the induction.

The proof for lower-triangular matrices is similar. □

Example 7.14.

$$\det \begin{bmatrix} 2 & 6 & 0 & 8 \\ 0 & -1 & 3 & 4 \\ 0 & 0 & -4 & 10 \\ 0 & 0 & 0 & 3 \end{bmatrix} = 2 \times (-1) \times (-4) \times 3 = 24.$$

♣

The effect of the elementary row operations on the determinant is described as follows.

Proposition 7.15. *Let A be a square matrix.*

(1) Multiplying one row of A by $r \in \mathbb{R}$ multiplies the determinant by r.
(2) Adding a multiple of one row of A to another row leaves the determinant unchanged.
(3) Swapping two rows of A multiplies the determinant by -1.

We will not prove these facts here, but note the following immediate consequences.

Corollary 7.16. *Let A be a square matrix.*

(1) If any row of A consists entirely of zeroes, then $\det A = 0$.
(2) If any row of A is a multiple of any other row, then $\det A = 0$.

All of this is suggestive that we might simplify the calculation of the determinant of an arbitrary square matrix by first putting it in to upper-triangular form using row operations. We must remember that the determinant changes when we multiply a row by a number or swap two rows!

Example 7.17. Calculate $\det \begin{bmatrix} 0 & 3 & 1 \\ 2 & -4 & 6 \\ 5 & 2 & -1 \end{bmatrix}$ using row operations.

$$\begin{aligned}
\begin{vmatrix} 0 & 3 & 1 \\ 2 & -4 & 6 \\ 5 & 2 & -1 \end{vmatrix} &= -\begin{vmatrix} 2 & -4 & 6 \\ 0 & 3 & 1 \\ 5 & 2 & -1 \end{vmatrix} && \text{(Swapping } R_1 \text{ and } R_2 \text{ introduces a minus sign)} \\
&= -(2)\begin{vmatrix} 1 & -2 & 3 \\ 0 & 3 & 1 \\ 5 & 2 & -1 \end{vmatrix} && \text{(a factor 2 from } R_1 \text{ comes outside the det sign)} \\
&= -(2)\begin{vmatrix} 1 & -2 & 3 \\ 0 & 3 & 1 \\ 0 & 12 & -16 \end{vmatrix} && \text{(} R_3 - 5R_1 \text{ doesn't change the determinant)} \\
&= -(2)\begin{vmatrix} 1 & -2 & 3 \\ 0 & 3 & 1 \\ 0 & 0 & -20 \end{vmatrix} && \text{(} R_3 - 4R_2 \text{ doesn't change the determinant)} \\
&= -(2)(1)(3)(-20) \\
&= 120.
\end{aligned}$$

♣

Definition 7.18. The *transpose* of a matrix A is the matrix A^T whose rows are the columns of A.

The transpose A^T of an $(m \times n)$-matrix A is therefore an $(n \times m)$-matrix, whose (i, j)-th entry is the (j, i)-th entry of A.

Example 7.19. The transpose of the matrix

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \qquad \text{is} \qquad A^T = \begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix}.$$

The transpose of

$$\mathbf{x} = \begin{bmatrix} x \\ y \\ z \end{bmatrix} \qquad \text{is} \qquad \mathbf{x}^T = \begin{bmatrix} x & y & z \end{bmatrix}.$$

♣

Proposition 7.20. *Let A be a square matrix. Then*
$$\det(A^T) = \det A.$$

Corollary 7.21. *The properties of determinants given in Proposition 7.15 and Corollary 7.16 remain true when the word 'row' is replaced by the word 'column'.*

Example 7.22. Calculate $\det C$ where
$$C = \begin{bmatrix} 1 & 0 & 0 & -3 \\ -3 & 2 & 0 & 9 \\ 6 & 0 & 8 & 0 \\ 4 & 5 & -1 & -5 \end{bmatrix}.$$

We could expand around the first row, which would result in us having to compute two 3×3 determinants. Better is to put C into lower-triangular form by adding 3 times the first column to the last column:
$$\begin{vmatrix} 1 & 0 & 0 & -3 \\ -3 & 2 & 0 & 9 \\ 0 & 6 & 8 & 0 \\ 4 & 5 & -1 & -5 \end{vmatrix}_{C_4+3C_1} = \begin{vmatrix} 1 & 0 & 0 & 0 \\ -3 & 2 & 0 & 0 \\ 0 & 6 & 8 & 0 \\ 4 & 5 & -1 & 7 \end{vmatrix} = 1 \times 2 \times 8 \times 7 = 112.$$

♣

Suggestions for further reading:

- http://en.wikipedia.org/wiki/Determinant
- Almost any book on Linear Algebra will have a chapter on determinants. One such is H. Anton, *Elementary Linear Algebra.*

8. Algebra of matrices

In this section we will define addition, subtraction, and multiplication of matrices. We can therefore do algebra with matrices, and can, in a certain sense, think of matrices as *generalized numbers*. We will work only with real matrices, but everything we say will be true for complex matrices also.

8.1. **Addition, scalar multiplication and subtraction of matrices.**

We refer to an $(m \times n)$-matrix as a matrix of *size* $(m \times n)$.

Definition 8.2 (Addition)**.** If A and B are two matrices of the same size, their *sum* $A + B$ is the matrix obtained by adding the corresponding entries of A and B. More formally, the sum of two $(m\times n)$-matrices $A = [a_{ij}]$ and $B = [b_{ij}]$ is the $(m \times n)$-matrix defined by $A + B = [a_{ij} + b_{ij}]$.

Definition 8.3 (Scalar multiplication)**.** If A is any matrix and r is any number, the matrix rA is obtained from A by multiplying all entries by r. If $A = [a_{ij}]$ then $rA = [ra_{ij}]$.

Definition 8.4 (Subtraction)**.** If A and B are two matrices of the same size, then $A - B = A + (-1)B$. Hence if $A = [a_{ij}]$ and $B = [b_{ij}]$ are both $(m \times n)$-matrices, then $A - B = [a_{ij} - b_{ij}]$.

Remark 8.5. Note that in the above definitions of $A + B$ and $A - B$, we insisted that A and B be the same size. If A and B are matrices of different sizes, then $A + B$ and $A - B$ are undefined.

Example 8.6. Consider the matrices

$$A = \begin{bmatrix} 2 & 4 & 3 \\ 0 & 1 & 6 \end{bmatrix}, \quad B = \begin{bmatrix} -1 & -2 & 0 \\ 3 & -4 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix}.$$

Then

$$\begin{aligned} A + B &= \begin{bmatrix} 2 & 4 & 3 \\ 0 & 1 & 6 \end{bmatrix} + \begin{bmatrix} -1 & -2 & 0 \\ 3 & -4 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 2+(-1) & 4+(-2) & 3+0 \\ 0+3 & 1+(-4) & 6+1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 2 & 3 \\ 3 & -3 & 7 \end{bmatrix}. \end{aligned}$$

$$\begin{aligned} 3A &= \begin{bmatrix} 3\times 2 & 3\times 4 & 3\times 3 \\ 3\times 0 & 3\times 1 & 3\times 6 \end{bmatrix} \\ &= \begin{bmatrix} 6 & 12 & 9 \\ 0 & 3 & 18 \end{bmatrix}. \end{aligned}$$

$$
\begin{aligned}
B - 2A &= B + (-2)A \\
&= \begin{bmatrix} -1 & -2 & 0 \\ 3 & -4 & 1 \end{bmatrix} + \begin{bmatrix} (-2)2 & (-2)4 & (-2)3 \\ (-2)0 & (-2)1 & (-2)6 \end{bmatrix} \\
&= \begin{bmatrix} -1 & -2 & 0 \\ 3 & -4 & 1 \end{bmatrix} + \begin{bmatrix} -4 & -8 & -6 \\ 0 & -2 & -12 \end{bmatrix} \\
&= \begin{bmatrix} -5 & -10 & -6 \\ 3 & -6 & -11 \end{bmatrix}
\end{aligned}
$$

The sum $B + C$ is undefined, since B and C are of different sizes. ♣.

8.7. **Multiplication of matrices.** Multiplication of matrices is somewhat more complicated. The naive approach of just multiplying corresponding entries turns out to be not very useful, one reason being that for the applications we have in mind we wish to multiply matrices of different sizes. Here is the correct definition.

Definition 8.8. If A and B are matrices such that the number of columns of A equals the number of rows of B, then the *product* AB is defined. The (i, j)-th entry of AB is obtained by multiplying each entry in the i-th row of A with the corresponding entry in the j-th column of B, and then taking the sum. More formally, the product of a $(k \times m)$-matrix $A = [a_{ij}]$ and an $(m \times n)$-matrix $B = [b_{ij}]$ is the $(k \times n)$-matrix AB whose (i, j)-th entry is given by

$$a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{im}b_{mj}.$$

Remark 8.9. If the number of columns of A *does not* equal the number of rows of B, then the product AB is undefined. Take note of the sizes in the definition of the product:

$$(k \times \cancel{m})(\cancel{m} \times n) = (k \times n).$$

All of this is best illustrated by example.

Example 8.10. Consider the (2×3)-matrix A and (3×2)-matrix B given by

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & 2 \\ 2 & 3 \\ 2 & 2 \end{bmatrix}.$$

Then we can form the products

$$\begin{aligned} AB &= \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 2 & 3 \\ 2 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 1\times 1 + 2\times 2 + 3\times 2 & 1\times 2 + 2\times 3 + 3\times 2 \\ 2\times 1 + 3\times 2 + 4\times 2 & 2\times 2 + 3\times 3 + 4\times 2 \end{bmatrix} \\ &= \begin{bmatrix} 11 & 14 \\ 16 & 21 \end{bmatrix}, \end{aligned}$$

$$\begin{aligned} \text{and} \quad BA &= \begin{bmatrix} 1 & 2 \\ 2 & 3 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{bmatrix} \\ &= \begin{bmatrix} 1\times 1 + 2\times 2 & 1\times 2 + 2\times 3 & 1\times 3 + 2\times 4 \\ 2\times 1 + 3\times 2 & 2\times 2 + 3\times 3 & 2\times 3 + 3\times 4 \\ 2\times 1 + 2\times 2 & 2\times 2 + 2\times 3 & 2\times 3 + 2\times 4 \end{bmatrix} \\ &= \begin{bmatrix} 5 & 8 & 11 \\ 8 & 13 & 18 \\ 6 & 10 & 14 \end{bmatrix}. \end{aligned}$$

♣

This example shows that with matrix multiplication, unlike with ordinary multiplication of numbers, *the order of multiplication matters*. The products AB and BA are not equal (they are not even the same size). This failure of commutativity can be even more dramatic, as in the next example.

Example 8.11. Let $A = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$ and let $\mathbf{x} = \begin{bmatrix} x \\ y \end{bmatrix}$. Then

$$A\mathbf{x} = \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2x + 5y \\ x + 3y \end{bmatrix},$$

but $\mathbf{x}A$ is undefined. ♣

Proposition 8.12. *Addition and multiplication of matrices satisfy the following properties (compare Proposition 3.9):*

(1) $A + B = B + A$ whenever A and B are of the same size;
(2) $A + (B + C) = (A + B) + C$ whenever A, B and C are of the same size;
(3) $A(BC) = (AB)C$ whenever the products are defined;
(4) $A(B + C) = AB + AC$ whenever the products are defined;
(5) $(A + B)C = AC + BC$ whenever the products are defined.

Example 8.13. Let $n \in \mathbb{N}$. We define $M_n(\mathbb{R})$ to be the set of $(n \times n)$-matrices with entries from $\mathbb{R}$, and $M_n(\mathbb{C})$ to be the set of $(n \times n)$-matrices with entries from $\mathbb{C}$. With the operations of matrix addition and multiplication, both $M_n(\mathbb{R})$ and $M_n(\mathbb{C})$ are examples of *non-commutative rings*.

