LINEAR ALGEBRA AND GEOMETRY: §1-18

§1. Distance, and coordinates in $\mathbb{R}^2$

§2. Lines in $\mathbb{R}^2$

§3. Circles, cosine, and sine

§4. Complex numbers and the complex plane

§5. Conic sections

§5A. Appendix: Derivation of formulae for conic sections

§6. Rigid motions of the plane

§7. Distance, lines and planes in $\mathbb{R}^3$.

§8. Distance, lines, and hyperplanes in $\mathbb{R}^n$

§9. Systems of linear equations and linear transformations

§10. Linear transformations from $\mathbb{R}^n$ to $\mathbb{R}^m$

§11. "Linearity" of linear transformations from $\mathbb{R}^n$ to $\mathbb{R}^m$

§12. Injective and surjective functions

§13. Injective linear transformations and kernels

§14. Matrices and representing linear transformations

§15. Echelon forms and elementary matrices

§16. Surjectivity, Injectivity, and Inverses

§16A. Appendix: Solving m linear equations in n variables, $m < n$

§17. Augmented matrices: a computational device

§18. Determinants and volumes

In mathematics, we are interested in quantifying things, and in describing relationships, regions, systems, and movement.

In this course we begin with some analytic geometry (some of which will be review), including some proofs; then we study systems of linear equations, vector spaces, and linear transformations, which help us organize information and more quickly make deductions regarding linear systems.

The course involves concepts, constructions, computations, and proofs. Objectives of §1-18 include:

> be familiar with cos, sin, conic sections, and rigid motions of the plane; be able to work with complex numbers; be able to recognize lines and hyperplanes in $\mathbb{R}^n$; be able to solve linear equations using elementary operations; be able to work with matrix algebras, including matrix multiplication, matrix inverses, determinants; be able to work with linear transformations from $\mathbb{R}^n$ to $\mathbb{R}^m$; be able to use matrices to represent linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$.

§1. The Pythagorean Theorem and distance in $\mathbb{R}^2$

We derive formulas for distance from the Pythagorean Theorem, which describes the relationship between the lengths of the sides of a right triangle.

Given a rectangle, we can construct 2 identical right triangles by cutting the rectangle along one diagonal. Recall that the sides of a right triangle that meet in a 90° angle are called *legs*; the side opposite the right angle is called the *hypotenuse.*

Discussion: The sum of the interior angles of a right triangle is 180°.

We use right triangles and the Pythagorean Theorem to find the distance between 2 points.

Theorem 1.1 (Pythagorean Theorem). *Say we have a right triangle with legs of lengths a and b, and hypotenuse of length c. Then $a^2 + b^2 = c^2$.*

Discussion of proof: We draw a square with side length $a + b$; moving anticlockwise around the square, we mark distance a along each side. We then join the marks on each pair of adjacent sides with a line segment, forming 4 right triangles within the square; each of these triangles has one leg of length a, and one of length b. Let c denote the length of the hypotenuse of each triangle.

We know that the interior angles of a triangle sum to 180°, and our 4 right triangles are identical; this allows us to conclude that the 4-sided polygon with edges of length c is in fact a square.

The square with side length $a+b$ has area $(a+b)^2 = a^2+2ab+b^2$. Also, we have divided this square into 4 right triangles, each with legs of lengths a and b, and a square with side length c; the sum of these areas is $4(\frac{1}{2}ab) + c^2 = 2ab + c^2$. Thus we have 2 expressions describing the area of the large square, so these expressions must be equal. Hence we have $a^2 + 2ab + b^2 = 2ab + c^2$, and so $a^2 + b^2 = c^2$. $\square$

Discussion: What happens if we increase or decrease the 90° angle of what is initially a right triangle? In particular, what happens to the side opposite this angle?

In the Exercises, you will verify the following

Theorem 1.2 (Fortified Pythagorean Theorem). *A triangle with sides of lengths* a, b, c *is a right triangle with hypotenuse of length* c *only if* $a^2 + b^2 = c^2$.

We use $\mathbb{R}$ to denote the set of real numbers, and $\mathbb{R}^2$ to denote the set of all ordered pairs of real numbers. The entries of a pair from $\mathbb{R}^2$ are also called Cartesian coordinates, and we depict pairs from $\mathbb{R}^2$ as points in the Cartesian plane, which uses a horizontal line (the x-axis) and a vertical line (the y-axis) for reference. We call the point where the axes cross the *origin*, and we label it $(0, 0)$.

Discussion: How do we plot $(1, -3)$ in the Cartesian plane?

Given a point $(a, b) \in \mathbb{R}^2$, we can determine the distance of this point from the origin using the Pythagorean Theorem: Draw a triangle with vertices $(0, 0)$, $(a, 0)$, (a, b); note that this is a right triangle since the leg connecting $(a, 0)$ to (a, b) is parallel to the y-axis, which is perpendicular to the x-axis. The length of the hypotenuse is the distance from (a, b) to the origin, and by the Pythagorean Theorem, this is $\sqrt{a^2 + b^2}$.

More generally, we have the following.

Theorem 1.3. *The distance between 2 points* (a, b) *and* (c, d) *is*

$$\sqrt{(a-c)^2 + (b-d)^2}.$$

Discussion of proof: Draw the right triangle with vertices (a, b), (c, d), and (c, b). Why is this a right triangle? What is the length of its hypotenuse? What if $a = c$ or $b = d$?

§2. Lines in $\mathbb{R}^2$

Recall that, given 2 points $(a, b), (c, d) \in \mathbb{R}^2$ with $a \neq c$, we call $\frac{b-d}{a-c}$ the *slope* of the line segment connecting (a, b) and (c, d). (Note that $\frac{b-d}{a-c} = \frac{d-b}{c-a}$.) Note that when $a = c$, the line segment connecting (a, b) and (c, d) is vertical; a vertical line is sometimes said to have infinite slope. A line is determined either by 2 points on the line, or by 1 point on the line and the line's slope (also called the line's *direction*).

Discussion: Say we have a line L with slope 5 containing the point $(-1, 2)$. Then $(x, y) \neq (-1, 2)$ is on L exactly when the slope between (x, y) and $(-1, 2)$ is 5, i.e. $\frac{y-2}{x-(-1)} = 5$, or equivalently, $y = 5x + 7$. (Note that $(-1, 2)$ is a solution to the equation $y = 5x + 7$, but not to $\frac{y-2}{x+1} = 5$.)

Given 2 points on a line L, we can compute a formula for L by first computing the slope of L, then by following the procedure demonstrated above.

Discussion: Say $(-4, 2), (3, -1)$ are points on a line L. What is an equation for L?

Given an equation $f(x, y) = 0$ where $f(x, y)$ is an expression in terms of x and y, the *graph* of $f(x, y) = 0$ consists of all points $(x, y) \in \mathbb{R}^2$ that satisfy the equation. (Notice that the equation $f(x, y) = g(x, y)$ is equivalent to $f(x, y) - g(x, y) = 0$, and we will sometimes refer to the graph of $f(x,y) = g(x,y)$, which is the graph of $f(x,y) - g(x,y) = 0$.)

Discussion: The graph of $y = -2x + 3$ consists of all points $(x, -2x + 3)$. So $(0,3)$ is a point on this graph. Given $a \neq 0$, the slope of the line between $(0,3)$ and $(a, -2a + 3)$ is $\frac{(-2a+3)-3}{a-0} = -2$. So $y = -2x + 3$ describes a line with slope -2, and the point $(0,3)$ (also described as having y-intercept 3).

Formula: In general, with m, b fixed real numbers, the equation $y = mx + b$ describes a line of slope m and y-intercept b.

Theorem 2.1. *A line with slope $m(\neq 0)$ is perpendicular to any line with slope $-\frac{1}{m}$. (Note: If L is a line with slope 0, then L is horizontal, and perpendicular to any vertical line.)*

Discussion of proof: This is simply a question about slopes, so let's look at 2 lines through the origin, $(0,0)$. Let's begin with a specific example.

Let L_1 be the line given by $y = 2x$, and L_2 the line given by $y = -\frac{1}{2}x$. We build a triangle using the origin and a point on each line, then we "test" the Pythagorean Theorem. Let's use $(0,0)$, and $(3,6)$ (a point on $y = 2x$) and $(2,-1)$ (a point on $y = -\frac{1}{2}x$) as the vertices of our triangle. What are the lengths of the triangle's sides that meet the origin? What is the length of the side opposite the origin? Is the conclusion of the Pythagorean Theorem satisfied? Can we conclude these 2 lines are perpendicular?

In the Exercises, you will mimic this argument to verify that a line with slope $m \neq 0$ is perpendicular to a line with slope $-\frac{1}{m}$. $\square$

§3. Circles, cosine, and sine

The circle with centre at the origin and radius $r(> 0)$ consists of all points (x,y) that are distance r from the origin. So this circle consists of all points (x,y) so that $\sqrt{(x-0)^2 + (y-0)^2} = r$, or equivalently, all points (x,y) so that $x^2 + y^2 = r^2$. (Since the quantities $\sqrt{x^2 + y^2}$ and r are non-negative, the equation $\sqrt{x^2 + y^2} = r$ is equivalent to the equation $x^2 + y^2 = r^2$. Is this always the case? For instance, do the equations $y = \sqrt{x-4}$ and $y^2 = x - 4$ have exactly the same set of solutions?)

More generally, the circle with centre (a,b) and radius r is the set of all points (x,y) that are distance r from (a,b).

Formula: The circle with centre (a,b) and radius $r(> 0)$ is described by the equation $\sqrt{(x-a)^2 + (y-b)^2} = r$, or equivalently $(x-a)^2 + (y-b)^2 = r^2$.

We now recall how the functions cosine and sine (abbreviated cos and sin) are defined using a right triangle, and then we extend their definitions with the aid of the circle in $\mathbb{R}^2$ with centre $(0,0)$ and radius 1.

Consider the right triangle with legs of lengths a and b (both positive). Let $c = \sqrt{a^2 + b^2}$; so c is the length of the hypotenuse. For convenience of reference, we draw this triangle in $\mathbb{R}^2$, placing its vertices at $(0,0)$, $(a,0)$, and (a,b). Let θ denote the (interior) angle at the origin (so it is the angle between the horizontal leg and the hypotenuse). We define $\cos(\theta) = a/c$ and $\sin(\theta) = b/c$.

Note: The Pythagorean Theorem states $a^2 + b^2 = c^2$, so $(\cos(\theta))^2 + (\sin(\theta))^2 = 1$ for θ between 0 and 90 degrees.

Now consider the circle in $\mathbb{R}^2$ with centre $(0,0)$ and radius 1; choose a point (a,b) on the circle with $a, b > 0$. Then $(0,0), (a,0), (a,b)$ are the vertices of a right triangle with hypotenuse 1; letting θ denote the interior angle at the origin, $a = \cos(\theta)$ and $b = \sin(\theta)$.

We extend the definitions of $\cos, \sin$ by allowing any value for θ, as follows. Given any value $\theta > 0$, construct an angle θ using the non-negative x-axis and a second ray (i.e. a half-line) emanating from $(0,0)$ so that, measuring anti-clockwise from the non-negative x-axis to this second ray, the enclosed angle is θ. We define $(\cos(\theta), \sin(\theta))$ to be the coordinates of the point where this second ray intersects the unit circle.

Discussion: Plot $(\cos(135°), \sin(135°))$, $(\cos(60°), \sin(60°)$, $(\cos(420°), \sin(420°)$.

Discussion: Why is $\cos(-\alpha) = \cos(\alpha)$? Why is $\sin(-\alpha) = -\sin(\alpha)$? Why is $\cos(\alpha \pm \pi) = -\cos(\alpha)$? Why is $\sin(\alpha \pm \pi) = -\sin(\alpha)$?

In Calculus it turns out to be more convenient to measure angles using *radians* rather than degrees. Just as there are 360° in an entire circle, there are 2π radians in an entire circle. Notice that 2π is the circumference of a unit circle. Using our circle in $\mathbb{R}^2$ with centre $(0,0)$ and radius 1, we measure θ radians (abbreviated θ rads) by beginning at the point $(1,0)$, then traveling anti-clockwise along the perimeter of the circle a distance of θ. We draw the ray through this point with endpoint $(0,0)$. The angle intercepted by the non-negative x-axis and this ray is θ radians.

Note: From now on, radian measure is our default measure for angles. So if we say an angle has measurement θ, we mean θ rads.