8.14. **Interpreting linear systems as matrix equations.** In Example 8.11, the (2×1)-matrix $\mathbf{x}$ could be viewed as having variable entries. Using variable matrices in this way allows us to view any system of linear equations as a single matrix equation. Take the general system of m linear equations in n unknowns:

$$\begin{cases} a_{11}x_1 & + & a_{12}x_2 & + & \dots & + & a_{1n}x_n = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \dots & + & a_{2n}x_n = & b_2 \\ \vdots & & & & \ddots & & \vdots & \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \dots & + & a_{mn}x_n = & b_m \end{cases}$$

This is equivalent to single matrix equation $A\mathbf{x} = \mathbf{b}$, where

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}, \quad \mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \quad \text{and } \mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}.$$

Remark 8.15. A matrix consisting of a single column may be referred to as a *vector* (or *column vector*). Vectors are usually denoted by boldface lower-case Roman letters, such as $\mathbf{v}$. When hand-written, they may be denoted using an underline $\underline{v}$ or an over-arrow $\vec{v}$.

Example 8.16. The system of equations

$$\begin{cases} x_1 & - & x_2 & + & x_3 = & -2 \\ 2x_1 & + & 3x_2 & + & x_3 = & 7 \\ x_1 & - & 2x_2 & - & x_3 = & -2 \end{cases}$$

can be written in matrix form as

$$\begin{bmatrix} 1 & -1 & 1 \\ 2 & 3 & 1 \\ 1 & -2 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} -2 \\ 7 \\ -2 \end{bmatrix}.$$

♣

It is tempting to think that by writing a linear system in the form $A\mathbf{x} = \mathbf{b}$ we have made it easier to solve. Can't we just divide through by the matrix A to give $\mathbf{x} = A^{-1}\mathbf{b}$? There is a certain sense in which we *can* do this, for some matrices A. This will be made precise in subsequent sections.

8.17. **Identity matrices.**

Definition 8.18. An *identity matrix* is a diagonal matrix, all of whose diagonal entries are 1. For example,

$$I_1 = [1] \text{ is the } (1 \times 1) \text{ identity matrix,}$$
$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ is the } (2 \times 2) \text{ identity matrix,}$$
$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ is the } (3 \times 3) \text{ identity matrix.}$$

Proposition 8.19. *Let I_n be the $(n \times n)$ identity matrix. Then*

(1) $\det I_n = 1$*;*
(2) If A is an $(n \times n)$-matrix, then

$$I_n A = A I_n = A.$$

(3) More generally, if B is an $(n \times \ell)$-matrix and C an $(m \times n)$-matrix, then

$$I_n B = B \qquad \text{and} \qquad C I_n = C.$$

The above properties indicate that identity matrices are to matrix multiplication somewhat as the number 1 is to ordinary multiplication of numbers.

8.20. **Inverse matrices.**

Definition 8.21. Let A be an $(n \times n)$-matrix. An *inverse* of A is an $(n \times n)$-matrix B such that

$$AB = BA = I_n.$$

Proposition 8.22. *Any matrix A admits at most one inverse.*

Proof. Suppose that B and C are both inverses of A. We have

$$\begin{array}{rrcll} & AB & = & I_n & \text{(since } B \text{ is an inverse of } A\text{)} \\ \Longrightarrow & C(AB) & = & CI_n & \text{(multiplying on the left by } C\text{)} \\ \Longrightarrow & (CA)B & = & C & \text{(by 8.12(3) and 8.19(2))} \\ \Longrightarrow & I_n B & = & C & \text{(since } C \text{ is an inverse of } A\text{)} \\ \Longrightarrow & B & = & C & \text{(by 8.19(2)).} \end{array}$$

Therefore $B = C$, which proves the claim of the Proposition. □

Definition 8.23. If A admits an inverse we say that A is *invertible*, and denote the inverse by A^{-1}.

Not all matrices are invertible, as the following result shows.

Theorem 8.24. *A square matrix A is invertible if and only if $\det A \neq 0$.*

We will not prove this result here, but give some indication of why it is true.

In order to see that an invertible matrix has nonzero determinant, we quote the following important property of determinants:

Proposition 8.25. *If A and B are square matrices of the same size, then*

$$\det(AB) = \det(A)\det(B).$$

Hence if A is invertible with inverse A^{-1}, we have

$$1 = \det I_n = \det(AA^{-1}) = \det(A)\det(A^{-1}).$$

This shows that $\det A \neq 0$. Note that it also shows that $\det A^{-1} = (\det A)^{-1}$.

In order to see that a matrix A with nonzero determinant is invertible, we will give (in the next subsection) a formula for A^{-1} which is valid whenever $\det A \neq 0$.

8.26. **Matrix Inversion.** We will give two methods for finding the inverse of a square matrix. The first method is sometimes called the *cofactor method*. It is theoretically useful because it gives a closed formula for the inverse of a matrix of any size. Due to the recursive nature of this formula, however, it is inefficient for finding the inverse of larger matrices. We begin by giving some definitions.

Let A be an $(n \times n)$-matrix.

Definition 8.27. Let $1 \leq i, j \leq n$. The (i, j)-th cofactor of A is

$$C_{ij} = (-1)^{i+j} \det A_{ij},$$

where A_{ij} is the (i, j)-th minor of A (see Definition 7.2).

Remark 8.28. The cofactors appeared in the Laplace expansion for the determinant of A (see Theorem 7.6). For any $1 \leq i, j \leq n$ we have

$$\det A = \sum_{k=1}^{n} a_{ik}C_{ik} = \sum_{k=1}^{n} a_{kj}C_{kj}.$$

Definition 8.29. Let $C = [C_{ij}]$ be the matrix of cofactors of A. The *adjugate matrix* of A is the transpose of C:

$$\operatorname{adj} A = C^T = [C_{ji}].$$

Proposition 8.30. *If A is invertible, then its inverse is given by*

$$A^{-1} = \frac{1}{\det A} \operatorname{adj} A.$$

Example 8.31. Use the cofactor method to find the inverse of the matrix

$$A = \begin{bmatrix} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 3 & 2 & 1 \end{bmatrix},$$

if it exists.

We first of all check whether the inverse exists by computing the determinant of A:

$$\begin{aligned} \det A = \begin{vmatrix} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 3 & 2 & 1 \end{vmatrix} &= \begin{vmatrix} 0 & 1 \\ 2 & 1 \end{vmatrix} - \begin{vmatrix} -1 & 1 \\ 3 & 1 \end{vmatrix} \\ &= -2 - (-4) \\ &= 2. \end{aligned}$$

Since the determinant is nonzero, we proceed to compute the cofactors:

$$\begin{aligned} C_{11} &= (-1)^{1+1} \begin{vmatrix} 0 & 1 \\ 2 & 1 \end{vmatrix} & C_{12} &= (-1)^{1+2} \begin{vmatrix} -1 & 1 \\ 3 & 1 \end{vmatrix} & C_{13} &= (-1)^{1+3} \begin{vmatrix} -1 & 0 \\ 3 & 2 \end{vmatrix} \\ &= -2, & &= 4, & &= -2, \\ C_{21} &= (-1)^{2+1} \begin{vmatrix} 1 & 0 \\ 2 & 1 \end{vmatrix} & C_{22} &= (-1)^{2+2} \begin{vmatrix} 1 & 0 \\ 3 & 1 \end{vmatrix} & C_{23} &= (-1)^{2+3} \begin{vmatrix} 1 & 1 \\ 3 & 2 \end{vmatrix} \\ &= -1, & &= 1, & &= 1, \\ C_{31} &= (-1)^{3+1} \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} & C_{32} &= (-1)^{3+2} \begin{vmatrix} 1 & 0 \\ -1 & 1 \end{vmatrix} & C_{33} &= (-1)^{3+3} \begin{vmatrix} 1 & 1 \\ -1 & 0 \end{vmatrix} \\ &= 1, & &= -1, & &= 1. \end{aligned}$$

The matrix of cofactors is

$$C = \begin{bmatrix} -2 & 4 & -2 \\ -1 & 1 & 1 \\ 1 & -1 & 1 \end{bmatrix},$$

therefore the adjugate matrix is

$$\operatorname{adj} A = C^T = \begin{bmatrix} -2 & -1 & 1 \\ 4 & 1 & -1 \\ -2 & 1 & 1 \end{bmatrix}.$$

Finally, the inverse of A is

$$\begin{aligned} A^{-1} &= \frac{1}{\det A} \operatorname{adj} A \\ &= \frac{1}{2}\begin{bmatrix} -2 & -1 & 1 \\ 4 & 1 & -1 \\ -2 & 1 & 1 \end{bmatrix} \\ &= \begin{bmatrix} -1 & -\frac{1}{2} & \frac{1}{2} \\ 2 & \frac{1}{2} & -\frac{1}{2} \\ -1 & \frac{1}{2} & \frac{1}{2} \end{bmatrix}. \end{aligned}$$

It's always worth checking at this stage that we haven't made some arithmetical error, by multiplying A by our proposed A^{-1}:

$$AA^{-1} = \begin{bmatrix} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} -1 & -\frac{1}{2} & \frac{1}{2} \\ 2 & \frac{1}{2} & -\frac{1}{2} \\ -1 & \frac{1}{2} & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

so we're good. ♣

Example 8.32. Use Example 8.31 to solve the system

$$\begin{cases} x_1 + x_2 = 3 \\ -x_1 + x_3 = 4 \\ 3x_1 + 2x_2 + x_3 = -8 \end{cases}.$$

This system in matrix form is

$$\begin{bmatrix} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 3 \\ 4 \\ -8 \end{bmatrix}.$$

Multiplying this equation on the left by the A^{-1} found in Example 8.31, we get

$$\begin{bmatrix} -1 & -\frac{1}{2} & \frac{1}{2} \\ 2 & \frac{1}{2} & -\frac{1}{2} \\ -1 & \frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 3 & 2 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} -1 & -\frac{1}{2} & \frac{1}{2} \\ 2 & \frac{1}{2} & -\frac{1}{2} \\ -1 & \frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} 3 \\ 4 \\ -8 \end{bmatrix},$$

which (since $A^{-1}A = I_3$) gives

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} -9 \\ 12 \\ -5 \end{bmatrix}.$$

Therefore the unique solution to the system is $(x_1, x_2, x_3) = (-9, 12, -5)$. ♣

The second method for finding the inverse of A uses Gaussian Elimination. It is more efficient for larger matrices, involving fewer individual computations. This is the method of matrix inversion used by computer algebra packages. These are the steps:

(1) Write down the augmented matrix $[A \mid I_n]$, with A to the left of the vertical line and the $(n \times n)$ identity matrix to the right.
(2) Perform elementary row operations to bring this matrix to reduced row echelon form.
(3) If the resulting matrix is in the form $[I_n \mid B]$, then $A^{-1} = B$. If the resulting matrix has a row which is zero to the left of the line, then $\det A = 0$ and A is not invertible.

Example 8.33. Find the inverse of the matrix A from Example 8.31 using Gaussian Elimination.

$$\left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 0 & 1 \end{array}\right]_{\substack{r_2+r_1 \\ r_3-3r_1}} \sim \left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & -1 & 1 & -3 & 0 & 1 \end{array}\right]_{r_3+r_2}$$

$$\sim \left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 2 & -2 & 1 & 1 \end{array}\right]_{\frac{1}{2}r_3} \sim \left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & -1 & \frac{1}{2} & \frac{1}{2} \end{array}\right]_{r_2-r_3}$$

$$\sim \left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 2 & \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 1 & -1 & \frac{1}{2} & \frac{1}{2} \end{array}\right]_{r_1-r_2} \sim \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -1 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 0 & 2 & \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 1 & -1 & \frac{1}{2} & \frac{1}{2} \end{array}\right].$$

This is in reduced row echelon form, and to the right of the vertical line is the matrix A^{-1} found in Example 8.31. ♣

Example 8.34. Find the inverse of the matrix

$$B = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 3 \\ 1 & 1 & -1 & 0 \\ -1 & 1 & -1 & 2 \end{bmatrix}$$

if it exists.

Proceeding as before,

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 3 & 0 & 1 & 0 & 0 \\ 1 & 1 & -1 & 0 & 0 & 0 & 1 & 0 \\ -1 & 1 & -1 & 2 & 0 & 0 & 0 & 1 \end{array}\right]_{\substack{r_3-r_1 \\ r_4+r_1}} \sim \left[\begin{array}{cccc|cccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 3 & 0 & 1 & 0 & 0 \\ 0 & 1 & -2 & -1 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 3 & 1 & 0 & 0 & 1 \end{array}\right]_{\substack{r_3-r_2 \\ r_4-r_2}}$$

$$\sim \left[\begin{array}{cccc|cccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 3 & 0 & 1 & 0 & 0 \\ 0 & 0 & -2 & -4 & -1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 1 \end{array}\right].$$

The final row tells us that $\det B = 0$ and so B has no inverse. ♣

Suggestions for further reading:

- http://en.wikipedia.org/wiki/Matrix_(mathematics)
- http://en.wikipedia.org/wiki/Invertible_matrix
- Any book on Linear Algebra, such as H. Anton, *Elementary Linear Algebra*.