In the Exercises, you will verify that

$$\begin{aligned}&\cos(\pi/6) = \sqrt{3}/2,\ \sin(\pi/6) = 1/2,\\ &\cos(\pi/3)1/2,\ \sin(\pi/3) = \sqrt{3}/2,\\ &\cos(\pi/4) = \sin(\pi/4) = \sqrt{2}/2 = 1/\sqrt{2}.\end{aligned}$$

Discussion: What is $\cos(\frac{\pi}{2})$? What is $\sin(\frac{2}{3}\pi)$? What is $\cos(-\frac{3}{4}\pi)$?

Theorem 3.1 (Extended Pythagorean Theorem). *For any* $\theta \in \mathbb{R}$, $(\cos\theta)^2 + (\sin\theta)^2 = 1$.

Note: Here $\cos\theta = \cos(\theta)$ and some people write $\cos^2\theta$ to mean $(\cos\theta)^2$.

Discussion of proof: The unit circle with centre $(0,0)$ consists of all points (x,y) so that $x^2 + y^2 = 1$. Since, for any $\theta \in \mathbb{R}$, $(\cos\theta, \sin\theta)$ is a point on this circle, we have $(\cos\theta)^2 + (\sin\theta)^2 = 1$. $\square$

Discussion: How do we plot $(4\cos\theta, 4\sin\theta)$? (Note that this is a point on the circle with radius 4 and centre $(0,0)$.)

§4. Complex numbers and the complex plane

Definition. We use i to denote $\sqrt{-1}$, meaning a root of x^2+1. So $i^2=-1$. We use $\mathbb{C}$ to denote the set $\{a+bi:\ a,b\in\mathbb{R}\ \}$. We call $\mathbb{C}$ the set of *complex numbers.*

Graphically, we represent $\mathbb{C}$ as a plane, where the horizontal axis is the "real" axis, and the vertical axis is the "imaginary" axis; the point $a+bi$ is plotted as we plotted (a,b) in the Cartesian plane $\mathbb{R}^2$. We call 0 the origin. Also, given a complex number $\alpha=a+bi$, we define $\mathrm{Re}\alpha=a$, $\mathrm{Im}\alpha=b$.

Given complex numbers $\alpha=a+bi, \beta=c+di$ (where we understand $a,b,c,d\in\mathbb{R}$), we have

$$\alpha+\beta=(a+c)+(b+d)i,\ \ \alpha\beta=(ac-bd)+(ad+bc)i.$$

Also, $\alpha=\beta$ exactly when $a=c$ and $b=d$.

Definitions. The *conjugate* of a complex number $a+bi$ is $a-bi$, and is denoted by $\overline{a+bi}$. Notice that $(a+bi)(a-bi)=a^2+b^2$, the square of the distance from $a+bi$ to the origin. We often use $|a+bi|$ to denote this distance; that is, for a complex number α, $|\alpha|=\sqrt{\alpha\overline{\alpha}}$.

The distance between 2 complex numbers $a+bi$ and $c+di$ is the same as the distance between the points (a,b) and (c,d) in the Cartesian plane; thus the distance between $\alpha=a+bi$ and $\beta=c+di$ is $\sqrt{(a-c)^2+(b-d)^2}$; notice this is equal to $|\alpha-\beta|$.

In Calculus, we see how to represent points in $\mathbb{R}^2$ using polar coordinates. We can do a similar thing in the complex plane.

In Calculus we see that the Taylor series for $\cos x, \sin x$, and e^x converge for all $x\in\mathbb{R}$. We have

$$\begin{aligned}\cos x &= 1-\frac{x^2}{2!}+\frac{x^4}{4!}-\frac{x^6}{6!}+\cdots,\\ \sin x &= x-\frac{x^3}{3!}+\frac{x^5}{5!}-\frac{x^7}{7!}+\cdots,\\ \mathrm{e}^x &= 1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\frac{x^4}{4!}+\frac{x^5}{5!}+\cdots.\end{aligned}$$

It turns out that these formulas also hold for $x\in\mathbb{C}$ (a proof of this is beyond the scope of this course). In particular,

$$\mathrm{e}^{i\theta}=\cos\theta+i\sin\theta.$$

As you will see in the Exercises, this identity can be used to find some useful identities involving cos and sin.

Discussion: Given $\theta\in\mathbb{R}$, we have

$$\begin{aligned}|\mathrm{e}^{i\theta}| &= |\cos\theta+i\sin\theta|\\ &= \sqrt{(\cos\theta+i\sin\theta)(\cos\theta-i\sin\theta)}\\ &= \sqrt{(\cos^2\theta+\sin^2\theta)}\\ &= 1.\end{aligned}$$

Theorem 4.1. *Given any $\alpha = a + bi \in \mathbb{C}$, there exist $r, \theta \in \mathbb{R}$ so that $\alpha = re^{i\theta}$.*

Discussion of proof: If $\alpha = 0$ then we can take $r = 0$ and any value for θ. So suppose $\alpha \neq 0$; set

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

(hence $r \neq 0$ since $a \neq 0$ or $b \neq 0$). Then $(a/r, b/r)$ is a point in $\mathbb{R}^2$ on the unit circle with centre $(0, 0)$; hence for some θ,

$$\frac{a}{r} = \cos\theta, \text{ and } \frac{b}{r} = \sin\theta.$$

Therefore $a + bi = r\cos\theta + ir\sin\theta = re^{i\theta}$. □

In the Exercises, you prove the following.

Theorem 4.2. *Say $\alpha, \beta \in \mathbb{C}$.*
(a) Suppose $\alpha = re^{i\theta}$ for some $r, \theta \in \mathbb{R}$. Then $|\alpha| = |r|$.
(b) $|\alpha\beta| = |\alpha|\,|\beta|$.

Discussion: When do we have $e^{i\theta} = e^{i\varphi}$? Notice that this is equivalent to $e^{i(\theta-\varphi)} = 1$, and we know $e^{i(\theta-\varphi)} = \cos(\theta - \varphi) + i\sin(\theta - \varphi)$. So the question becomes: When is $\cos(\theta - \varphi) = 1$ and $\sin(\theta - \varphi) = 0$?

In the Exercises you verify the following.

Theorem 4.3 (Triangle Inequality). *Given complex numbers α, β, $|\alpha\beta| = |\alpha| \cdot |\beta|$ and $|\alpha + \beta| \le |\alpha| + |\beta|$.*

(Later in the course, you will use that $\mathbb{C}$ is "algebraically closed", meaning that any polynomial with complex coefficients factors into a product of polynomials of degree 1.)

§5. Conic sections

Conic sections can be obtain by intersecting a cone in 3-space with a plane; they can also be defined using distance in $\mathbb{R}^2$, as follows.

A *parabola* in $\mathbb{R}^2$ consists of all points P that are equidistant from a fixed point F, called the *focus*, and a fixed line L, called the *directrix.* When the focus is $(c, 0)$ and the directrix is $x = -c$ ($c \neq 0$), the equation describing this parabola is

$$y^2 = 4cx.$$

The point $(0, 0)$ is on the parabola, and is midway between the focus and the directrix; this point is the the *vertex* of the parabola described by $y^2 = 4cx$. Note that this parabola can also be described as the set of all points P so that

$$\frac{\text{distance from } P \text{ to } F}{\text{distance from } P \text{ to the line } L} = 1.$$

An *ellipse* consists of every point P where the sum of the distances from the point to each of two fixed points F_1 and F_2, called foci, is a given (positive) constant.

Suppose the foci are $F_1 = (c, 0)$ and $F_2 = (-c, 0)$ $(c > 0)$, and the fixed sum of distances from a point P on the parabola to the foci is $2a$, $0 < c < a$. Then with $b^2 = a^2 - c^2$, an equation describing this ellipse is

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1.$$

In this situation the x-axis is called the *major axis*, as the foci are on the x-axis; the y-axis is called the *minor axis.* The points $(\pm a, 0)$ are the points where the ellipse intersects the major axis, and these points $(\pm a, 0)$ are called the *vertices* of the ellipse. This ellipse can also be described as the set of points P so that

$$\frac{\text{distance from } P \text{ to } F_1}{\text{distance from } P \text{ to the line } x = a^2/c} = \frac{c}{a}.$$

The quotient c/a is called the *eccentricity* of the ellipse; notice that the eccentricity here is less than 1.

A *hyperbola* consists of every point P where the absolute value of the difference of the distances from the point to each of two fixed points F_1 and F_2, again called foci, is constant. Suppose the foci are $F_1 = (c, 0)$ and $F_2(-c, 0)$ $(c > 0)$, and the fixed difference of distances from a point P on the hyperbola to the foci is $2a$, $0 < a < c$. Then with $b^2 = c^2 - a^2$, an equation describing this ellipse is

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1.$$

In this situation the x-axis is called the *major axis*, as the foci are on the x-axis; the y-axis is called the *minor axis.* The points $(\pm a, 0)$ are the points where the hyperbola intersects the major axis, and these points $(\pm a, 0)$ are called the *vertices* of the hyperbola. This hyperbola can also be described as the set of points P so that

$$\frac{\text{distance from } P \text{ to } F_1}{\text{distance from } P \text{ to the line } x = a^2/c} = \frac{c}{a}.$$

The quotient c/a is called the *eccentricity* of the hyperbola; notice that the eccentricity here is greater than 1.

Discussion: What is an equation for the parabola with vertex $(0, 0)$ and directrix $y = -1$? What is an equation for the ellipse with foci $(-3, 0), (3, 0)$ and the point $(0, 2)$? What is an equation for the hyperbola with foci $(-1, 0), (1, 0)$ and the point $(2, 0)$?

In §6, we find formulae for conic sections whose foci are not on the x-axis.

§5A. Appendix: Derivation of formulae for conic sections

A *parabola* in $\mathbb{R}^2$ consists of all points that are equidistant from a fixed point, called the *focus*, and a fixed line, called the *directrix.* We consider parabolas where the focus is on the x-axis, and the directrix is parallel to the y-axis. So suppose a parabola has focus $(c, 0)$ and, for simplicity, directrix $x = -c$. The distance from a point (u, v) to the line $x = -c$ is the length of the line segment perpendicular to the line $x = -c$ with endpoints (u, v) and a point on the line $x = -c$; thus this distance is from (u, v) to $(-c, v)$, which is $\sqrt{(u+c)^2} = |u + c|$. Hence (u, v) is on the parabola exactly when

$$\sqrt{(u-c)^2 + v^2} = \sqrt{(u+c)^2},$$

or equivalently, when $(u - c)^2 + v^2 = (u + c)^2$. Simplifying, we find that (u, v) is on this parabola exactly when $v^2 = 4cu$. Hence an equation for this parabola is

$$y^2 = 4cx$$

(meaning that a point (x, y) is on the parabola exactly when the above equation is satisfied by those values of x, y).