9. Geometry of matrices

In this section we will explore the relationship between $(m \times n)$-matrices and linear transformations $\mathbb{R}^n \to \mathbb{R}^m$. We will focus mainly on the case of transformations $\mathbb{R}^2 \to \mathbb{R}^2$, to aid visualization. We shall see that the properties of matrices studied in previous sections can be given concrete geometric meaning.

9.1. **Linear transformations.** Recall that, for $n \in \mathbb{N}$,

$$\mathbb{R}^n = \{(x_1, \dots, x_n) \mid x_i \in \mathbb{R} \text{ for } i = 1, \dots, n\}$$

denotes the set of n-*tuples* of real numbers (ordered lists of n real numbers). Given $n, m \in \mathbb{N}$, a *function* $f\colon \mathbb{R}^n \to \mathbb{R}^m$ is a rule which assigns to each element of the set $\mathbb{R}^n$ a unique element of the set $\mathbb{R}^m$.

Example 9.2. The following are all functions:

(1) $f\colon \mathbb{R}^2 \to \mathbb{R}(= \mathbb{R}^1)$ given by $f(x_1, x_2) = x_1^2 + x_2^2$;
(2) $f\colon \mathbb{R}^n \to \mathbb{R}$ given by $f(x_1, \dots, x_n) = x_1^2 + \dots + x_n^2$;
(3) $f\colon \mathbb{R} \to \mathbb{R}^2$ given by $f(t) = (\cos t, \sin t)$;
(4) $f\colon \mathbb{R}^2 \to \mathbb{R}^3$ given by $f(x_1, x_2) = (x_1 + x_2, 2x_1 - x_2, 0)$.

♣

More generally, suppose we have m functions $f_1, \dots, f_m\colon \mathbb{R}^n \to \mathbb{R}$. Then we can assemble these into a function $f\colon \mathbb{R}^n \to \mathbb{R}^m$ given by

$$f(x_1, \dots, x_n) = \big(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\big).$$

The functions $f_1, \dots, f_m$ are called the *coordinate functions* of f.

Definition 9.3. A function $f\colon \mathbb{R}^n \to \mathbb{R}^m$ as above is called a *linear transformation* if each of its coordinate functions $f_1, \dots, f_m$ is a linear polynomial in the variables $x_1, \dots, x_n$ with zero constant term.

Example 9.4. The following functions are linear transformations:

(1) $f\colon \mathbb{R}^3 \to \mathbb{R}^2$ given by $f(x_1, x_2, x_3) = (5x_1 - \frac{1}{2}x_2, x_1 + x_2 + x_3)$;
(2) $g\colon \mathbb{R}^4 \to \mathbb{R}^1$ given by $f(x_1, x_2, x_3, x_4) = x_1 + 2x_2 + 3x_3 + 4x_4$.

The following functions are not linear transformations:

(3) $h\colon \mathbb{R}^3 \to \mathbb{R}^3$ given by

$$h(x_1, x_2, x_3) = (x_1x_2x_3, x_1x_2 + x_2x_3 + x_3x_1, x_1 + x_2 + x_3);$$

(4) $k\colon \mathbb{R}^2 \to \mathbb{R}^3$ given by $k(x_1, x_2) = (\sin(x_1x_2), \sqrt{x_1^2 + x_2^2}, x_1^2 + x_2^2)$;
(5) $\ell\colon \mathbb{R}^2 \to \mathbb{R}^2$ given by $\ell(x_1, x_2) = (x_1 + x_2 + 3, x_1 - x_2 - 4)$.

♣

9.5. **Matrices and linear transformations.** There is a very tight relationship between linear transformations $f\colon \mathbb{R}^n \to \mathbb{R}^m$ and $(m \times n)$-matrices. To understand it, we will start to view elements of $\mathbb{R}^n$ as *column vectors*

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \in \mathbb{R}^n.$$

Note that such a column vector $\mathbf{x}$ is nothing but an $(n \times 1)$-matrix. Given an $(m \times n)$-matrix A, we can therefore multiply $\mathbf{x}$ on the left by A to obtain an $(m \times 1)$-matrix $A\mathbf{x}$, which can be viewed as an element of $\mathbb{R}^m$. Therefore, left-multiplication by A defines a function

$$f_A\colon \mathbb{R}^n \to \mathbb{R}^m, \qquad f_A(\mathbf{x}) = A\mathbf{x}.$$

Proposition 9.6. *The function f_A associated to the matrix A in this way is a linear transformation. Conversely, any linear transformation $f\colon \mathbb{R}^n \to \mathbb{R}^m$ is given by left-multiplication by some $(m \times n)$-matrix A. We say that f is represented by the matrix A.*

Proof. If $A = [a_{ij}]$ is a general $(m \times n)$-matrix, then

$$\begin{aligned} f_A(\mathbf{x}) &= \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \\ &= \begin{bmatrix} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n \end{bmatrix}. \end{aligned}$$

The coordinate functions of f_A are clearly linear polynomials with zero constant term, and so f_A is a linear transformation.

Conversely, given a linear transformation $f\colon \mathbb{R}^n \to \mathbb{R}^m$, extracting the coefficients of $x_1, \dots, x_n$ in the linear polynomials $f_1, \dots, f_m$ gives an $(m \times n)$-matrix A. It is easily seen that left-multiplication by A represents the function f. □

For any $n \in \mathbb{N}$, the set $\mathbb{R}^n$ carries operations of addition and scalar multiplication. For $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ and $r \in \mathbb{R}$ we have

$$\mathbf{x} + \mathbf{y} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{bmatrix}, \qquad r\mathbf{x} = r\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} rx_1 \\ \vdots \\ rx_n \end{bmatrix}.$$

Here we are viewing elements of $\mathbb{R}^n$ as $(n \times 1)$-matrices, and applying the results of subsection 8.1. The following is often taken as the *definition* of a linear transformation.

Proposition 9.7. *A function $f\colon \mathbb{R}^n \to \mathbb{R}^m$ is a linear transformation if and only if it satisfies the following properties:*

- $f(\mathbf{x}+\mathbf{y}) = f(\mathbf{x}) + f(\mathbf{y})$ *for all* $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$*;*
- $f(r\mathbf{x}) = rf(\mathbf{x})$ *for all* $\mathbf{x} \in \mathbb{R}^n$ *and* $r \in \mathbb{R}$.

That is, f is a linear transformation if and only if it takes the addition and scalar multiplication in $\mathbb{R}^n$ to the addition and scalar multiplication in $\mathbb{R}^m$.

Proof. Let $f\colon \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation. Then f is represented by some matrix A, by Proposition 9.6. Therefore, for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ and $r \in \mathbb{R}$, we have

$$\begin{aligned} f(\mathbf{x}+\mathbf{y}) &= A(\mathbf{x}+\mathbf{y}) \\ &= A\mathbf{x} + A\mathbf{y} \qquad \text{(by property (4) of Proposition 8.12)} \\ &= f(\mathbf{x}) + f(\mathbf{y}), \\ f(r\mathbf{x}) &= A(r\mathbf{x}) \\ &= rA\mathbf{x} \\ &= rf(\mathbf{x}), \end{aligned}$$

and so f satisfies the properties in the Proposition.

Now suppose $f\colon \mathbb{R}^n \to \mathbb{R}^m$ satisfies the properties in the Proposition. We will find a matrix A representing f, hence showing f to be a linear transformation by Proposition 9.6.

For this, we introduce the *standard basis vectors*

$$\mathbf{e_1} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad \mathbf{e_2} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \cdots, \mathbf{e_n} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix},$$

where $\mathbf{e_i}$ for $i = 1, \ldots, n$ has a 1 in the $(i,1)$-th entry and zeroes elsewhere. Note that any $\mathbf{x} \in \mathbb{R}^n$ can be written as a sum of scalar multiples of the standard basis vectors, thus:

$$\mathbf{x} = x_1\mathbf{e_1} + x_2\mathbf{e_2} + \cdots + x_n\mathbf{e_n}.$$

It follows that our f is *completely determined by where it sends the standard basis vectors*, since

$$\begin{aligned} f(\mathbf{x}) &= f(x_1\mathbf{e_1} + x_2\mathbf{e_2} + \cdots + x_n\mathbf{e_n}) \\ &= x_1 f(\mathbf{e_1}) + x_2 f(\mathbf{e_2}) + \cdots + x_n f(\mathbf{e_n}). \end{aligned}$$

Now we form the $(m \times n)$-matrix A whose i-th column is the vector $f(\mathbf{e_i}) \in \mathbb{R}^m$:

$$A = \begin{bmatrix} f(\mathbf{e_1}) & f(\mathbf{e_2}) & \cdots & f(\mathbf{e_n}) \end{bmatrix}.$$

Then for all $\mathbf{x} \in \mathbb{R}^n$,

$$\begin{aligned} A\mathbf{x} &= \begin{bmatrix} f(\mathbf{e_1}) & f(\mathbf{e_2}) & \cdots & f(\mathbf{e_n}) \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \\ &= x_1 f(\mathbf{e_1}) + x_2 f(\mathbf{e_2}) + \cdots + x_n f(\mathbf{e_n}) \\ &= f(\mathbf{x}), \end{aligned}$$

and so A represents f as claimed. $\square$

Note that in the course of the proof we have shown the following.

Corollary 9.8. *Let $f\colon \mathbb{R}^n \to \mathbb{R}^m$ be a linear transformation. Then f is represented by the $(m \times n)$-matrix*

$$A = \begin{bmatrix} f(\mathbf{e_1}) & f(\mathbf{e_2}) & \cdots & f(\mathbf{e_n}) \end{bmatrix}$$

whose i-th column is $f(\mathbf{e_i})$. Here $\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_n}$ are the standard basis vectors of $\mathbb{R}^n$.

9.9. **Compositions and matrix multiplication.** Suppose we're given functions $f\colon \mathbb{R}^n \to \mathbb{R}^m$ and $g\colon \mathbb{R}^m \to \mathbb{R}^\ell$. Then we can *compose* these functions to get a new function

$$g \circ f\colon \mathbb{R}^n \to \mathbb{R}^\ell, \qquad g \circ f(\mathbf{x}) = g\big(f(\mathbf{x})\big).$$

The rule $g \circ f$ applied to a vector $\mathbf{x} \in \mathbb{R}^n$ does the following: We first apply f to $\mathbf{x}$ to get a vector $f(\mathbf{x}) \in \mathbb{R}^m$, then we apply g to this vector to get a vector $g(f(\mathbf{x}))$ in $\mathbb{R}^\ell$. Composition of linear transformations corresponds to matrix multiplication:

Proposition 9.10. *If $f\colon \mathbb{R}^n \to \mathbb{R}^m$ is represented by the $(m \times n)$-matrix A and $g\colon \mathbb{R}^m \to \mathbb{R}^\ell$ is represented by the $(\ell \times m)$-matrix B, then $g \circ f\colon \mathbb{R}^n \to \mathbb{R}^\ell$ is represented by the $(\ell \times n)$-matrix BA.*

Proof. We have

$$\begin{aligned} g \circ f(\mathbf{x}) &= g\big(f(\mathbf{x})\big) \\ &= g(A\mathbf{x}) \\ &= B(A\mathbf{x}) \\ &= (BA)\mathbf{x} \qquad \text{(by property (3) of Proposition 8.12.)} \end{aligned}$$

□

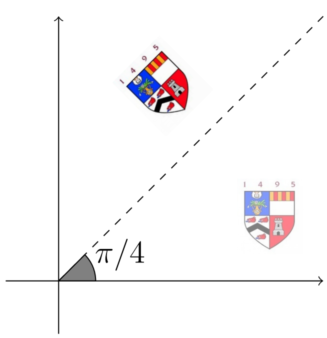
The above Proposition, together with the observation made in subsection 8.7 that matrix multiplication is not commutative in general, illustrates that in general the compositions $g \circ f$ and $f \circ g$ are not the same function.