An *ellipse* consists of every point where the sum of the distances from the point to each of two fixed points, called foci, is a given (positive) constant. Suppose the foci for an ellipse are the points $(-c, 0)$ and $(c, 0)$; for convenience of reference, suppose $c > 0$. (Note that if $c = 0$ we are describing a circle, which we discussed earlier.) Suppose also the sum of the distances from a point on the ellipse and the foci is $2a$. (We use $2a$ here rather than a for later convenience when simplifying algebraic expressions.) We assume $a > c$. (One can prove that if $a = c$, then the "ellipse" is the line segment joining the foci; if $a < c$, then the "ellipse" has no points at all.) A point (x, y) is on this ellipse exactly when

$$\sqrt{(x+c)^2 + y^2} + \sqrt{(x-c)^2 + y^2} = 2a.$$

To simplify this equation, we first subtract $\sqrt{(x+c)^2 + y^2}$ across the equation, then square both sides of the equation and simplify, obtaining

$$a^2 + cx = a\sqrt{(x+c)^2 + y^2}.$$

Now we square both sides of this equation and simplify to get

$$a^2(a^2 - c^2) = (a^2 - c^2)x^2 + a^2y^2.$$

Since $a > c > 0$, we can (and do) choose b so that $b^2 = a^2 - c^2$. (Note also that $(b, 0)$ and $(-b, 0)$ are points on this ellipse.) Thus, if (x, y) is a point on the ellipse then $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$. Conversely, if (x, y) satisfies this last equation then (x, y) satisfies the original equation. Hence (x, y) is a point on the ellipse exactly when

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1.$$

A *hyperbola* consists of every point where the absolute value of the difference of the distances from the point to each of two fixed points, again called foci, is constant; also, this difference is to be smaller than the distance between the two foci. Suppose the foci are $(-c, 0)$ and $(c, 0)$ $(c > 0)$, and the fixed difference of distances from a point on the hyperbola to the foci is $2a$, $0 < a < c$. So we want to find all points (x, y) so that

$$\sqrt{(x-c)^2+y^2}-\sqrt{(x+c)^2+y^2}=2a, \text{ or } \sqrt{(x+c)^2+y^2}-\sqrt{(x-c)^2+y^2}=2a.$$

Consider the first of these equations; adding $\sqrt{(x+c)^2+y^2}$ and squaring, we obtain the equation

$$-a^2-cx=a\sqrt{(x+c)^2+y^2}.$$

Since $a > 0$, the solutions (x, y) to this equation will necessarily have $x \leq -a^2/c$. In fact, squaring this equation and simplifying, we find that if (x, y) satisfies $\sqrt{(x-c)^2+y^2}-\sqrt{(x+c)^2+y^2}=2a$ then $\frac{x^2}{a^2}-\frac{y^2}{b^2}=1$ and $x \leq -a^2/c$ where b is chosen so that $b^2 = c^2 - a^2$. Conversely, if $x \leq -a^2/c$ and (x, y) satisfies $\frac{x^2}{a^2}-\frac{y^2}{b^2}=1$, then (x, y) satisfies $\sqrt{(x-c)^2+y^2}-\sqrt{(x+c)^2+y^2}=2a$. Similarly, (x, y) satisfies the equation $\sqrt{(x+c)^2+y^2}-\sqrt{(x-c)^2+y^2}=2a$ exactly when $\frac{x^2}{a^2}-\frac{y^2}{b^2}=1$ and $x \geq a^2/c$. Thus (x, y) is on the hyperbola exactly when

$$\frac{x^2}{a^2}-\frac{y^2}{b^2}=1.$$

Notice that with $x^2/a^2 - y^2/b^2 = 1$, we always have $b^2x^2/a^2 > y^2$. Consequently, points on the hyperbola lie in the two regions between the lines $y = \pm\frac{b}{a}x$ that contain the vertices of the hyperbola. Also, as $x \to \pm\infty$, $y \to \pm\frac{b}{a}x$; so the lines $y = \pm\frac{b}{a}x$ are asymptotes for the hyperbola.

§6. Rigid motions of the plane

We discuss here how to find an equation for a geometric object in $\mathbb{R}^2$ after we shift or rotate the object.

Suppose we want to shift the centre of a circle from $(0, 0)$ to another point. We first consider a specific example: Consider the circle described by $x^2 + y^2 = 4$; so this has centre $(0, 0)$ and radius 2. Say we want to shift the centre to $(5, -3)$. First we can shift the circle 5 units to the right. Thus a point that was distance u from the y-axis is now distance $u + 5$ from the y-axis. So a point (u, v) is on this shifted circle if and only if $(u - 5, v)$ is a point on the original circle. Similarly, if we now shift the circle 3 units down, a point that was distance v from the x-axis is now distance $v + 3$ from the x-axis. Consequently, a point (u, v) is on the shifted circle with centre $(5, -3)$ if and only if $(u - 5, v + 3)$ is on the original circle with centre $(0, 0)$. Thus an equation for the shifted circle is $(x - 5)^2 + (y + 3)^2 = 4$.

Discussion: In general, how do we shift the graph of $f(x, y) = 0$?

Formula: To shift the graph $f(x, y) = 0$ to the right a units and up b units, we replace x by $x - a$ and y by $y - b$. The resulting equation for the shifted graph is $f(x - a, y - b) = 0$.

Discussion: What is a formula for the parabola with focus $(-1,-3)$ and directrix $y=-5$? What is a formula for the ellipse with foci $(3,2)$ and $(9,2)$ and the point $(6,6)$? What is a formula for the hyperbola with foci $(2,-2)$ and $(4,-2)$ and the point $(5,-2)$?

Now consider rotating an object in the plane anti-clockwise about the origin by a specified amount. For instance, suppose we rotate the point $(1/2,\sqrt{3}/2)$ $\pi/4$ radians about the origin. Notice that $(1/2,\sqrt{3}/2)$ is a point on the unit circle; in fact, $(1/2,\sqrt{3}/2)=(\cos(\pi/3),\sin(\pi/3))$. Rotating this point by $\pi/4$, we obtain another point on the circle; in fact, we obtain the point $(\cos(\pi/3+\pi/4),\sin(\pi/3+\pi/4))$.

Discussion: More generally, given any point (a,b) in $\mathbb{R}^2$, we can find r,θ so that $(a,b)=(r\cos(\theta),r\sin(\theta))$. Rotating this point α radians anti-clockwise about the origin, we obtain the point $(r\cos(\theta+\alpha),r\sin(\theta+\alpha))$.

Formula: Suppose we rotate an object in $\mathbb{R}^2$ α radians anti-clockwise about the origin. Then a point (a,b) on the object rotates to the point

$$(a\cos\alpha-b\sin\alpha,a\sin\alpha+b\cos\alpha).$$

Now say we want to rotate the graph of $f(x,y)=0$ α radians anti-clockwise. A point $(a,b)=(r\cos\theta,r\sin\theta)$ is on the rotated graph exactly when $(r\cos(\theta-\alpha),r\sin(\theta-\alpha))$ is on the original graph, or in other words, when the point $(a\cos\alpha+b\sin\alpha,-a\sin\alpha+b\cos\alpha)$ is on the original graph (recall that $\cos(-\alpha)=\cos\alpha$, and $\sin(-\alpha)=-\sin\alpha$).

Formula: An equation for the graph of $f(x,y)=0$ rotated by α radians is $f(x\cos\alpha+y\sin\alpha,-x\sin\alpha+y\cos\alpha)=0$.

Discussion: We will rotate by $\pi/2$ the parabola $x=y^2$, then shift its vertex to $(-1,3)$. To rotate the graph, in the equation $y=x^2$ (or equivalently, $y-x^2=0$), we replace x by $x\cos(\pi/2)+y\sin(\pi/2)=y$, and we replace y by $-x\sin(\pi/2)+y\cos(\pi/2)=-x$. Thus we get the equation $y=x^2$ for the rotated parabola. To now shift its vertex from $(0,0)$ to $(-1,3)$, we replace x by $x+1$ and y by $y-3$; thus we obtain the equation $y-3=(x+1)^2$, or equivalently, $y=x^2+2x+4$.

Discussion: Rotate by $\pi/4$ the hyperbola $\frac{x^2}{9}-\frac{y^2}{4}=1$.

Discussion: Consider the equation $32x^2-12y^2-96x+12y-27=0$. Although it may not be readily apparent, this is an equation for a hyperbola. To see that, we complete squares to get the equivalent equation

$$32\left[(x-\frac{3}{2})^2-\frac{9}{4}\right]-12\left[(y-\frac{1}{2})^2-\frac{1}{4}\right]=27.$$

This is equivalent to $32(x-3/2)^2-12(y-1/2)^2=96$, or

$$\frac{(x-3/2)^2}{3}-\frac{(y-1/2)^2}{8}=1,$$

an equation for a hyperbola shifted 3/2 units right and 1/2 unit up. Here $a^2 = 3$ and $b^2 = 8$; thus $a = \sqrt{3}$ and $c = \sqrt{11}$. Hence the vertices of the hyperbola are $(\pm\sqrt{3}, 0) + (3/2, 1/2)$ and the foci are $(\pm\sqrt{11}, 0) + (3/2, 1/2)$.

§7. Distance, lines and planes in $\mathbb{R}^3$.

$\mathbb{R}^3$ consists of all ordered triples (a, b, c) where $a, b, c \in \mathbb{R}$. Graphically, we depict $\mathbb{R}^3$ using 3 mutually orthogonal (i.e. perpendicular) lines that intersect at a single point that we label $(0, 0, 0)$ and call the origin. We typically call these perpendicular lines the x-, y-, and z-axes.

We will use the Pythagorean Theorem to find a formula for distance in $\mathbb{R}^3$, and to find a method for detecting right angles.

First, take $(a, b, c) \in \mathbb{R}^3$; we want to find the distance from this point to the origin. Consider the triangle in $\mathbb{R}^3$ with vertices $(0, 0, 0)$, $(a, b, 0)$ and (a, b, c). So the line segment connecting $(0, 0, 0)$ to $(a, b, 0)$ lies in the x, y-plane and has length $\sqrt{a^2 + b^2}$, and the segment connecting $(a, b, 0)$ to (a, b, c) has length c. Also, the angle between these two line segments is a right angle, since the first segment lies in the x, y-plane, and the second segment is parallel to the z-axis. Thus the Pythagorean Theorem tells us that the length of the hypotenuse of this triangle is $\sqrt{(\sqrt{a^2 + b^2})^2 + c^2} = \sqrt{a^2 + b^2 + c^2}$. Thus we have:

Formula: The distance from $(0, 0, 0)$ to (a, b, c) is

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

To find the distance between two points (a, b, c) and (a', b', c'), we shift the line segment connecting these points to have one endpoint at the origin, and the other endpoint at $(a - a', b - b', c - c')$. Thus we get:

Formula: The distance from (a, b, c) to (a', b', c') is

$$\sqrt{(a - a')^2 + (b - b')^2 + (c - c')^2}.$$

A line in $\mathbb{R}^3$ is given by 1 point and a direction; equivalently, a line is determined by 2 points that lie on it.

Discussion: Consider the line through the origin containing the point $(1, 2, 3)$. The line segment between these 2 points determines the direction of the line. The line consists of all points $(r, 2r, 3r)$ where $r \in \mathbb{R}$.

More generally, a line through the origin containing the point (a, b, c) where a, b, c are not all 0 consists of all points (ra, rb, rc) where $r \in \mathbb{R}$.

Given a line through the origin, we can rigidly shift it by adding a fixed point to each point on the line. (We add points coordinate-wise: $(x, y, z) + (x', y', z') = (x + x', y + y', z + z')$.)

Discussion: How can we describe the line containing the points $(2, -1, 3)$ and $(3, 1, 6)$? Notice that we can view this line as the shift of the line through the origin and $(1, 2, 3)$.

Formula: The line through the points (a, b, c) and (a', b', c') consists of all points $r(a - a', b - b', c - c') + (a, b, c)$ where $r \in \mathbb{R}$. (Here $r(x, y, z) = (rx, ry, rz)$.) So $(a - a', b - b', c - c')$ tells us the direction of this line.

We can also describe a line by describing the relationship between the coordinates of the points on the line: Consider again the line through the origin and the point $(1, 2, 3)$. So (x, y, z) is a point on this line exactly when $y = 2x$ and $z = 3x$.

Consider the line consisting of all points $(x, y, z) = (2r + 3, -r + 5, 7r + 4)$, $r \in \mathbb{R}$. To find equations for y and z in terms of x, we first solve $x = 2r + 5$ for r, giving us $r = \frac{1}{2}x - \frac{3}{2}$. Thus $y = -r + 5 = -\frac{1}{2}x + \frac{7}{2}$ and $z = \frac{7}{2}x - \frac{13}{2}$. Alternatively, we could solve the equation $y = -r + 5$ for r and write x and z in terms of y: $x = -2y + 13$, $z = -7y + 39$.

We often find it convenient to think of an element $(a, b, c) \in \mathbb{R}^3$ as the (directed) line segment, or *vector*, from the origin to the point (a, b, c). We will use $\underline{v}$ to denote the vector with endpoint $v = (a, b, c)$.

Given $v = (a, b, c), v' = (a', b', c') \in \mathbb{R}^3$, when are $\underline{v}, \underline{v}'$ orthogonal (i.e. perpendicular)? Equivalently, when are $\underline{v}, \underline{v}'$ the legs of a right triangle? Letting $|\underline{v}|$ denote the length of $\underline{v}$, we see by Theorem 1.2 that $\underline{v}, \underline{v}'$ are the legs of a right triangle exactly when

$$(\text{distance from } v \text{ to } v')^2 = |\underline{v}|^2 + |\underline{v}'|^2.$$

Since $|\underline{v}| = \sqrt{a^2 + b^2 + c^2}$, $|\underline{v}'| = \sqrt{(a')^2 + (b')^2 + (c')^2}$, and the distance between v and v' is $\sqrt{(a - a')^2 + (b - b')^2 + (c - c')^2}$,we see that $\underline{v}, \underline{v}'$ are orthogonal exactly when

$$(a^2 + b^2 + c^2) + ((a')^2 + (b')^2 + (c')^2) = (a - a')^2 + (b - b')^2 + (c - c')^2,$$

or equivalently, when $aa' + bb' + cc' = 0$.