9.11. **Transformations of the plane.** In this section we will look at some examples of linear transformations $\mathbb{R}^2 \to \mathbb{R}^2$ and their matrices. A column vector $\mathbf{x} = \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^2$ can be viewed geometrically, either as a point in the xy-plane, or as an arrow with tail at the origin and head at the given point. Together with Corollary 9.8, this will aid us in determining the matrices which represent several important types of transformation, including *rotations*, *scalings* and *reflections*.

Rotation matrices. Consider the transformation of the plane

$$R_\theta \colon \mathbb{R}^2 \to \mathbb{R}^2$$

which rotates everything by θ radians anti-clockwise around the origin.

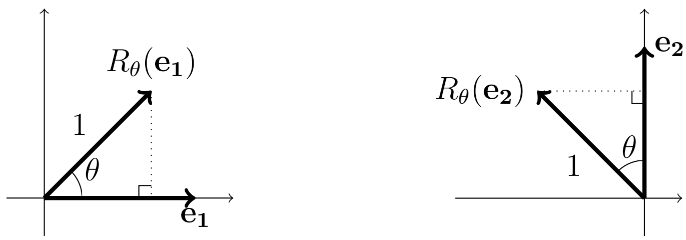


Pictured here is an object together with its image under the transformation $R_{\pi/4}$.

The transformation R_θ is linear, and as such is represented by a (2×2)-matrix. To determine this matrix, we use Corollary 9.8. We need to determine the images $R_\theta(\mathbf{e_1})$ and $R_\theta(\mathbf{e_2})$ of the standard basis vectors

$$\mathbf{e_1} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{and} \quad \mathbf{e_2} = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

as these will form the columns of our matrix.



As indicated by the above pictures, basic trigonometry tells us that

$$R_\theta(\mathbf{e_1}) = \begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix} \quad \text{and} \quad R_\theta(\mathbf{e_2}) = \begin{bmatrix} -\sin\theta \\ \cos\theta \end{bmatrix}.$$

Hence by Corollary 9.8, rotation by θ is represented by the (2×2)-matrix

$$R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

Here we are abusing notation slightly and using the same name for the matrix as the transformation it represents.

Example 9.12. Find the new coordinates of the point $(2,-4)$ after a rotation of the plane through an angle of $\pi/6$ radians clockwise.

Rotation by $\pi/6$ clockwise is rotation by $-\pi/6$ anti-clockwise. So this transformation is represented by the rotation matrix

$$R_{-\pi/6} = \begin{bmatrix} \cos(-\pi/6) & -\sin(-\pi/6) \\ \sin(-\pi/6) & \cos(-\pi/6) \end{bmatrix} = \begin{bmatrix} \sqrt{3}/2 & 1/2 \\ -1/2 & \sqrt{3}/2 \end{bmatrix}.$$

The coordinates of the new point are therefore given by

$$\begin{aligned} R_{-\pi/6}\begin{bmatrix} 2 \\ -4 \end{bmatrix} &= \begin{bmatrix} \sqrt{3}/2 & 1/2 \\ -1/2 & \sqrt{3}/2 \end{bmatrix}\begin{bmatrix} 2 \\ -4 \end{bmatrix} \\ &= \begin{bmatrix} \sqrt{3}-2 \\ -1-2\sqrt{3} \end{bmatrix} \\ &\approx \begin{bmatrix} -0.268 \\ -4.464 \end{bmatrix}. \end{aligned}$$

♣

Example 9.13. Let θ and ϕ be two angles. It is clear that a rotation through θ followed by a rotation through ϕ has the same effect as a single rotation through $\theta+\phi$. Thus the composition $R_\phi \circ R_\theta$ is represented by the same matrix as $R_{\theta+\phi}$. By Proposition 9.10, the matrix representing the composition $R_\phi \circ R_\theta$ is

$$\begin{aligned} R_\phi R_\theta &= \begin{bmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \\ &= \begin{bmatrix} \cos\phi\cos\theta - \sin\phi\sin\theta & -(\cos\phi\sin\theta + \sin\phi\cos\theta) \\ \sin\phi\cos\theta + \cos\phi\sin\theta & \cos\phi\cos\theta - \sin\phi\sin\theta \end{bmatrix}. \end{aligned}$$

Comparing this with the matrix

$$R_{\theta+\phi} = \begin{bmatrix} \cos(\theta+\phi) & -\sin(\theta+\phi) \\ \sin(\theta+\phi) & \cos(\theta+\phi) \end{bmatrix}$$

allows us to derive the well-known angle sum formulae for cosine and sine. ♣

Scaling matrices. Let $a \in \mathbb{R}$, and consider the transformation

$$S_a \colon \mathbb{R}^2 \to \mathbb{R}^2$$

which multiplies every vector in $\mathbb{R}^2$ by a. Such a transformation is called a *scaling* of the plane, with scale factor a.

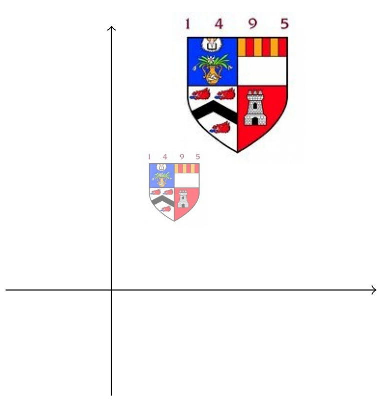
It is easy to see that

$$S_a(\mathbf{e_1}) = \begin{bmatrix} a \\ 0 \end{bmatrix} \qquad \text{and} \qquad S_a(\mathbf{e_2}) = \begin{bmatrix} 0 \\ a \end{bmatrix}.$$

Therefore a scaling with scale factor a is represented by the matrix

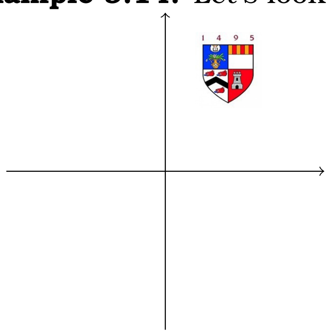
$$S_a = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}.$$

Note that S_a is a times the (2×2) identity matrix.

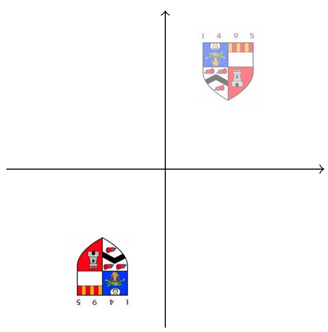


Pictured here is an object together with its image under the transformation S_2.

Example 9.14. Let's look at some special cases.



When $a = 1$, the transformation S_1 is the *identity transformation* which leaves every vector where it is.



When $a = -1$, the transformation S_{-1} negates every vector. Since

$$\begin{aligned} S_{-1} &= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \\ &= \begin{bmatrix} \cos\pi & -\sin\pi \\ \sin\pi & \cos\pi \end{bmatrix} \\ &= R_\pi, \end{aligned}$$

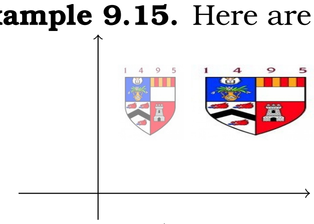
this is the same as rotation through an angle of π radians.

♣

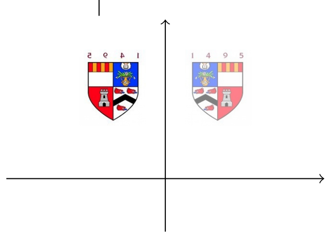
More generally, we can scale the plane by a different scale factor in the direction of each coordinate axis. A scaling which scales by a factor of a in the direction of the x-axis and by a factor of b in the direction of the y-axis is represented by the diagonal matrix

$$S_{a,b} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}.$$

Example 9.15. Here are some examples:



The matrix $S_{2,1} = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ scales by a factor of 2 in the direction of the x-axis.

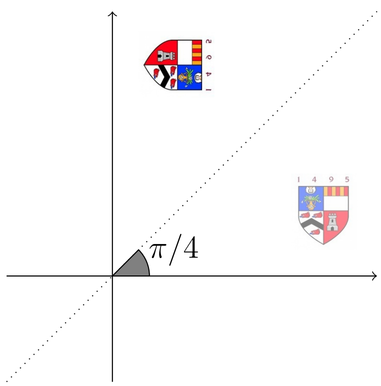


The matrix $S_{-1,1} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ scales by a factor of -1 in the direction of the x-axis. (Note that the orientation of the object has changed under this transformation.)

♣

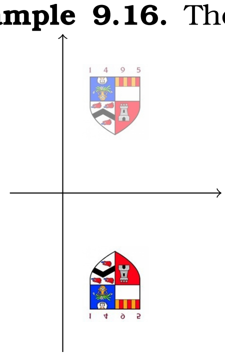
Reflection matrices. We now consider transformations given by reflection in a line through the origin in $\mathbb{R}^2$. Such a line is determined by the angle α it makes with the positive x-axis, measured anti-clockwise in radians. Therefore we have a family of such transformations

$$T_\alpha \colon \mathbb{R}^2 \to \mathbb{R}^2.$$



Pictured here is an object together with its image under the reflection $T_{\pi/4}$.

Example 9.16. The transformation T_0 is reflection in the x-axis.



This has matrix $T_0 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. Note that $T_0 = S_{1,-1}$. ♣

In order to determine the matrix representation of T_α for a general α, we will use Example 9.16 together with Proposition 9.10 and our knowledge of rotation matrices. The general reflection transformation T_α can be viewed as the composition of three transformations:

- Firstly rotate the plane so that the line with angle α becomes the x-axis;
- Next reflect in the x-axis;
- Finally rotate everything back again.

It follows that T_α is the composition $R_\alpha \circ T_0 \circ R_{-\alpha}$. Note the order: the first rotation is through $-\alpha$. Now applying Proposition 9.10 (with three factors) the matrix representation of this reflection is

$$\begin{aligned}
T_\alpha &= R_\alpha T_0 R_{-\alpha} \\
&= \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{bmatrix} \\
&= \begin{bmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{bmatrix} \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix} \\
&= \begin{bmatrix} \cos^2\alpha - \sin^2\alpha & 2\sin\alpha\cos\alpha \\ 2\sin\alpha\cos\alpha & \sin^2\alpha - \cos^2\alpha \end{bmatrix} \\
&= \begin{bmatrix} \cos(2\alpha) & \sin(2\alpha) \\ \sin(2\alpha) & -\cos(2\alpha) \end{bmatrix},
\end{aligned}$$

where at the last step we have used the double angle formulae for $\cos$ and $\sin$.

Example 9.17. Give the new coordinates of the point $(-1, 8)$ after reflection in the line through the origin at angle $\pi/6$.

The matrix representing this reflection is

$$T_{\pi/6} = \begin{bmatrix} \cos(\pi/3) & \sin(\pi/3) \\ \sin(\pi/3) & -\cos(\pi/3) \end{bmatrix} = \begin{bmatrix} 1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{bmatrix}.$$

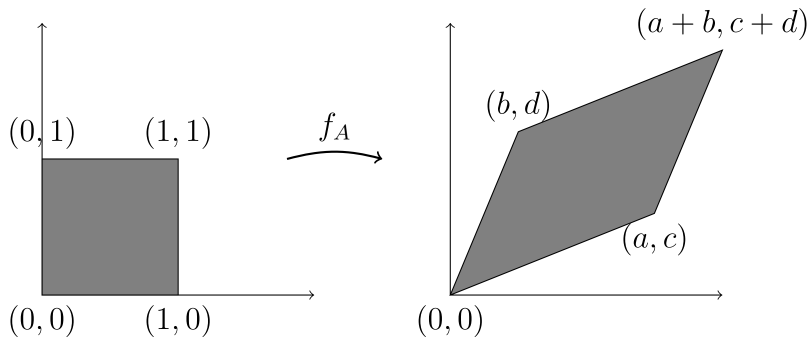
Hence the coordinates of the new point are given by

$$\begin{aligned}
\begin{bmatrix} 1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{bmatrix} \begin{bmatrix} -1 \\ 8 \end{bmatrix} &= \begin{bmatrix} -1/2 + 4\sqrt{3} \\ -\sqrt{3}/2 - 4 \end{bmatrix} \\
&\approx \begin{bmatrix} 6.428 \\ -4.289 \end{bmatrix}
\end{aligned}$$

♣

9.18. **Determinants as scale factors and inversion.** The determinant of a (2×2)-matrix A gives the scale factor by which areas of finite regions in the plane are multiplied under the associated linear transformation f_A. More precisely, the absolute value of the determinant gives the scale factor, and its sign determines whether the orientation of the region gets reversed (the image of the region under a transformation with negative determinant will appear 'flipped', as if we were looking at it in a mirror). This general statement can be made precise using the following result.