Definition. We define the *dot product* of $\underline{v} = (a, b, c)$ and $\underline{v}' = (a', b', c')$ to be

$$\underline{v} \cdot \underline{v}' = aa' + bb' + cc'.$$

By the above discussion, we see that $\underline{v}, \underline{v}'$ are orthogonal exactly when $\underline{v} \cdot \underline{v}' = 0$.

Consider a vector $\underline{v}$ in $\mathbb{R}^3$ where $v = (a, b, c) \neq (0, 0, 0)$. The set of all vectors $\underline{w}$ orthogonal to $\underline{v}$ is the set of all $\underline{w} = \underline{(x, y, z)}$ so that $\underline{v} \cdot \underline{w} = 0$, i.e. $ax + by + cz = 0$, and these vectors form a plane through the origin, orthogonal to $\underline{v}$.

Example: The plane orthogonal to $\underline{(1, 2, 3)}$ is described by $x + 2y + 3z = 0$.

We can shift such a plane away from the origin by shifting any (or all) the variables x, y, z.

Discussion: How do we shift the plane $x + 2y + 3z = 0$ to contain the point $(-1, 5, -7)$? At what point does this shifted plane intersect the z-axis?

Formula: Provided not all a, b, c are 0, $ax + by + cz = d$ is a formula for a plane orthogonal to the vector $\underline{(a, b, c)}$. If $a \neq 0$, this plane contains the point $(d/a, 0, 0)$; if $b \neq 0$, this plane contains the point $(0, d/b, 0)$; if $c \neq 0$, this plane contains the point $(0, 0, d/c)$.

Discussion: How do we describe the x, y-plane in $\mathbb{R}^3$?

Now we consider the intersection of 2 planes in $\mathbb{R}^3$.

Discussion: Consider $x+2y+3z=0$ and $x-y+5z=4$. These equations describe 2 planes that intersect at points (x, y, z) that satisfy both equations. So suppose we have such (x, y, z); thus

$$x=-2y-3z,$$

and also

$$(-2y-3z)-y+5z=4.$$

So $x=-2y-3z$ and $-3y+2z=4$. Simplifying further,

$$y=\frac{2}{3}z-\frac{4}{3},\ x=-2(\frac{2}{3}z-\frac{4}{3})-3z=-\frac{13}{3}z+\frac{8}{3}.$$

Thus the intersection of the 2 planes is the line

$$x=-\frac{13}{3}z+\frac{8}{3},\ y=\frac{2}{3}z-\frac{4}{3}.$$

§8. Distance, lines, and hyperplanes in $\mathbb{R}^n$

For $n \in \mathbb{Z}_+$ (i.e. n a positive integer), $\mathbb{R}^n$ denotes the set of all ordered n-tuples of real numbers. Geometrically, we think of $\mathbb{R}^n$ in terms of n coordinate axes that are all mutually orthogonal and intersecting at one point called the origin. So a point $(a, 0, 0, \dots, 0) \in \mathbb{R}^n$ is orthogonal to any point of the form $(0, b_2, b_3, \dots, b_n)$, and $(0, a, 0, \dots, 0)$ is orthogonal to any point of the form $(b_1, 0, b_3, \dots, b_n)$, etc.

Theorem 8.1. *The distance from the origin to a point* $(a_1, a_2, \dots, a_n) \in \mathbb{R}^n$ *is*

$$\sqrt{a_1^2+a_2^2+\cdots+a_n^2}.$$

Discussion of proof: We can use the technique of mathematical induction here: we assume the formula holds in $\mathbb{R}^{n-1}$ for some $n \geq 3$, then deduce it holds in $\mathbb{R}^n$. Since we know the formula holds in $\mathbb{R}^2$, this will show it holds in $\mathbb{R}^3$; then, since the formula holds in $\mathbb{R}^3$, this will show it holds in $\mathbb{R}^4$; etc.

So we suppose $n \geq 3$ and that in $\mathbb{R}^{n-1}$, the distance from the origin to the point $(a_1, a_2, \dots, a_{n-1})$ is $\sqrt{a_1^2+a_2^2+\cdots+a_{n-1}^2}$. Embed $\mathbb{R}^{n-1}$ into $\mathbb{R}^n$ by adding an nth dimension; so we map $(a_1, a_2, \dots, a_{n-1}) \in \mathbb{R}^{n-1}$ to $(a_1, a_2, \dots, a_{n-1}, 0) \in \mathbb{R}^n$. (Example: Say $n=3$. Then we map any point (x, y) to $(x, y, 0)$; so we view $\mathbb{R}^2$ as the x, y-plane in $\mathbb{R}^3$.)

Now take $(a_1, a_2, \dots, a_n) \in \mathbb{R}^n$. So $(a_1, a_2, \dots, a_{n-1}, 0)$ lies in our copy of $\mathbb{R}^{n-1}$ embedded in $\mathbb{R}^n$. Together with the origin, these points give us the vertices of a right triangle, whose hypotenuse is the line segment from the origin to $(a_1, a_2, \dots, a_n)$. The lengths of the 2 legs are $\sqrt{a_1^2+a_2^2+\cdots+a_{n-1}^2}$ and $|a_n|=\sqrt{a_n^2}$; thus, by the

Pythagorean Theorem, the length of the hypotenuse is $\sqrt{a_1^2 + a_2^2 + \cdots + a_{n-1}^2 + a_n^2}$.
□

To find the distance between two points $(a_1, \dots, a_n)$ and $(b_1, \dots, b_n)$ we translate the line segment connecting them to have one point at the origin, and the other endpoint at $(a_1 - b_1, \dots, a_n - b_n)$. Then the length of this line segment is the distance between the two original points. Thus we have the following.

Theorem 8.2. *The distance between* $(a_1, \dots, a_n)$ *and* $(b_1, \dots, b_n)$ *is*

$$\sqrt{(a_1 - b_1)^2 + \cdots + (a_n - b_n)^2}.$$

Theorems 1.2 and 8.2 give us the following.

Theorem 8.3. *Given* $v = (a_1, \dots, a_n)$ *and* $w = (b_1, \dots, b_n)$*, we define*

$$\underline{v} \cdot \underline{w} = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n.$$

Then $\underline{v}, \underline{w}$ *are orthogonal exactly when* $\underline{v} \cdot \underline{w} = 0$.

Discussion of proof: By Theorem 1.2, $\underline{v}, \underline{w}$ are orthogonal exactly when

$$|\underline{v}|^2 + |\underline{w}|^2 = (\text{distance from } \underline{v} \text{ to } \underline{w})^2.$$

Note that $|\underline{v}|$ is the distance from v to the origin, and $|uw|$ is the distance from w to the origin. So using Theorem 8.2, we compute $|\underline{v}|$, $|uw|$, and the distance from v to w. Substituting into the above equation and then simpifying yields the result.
□

A line in $\mathbb{R}^n$ is determined by one point and the direction of the line, or by two points on the line. The line through the origin containing also the point $(a_1, \dots, a_n)$ has its direction given by this second point, and the points on this line are exactly the points $r(a_1, \dots, a_n) = (ra_1, \dots, ra_n)$ where $r \in \mathbb{R}$. The line through $(a_1, \dots, a_n)$ and $(b_1, \dots, b_n)$ $((a_1, \dots, a_n) \neq (b_1, \dots, b_n))$ has its direction given by $(a_1 - b_1, \dots, a_n - b_n)$, and the points on this line are exactly the points $r(a_1 - b_1, \dots, a_n - b_n) + (b_1, \dots, b_n)$, $r \in \mathbb{R}$.

We can also describe a line using a system of equations.

Discussion: When $d_1 \neq 0$, the line consisting of all points

$$(x_1, x_1, \dots, x_n) = r(d_1, \dots, d_n) + (c_1, \dots, c_n), \ r \in \mathbb{R},$$

is also described by the system of equations

$$x_2 = \frac{d_2}{d_1}(x_1 - c_1) + c_2, \dots, x_n = \frac{d_n}{d_1}(x_1 - c_1) + c_n.$$

What if $d_1 = 0$?

We can generalize the notion of a plane in $\mathbb{R}^3$ to this setting as follows. Given a nonzero vector $\underline{v}$ in $\mathbb{R}^n$, consider the set of all points w so that $\underline{w}$ is orthogonal to $\underline{v}$, i.e. $\underline{v} \cdot \underline{w} = 0$; these points w form an object in $\mathbb{R}^n$ we call a hyperplane (or more simply, a plane) that passes through the origin. We can shift this hyperplane away from the origin by adding to each w in the plane a fixed point. Thus we have the following.

Theorem 8.4. *Given* $a_1, \dots, a_n, d \in \mathbb{R}$ *with the* a_i *not all 0, the equation* $a_1x_1 + \cdots + a_nx_n = d$ *is an equation for a hyperplane in* $\mathbb{R}^n$*. If* $a_1 \neq 0$ *then the hyperplane contains the point* $(d/a_1, 0, \dots, 0)$*; if* $a_2 \neq 0$ *then the hyperplane contains* $(0, d/a_2, 0, \dots, 0)$*; etc.*

§9. Systems of linear equations and linear transformations

Previously we looked for simultaneous solutions to a system of several linear equations. We can view such solutions as those points where several planes intersect; alternatively, we can view the system as describing a function from $\mathbb{R}^n$ to $\mathbb{R}^m$.

Discussion: Consider the equations:

$$\begin{aligned} x + 2y + 3z &= 3 \\ 5x - y + 2z &= 13 \\ 2x + 3y - z &= 0 \end{aligned}$$

We can view each equation as describing a plane in $\mathbb{R}^3$; a simultaneous solution to these equations is a point (x, y, z) that is on all 3 planes. So we can view simultaneous solutions to this system of equations as the points where the planes intersect.

To find the points on the intersection of these planes, we use algebraic operations to rearrange these equations into an equivalent system of equations from which it is easy to determine the simultaneous solutions. There are several elementary operations we can perform so that we do not lose any information conveyed by these equations:

1. Add (or subtract) a multiple of one equation to another (but do not eliminate from the system the one equation);
2. Multiply an equation by a nonzero number;
3. Rearrange the order of the equations.

To demonstrate, we look for the simultaneous solutions to the above system of 3 equations.

First, let us subtract 5 times Equation 1 from Equation 2, eliminating x from the 2nd equation, and obtaining the equivalent system of equations:

$$\begin{aligned} x + 2y + 3z &= 3 \\ -11y - 13z &= -2 \\ 2x + 3y - z &= 0 \end{aligned}$$

Now we can subtract 2 times Equation 1 from Equation 3, obtaining the equivalent system of equations:

$$\begin{aligned} x + 2y + 3z &= 3 \\ -11y - 13z &= -2 \\ -y - 7z &= -6 \end{aligned}$$

Now let's multiply (the new) Equation 3 by -1, then swap its order with (the new) Equation 3, obtaining the equivalent system of equations:

$$\begin{aligned} x+2y+3z&=3\\ y+7z&=6\\ -11y-13z&=-2 \end{aligned}$$

Now we add 11 times (the new) Equation 2 to (the new) Equation 3 to get an equivalent system:

$$\begin{aligned} x+2y+3z&=3\\ y+7z&=6\\ 64z&=64 \end{aligned}$$

The system of equations above is equivalent to our original system, yet from this last system we can easily determine which (x, y, z) satisfy the system: We must have $z = 1$, and hence $y + 7 = 6$, or $y = -1$, and so $x - 2 + 3 = 3$, or $x = 2$. (To check, one can substitute these values into the original system of equations, and verify one's algebra was done correctly.)

Note: We could also carry on with manipulating the system of equations to arrive at this solution: Multiply (the new) Equation 3 by $1/64$, then subtract 7 times (the newest) Equation 3 from Equation 2, obtaining:

$$\begin{aligned} x+2y+3z&=3\\ y&=-1\\ z&=1 \end{aligned}$$

Finally, we subtract 2 times (the new) Equation 2 from Equation 1, and we subtract 3 times (the new) Equation 3 from (the new) Equation 1, obtaining:

$$\begin{aligned} x&=2\\ y&=-1\\ z&=1 \end{aligned}$$

Discussion: Not every system of linear equations has a solution; when this occurs, we call the system *inconsistent.* For example,

$$\begin{aligned} x-3y&=1\\ 7x-21y&=1 \end{aligned}$$

is inconsistent. Also, a system of linear equations can have many solutions; for instance, consider

$$\begin{aligned} x-y+z&=1\\ x+y+2z&=0; \end{aligned}$$

this is equivalent to the system

$$\begin{aligned} x - y + z &= 1 \\ 2x + 3z &= 1, \end{aligned}$$

which is equivalent to $z = -2x/3 + 1/3$, $y = x/3 - 2/3$. Thus for any $x \in \mathbb{R}$, $(x, x/3 - 2/3, -2x/3 + 1/3)$ is a solution to the original system.

Discussion: Consider again the system:

$$\begin{aligned} x + 2y + 3z &= 3 \\ 5x - y + 2z &= 13 \\ 2x + 3y - z &= 0 \end{aligned}$$

Instead of looking at this system as planes in $\mathbb{R}^3$, we can take a function point of view: Define $T : \mathbb{R}^3 \to \mathbb{R}^3$ by

$$T((x, y, z)) = (x + 2y + 3z, 5x - y + 2z, 2x + 3y - z).$$

Then we translate the previous system of equations to the single equation:

$$T((x, y, z)) = (3, 13, 0).$$

Solving the system of 3 equations is equivalent to solving this last equation.

Note: Since an element v of $\mathbb{R}^3$ is of the form (x, y, z), $T(v)$ literally translates to $T((x, y, z))$. However, this use of double parentheses is awkward, so sometimes we will write $T(x, y, z)$ when what we really mean is $T((x, y, z))$.

§10. Linear transformations from $\mathbb{R}^n$ to $\mathbb{R}^m$

The function T in the preceeding discussion is an example of a "linear transformation", which is a particular type of function from $\mathbb{R}^n$ to $\mathbb{R}^m$, as defined below. (Later in the course these will be defined more generally, as functions from one "vector space" to another; here we give the translation of that definition when the vector spaces are $\mathbb{R}^n$ and $\mathbb{R}^m$.)

Remark: We will often refer to elements of $\mathbb{R}^n$ as vectors, but we will ease our notation and write v rather than $\underline{v}$. Also, we often write 0 to denote $(0, 0, \dots, 0) \in \mathbb{R}^n$.

We recall the operations on elements of $\mathbb{R}^n$ introduced earlier: Given $v = (x_1, \dots, x_n)$ and $v' = (x'_1, \dots, x'_n)$ in $\mathbb{R}^n$ and $\alpha \in \mathbb{R}$, we have

$$v + v' = (x_1 + x'_1, \dots, x_n + x'_n)$$

and

$$\alpha v = (\alpha x_1, \dots, \alpha x_n).$$

Note that for any $v \in \mathbb{R}^n$,

$$v + (0, \dots, 0) = (0, \dots, 0) + v = v,$$

and if $v + w = v$ then $w = (0, \dots, 0)$. Thus $(0, \dots, 0)$ is the (unique) additive identity in $\mathbb{R}^n$. Also, for any $v = (x_1, \dots, x_n) \in \mathbb{R}^n$, we have

$$v + w = (0, \dots, 0) \text{ if and only if } w = (-x_1, \dots, -x_n) = -1 \cdot v.$$

Thus each $v \in \mathbb{R}^n$ has a unique additive identity, denoted $-v$ (and equal to $-1 \cdot v$).

Definition. A function $T : \mathbb{R}^n \to \mathbb{R}^m$ is a *linear transformation* if, for all $v, v' \in \mathbb{R}^n$ and all $\alpha \in \mathbb{R}$, we have

$$T(v + v') = T(v) + T(v'),$$

and

$$T(\alpha v) = \alpha T(v).$$

As we will discuss in subsequent sections, this function point of view is useful as it allows us to use things we know about functions, systematising and simplifying some of our computations and explanations. We consider now some examples.

Discussion: Consider the function $T : \mathbb{R}^2 \to \mathbb{R}^2$ defined by $T(x, y) = (x^2 + y, x + y^2)$. To test whether T is a linear transformation, we take arbitrary $v, v' \in \mathbb{R}^2$, $\alpha \in \mathbb{R}$; so for some $x, y, x', y' \in \mathbb{R}$, $v = (x, y)$, $v' = (x', y')$. Therefore

$$T(v + v') = T(x + x', y + y') = (x + x' + (y + y')^2, (x + x')^2 + y + y').$$

On the other hand,

$$\begin{aligned} T(v) + T(v') &= (x + y^2, x^2 + y) + (x' + (y')^2, (x')^2 + y') \\ &= (x + y^2 + x' + (y')^2, x^2 + y + (x')^2 + y'). \end{aligned}$$

So it is not always the case that $T(v + v') = T(v) + T(v')$ (although sometimes this equality does hold); in particular, with $v = (1, 1)$ and $v' = (2, 2)$ we have $T(v + v') = T(3, 3) = (12, 12)$, while $T(v) + T(v') = (2, 2) + (5, 5) = (7, 7)$. Thus T fails to meet the first condition of a linear transformation.

Also, T fails to meet the second condition of a linear transformation: Let us first compare $T(\alpha v)$ and $\alpha T(v)$ for general α, v. So say $v = (x, y) \in \mathbb{R}^2$, $\alpha \in \mathbb{R}$. Then

$$T(\alpha v) = T(\alpha x, \alpha y) = ((\alpha x)^2 + y, \alpha x + (\alpha y)^2).$$

On the other hand,

$$\alpha T(v) = \alpha(x^2 + y, x + y^2) = (\alpha x^2 + \alpha y, \alpha x + \alpha y^2).$$

Thus it is not always the case that $T(\alpha v) = \alpha T(v)$. In particular, say $\alpha = 3$ and $v = (1, 1)$; then $T(\alpha v) = T(3, 3) = (12, 12)$ while $\alpha T(v) = 3(2, 2) = (6, 6)$.

(Note that to show T is not a linear transformation, it suffices to show either that $T(v+v')$ is not always $T(v)+T(v')$, or that $T(\alpha v)$ is not always $\alpha T(v)$.)

Discussion: Consider the function $T:\mathbb{R}^2\to\mathbb{R}^2$ defined by

$$T(x,y)=(x-y,x+y).$$

We first verify that T meets the definition of a linear transformation; then we find the solutions (x,y) to $T(x,y)=(1,1)$.

To verify T is a linear transformation, let us choose arbitrary $v,v'\in\mathbb{R}^2$. Thus for some $x,y,x',y'\in\mathbb{R}$, we have $v=(x,y)$ and $v'=(x',y')$. Then, using the definition of T in this example we have

$$\begin{aligned}T(v+v')&=T(x+x',y+y')\\&=\big((x+x')-(y+y'),(x+x')+(y+y')\big)\\&=(x+x'-y-y',x+x'+y+y').\end{aligned}$$

On the other hand,

$$\begin{aligned}T(v)+T(v')&=T(x,y)+T(x',y')\\&=(x-y,x+y)+(x'-y',x'+y')\\&=(x-y+x'-y',x+y+x'+y')\\&=(x+x'-y-y',x+x'+y+y')\\&=T(v+v').\end{aligned}$$

So in testing whether T is a linear transformation, we see the first condition of the definition is met. Now we take v as above, and choose an arbitrary $\alpha\in\mathbb{R}$. We now test the second condition for T to be a linear transformation:

$$\begin{aligned}T(\alpha v)&=T(\alpha(x,y))\\&=T(\alpha x,\alpha y)\\&=(\alpha x-\alpha y,\alpha x+\alpha y)\\&=\big(\alpha(x-y),\alpha(x+y)\big)\\&=\alpha(x-y,x+y)\\&=\alpha T(x,y)\\&=\alpha T(v).\end{aligned}$$

Thus T also meets this second condition, showing T is a linear transformation.

Now we determine solutions $v=(x,y)$ to the equation $T(x,y)=(1,1)$. Equivalently, we want to solve the system:

$$\begin{aligned}x-y&=1\\x+y&=1\end{aligned}$$

Proceeding as we did in the previous discussion, we obtain an equivalent system of equations:

$$\begin{aligned} x &= 1 \\ y &= 0 \end{aligned}$$

This shows we have exactly one solution to the equation $T(x, y) = (1, 1)$. However, this is not always the case.

Discussion: Consider the function $T : \mathbb{R}^2 \to \mathbb{R}^2$ defined by

$$T(x, y) = (x - 2y, -3x + 6y).$$

We first verify that T is a linear transformation; then we look for all solutions to $T(x, y) = (1, 1)$, and all solutions to $T(x, y) = (7, -21)$.

To show T is a linear transformation, we choose arbitrary $v, v' \in \mathbb{R}^2$; so $v = (x, y)$ and $v' = (x', y')$ for some $x, y, x', y' \in \mathbb{R}$. Then we compare $T(v + w)$ and $T(v) + T(w)$:

$$\begin{aligned} T(v + v') &= T(x + x', y + y') \\ &= \big((x + x') - 2(y + y'), -3(x + x') + 6(y + y')\big) \\ &= (x - 2y + x' - 2y', -3x + 6y - 3x' + 6y') \\ &= (x - 2y, -3x + 6y) + (x' - 2y', -3x' + 6y') \\ &= T(x, y) + T(x', y') \\ &= T(v) + T(v'). \end{aligned}$$

Next, we take v as above (i.e. $v = (x, y)$ is an arbitrary element of $\mathbb{R}^2$) and we choose an arbitrary element $\alpha \in \mathbb{R}$; we compare $T(\alpha v)$ and $\alpha T(v)$:

$$\begin{aligned} T(\alpha v) &= T(\alpha x, \alpha y) \\ &= (\alpha x - 2\alpha y, -3\alpha x + 6\alpha y) \\ &= \alpha(x - 2y, -3x + 6y) \\ &= \alpha T(x, y) \\ &= \alpha T(v). \end{aligned}$$

Thus T is a linear transformation.

Now we look for solutions to $T(x, y) = (1, 1)$; so we need to solve the system of equations:

$$\begin{aligned} x - 2y &= 1 \\ -3x + 6y &= 1 \end{aligned}$$

Adding 3 times Equation 1 to Equation 2, we see this system is equivalent to:

$$\begin{aligned} x - 2y &= 1 \\ 0 &= 4 \end{aligned}$$

The second equation in this last system is clearly false; this means there can be no solution to this, or to the equivalent, original, system of equations.

Last, we look for solution to $T(x, y) = (7, -21)$. We look to solve the system of equations:

$$\begin{aligned} x - 2y &= 7 \\ -3x + 6y &= -21 \end{aligned}$$

Adding 3 times Equation 1 to Equation 2, we obtain the equivalent system of equations:

$$\begin{aligned} x - 2y &= 7 \\ 0 &= 0 \end{aligned}$$

The last equation in this last system is always true, regardless of our choices of x, y. So a solution (x, y) to the original system of equations only needs to satisfy $x - 2y = 7$, or equivalently, $x = 2y + 7$. Thus the solutions to the system are all $(2y + 7, y)$ where y is any real number. So there are infinitely many solutions (x, y) to the equation $T(x, y) = (7, -21)$.

In the Exercises, you prove the following.

Theorem 10.1. *(a) Suppose* $S, T : \mathbb{R}^n \to \mathbb{R}^m$ *are linear transformations. Then* $S + T : \mathbb{R}^n \to \mathbb{R}^m$ *is a linear transformation.*
(b) Suppose $T : \mathbb{R}^n \to \mathbb{R}^m$ *and* $S : \mathbb{R}^m \to \mathbb{R}^k$ *are linear transformations. Then* $S \circ T : \mathbb{R}^n \to \mathbb{R}^k$ *is a linear transformation.*

Theorem 10.2. *Suppose* $S, T : \mathbb{R}^n \to \mathbb{R}^m$ *and* $R : \mathbb{R}^m \to \mathbb{R}^k$ *are linear transformations. Then*

$$R \circ (S + T) = R \circ S + R \circ T.$$

Our next two major avenues of investigation are (1) understanding when functions, especially linear transformations, have no solutions or multiple solutions, and (2) using "matrices" to represent systems of equations, or equivalently, to represent linear transformations. We will then develop methods for testing the matrix associated to a linear transformation T to determine whether an equation $T(v) = w$ has no solutions, a unique solution, or multiple solutions. But before we proceed to these topics, we discuss the "linearity" of linear transformations.