Proposition 9.19. *Let $f_A\colon \mathbb{R}^2 \to \mathbb{R}^2$ be the linear transformation associated to the matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. The image under f_A of the square* *with vertices at* $(0, 0)$*,* $(1, 0)$*,* $(0, 1)$ *and* $(1, 1)$ *is a parallelogram with vertices at* $(0, 0)$*,* (a, c)*,* (b, d) *and* $(a + b, c + d)$*.*

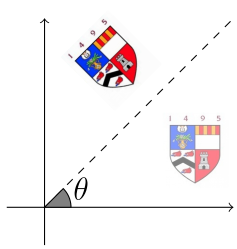


The area of this parallelogram is

- $\det A = ad - bc$ *if the vertices of the parallelogram are met in the order* $(0, 0)$*,* (a, c)*,* $(a + b, c + d)$*,* (b, d) *as we traverse its perimeter in the anti-clockwise direction;*
- $-\det A = bc - ad$ *if the vertices of the parallelogram are met in the order* $(0, 0)$*,* (b, d)*,* $(a + b, c + d)$*,* (a, c) *as we traverse its perimeter in the anti-clockwise direction.*

Remark 9.20. There is a corresponding statement about volume and (3×3)-determinants. More generally, mathematicians have a notion of n*-dimensional volume* for every $n \in \mathbb{N}$, and there is a corresponding statement about this n-dimensional volume and $(n \times n)$-determinants.

Example 9.21. Let's consider how the special matrices from the previous section affect areas.



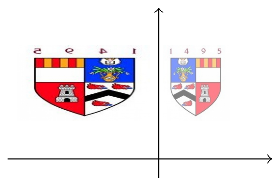
The rotation matrix

$$R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

has determinant

$$\det R_\theta = \cos^2\theta + \sin^2\theta = 1$$

for all θ. Hence rotations preserve area and orientation.



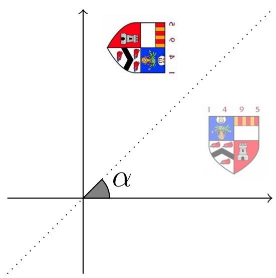
The scaling matrix

$$S_{a,b} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$

has determinant

$$\det S_{a,b} = ab$$

and therefore scales areas by $|ab|$. If ab is negative, the orientation is reversed. Pictured here is the transformation $S_{-2,1}$ with determinant -2.



The reflection matrix

$$T_\alpha = \begin{bmatrix} \cos(2\alpha) & \sin(2\alpha) \\ \sin(2\alpha) & -\cos(2\alpha) \end{bmatrix}$$

has determinant

$$\det T_\alpha = -\cos^2(2\alpha) - \sin^2(2\alpha) = -1$$

for all α. Hence reflections preserve area and reverse orientation.

♣

Suppose the matrix A has $\det A = ad - bc = 0$. This happens exactly when one column of A is a scalar multiple of the other, and so the parallelogram in Proposition 9.19 is *degenerate*; its vertices all lie on a straight line, and its area is 0. Thus the Proposition holds in this case, too.

Definition 9.22. The linear transformation $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ is called *invertible* if there exists a linear transformation $f^{-1}\colon \mathbb{R}^2 \to \mathbb{R}^2$ such that the compositions

$$f \circ f^{-1}\colon \mathbb{R}^2 \to \mathbb{R}^2 \qquad \text{and} \qquad f^{-1} \circ f\colon \mathbb{R}^2 \to \mathbb{R}^2$$

are both equal to the identity transformation (see Example 9.14). The transformation f^{-1} is called the *inverse* of f.

Proposition 9.23. *The linear transformation $f_A\colon \mathbb{R}^2 \to \mathbb{R}^2$ represented by the matrix A is invertible if and only if A is an invertible matrix. In this case, the inverse of f_A is $f_{A^{-1}}$.*

Proof. First suppose that A is invertible with inverse A^{-1}. Then the compositions $f_A \circ f_{A^{-1}}$ and $f_{A^{-1}} \circ f_A$ are represented by the matrices $AA^{-1} = I_2$ and $A^{-1}A = I_2$, and hence are both the identity transformation. This shows that f_A is invertible with inverse $f_{A^{-1}}$.

Conversely, if f_A is invertible with inverse f_A^{-1}, then f_A^{-1} is represented by some matrix B. Since the compositions $f_A \circ f_A^{-1}$ and

$f_A^{-1} \circ f_A$ are both the identity, it follows from Proposition 9.10 that the matrix products AB and BA both equal I_2. Hence $B = A^{-1}$, and A is invertible. $\square$

It stands to reason that a transformation with determinant zero will not be invertible, since it sends regions of positive area to regions of zero area, losing information in the process. What is really happening is that such a transformation *lowers dimension*. We will come back to this later.

Suggestions for further reading:

- http://mathinsight.org/matrices_linear_transformations
- http://mathinsight.org/determinant_linear_transformation
- http://en.wikipedia.org/wiki/Linear_map
- Any book on Linear Algebra, such as H. Anton, *Elementary Linear Algebra*.

10. Eigenvalues and eigenvectors

In the last section we saw that the transformation of the plane associated to the diagonal matrix

$$S_{a,b} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$

produced a scaling by a factor of a in the direction of the x-axis and a scaling by a factor of b in the direction of the y-axis. More generally, given a square matrix A one can often identify certain directions in which the associated linear transformation f_A produces a scaling. A vector which points in such a direction is called an *eigenvector* of A, and the associated scale factor is an *eigenvalue*. Eigenvalues and eigenvectors are important quantities attached to a matrix (the prefix *eigen-* comes from the German for *own-*) with many and varied applications.

Definition 10.1. Let A be an $(n \times n)$-matrix. A nonzero vector $\mathbf{x} \in \mathbb{R}^n$ is called an *eigenvector* of A if there exists a number $\lambda \in \mathbb{R}$ such that

$$A\mathbf{x} = \lambda\mathbf{x}.$$

Such a λ is called the *eigenvalue* of A associated with the eigenvector $\mathbf{x}$.

Remarks 10.2.

(1) The zero vector $\mathbf{0} \in \mathbb{R}^n$ (all of whose entries are zero) satisfies the defining equation $A\mathbf{0} = \lambda\mathbf{0}$ for all $\lambda \in \mathbb{R}$, however it is *not* considered an eigenvector of A (as it's too boring).

(2) We define the eigenvalues and eigenvectors of the linear map $f_A\colon \mathbb{R}^n \to \mathbb{R}^n$ similarly, as solutions of the equation

$$f_A(\mathbf{x}) = \lambda\mathbf{x}.$$

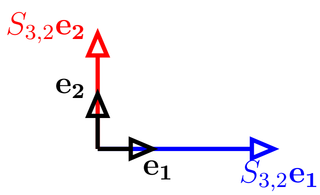
(3) One can also define eigenvalues and eigenvectors of $(n \times n)$ *complex* matrices, in which case an eigenvector is an element of $\mathbb{C}^n$ and an eigenvalue is a complex number.

Observe that if $\mathbf{x}$ is an eigenvector of A with the eigenvalue λ then any nonzero multiple $r\mathbf{x}$, where $0 \neq r \in \mathbb{R}$ is also an eigenvector with the same eigenvalue. Indeed,

$$A(r\mathbf{x}) = rA\mathbf{x} = r\lambda\mathbf{x} = \lambda(r\mathbf{x}).$$

Hence each eigenvalue is associated to infinitely many eigenvectors.

Example 10.3. Consider the scaling matrix $S_{3,2}$.



We have

$$S_{3,2}\mathbf{e_1} = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 0 \end{bmatrix} = 3\mathbf{e_1},$$

which shows that $\mathbf{e_1}$ is an eigenvector of $S_{3,2}$ with associated eigenvalue 3. Any nonzero multiple $r\mathbf{e_1}$, $0 \neq r \in \mathbb{R}$ is also an eigenvector with eigenvalue 3.

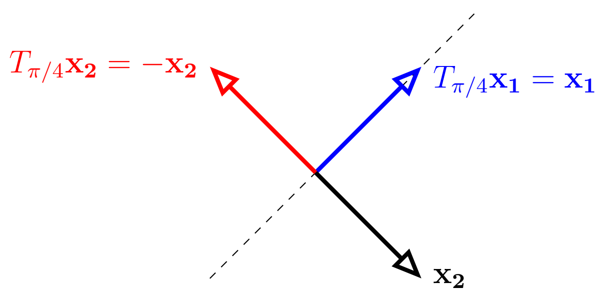
Similarly,

$$S_{3,2}\mathbf{e_2} = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 2 \end{bmatrix} = 2\mathbf{e_2},$$

so $\mathbf{e_2}$ is an eigenvector with associated eigenvalue 2. So is $s\mathbf{e_2}$ for any $0 \neq s \in \mathbb{R}$.

♣

Example 10.4. Consider the reflection matrix $T_{\pi/4}$.



This leaves fixed all vectors on the line $x = y$, so every vector of the form

$$\mathbf{x_1} = \begin{bmatrix} r \\ r \end{bmatrix}, \quad 0 \neq r \in \mathbb{R}$$

is an eigenvector with associated eigenvalue 1.

Any vector perpendicular to the line $x = y$ gets sent to its negative, and hence every vector of the form

$$\mathbf{x_2} = \begin{bmatrix} s \\ -s \end{bmatrix}, \quad 0 \neq s \in \mathbb{R}$$

is an eigenvector with associated eigenvalue -1. ♣

Example 10.5. The rotation matrix R_θ has no eigenvectors whatsoever, unless $\theta = 0$, in which case every nonzero $\mathbf{x} \in \mathbb{R}^2$ is an eigenvector with eigenvalue 1, or $\theta = \pi$, in which case every nonzero $\mathbf{x} \in \mathbb{R}^2$ is an eigenvector with eigenvalue -1. ♣

10.6. **How to find the eigenvalues.** We now describe a procedure for finding the eigenvalues and eigenvectors of an $(n \times n)$-matrix A. The first step is to find the eigenvalues. Note that we can rewrite the defining equation (by subtracting $\lambda \mathbf{x} = \lambda I_n \mathbf{x}$ from both sides) as follows:

$$\begin{aligned} A\mathbf{x} &= \lambda \mathbf{x} \\ \iff \quad A\mathbf{x} - \lambda I_n \mathbf{x} &= \mathbf{0} \\ \iff \quad (A - \lambda I_n)\mathbf{x} &= \mathbf{0}. \end{aligned}$$

This final matrix equation can be viewed as a linear system. Since the right-hand sides are all zero, we will always have $\mathbf{x} = \mathbf{0}$ as a solution. We want to know for which values of λ the system has nonzero solutions $\mathbf{x} \neq \mathbf{0}$, since such solutions will be eigenvectors with associated eigenvalue λ. The answer depends on the determinant $\det(A - \lambda I_n)$, which is a polynomial in λ.

Definition 10.7. The polynomial

$$p_A(\lambda) = \det(A - \lambda I_n)$$

is called the *characteristic polynomial* of A, and the resulting polynomial equation

$$\det(A - \lambda I_n) = 0$$

is called the *characteristic equation* of A.

Proposition 10.8. *The eigenvalues of A are the roots of $p_A(\lambda)$.* $\square$

Example 10.9. Find the eigenvalues of the matrix $A = \begin{bmatrix} 3 & -1 \\ 2 & 0 \end{bmatrix}$.