§11. "Linearity" of linear transformations from $\mathbb{R}^n$ to $\mathbb{R}^m$

We want to show that $T : \mathbb{R}^n \to \mathbb{R}^m$ is a linear transformation exactly when T is described by an m-tuple of linear expressions in the variables $x_1, x_2, \ldots, x_n$. (In the Exercises, you looked at specific examples of this.) We will then show that a linear transformation maps lines to lines.

Theorem 11.1. *Say* $T : \mathbb{R}^n \to \mathbb{R}$ *is given by a linear expression in* $x_1, \dots, x_n$*; that is, say* T *is given by* $T(x_1, \dots, x_n) = a_1x_1 + \dots + a_nx_n$ *for fixed* $a_1, \dots, a_n \in \mathbb{R}$*. Then* T *is a linear transformation.*

Discussion of proof: Given this definition of T, we verify it satisfies the conditions in the definition of linear transformation. So choose $v, v' \in \mathbb{R}^n$ and $\alpha \in \mathbb{R}$; we need to show $T(v + v') = T(v) + T(v')$ and $T(\alpha v) = \alpha T(v)$. We know $v = (x_1, \dots, x_n)$ and $v' = (x'_1, \dots, x'_n)$ for some $x_i, x'_i \in \mathbb{R}$. Thus:

$$\begin{aligned} T(v + v') &= T((x_1, \dots, x_n) + (x'_1, \dots, x'_n)) \\ &= T(x_1 + x'_1, \dots, x_n + x'_n) \\ &= a_1(x_1 + x'_1) + \dots + a_n(x_n + x'_n) \\ &= (a_1x_1 + \dots + a_nx_n) + (a_1x'_1 + \dots + a_nx'_n) \\ &= T(x_1, \dots, x_n) + T(x'_1, \dots, x'_n) \\ &= T(v) + T(v'). \end{aligned}$$

In the Exercises, you will show that for $v \in \mathbb{R}^n$, $\alpha \in \mathbb{R}$, $T(\alpha v) = \alpha T(v)$, completing the proof that this T is a linear transformation. □

Theorem 11.2. *Say for* $i = 1, \dots, m$*,* $T_i : \mathbb{R}^n \to \mathbb{R}$ *is given by a linear expression in* $x_1, \dots, x_n$ *(and hence each* T_i *is a linear transformation). Then with* $T : \mathbb{R}^n \to \mathbb{R}^m$ *defined by*

$$T(v) = (T_1(v), \dots, T_m(v)),$$

T *is a linear transformation.*

Discussion of proof: Choose $v, v' \in \mathbb{R}^n$ and $\alpha \in \mathbb{R}$. In the Exercises you will show that $T(v + v') = T(v) + T(v')$.

By the preceeding Propostion, each T_i is a linear transformation. Thus $T_i(\alpha v) = \alpha T_i(v)$ for each i, so we have:

$$\begin{aligned} T(\alpha v) &= (T_1(\alpha v), \dots, T_m(\alpha v)) \\ &= (\alpha T_1(v), \dots, \alpha T_m(v)) \\ &= \alpha(T_1(v), \dots, T_m(v)) \\ &= \alpha T(v). \end{aligned}$$

Thus T is a linear transformation. □

Theorem 11.3. *Say* $T : \mathbb{R}^n \to \mathbb{R}$ *is a linear transformation. Then for some* $a_1, \dots, a_n \in \mathbb{R}$*,* T *is defined by*

$$T(x_1, \dots, x_n) = a_1x_1 + \dots + a_nx_n.$$

Discussion of proof: Let's first consider $n = 2$. We have $T(1,0) = a_1$ for some $a_1 \in \mathbb{R}$, and $T(0,1) = a_2$ for some $a_2 \in \mathbb{R}$. Now take any $(x_1, x_2) \in \mathbb{R}^2$. Since T is a linear transformation, we have:

$$\begin{aligned}
T((x_1,x_2)) &= T((x_1,0)+(0,x_2)) \\
&= T((x_1,0)) + T((0,x_2)) \\
&= T(x_1(1,0)) + T(x_2(0,1)) \\
&= x_1 T((1,0)) + x_2 T((0,1)) \\
&= x_1 a_1 + x_2 a_2 \\
&= a_1 x_1 + a_2 x_2.
\end{aligned}$$

Now say $n > 2$; how does this argument change? □

Theorem 11.4. *Say $T : \mathbb{R}^n \to \mathbb{R}^m$ is a linear tranformation. For $v \in \mathbb{R}^n$, write $T(v)$ as $(T_1(v), \dots, T_m(v))$. (So for each i, $1 \le i \le m$, T_i maps $\mathbb{R}^n$ into $\mathbb{R}$.) Then for each i, T_i is a linear transformation.*

Discussion of proof: Choose $v, v' \in \mathbb{R}^n$, $\alpha \in \mathbb{R}$. Since $T(v+v') = T(v) + T(v')$, we have

$$\begin{aligned}
\big(T_1(v+v'), \dots, T_m(v+v')\big) &= \big(T_1(v), \dots, T_m(v)) + (T_1(v'), \dots, T_m(v')\big) \\
&= \big(T_1(v) + T_1(v'), \dots, T_m(v) + T_m(v')\big).
\end{aligned}$$

For these two vectors to be equal, the corresponding components must be equal, meaning

$$T_1(v+v') = T_1(v) + T_1(v'), \dots, T_m(v+v') = T_m(v) + T_m(v').$$

In the Exercises, you will verify that for $v \in \mathbb{R}^n$, $\alpha \in \mathbb{R}$, $T_i(\alpha v) = \alpha T_i(v)$ for each i $(1 \le i \le m)$. Hence $T_1, \dots, T_m$ are linear transformations from $\mathbb{R}^n$ to $\mathbb{R}$. □

Together, these theorems show the following.

Theorem 11.5. *A map $T : \mathbb{R}^n \to \mathbb{R}^m$ is a linear transformation if and only if T is given by an m-tuple of linear expressions in n variables.*

Discussion of proof: Suppose first that $T\mathbb{R}^n \to \mathbb{R}^m$ is a linear transformation; define $T_1, \dots, T_m : \mathbb{R}^n \to \mathbb{R}$ so that

$$T(v) = \big(T_1(v), \dots, T_m(v)\big).$$

Then by Theorem 11.4, each T_i is a linear transformation, and by Theorem 11.3, $T_i(x_1, \dots, x_n)$ is given by a linear expression in $x_1, \dots, x_n$ $(1 \le i \le m)$.

Now suppose $T : \mathbb{R}^n \to \mathbb{R}^m$, and $T(x_1, \dots, x_n)$ is given by an m-tuple of linear expressions in $x_1, \dots, x_n$. So

$$T(v) = \big(T_1(v), \dots, T_m(v)\big)$$

where for each i $(1 \le i \le m)$, $T_i(x_1, \dots, x_n)$ is a linear expression in $x_1, \dots, x_n$. So by Theorem 11.1, each $T_i : \mathbb{R}^n \to \mathbb{R}$ is a linear transformation, and so by Theorem 11.2, $T : \mathbb{R}^n \to \mathbb{R}^m$ is a linear transformation. □

Another property of a linear transformation is that it maps lines to lines (or points).

Theorem 11.6. *Say $T : \mathbb{R}^n \to \mathbb{R}^m$ is a linear transformation. Then T maps any line in $\mathbb{R}^n$ either to a line in $\mathbb{R}^m$ or to a point in $\mathbb{R}^m$.*

Discussion of proof: Recall that we can describe any line in $\mathbb{R}^n$ by its "direction" and a point on the line; thus a line L in $\mathbb{R}^n$ can be described as the set of points

$$L = \{\alpha v + w : \ \alpha \in \mathbb{R}\ \}$$

where $v, w \in \mathbb{R}^n$ are fixed. (So v tells us the direction of the line, and w is a point on the line.) Then the image of L under T is

$$\begin{aligned} T(L) &= \{T(\alpha v + w) : \ \alpha \in \mathbb{R}\ \} \\ &= \{T(\alpha v) + T(w) : \ \alpha \in \mathbb{R}\ \} \\ &= \{\alpha T(v) + T(w) : \ \alpha \in \mathbb{R}\ \}. \end{aligned}$$

When $T(v) = 0$, $T(L) = \{T(w)\}$, a point in $\mathbb{R}^m$ When $T(v) \neq 0$, then $T(L)$ is a line in $\mathbb{R}^m$ with direction $T(v)$ and containing the point $T(w)$. $\square$

Discussion: Notice that when L, L' are parallel lines in $\mathbb{R}^n$ and $T(L)$ is a line in $\mathbb{R}^m$, then $T(L')$ is also a line and is parallel to $T(L)$. T maps parallel lines to parallel lines: A line L' is parallel to L exaclty when L' has the same direction as L. So for L' parallel to L, we have

$$L = \{\alpha v + w : \ \alpha \in \mathbb{R}\ \},\ L' = \{\alpha v + w' : \ \alpha \in \mathbb{R}\ \}$$

where $v, w, w' \in \mathbb{R}^n$ are fixed, with $v \neq 0$. For $T(L)$ to be a line, we need $T(v) \neq 0$. In this case

$$T(L') = \{\alpha T(v) + T(w') : \ \alpha \in \mathbb{R}\ \},$$

so both $T(L)$ and $T(L')$ are lines with direction $T(v)$.

§12. Injective and surjective functions

As we discussed previously, when $T : \mathbb{R}^2 \to \mathbb{R}^2$ is defined by

$$T(x, y) = (x - 2y, -3x + 6y),$$

the equation $T(x, y) = (1, 1)$ has no solutions, while the equation $T(x, y) = (7, -21)$ has infinitely many. That the one equation has no solutions shows that T does not map $\mathbb{R}^2$ *onto* $\mathbb{R}^2$, and that the second equation has infinitely many solutions shows that T does not create a *one-to-one* correspondence between elements of the domain of T and elements in the range, or *image*, of T. We present here the formal definitions of these concepts.

Note: We write $f : A \to B$ to mean f is a function mapping elements of the set A into the set B (so implicitly the notation $f : A \to B$ tells us that A, B are sets, and f is a function).

Definitions. Say $f : A \to B$. We call A the *domain* of f, and B the *codomain* of f. The *image* of f is

$$\begin{aligned} f(A) &= \{f(a) :\ a \in A\ \} \\ &= \{b \in B :\ b = f(a) \text{ for some } a \in A\ \}. \end{aligned}$$

We say f is *surjective*, or that f maps A *onto* B, if $f(A) = B$. We say f is *injective*, or *one-to-one*, if f maps distinct points of A to distinct points of B; that is, f is injective if $f(a) \neq f(a')$ whenever $a \neq a'$ $(a, a' \in A)$. If f is both surjective and injective, we say f is *bijective.*

Theorem 12.1. *A function $f : A \to B$ is surjective if and only if for every $b \in B$, there is some $a \in A$ so that $f(a) = b$.*

Discussion of proof: By definition, f is injective if and only if $a \neq a'$ implies $f(a) \neq f(a')$. The contrapositive of the statement $A \implies B$ is not $B \implies$ not A, and these 2 statements are equivalent. Thus f is injective if and only if $f(a) = f(a')$ implies $a = a'$. $\square$

Discussion: A function $f : A \to B$ is injective if and only if $f(a) = f(a')$ implies $a = a'$. (Here it is implicit that $a, a' \in A$.)

Discussion: Define $f, g : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^3 + 3x^2 - 9x + 1$, $g(x) = \mathrm{e}^x$. Are either of these functions injective? Are either surjective? (What does Calculus tell us about the graphs of these functions?)

Theorem 12.2. *Suppose $f : A \to B$, $g : B \to C$, and g is bijective. Then $g \circ f$ is injective if and only if f is injective, and $g \circ f$ is surjective if and only if f is surjective.*

Discussion of proof: First suppose $g \circ f$ is injective; we show this implies f is injective. To do this, suppose we have $f(a) = f(a')$ for some $a, a' \in A$. Then $g(f(a)) = g(f(a'))$, which means $g \circ f(a) = g \circ f(a')$. We have assumed that $g \circ f$ is injective, so this means we must have $a = a'$. Hence f is injective.

Now suppose f is injective; we show this imples $g \circ f$ is injective. Suppose $g \circ f(a) = g \circ f(a')$ for some $a, a' \in A$. Thus $g(f(a)) = g(f(a'))$. Since g is bijective, we know g is injective; thus, since $g(f(a)) = g(f(a'))$, we must have $f(a) = f(a')$. Since f is injective, this means $a = a'$. Hence $g \circ f$ is injective.

Now suppose $g \circ f$ is surjective; we show this implies f is surjective. Choose $b \in B$; we must find some $a \in A$ so that $f(a) = b$. Let $c = g(b)$ (so $c \in C$). We know that $g \circ f$ is surjective, so there is some $a \in A$ so that $g \circ f(a) = c$. Hence $g(f(a)) = c$. We also have $g(b) = c$, and we know g is bijective, hence injective; thus we must have $f(a) = b$. So we have found $a \in A$ so that $f(a) = b$ where b was chosen arbitrarily from B; this shows f is surjective.

Finally, suppose f is surjective; we show this implies $g \circ f$ is surjective. Choose $c \in C$. We know g is bijective, hence surjective, so there is some $b \in B$ so that $g(b) = c$. Also, f is surjective, so there is some $a \in A$ so that $f(a) = b$. Hence

$$g \circ f(a) = g(f(a)) = g(b) = c.$$

Since c was chosen arbitrarily from C, this shows $g \circ f$ is surjective. $\square$

Note: Suppose $f : A \to B$, $g : B \to C$. Arguments similar to those above show:
(a) if $g \circ f$ is injective, then so is f;
(b) if f and g are injective, then so is $g \circ f$;
(c) if $g \circ f$ is surjective, then so is g;
(d) if f and g are surjective, then so is $g \circ f$.
(The proofs of these statements are Exercises.)

Discussion: It is possible to have $f : A \to B$, $g : B \to C$ where f is injective but $g \circ f$ is not: Define $f, g : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^3$, $g(x) = x^2$. What is $g \circ f$? Is $g \circ f$ injective?

Discussion: It is possible to have $f : A \to B$, $g : B \to C$ where g is surjective but $g \circ f$ is not: Define $f, g : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2 + 1$, $g(x) = x + 4$. What is $g \circ f$? Is $g \circ f$ surjective?

Definition. Suppose $f : A \to B$ is bijective; we define $f^{-1} : B \to A$ by the rule $f^{-1}(b) = a$ where a is the unique element of A so that $f(a) = b$. Note that since f is surjective, given an arbitrary element $b \in B$, there must be some $a \in A$ so that $f(a) = b$; since f is injective, there is no other element of A that f maps to b.

Discussion: Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = 3x + 1$. Then f is injective: Suppose $f(x) = f(x')$; then $3x + 1 = 3x' + 1$, so $3x = 3x'$, and hence $x = x'$. Also, f is surjective: Given any $y \in \mathbb{R}$, we have $y = 3x + 1$ for $x = (y - 1)/3$. Thus f is bijective, and we can define f^{-1} by the rule $f^{-1}(y) = (y - 1)/3$.

Theorem 12.3. *Suppose $f : A \to B$ is bijective. Then $f^{-1} \circ f$ is the identity map on A, and $f \circ f^{-1}$ is the identity map on B.*

Discussion of proof: We show that $f^{-1} \circ f$ is the identity map on A; in the Exercises you will show $f \circ f^{-1}$ is the identity map on B.

We need to show that for any $a \in A$, $f^{-1} \circ f(a) = a$. Take $b \in B$ so that $f(a) = b$. Then

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

By definition, $f^{-1}(b) = a'$ where a' is the unique element of A so that $f(a') = b$. But we know $f(a) = b$, so a' must equal a (remember that f is injective by assumption). Thus $f^{-1}(b) = a$, so

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

Thus $f^{-1} \circ f$ is the identity map on A. $\square$

Discussion: In the preceeding examples, we looked at functions f, g that are not linear transformations. Here we consider a linear transformation $T : \mathbb{R}^2 \to \mathbb{R}^3$ defined by

$$T(x, y) = (2x - y, x + 3y, 5y).$$

(Why is this a linear transformation?) We claim that T is injective, but not surjective.

To show T is injective, suppose $T(x,y) = T(x',y')$ for some $(x,y),(x',y') \in \mathbb{R}^2$. Thus we are assuming

$$(2x - y, x + 3y, 5y) = (2x' - y', x' + 3y', 5y').$$

Hence $5y = 5y'$, so $y = y'$. Also, $2x - y = 2x' - y'$; this together with $y = y'$ implies $2x = 2x'$, so $x = x'$. Thus $(x,y) = (x',y')$ whenever $T(x,y) = T(x',y')$.

To show T is not surjective, we need to find some $w \in \mathbb{R}^3$ so that $w \neq T(v)$ for any $v \in \mathbb{R}^2$. So suppose there is some $v = (x,y) \in \mathbb{R}^2$ so that $T(v) = (0,0,5)$; we will deduce from this something patently false, which means we cannot have $T(v) = (0,0,5)$. The assumption $T(x,y) = (0,0,5)$ means $2x - y = 0$, $x + 3y = 0$, and $5y = 5$. From this last equation, we must have $y = 1$. Then the other equations tell us $2x = 1$ and $x = -3$; for these to both be true, we must have $1/2 = -3$, which is absurd. Hence there is no $v \in \mathbb{R}^2$ so that $T(v) = (0,0,5)$.

To show a function f does not satisfy the definition of surjective, we must produce an element in the codomain of f that is not in the image of f; this is not always a trivial task. However, for a linear transformation $T : \mathbb{R}^n \to \mathbb{R}^m$ we can "row reduce the matrix for T", a systematic process, to determine whether T is surjective; this is developed in §15.

An important result regarding bijective linear transformations is the following.

Theorem 12.4. *Suppose $T : \mathbb{R}^n \to \mathbb{R}^m$ is a bijective linear transformation. Then $T^{-1} : \mathbb{R}^m \to \mathbb{R}^n$ is a linear transformation.*

Discussion of proof: First, we know $T^{-1} : \mathbb{R}^m \to \mathbb{R}^n$ is defined (why?). Take $w, w' \in \mathbb{R}^m$. So there exist $v, v' \in \mathbb{R}^n$ such that $T(v) = w$, $T(v') = w'$ (why?), and hence $T^{-1}(w) = v$, $T^{-1}(w') = v'$. Also, $T(v + v') = w + w'$ (why?). Thus

$$T^{-1}(w + w') = v + v' = T^{-1}(w) + T^{-1}(w').$$

A similar argument show that for $\alpha \in \mathbb{R}$, $w \in \mathbb{R}^m$, $T^{-1}(\alpha w) = \alpha T^{-1}(w)$ (Exercise 12.8). □

§13. Injective linear transformations and kernels

In the previous section we discussed how to determine whether a function is injective. It is in fact easier to determine whether a linear transformation is injective, for as we will see, we only need to determine how many elements it maps to 0.

Theorem 13.1. *Say $T : \mathbb{R}^n \to \mathbb{R}^m$ is a linear transformation.*

(a) $T(0) = 0$.

(b) For any $v \in \mathbb{R}^n$, we have $T(-v) = -T(v)$.

Note: For $v \in \mathbb{R}^n$, $-v$ denotes the additive inverse of v in $\mathbb{R}^n$, while $-T(v)$ denotes the additive inverse of $T(v)$ in $\mathbb{R}^m$. For example, consider $T : \mathbb{R}^2 \to \mathbb{R}$ defined by $T(x,y) = x - 2y$. Then for $v = (3,5) \in \mathbb{R}^2$, $-v = (-3,-5)$, while $T(v) = T(3,5) = -7$ and so $-T(v) = 7$.

Discussion of proof: (a) You prove this in the Exercises.

(b) (In the Exercises, you give an alternate proof of the theorem by using the fact that $-1 \cdot (x_1, \ldots, x_n)$ is the additive inverse of $(x_1, \ldots, x_n)$, and that T is a linear transformation.)

Take $v \in \mathbb{R}^n$. Then $0 = v - v = v + (-v)$. Thus $T(0) = T(v + (-v))$. From the Exercises, we know $T(0) = 0$. Since T is a linear transformation, we know $T(v + (-v)) = T(v) + T(-v)$. Thus

$$0 = T(v) + T(-v).$$

Subtracting $T(v)$ (i.e. adding $-T(v)$, the additive inverse of $T(v)$), we get $-T(v) = T(-v)$, as desired. $\square$

Definition. With $T : \mathbb{R}^n \to \mathbb{R}^m$ a linear transformation, we define the *kernel* of T to be

$$\mathrm{ker}T = \{v \in \mathbb{R}^n : \ T(v) = 0 \ \}.$$

Discussion: Consider the linear transformation $T : \mathbb{R}^2 \to \mathbb{R}^2$ defined by

$$T((x, y)) = (x - 2y, -3x + 6y).$$

What is $\mathrm{ker}T$? In this case the equations $x - 2y = 0$, $-3x + 6y = 0$ each say $x = 2y$. Thus we have $T(v) = 0$ exactly when $v = (2y, y)$ with $y \in \mathbb{R}$.

Theorem 13.2. *Say $T : \mathbb{R}^n \to \mathbb{R}^m$ is a linear transformation. Then T is injective if and only if $kerT = \{0\}$.*

Discussion of proof: First, say T is injective. From Theorem 13.1 (a), we know $T(0) = 0$; since T is injective, T can map at most one element to 0, hence $0 \in \mathbb{R}^n$ is the only element T maps to $0 \in \mathbb{R}^m$.

Now say $T(v) = 0$ only for $v = 0$. To show T is injective, let us suppose $T(v_1) = T(v_2)$ for some $v_1, v_2 \in \mathbb{R}^n$. Then we have

$$0 = T(v_1) - T(v_2).$$

From the previous theorem, we know $-T(v_2) = T(-v_2)$; hence

$$0 = T(v_1) + T(-v_2).$$

Since T is a linear transformation, we know $T(v_1) + T(-v_2) = T(v_1 + (-v_2)) = T(v_1 - v_2)$. Thus we have $0 = T(v_1 - v_2)$. We have assumed that T maps only 0 to 0, so we must have $v_1 - v_2 = 0$. Adding v_2, we get $v_1 = v_2$. Thus we have shown that if $T(v_1) = T(v_2)$ for some $v_1, v_2 \in \mathbb{R}^n$, then $v_1 = v_2$, or in other words, we have shown that T is injective. $\square$

Discussion: Again consider the linear transformation $T : \mathbb{R}^2 \to \mathbb{R}^2$ defined by

$$T((x, y)) = (x - 2y, -3x + 6y),$$

and consider the equation $T(v) = (-1, 3)$. Then $v = (1, 1)$ is a solution to this equation. Since $T(v + w) = T(v) + T(w)$ for all $v, w \in \mathbb{R}^2$, $v = (1, 1) + (2y, y) = (1 + 2y, 1 + y)$ ($y \in \mathbb{R}$) is also a solution to the equation $T(v) = (-1, 3)$. In fact, this is a specific example of a general phenomenon:

Theorem 13.3. *Say* $T : \mathbb{R}^n \to \mathbb{R}^m$ *is a linear transformation, and* $w_1 \in \mathbb{R}^m$ *is fixed. Say* $v_1 \in \mathbb{R}^n$ *so that* $T(v_1) = w_1$. *Then* $T(v) = w_1$ *if and only if* $v = v_0 + v_1$ *where* $v_0 \in kerT$.

Discussion of proof: First, suppose $v \in \mathbb{R}^n$ satisfies $T(v) = w_1$. Thus $T(v) = T(v_1)$, and so

$$0 = T(v) - T(v_1) = T(v) + T(-v_1) = T(v - v_1).$$

Hence $v - v_1 \in \ker T$; set $v_0 = v - v_1$. Thus $v = v_0 + v_1$ where $v_0 \in \ker T$.

Now suppose $v_0 \in \ker T$; set $v = v_0 + v_1$. Then

$$T(v) = T(v_0 + v_1) = T(v_0) + T(v_1) = 0 + w_1 = w_1,$$

completing the proof. □

§14. Matrices and representing linear transformations

An $m \times n$ matrix is an array with m rows and n columns. We will see that we can use an $m \times n$ matrix of real numbers to represent a linear transformation $T : \mathbb{R}^n \to \mathbb{R}^m$, and we will see how to use matrices and matrix multiplication to solve systems of linear equations.