The eigenvalues are the roots of the characteristic polynomial

$$\begin{aligned} p_A(\lambda) &= \det(A - \lambda I_2) \\ &= \begin{vmatrix} 3-\lambda & -1 \\ 2 & -\lambda \end{vmatrix} \\ &= (3-\lambda)(-\lambda) + 2 \\ &= \lambda^2 - 3\lambda + 2 \\ &= (\lambda - 1)(\lambda - 2). \end{aligned}$$

Hence the eigenvalues are $\lambda = 1$ and $\lambda = 2$. ♣

Example 10.10. Find the eigenvalues of the matrix $B = \begin{bmatrix} 4 & 0 & 1 \\ -2 & 1 & 0 \\ -2 & 0 & 1 \end{bmatrix}$.

The characteristic polynomial is

$$\begin{aligned}
p_B(\lambda) &= \det(B - \lambda I_3) \\
&= \begin{vmatrix} 4-\lambda & 0 & 1 \\ -2 & 1-\lambda & 0 \\ -2 & 0 & 1-\lambda \end{vmatrix} \\
&= (1-\lambda)\big[(4-\lambda)(1-\lambda)+2\big] \quad \text{(expanding around the 2}^{\text{nd}}\text{ column)} \\
&= (1-\lambda)(\lambda^2 - 5\lambda + 6) \\
&= (1-\lambda)(\lambda-2)(\lambda-3).
\end{aligned}$$

Hence the eigenvalues are $\lambda = 1$, $\lambda = 2$ and $\lambda = 3$. ♣

The eigenvalues of a real $(n \times n)$-matrix are the real roots of its characteristic polynomial, a real polynomial of degree n. Hence there are at most n eigenvalues. It may happen that the characteristic polynomial has complex roots — we will not consider these as eigenvalues (although in the analogous theory of complex matrices and linear maps $f\colon \mathbb{C}^n \to \mathbb{C}^n$, they would be considered as such).

Example 10.11. Returning to the rotation matrix R_θ, its characteristic polynomial is

$$\begin{aligned}
\begin{vmatrix} \cos\theta - \lambda & -\sin\theta \\ \sin\theta & \cos\theta - \lambda \end{vmatrix} &= (\cos\theta - \lambda)^2 + \sin^2\theta \\
&= \lambda^2 - 2\lambda\cos\theta + \cos^2\theta + \sin^2\theta \\
&= \lambda^2 - 2\lambda\cos\theta + 1,
\end{aligned}$$

the roots of which are found by the quadratic formula to be

$$\lambda = \frac{2\cos\theta \pm \sqrt{4(\cos^2\theta - 1)}}{2} = \frac{2\cos\theta \pm \sqrt{-4\sin^2\theta}}{2} = \cos\theta \pm i\sin\theta.$$

Hence the eigenvalues are real precisely when $\sin\theta = 0$, so when θ is an integer multiple of π (compare Example 10.5 above). ♣

10.12. **Finding the eigenvectors associated to an eigenvalue.** Suppose we have found λ to be an eigenvalue of the $(n \times n)$-matrix A. An eigenvector associated to λ is then a nonzero solution $\mathbf{x}$ to the equation

$$(A - \lambda I_n)\mathbf{x} = \mathbf{0}.$$

The fact that λ is an eigenvalue means precisely that such solutions exist. So finding the eigenvectors boils down to solving a linear system.

Example 10.13. Find the eigenvectors of the matrix $A = \begin{bmatrix} 3 & -1 \\ 2 & 0 \end{bmatrix}$ corresponding to the eigenvalues $\lambda = 1$ and $\lambda = 2$ found in Example 10.9.

When $\lambda = 1$ we have

$$A - \lambda I_2 = A - I_2 = \begin{bmatrix} 2 & -1 \\ 2 & -1 \end{bmatrix},$$

so the eigenvectors are nonzero solutions of the system

$$\left\{ \begin{array}{rcrcl} 2x_1 & - & x_2 & = & 0 \\ 2x_1 & - & x_2 & = & 0 \end{array} \right. .$$

By inspection, this is equivalent to $x_2 = 2x_1$. We may then consider $x_1 = s$ as a free parameter, and the eigenvectors associated to $\lambda = 1$ are all vectors of the form

$$\begin{bmatrix} s \\ 2s \end{bmatrix} = s \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \quad 0 \neq s \in \mathbb{R}.$$

When $\lambda = 2$ we have

$$A - \lambda I_2 = A - 2I_2 = \begin{bmatrix} 1 & -1 \\ 2 & -2 \end{bmatrix},$$

so the eigenvectors are nonzero solutions of the system

$$\left\{ \begin{array}{rcrcl} x_1 & - & x_2 & = & 0 \\ 2x_1 & - & 2x_2 & = & 0 \end{array} \right. .$$

By inspection, this is equivalent to $x_2 = x_1$. The eigenvectors associated to $\lambda = 2$ are all vectors of the form

$$\begin{bmatrix} t \\ t \end{bmatrix} = t \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad 0 \neq t \in \mathbb{R}.$$

♣

Example 10.14. Find the eigenvectors of the matrix $B = \begin{bmatrix} 4 & 0 & 1 \\ -2 & 1 & 0 \\ -2 & 0 & 1 \end{bmatrix}$ corresponding to the eigenvalues $\lambda = 1, 2, 3$ found in Example 10.10.

When $\lambda = 1$, the eigenvectors solve the system

$$\begin{bmatrix} 3 & 0 & 1 \\ -2 & 0 & 0 \\ -2 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

The second and third rows give $x_1 = 0$, which on substitution into the first row gives $x_3 = 0$. This leaves x_2 as a free variable. So the eigenvectors associated to $\lambda = 1$ are

$$\begin{bmatrix} 0 \\ s \\ 0 \end{bmatrix} = s \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad 0 \neq s \in \mathbb{R}.$$

When $\lambda = 2$, the eigenvectors solve the system

$$\begin{bmatrix} 2 & 0 & 1 \\ -2 & -1 & 0 \\ -2 & 0 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

The first and third rows give $x_3 = -2x_1$, and the second row gives $x_2 = -2x_1$. Treating x_1 as a free variable, we see that the eigenvectors associated to $\lambda = 2$ are

$$\begin{bmatrix} t \\ -2t \\ -2t \end{bmatrix} = t \begin{bmatrix} 1 \\ -2 \\ -2 \end{bmatrix}, \quad 0 \neq t \in \mathbb{R}.$$

Finally, when $\lambda = 3$ the eigenvectors solve the system

$$\begin{bmatrix} 1 & 0 & 1 \\ -2 & -2 & 0 \\ -2 & 0 & -2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

The first and third rows give $x_3 = -x_1$, and the second row gives $x_2 = -x_1$, so the eigenvectors associated to $\lambda = 3$ are

$$\begin{bmatrix} u \\ -u \\ -u \end{bmatrix} = u \begin{bmatrix} 1 \\ -1 \\ -1 \end{bmatrix}, \quad 0 \neq u \in \mathbb{R}.$$

♣

It can happen that the characteristic polynomial has a repeated root λ. In that case, the eigenvectors associated to the eigenvalue λ may not all be scalar multiples of each other.

Example 10.15. Find the eigenvalues and associated eigenvectors of the matrix

$$C = \begin{bmatrix} 1 & 0 & 2 \\ 2 & 3 & -2 \\ 4 & 0 & -1 \end{bmatrix}.$$

The eigenvalues are the roots of

$$\begin{aligned}\begin{vmatrix}1-\lambda & 0 & 2\\ 2 & 3-\lambda & -2\\ 4 & 0 & -1-\lambda\end{vmatrix} &= (3-\lambda)\big[(1-\lambda)(-1-\lambda)-8\big]\\ &= (3-\lambda)(\lambda^2-9)\\ &= (3-\lambda)(\lambda-3)(\lambda+3),\end{aligned}$$

so the eigenvalues are $\lambda = -3$ and $\lambda = 3$ (with multiplicity 2).

The eigenvectors associated to $\lambda = -3$ are nonzero solutions of the system

$$\begin{bmatrix}4 & 0 & 2\\ 2 & 6 & -2\\ 4 & 0 & 2\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix} = \begin{bmatrix}0\\ 0\\ 0\end{bmatrix}$$
$$\sim \begin{bmatrix}2 & 6 & -2\\ 0 & -12 & 6\\ 0 & 0 & 0\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix} = \begin{bmatrix}0\\ 0\\ 0\end{bmatrix}$$

which is easily solved by back-substitution, giving $x_3 = 2x_2$ and $x_1 = -x_2$. These eigenvectors are therefore of the form

$$\begin{bmatrix}-s\\ s\\ 2s\end{bmatrix} = s\begin{bmatrix}-1\\ 1\\ 2\end{bmatrix}, \quad 0 \neq s \in \mathbb{R}.$$

The eigenvalues associated to the repeated eigenvalue $\lambda = 3$ are nonzero solutions to the system

$$\begin{bmatrix}-2 & 0 & 2\\ 2 & 0 & -2\\ 4 & 0 & -4\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix} = \begin{bmatrix}0\\ 0\\ 0\end{bmatrix}$$
$$\sim \begin{bmatrix}-2 & 0 & 2\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\end{bmatrix} = \begin{bmatrix}0\\ 0\\ 0\end{bmatrix}$$

which is solved by $x_1 = x_3$. Letting x_1 and x_2 be free parameters, we have that the eigenvalues are of the form

$$\begin{bmatrix}t\\ u\\ t\end{bmatrix} = t\begin{bmatrix}1\\ 0\\ 1\end{bmatrix} + u\begin{bmatrix}0\\ 1\\ 0\end{bmatrix}, \quad 0 \neq t, u \in \mathbb{R}.$$

Here there are two types of eigenvector, corresponding to two different directions in which the matrix C produces a scaling with scale factor 3. We say that the *eigenspace* associated to the eigenvalue $\lambda = 3$ is two-dimensional. ♣

10.16. **More about the characteristic equation.**

Proposition 10.17. *A square matrix A is invertible if and only if it does not have $\lambda = 0$ as an eigenvalue.*

Proof. We can write the characteristic polynomial in the form

$$p_A(\lambda) = \det(A - \lambda I_n) = (-1)^n \lambda^n + c_{n-1}\lambda^{n-1} + \cdots + c_1\lambda + c_0,$$

where the $c_i \in \mathbb{R}$ are the coefficients. [Why is the leading coefficient always $(-1)^n$?] Upon setting $\lambda = 0$, we get

$$p_A(0) = \det(A) = c_0.$$

Thus *the constant term of $p_A(\lambda)$ is the determinant of A.* It follows that 0 is not a root of $p_A(\lambda)$ if and only if $\det(A) \neq 0$. $\square$

The above proof raises the question of whether the remaining coefficients in the characteristic polynomial $p_A(\lambda)$ can be expressed in terms of known quantities associated to the matrix A. We'll give the answer in the (2×2)-case.

Definition 10.18. The *trace* of an $(n \times n)$-matrix $A = [a_{ij}]$, denoted $\mathrm{tr}(A)$, is the sum of its diagonal entries:

$$\mathrm{tr}(A) = a_{11} + a_{22} + \cdots + a_{nn} = \sum_{i=1}^{n} a_{ii}.$$

Proposition 10.19. *The characteristic polynomial of a (2×2)-matrix A is given by*

$$p_A(\lambda) = \lambda^2 - \mathrm{tr}(A)\lambda + \det(A).$$

Proof. Exercise! $\square$

Given any square matrix A, we can take its powers

$$A^k = \underbrace{A \times A \times \cdots \times A}_{k \text{ times}}, \qquad k \in \mathbb{N}.$$

Now given any real polynomial

$$p(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0,$$

it makes sense to evaluate this polynomial *at the matrix A*, thus:

$$p(A) = c_n A^n + c_{n-1}A^{n-1} + \cdots c_1 A + c_0 I_n.$$

Notice that the constant term gets multiplied by the identity matrix of the appropriate size, so that this expression is defined as a matrix sum.

We can now state the following curious result from Linear Algebra.

Theorem 10.20 (The Cayley–Hamilton Theorem)**.** *Any square matrix satisfies its own characteristic equation. That is, if A is a square matrix with characteristic polynomial $p_A(\lambda)$, then $p_A(A) = 0$, the zero matrix.*

There is a famous bogus proof of this Theorem which goes along the lines of

$$p_A(A) = \det(A - AI_n) = \det(0) = 0.$$

To see why this is wrong, we just have to remember that $p_A(A)$ is a matrix, while the determinant is a scalar.

Example 10.21. The Cayley–Hamilton Theorem is not just a curiosity. It can be used to calculate powers of square matrices. Take for example the matrix

$$A = \begin{bmatrix} 3 & -1 \\ 2 & 0 \end{bmatrix}$$

from Example 10.9. It satisfies its own characteristic equation, meaning

$$p_A(A) = A^2 - 3A + 2I_2 = 0,$$

or equivalently,

$$A^2 = 3A - 2I_2.$$

Multiplying this equation repeatedly by A on the left, we find

$$A^3 = 3A^2 - 2A, \quad A^4 = 3A^3 - 2A^2, \quad A^5 = 3A^4 - 2A^3, \ldots.$$

This gives a recursive method to calculate powers of A, without actually doing any matrix multiplication! One can easily check using this method that

$$A^2 = \begin{bmatrix} 7 & -3 \\ 6 & -2 \end{bmatrix}, \quad A^3 = \begin{bmatrix} 15 & -7 \\ 14 & -6 \end{bmatrix}, \ldots.$$

♣

Suggestions for further reading:

- http://en.wikipedia.org/wiki/Eigenvalues_and_eigenvectors
- Any book on Linear Algebra, such as H. Anton, *Elementary Linear Algebra*.

11. Diagonalization and diagonalizability

Recall from Section 9.11 that we computed the reflection matrix T_α as a matrix product

$$\begin{aligned} T_\alpha &= R_\alpha \, T_0 \, R_{-\alpha} \\ &= \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}. \end{aligned}$$

This technique is quite prevalent in Linear Algebra, and is called making a *change of basis*. Writing down the matrix T_α directly was difficult because the standard coordinate axes were not suited to the task at hand. By rotating the plane through $-\alpha$ we effectively chose new coordinates in which we were able to solve the problem. Then by rotating the plane back again through α, we converted the answer to our easier problem into an answer to our original, harder problem.

Since it is easily verified that $R_{-\alpha} = (R_\alpha)^{-1}$, what we have actually used is that the matrix T_α is *similar* to the diagonal matrix T_0.

Definition 11.1. Let A and B be square matrices of the same size. We say that B is *similar* to A if there exists some invertible matrix P such that

$$B = P^{-1}AP.$$

It follows that A is similar to B, since

$$A = PBP^{-1}$$

and P^{-1} is an invertible matrix with $(P^{-1})^{-1} = P$. We may therefore say that the matrices A and B are *similar*.

Similar matrices share a lot of the same properties.

Proposition 11.2. *Let A and B be similar matrices. Then*

(1) A and B have the same determinant;
(2) A is invertible if and only if B is invertible;
(3) A and B have the same characteristic polynomial;
(4) A and B have the same eigenvalues;
(5) A and B have the same trace.

The proofs of (1) and (3) are straightforward, and the other statements follow from these two.

Diagonal matrices form a particularly nice class of matrices for which many quantities associated to the matrix (such as its determinant, inverse, eigenvalues and eigenvectors) can be read off directly. It is therefore often useful to know that a matrix is similar to a diagonal matrix.

Definition 11.3. A square matrix A is called *diagonalizable* if it is similar to a diagonal matrix D. If P is an invertible matrix such that $P^{-1}AP = D$ then P is said to *diagonalize* A.

The question arises, which matrices are diagonalizable? And how do we find a diagonalizing matrix? The answer lies in the eigenvalues and eigenvectors.

11.4. **A criterion for diagonalizability.**

Theorem 11.5. *Let A be an $(n \times n)$-matrix. Then A is diagonalizable if and only if there is an invertible matrix*

$$P = \begin{bmatrix} \mathbf{x_1} & \mathbf{x_2} & \cdots & \mathbf{x_n} \end{bmatrix}$$

whose columns are eigenvectors of A. If such a P exists, then

$$P^{-1}\,A\,P = \begin{bmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{bmatrix}$$

where for $i = 1, \dots, n$ the diagonal entry λ_i is the eigenvalue associated to the eigenvector $\mathbf{x_i}$.

Proof. Suppose there is an invertible matrix $P = \begin{bmatrix} \mathbf{x_1} & \mathbf{x_2} & \cdots & \mathbf{x_n} \end{bmatrix}$ whose columns are eigenvectors of A, and let $\lambda_1, \lambda_2, \dots \lambda_n$ be associated eigenvalues. Then

$$\begin{aligned} A\,P &= A\begin{bmatrix} \mathbf{x_1} & \mathbf{x_2} & \cdots & \mathbf{x_n} \end{bmatrix} \\ &= \begin{bmatrix} A\mathbf{x_1} & A\mathbf{x_2} & \cdots & A\mathbf{x_n} \end{bmatrix} \\ &= \begin{bmatrix} \lambda_1\mathbf{x_1} & \lambda_2\mathbf{x_2} & \cdots & \lambda_n\mathbf{x_n} \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{x_1} & \mathbf{x_2} & \cdots & \mathbf{x_n} \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{bmatrix} \\ &= P\,D, \end{aligned}$$

where D is the diagonal matrix of eigenvalues as in the statement of the Theorem. Since P is invertible, we can multiply both sides of this equation on the left by P^{-1}, giving $P^{-1}AP = D$ as claimed.

Now suppose A is diagonalizable. Thus there is an invertible matrix P and diagonal matrix D such that $P^{-1}AP = D$. Multiplying on the left by P gives $AP = PD$. Write

$$P = \begin{bmatrix} \mathbf{p_1} & \mathbf{p_2} & \cdots & \mathbf{p_n} \end{bmatrix} \quad \text{and} \quad D = \begin{bmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_n \end{bmatrix}.$$

Then $AP = \begin{bmatrix} A\mathbf{p_1} & A\mathbf{p_2} & \cdots & A\mathbf{p_n} \end{bmatrix}$ and

$$\begin{aligned} PD &= \begin{bmatrix} \mathbf{p_1} & \mathbf{p_2} & \cdots & \mathbf{p_n} \end{bmatrix} \begin{bmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_n \end{bmatrix} \\ &= \begin{bmatrix} d_1\mathbf{p_1} & d_2\mathbf{p_2} & \cdots & d_n\mathbf{p_n} \end{bmatrix}. \end{aligned}$$

Comparing columns of AP and PD, we see that $A\mathbf{p_i} = d_i\mathbf{p_i}$ for $i = 1, \dots, n$. Since P is invertible, its columns are all nonzero. Hence they are eigenvectors of A with eigenvalues the diagonal entries d_i of D. □

The above theorem gives a procedure for diagonalizing an $(n \times n)$-matrix:

(1) Find n eigenvectors $\mathbf{x_1}, \dots, \mathbf{x_n}$ of A which form the columns of an invertible matrix P (if possible).
(2) The matrix $P^{-1}AP$ will then be diagonal with diagonal entries $\lambda_1, \dots, \lambda_n$ the corresponding eigenvalues.

Example 11.6. Diagonalize the matrix

$$B = \begin{bmatrix} 4 & 0 & 1 \\ -2 & 1 & 0 \\ -2 & 0 & 1 \end{bmatrix}$$

from Example 10.10.

We already found in Examples 10.10 and 10.14 the eigenvalues and associated eigenvectors:

$$\lambda = 1: \quad \begin{bmatrix} 0 \\ s \\ 0 \end{bmatrix}, \qquad \lambda = 2: \quad \begin{bmatrix} t \\ -2t \\ -2t \end{bmatrix}, \qquad \lambda = 3: \quad \begin{bmatrix} u \\ -u \\ -u \end{bmatrix}$$

There are many possible choices for the columns of P. If we choose the simplest possible eigenvectors (i.e, take $s = t = u = 1$) we get

$$P = \begin{bmatrix} 0 & 1 & 1 \\ 1 & -2 & -1 \\ 0 & -2 & -1 \end{bmatrix}$$

which is invertible with inverse

$$P^{-1} = \begin{bmatrix} 0 & 1 & -1 \\ -1 & 0 & -1 \\ 2 & 0 & 1 \end{bmatrix}$$

(check for yourself!). According to Theorem 11.5, we should have $P^{-1}BP = D$ where D is the diagonal matrix with the eigenvalues of B on the diagonal. One easily checks that

$$\begin{bmatrix} 0 & 1 & -1 \\ -1 & 0 & -1 \\ 2 & 0 & 1 \end{bmatrix} \begin{bmatrix} 4 & 0 & 1 \\ -2 & 1 & 0 \\ -2 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & -2 & -1 \\ 0 & -2 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}$$

as claimed.

Note that we could choose to write the columns of P in a different order. We would still get a diagonalizing matrix, and the eigenvalues showing up on the diagonal would be ordered correspondingly. For instance, we could take

$$P' = \begin{bmatrix} 1 & 0 & 1 \\ -2 & 1 & -1 \\ -2 & 0 & -1 \end{bmatrix}$$

as our diagonalizing matrix, giving

$$(P')^{-1}BP' = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{bmatrix}.$$

♣

It is not always possible to find an invertible matrix P whose columns are eigenvectors, as the following example shows.

Example 11.7. Show that the matrix

$$U = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

is not diagonalizable.

Since U is upper-triangular, one sees by inspection that the characteristic polynomial is $p_U(\lambda) = (1-\lambda)^3$. Hence there is only one eigenvalue $\lambda = 1$ with multiplicity 3. The eigenvectors solve

$$\begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

and so are of the form $\begin{bmatrix} s \\ 0 \\ 0 \end{bmatrix} = s \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ where $0 \neq s \in \mathbb{R}$. Since all of the eigenvectors are scalar multiples of each other, any matrix whose columns are formed from the eigenvectors will have determinant zero. Therefore U is not diagonalizable. ♣.

To make precise what's going on here, we introduce the important notion of linear independence.

Definition 11.8. A set of vectors $\{\mathbf{v_1}, \dots, \mathbf{v_r}\}$ in $\mathbb{R}^n$ is said to be *linearly independent* if no vector in the set can be written as a sum of scalar multiples of the other vectors in the set. More formally, the set $\{\mathbf{v_1}, \dots, \mathbf{v_r}\}$ is linearly independent if whenever we have an equality of the form

$$k_1\mathbf{v_1} + \cdots + k_r\mathbf{v_r} = \mathbf{0}, \qquad k_i \in \mathbb{R}$$

it follows that $k_1 = \cdots = k_r = 0$. A set of vectors which is not linearly independent is called *linearly dependent*.

To see the equivalence of the two definitions, suppose we have an equality

$$k_1\mathbf{v_1} + k_2\mathbf{v_2} + \cdots + k_r\mathbf{v_r} = \mathbf{0}$$

where the k_i are not all zero (so that the set $\{\mathbf{v_1}, \dots, \mathbf{v_r}\}$ is linearly dependent). We can assume, without loss of generality, that k_1 is nonzero. Then we can rearrange to get

$$\mathbf{v_1} = -\frac{k_2}{k_1}\mathbf{v_2} - \cdots - \frac{k_r}{k_1}\mathbf{v_r}$$

which shows that $\mathbf{v_1}$ is a sum of multiples of the other vectors in the set. Conversely, if, say,

$$\mathbf{v_1} = \ell_2\mathbf{v_2} + \cdots + \ell_r\mathbf{v_r}$$

is a sum of scalar multiples of the other vectors in the set, then we have an equality of the form

$$\ell_1\mathbf{v_1} - \ell_2\mathbf{v_2} - \cdots - \ell_r\mathbf{v_r} = \mathbf{0}$$

where $\ell_1 = 1 \neq 0$.

Example 11.9. The vectors

$$\mathbf{e_1} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \qquad \mathbf{e_2} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \qquad \mathbf{e_3} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

form a linearly independent set in $\mathbb{R}^3$. For suppose $k_1, k_2, k_3 \in \mathbb{R}$ and

$$k_1\mathbf{e_1} + k_2\mathbf{e_2} + k_3\mathbf{e_3} = \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

Then it follows that $k_1 = k_2 = k_3 = 0$. ♣

Example 11.10. The vectors

$$\mathbf{v_1} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \qquad \mathbf{v_2} = \begin{bmatrix} 0 \\ 1 \\ -1 \end{bmatrix}, \qquad \mathbf{v_2} = \begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix}$$

form a linearly dependent set in $\mathbb{R}^3$. To see this, it suffices to note that $3\mathbf{v_1} - \mathbf{v_2} = \mathbf{v_3}$. ♣

Lemma 11.11. *Let $P = \begin{bmatrix} \mathbf{v_1} & \cdots & \mathbf{v_n} \end{bmatrix}$ be an $(n \times n)$-matrix. Then P is invertible if and only if the set of columns $\{\mathbf{v_1}, \ldots, \mathbf{v_n}\}$ is a linearly independent set in $\mathbb{R}^n$.*

Proof. We know from our study of linear systems that P is invertible if and only if the linear system $P\mathbf{x} = \mathbf{0}$ has only the trivial solution $\mathbf{x} = \mathbf{0}$. We can write this linear system as

$$x_1\mathbf{v_1} + x_2\mathbf{v_2} + \cdots + x_n\mathbf{v_n} = \mathbf{0}.$$

To say that $x_1 = x_2 = \cdots = x_n = 0$ is the only solution is precisely the same as saying that the set $\{\mathbf{v_1}, \ldots, \mathbf{v_n}\}$ of columns of P is linearly independent. □

Theorem 11.12. *An $(n \times n)$-matrix A is diagnonalizable if and only if it admits n linearly independent eigenvectors.*

Proof. This follows immediately from Theorem 11.5 and Lemma 11.11. □

Proposition 11.13. *Let $\mathbf{x_1}, \ldots, \mathbf{x_r}$ be eigenvectors of the $(n \times n)$-matrix A corresponding to distinct eigenvalues $\lambda_1, \ldots, \lambda_r$. Then $\{\mathbf{x_1}, \ldots, \mathbf{x_r}\}$ is a linearly independent set in $\mathbb{R}^n$.*

Proof. Not given. □

Corollary 11.14. *If an $(n \times n)$-matrix A has n distinct real eigenvalues, then A is diagonalizable.*

The converse to this result would say that a diagonalizable matrix has $(n \times n)$-matrix has n distinct eigenvalues. This is false, as the following example shows.

Example 11.15. Recall the matrix

$$C = \begin{bmatrix} 1 & 0 & 2 \\ 2 & 3 & -2 \\ 4 & 0 & -1 \end{bmatrix}$$

from Example 10.15. The eigenvalues and corresponding eigenvectors were found there to be

$$\lambda = -3: \quad \begin{bmatrix} -s \\ s \\ 2s \end{bmatrix}, \qquad \lambda = 3: \quad \begin{bmatrix} t \\ u \\ t \end{bmatrix} = t \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} + u \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}.$$

The eigenvectors $\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ corresponding to the repeated eigenvalue $\lambda = 3$ are clearly linearly independent, and so

$$P = \begin{bmatrix} -1 & 1 & 0 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix}$$

is a diagonalizing matrix for C. ♣

11.16. **Applications of diagonalization.** We now begin to reap the rewards of our hard work. The first application of diagonalization is to computing large powers of square matrices. We first note that computing powers of diagonal matrices is easy.

Lemma 11.17. *Let*

$$D = \begin{bmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{bmatrix}$$

be a diagonal matrix, and let $k \in \mathbb{N}$ be a natural number. Then

$$D^k = \begin{bmatrix} \lambda_1^k & 0 & \dots & 0 \\ 0 & \lambda_2^k & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n^k \end{bmatrix}.$$

Proof. By induction on k and the definition of matrix multiplication. We omit the details. □

Now suppose that the square matrix A is diagonalizable, with diagonalizing matrix P. This means that $P^{-1}AP = D$, where D is a diagonal matrix. Left-multiplying by P and right-multiplying by P^{-1}, we obtain

$$A = PDP^{-1}.$$

This enables easier computation of the powers A^k for $k \in \mathbb{N}$, since we have

$$\begin{aligned} A^k &= \underbrace{(PDP^{-1})(PDP^{-1}) \cdots (PDP^{-1})}_{k \text{ times}} \\ &= PD(P^{-1}P)D(P^{-1}P) \cdots D(P^{-1}P)DP^{-1} \\ &= P\underbrace{DIDI \cdots DI}_{k-1 \text{ times}}DP^{-1} \\ &= PD^kP^{-1}, \end{aligned}$$

and D^k is readily computed by the Lemma.

Example 11.18. Diagonalize the matrix $A = \begin{bmatrix} 4 & 2 \\ -3 & -1 \end{bmatrix}$, and hence compute A^6.

One finds without too much difficulty the eigenvalues and associated eigenvectors

$$\lambda = 1 : \quad \begin{bmatrix} -2s \\ 3s \end{bmatrix} \text{ for } 0 \neq s \in \mathbb{R}, \qquad \lambda = 2 : \quad \begin{bmatrix} t \\ -t \end{bmatrix} \text{ for } 0 \neq t \in \mathbb{R}.$$

We can take $P = \begin{bmatrix} -2 & 1 \\ 3 & -1 \end{bmatrix}$ as our diagonalizing matrix, with inverse

$$P^{-1} = \frac{1}{-1} \begin{bmatrix} -1 & -1 \\ -3 & -2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 3 & 2 \end{bmatrix}.$$

We then have $A = PDP^{-1}$, where $D = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$. It follows that

$$\begin{aligned} A^6 &= PD^6P^{-1} \\ &= \begin{bmatrix} -2 & 1 \\ 3 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 64 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 3 & 2 \end{bmatrix} \\ &= \begin{bmatrix} -2 & 1 \\ 3 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 192 & 128 \end{bmatrix} \\ &= \begin{bmatrix} 190 & 126 \\ -189 & -125 \end{bmatrix}. \end{aligned}$$

♣

Remark 11.19. We now have two methods of computing powers of square matrices: diagonalization and the Cayley–Hamilton Theorem (compare Example 10.21). Each have their strengths and weaknesses. The Cayley–Hamilton method applies to any matrix, but can be cumbersome due to its recursive nature (to calculate a given power we have to calculate all the preceding powers). The diagonalization method is non-recursive, but can only be used to find powers of diagonalizable matrices.

Our next application of diagonalization is to matrix exponentiation.

Definition 11.20. The *exponential* of an $(n \times n)$-matrix A is the square matrix

$$\begin{aligned} e^A &= I_n + A + \frac{1}{2!}A^2 + \frac{1}{3!}A^3 + \cdots + \frac{1}{k!}A^k + \cdots \\ &= \sum_{k=0}^{\infty} \frac{1}{k!}A^k. \end{aligned}$$

Since we are adding together infinitely many matrices, it is not at all obvious that the sum converges to some matrix with finite entries. It does, however, and for all square matrices A. Computing the entries of e^A in terms of the entries of A is a difficult problem in general. It becomes easier for diagonal and diagonalizable matrices.

Lemma 11.21. *Let D be a diagonal matrix with diagonal entries $\lambda_1, \ldots, \lambda_n$. Then its exponential e^D is a diagonal matrix with diagonal entries $e^{\lambda_1}, \ldots, e^{\lambda_n}$.*

Proof. We have

$$e^D = \sum_{k=0}^{\infty} \frac{1}{k!}D^k.$$

Each matrix D^k in the sum is a diagonal matrix with diagonal entries $\lambda_1^k, \ldots, \lambda_n^k$, by Lemma 11.17. It follows that e^D is a diagonal matrix with diagonal entries

$$\sum_{k=0}^{\infty} \frac{\lambda_1^k}{k!} = e^{\lambda_1}, \ldots, \sum_{k=0}^{\infty} \frac{\lambda_n^k}{k!} = e^{\lambda_n}$$

as claimed. □

This makes computing the exponential of a diagonalizable matrix A an easier task. We simply write $A = PDP^{-1}$ where D is diagonal,

and then
$$e^A = \sum_{k=0}^{\infty} \frac{1}{k!} P D^k P^{-1} = P \left(\sum_{k=0}^{\infty} \frac{1}{k!} D^k \right) P^{-1} = P e^D P^{-1}.$$

Example 11.22. The exponential of the matrix A from Example 11.18 is given by
$$\begin{aligned} e^A &= P e^D P^{-1} \\ &= \begin{bmatrix} -2 & 1 \\ 3 & -1 \end{bmatrix} \begin{bmatrix} e & 0 \\ 0 & e^2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 3 & 2 \end{bmatrix} \\ &= \begin{bmatrix} -2e + 3e^2 & -2e + 2e^2 \\ 3e - 3e^2 & 3e - 2e^2 \end{bmatrix}. \end{aligned}$$

♣

Matrix exponentials occur in many areas of Mathematics. Their main application in Science and Engineering is to the solution of systems of 1^{st} order linear differential equations.

The following is non-examinable, and may only be understandable if you have studied differential equations before.

Let $x = x(t)$ be a function of the variable t. We write x' for the first derivative $\dfrac{dx}{dt}$, which is also a function of t. Recall that the (1^{st} order, linear) differential equation
$$x' = ax, \qquad a \in \mathbb{R} \text{ constant}$$
has as its general solution
$$x = Ce^{at} = e^{at}C, \qquad \text{where } C \in \mathbb{R} \text{ is an arbitrary constant.}$$
(It will become clear why we have moved the constant to after the exponential in a moment.)

Now suppose that we wish to solve a system of 1^{st} order linear differential equations
$$\begin{cases} x_1' &= ax_1 + bx_2 \\ x_2' &= cx_1 + dx_2 \end{cases}.$$
This system can be written as the single matrix differential equation $\mathbf{x}' = A\mathbf{x}$, where
$$\mathbf{x}' = \begin{bmatrix} x_1' \\ x_2' \end{bmatrix}, \qquad \mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \quad \text{and} \quad A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$
The general solution is then given by
$$\mathbf{x} = e^{tA}\mathbf{C}, \qquad \text{where } \mathbf{C} = \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} \in \mathbb{R}^2 \text{ is an arbitrary constant.}$$

Thus to solve the system we are required to compute the exponential of a matrix, which requires diagonalization.

Example 11.23. Solve the system of differential equations

$$\begin{cases} x_1' &= 4x_1 + 2x_2 \\ x_2' &= -3x_1 + -x_2 \end{cases}.$$

In matrix form this is $\mathbf{x}' = A\mathbf{x}$, where A is the matrix from Example 11.18. Since

$$tA = P \begin{bmatrix} t & 0 \\ 0 & 2t \end{bmatrix} P^{-1},$$

we find

$$\begin{aligned} e^{tA} &= \begin{bmatrix} -2 & 1 \\ 3 & -1 \end{bmatrix} \begin{bmatrix} e^t & 0 \\ 0 & e^{2t} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 3 & 2 \end{bmatrix} \\ &= \begin{bmatrix} -2 & 1 \\ 3 & -1 \end{bmatrix} \begin{bmatrix} e^t & e^t \\ 3e^{2t} & 2e^{2t} \end{bmatrix} \\ &= \begin{bmatrix} -2e^t + 3e^{2t} & -2e^t + 2e^{2t} \\ 3e^t - 3e^{2t} & 3e^t - 2e^{2t} \end{bmatrix}. \end{aligned}$$

The general solution is then

$$\begin{aligned} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} &= e^{tA}\mathbf{C} \\ &= \begin{bmatrix} -2e^t + 3e^{2t} & -2e^t + 2e^{2t} \\ 3e^t - 3e^{2t} & 3e^t - 2e^{2t} \end{bmatrix} \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} \\ &= \begin{bmatrix} (-2e^t + 3e^{2t})C_1 + (-2e^t + 2e^{2t})C_2 \\ (3e^t - 3e^{2t})C_1 + (3e^t - 2e^{2t})C_2 \end{bmatrix} \\ &= \begin{bmatrix} (-2C_1 - 2C_2)e^t + (3C_1 + 2C_2)e^{2t} \\ (3C_1 + 3C_2)e^t + (-3C_1 - 2C_2)e^{2t} \end{bmatrix}. \end{aligned}$$

♣

Remark 11.24. Note that in the above example, the general solution could also be written as

$$\mathbf{x} = e^{\lambda_1 t}\mathbf{v_1} + e^{\lambda_2 t}\mathbf{v_2},$$

where $\mathbf{v_1}$ and $\mathbf{v_2}$ are the eigenvectors of A with associated eigenvalues λ_1 and λ_2.

Suggestions for further reading:

- http://en.wikipedia.org/wiki/Diagonalizable_matrix
- Any book on Linear Algebra, such as H. Anton, *Elementary Linear Algebra*.