Discussion: Consider again the linear transformation $T : \mathbb{R}^3 \to \mathbb{R}^3$ defined by

$$T(x, y, z) = (x + 2y + 3z, 5x - y + 2z, 2x + 3y - z).$$

We can represent T by the 3×3 matrix

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 5 & -1 & 2 \\ 2 & 3 & -1 \end{pmatrix}.$$

So column 1 has the coefficients on x in our definition of T, column 2 the coefficients on y, and column 3 the coefficients on z; row 1 corresponds to the first entry in the triple given by $T(x, y, z)$, row 2 corresponds to the second entry of this triple, and row 3 to the third. To rewrite our definition of T using matrices, we define the product:

$$\begin{pmatrix} 1 & 2 & 3 \\ 5 & -1 & 2 \\ 2 & 3 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1x + 2y + 3z \\ 5x - 1y + 2z \\ 2x + 3y - 1z \end{pmatrix}.$$

Then solving the equation $T(x, y, z) = (3, 13, 0)$ is equivalent to solving

$$A \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3 \\ 13 \\ 0 \end{pmatrix}.$$

When we solved this equation in §9, we looked at a system of 3 equations and used 3 types of elementary operations on the system to obtain an equivalent system from which our solution was easily obtained. In the next section we will discuss how to use multiplication by "elementary matrices" to solve this matrix equation. Let us first discuss why we can represent any linear transformation $T:\mathbb{R}^n \to \mathbb{R}^m$ using an $m \times n$ matrix, and how to define multiplication of matrices.

Discussion: Say $T:\mathbb{R}^n \to \mathbb{R}^m$ is a linear transformation. Then as we saw in §11, T is described by an m-tuple of linear expressions in the variables $x_1, \dots, x_n$: For $v = (x_1, \dots, x_n) \in \mathbb{R}^n$, we saw

$$T(v) = (T_1(v), \dots, T_m(v))$$

where each T_i is a linear transformation from $\mathbb{R}^n$ to $\mathbb{R}$; also, we saw that each T_i is given by a linear equation

$$T_i(x_1, \dots, x_n) = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = \sum_{j=1}^{n} a_{ij}x_j$$

for some $a_{ij} \in \mathbb{R}$. Hence by knowing the values of each a_{ij}, $1 \le i \le m$, $1 \le j \le n$, we can reconstruct T; thus we represent T by the $m \times n$ matrix A whose i,j-entry is a_{ij}:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

(So row i corresponds to T_i, and column j corresponds to the coefficients on x_j in the equations for the T_i.) We sometimes abbreviate and refer to this matrix as (a_{ij}). We define

$$A\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{n} a_{1j}x_j \\ vdots \\ sum_{j=1}^{n} a_{mj}x_j \end{pmatrix}.$$

Note that

$$T(x_1, \dots, x_n) = \left(\sum_{j=1}^{n} a_{1j}x_j, \dots, \sum_{j=1}^{n} a_{mj}x_j \right),$$

so the ith row of $A\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ is the ith entry of $T(x_1, \dots, x_n)$.

Definition. Define $T : \mathbb{R}^n \to \mathbb{R}^n$ to be the identity map, meaning that for any $v \in \mathbb{R}^n$, $T(v) = v$. Equivalently, T is defined by $T(x_1, \dots, x_n) = (x_1, \dots, x_n)$. Then the matrix representing T is

$$I_n = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix},$$

meaning I_n has 1 for each i, i-entry, and 0 for every other entry. I_n is called the $n \times n$ *identity matrix*; sometimes we simply write I for I_n, and call I the identity matrix.

Note: For A an $m \times n$ matrix, $I_m A = A$ and $AI_n = A$.

As we are using matrices to represent linear transformations, which are functions, we define addition and multiplication of matrices to reflect addition and composition of linear transformations.

Definition. Let $A = (a_{ij})$, $B = (b_{ij})$ be $n \times m$ matrices. We define $A + B$ to be the matrix with i, j-entry $a_{ij} + b_{ij}$, and we write $A + B = (a_{ij} + b_{ij})$. Note that since addition in $\mathbb{R}$ is commutative, $A + B = B + A$.

Discussion: Let $S, T : \mathbb{R}^2 \to \mathbb{R}^2$ be linear transformations represented by matrices

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \ B = \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix}.$$

Thus

$$A + B = \begin{pmatrix} 6 & 8 \\ 10 & 12 \end{pmatrix}.$$

Also, $S(x, y) = (x + 2y, 3x + 4y)$, and $T(x, y) = (5x + 6y, 7x + 8y)$. We define the function $S + T$ by $(S + T)(v) = S(v) + T(v)$; thus

$$\begin{aligned} (S + T)(x, y) &= S(x, y) + T(x, y) \\ &= (x + 2y, 3x + 4y) + (5x + 6y, 7x + 8y) \\ &= (6x + 8y, 10x + 12y). \end{aligned}$$

More generally, we have:

Theorem 14.1. *Say $S, T : \mathbb{R}^n \to \mathbb{R}^m$ are linear transformations; let $A = (a_{ij})$ be the matrix representing S, $B = (b_{ij})$ the matrix representing T. Then $S + T$ is a linear transformation represented by the matrix $A + B$.*

Discussion of proof: We know from Theorem 10.1 (a) that $S + T$ is a linear transformation. Also, since A represents S and B represents T, we have

$$S(x_1, \dots, x_n) = \left(\sum_{j=1}^{n} a_{1j} x_j, \dots, \sum_{j=1}^{n} a_{mj} x_j \right),$$

$$T(x_1, \dots, x_n) = \left(\sum_{j=1}^{n} b_{1j} x_j, \dots, \sum_{j=1}^{n} b_{mj} x_j \right).$$

Thus

$$\begin{aligned}(S+T)(x_1,\dots,x_n) &= \left(\sum_{j=1}^{n} a_{1j}x_j,\dots,\sum_{j=1}^{n} a_{mj}x_j\right) + \left(\sum_{j=1}^{n} b_{1j}x_j,\dots,\sum_{j=1}^{n} b_{mj}x_j\right)\\ &= \left(\sum_{j=1}^{n} a_{1j}x_j + \sum_{j=1}^{n} b_{1j}x_j,\dots,\sum_{j=1}^{n} a_{mj}x_j + \sum_{j=1}^{n} b_{mj}x_j\right)\\ &= \left(\sum_{j=1}^{n}(a_{1j}+b_{1j})x_j,\dots,\sum_{j=1}^{n}(a_{mj}+b_{mj})x_j\right).\end{aligned}$$

Since

$$\begin{aligned}(A+B)\begin{pmatrix} x_1\\ x_2\\ \vdots\\ x_n\end{pmatrix} &= \begin{pmatrix} (a_{11}+b_{11})x_1 + (a_{12}+b_{12})x_2 + \cdots + (a_{1n}+b_{1n})x_n\\ (a_{21}+b_{21})x_1 + (a_{22}+b_{22})x_2 + \cdots + (a_{2n}+b_{2n})x_n\\ \vdots\\ (a_{m1}+b_{m1})x_1 + (a_{m2}+b_{m2})x_2 + \cdots + (a_{mn}+b_{mn})x_n\end{pmatrix}\\ &= \begin{pmatrix} \sum_j (a_{1j}+b_{1j})x_j\\ \sum_j (a_{2j}+b_{2j})x_j\\ \vdots\\ \sum_j (a_{mj}+b_{mj})x_j\end{pmatrix},\end{aligned}$$

we see matrix addition is equivalent to addition of the linear transformations the matrices represent. □

We now define multiplication of matrices; as we will see, this corresponds to composition of linear transformations.

Definition. Say $A = (a_{ij})$ is an $m \times n$ matrix, and $B = (b_{ij})$ is an $n \times r$ matrix. Then AB is the $m \times r$ matrix with i,j-entry

$$(\text{row } i \text{ of } A)\cdot(\text{column } j \text{ of } B)^t = \sum_{k=1}^{n} a_{ik}b_{kj},$$

where (column j of $B)^t$ denotes the *transpose* of column j of B, meaning we transpose the column into a row.

Discussion: Let $A = \begin{pmatrix} 1 & 2\\ 3 & 4\end{pmatrix}$, $B = \begin{pmatrix} 5 & 6\\ 7 & 8\end{pmatrix}$. Then AB has $1,1$-entry

$$(1,2)\cdot(5,7) = 1\cdot 5 + 2\cdot 7 = 19,$$

AB has $1,2$-entry

$$(1,2)\cdot(6,8) = 1\cdot 6 + 2\cdot 8 = 22,$$

AB has $2,1$-entry

$$(3,4)\cdot(5,7) = 3\cdot 5 + 4\cdot 7 = 43,$$

and AB has $2,2$-entry

$$(3,4)\cdot(6,8) = 3\cdot 6 + 4\cdot 8 = 50.$$

(Note that here we have inserted commas between the entries of the matrix entries.) Thus

$$AB = \begin{pmatrix} 19 & 22 \\ 43 & 50 \end{pmatrix}.$$

Discussion: Given matrices A, B, when can we take their product? We need to be able to compute these dot products. Can we take the dot product of any two vectors? For instance, does $(1,2)\cdot(3,4,5)$ make sense?

Say $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$, $B = \begin{pmatrix} 7 & 8 \\ 9 & 10 \end{pmatrix}$. Then we cannot multiply AB, but

$$\begin{aligned} BA &= \begin{pmatrix} 7 & 8 \\ 9 & 10 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 7\cdot 1 + 8\cdot 4 & 7\cdot 2 + 8\cdot 5 & 7\cdot 3 + 8\cdot 6 \\ 9\cdot 1 + 10\cdot 4 & 9\cdot 2 + 10\cdot 5 & 9\cdot 3 + 10\cdot 6 \end{pmatrix} \\ &= \begin{pmatrix} 39 & 54 & 69 \\ 49 & 68 & 87 \end{pmatrix}. \end{aligned}$$

Definition. Say A is an $m \times n$ matrix. It is not difficult to verify that for I_m the $m \times m$ identity matrix, $I_m A = A$, and for I_n the $n \times n$ identity matrix, $AI_n = A$.

Discussion: Say $T, S : \mathbb{R}^2 \to \mathbb{R}^2$ are the linear transformations defined by

$$T(x,y) = (2x + y, -x + 3y),\ S(x,y) = (x + 5y, -7x + 4y).$$

Then the composition $S \circ T$ is given by

$$\begin{aligned} S \circ T(x,y) &= S(T(x,y)) \\ &= S(2x + y, -x + 3y) \\ &= ((2x + y) + 5(-x + 3y), -7(2x + y) + 4(-x + 3y)) \\ &= (-3x + 16y, -18x + 5y). \end{aligned}$$

Now let A be the matrix for S, B the matrix for T. So

$$A = \begin{pmatrix} 1 & 5 \\ -7 & 4 \end{pmatrix},\ B = \begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix}.$$

The product AB is

$$\begin{pmatrix} 1 & 5 \\ -7 & 4 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} -3 & 16 \\ -18 & 5 \end{pmatrix},$$

which is the matrix representing $S \circ T$.

In general, we have:

Theorem 14.3. *Say* $S : \mathbb{R}^m \to \mathbb{R}^t$*,* $T : \mathbb{R}^n \to \mathbb{R}^m$ *are linear transformations represented by the matrices* $A = (a_{ij}), B = (b_{ij})$ *(respectively). Then* $S \circ T$ *is a linear transformation represented by the matrix* AB*.*

Discussion of proof: (In the Exercise, you verify this theorem when $n = m = t = 2$.) We know from Theorem 10.1 (b) that $S \circ T$ is a linear transformation. Since $B = (b_{ij})$ represents T, we know

$$T(x_1, \dots, x_n) = \left(\sum_j b_{1j} x_j, \dots, \sum_j b_{nj} x_j \right)$$

(where in these sums j runs from 1 to n). Similarly,

$$S(y_1, \dots, y_m) = \left(\sum_k a_{1k} y_k, \dots, \sum_k a_{tk} y_k \right)$$

(where k runs from 1 to m). Thus

$$\begin{aligned} S \circ T(x_1, \dots, x_n) &= S \left(\sum_j b_{1j} x_j, \dots, \sum_j b_{nj} x_j \right) \\ &= \left(\sum_k a_{1k} \left(\sum_j b_{kj} x_j \right), \dots, \sum_k a_{tk} \left(\sum_j b_{kj} x_j \right) \right) \\ &= \left(\sum_{k,j} a_{1k} b_{kj} x_j, \dots, \sum_{k,j} a_{mk} b_{kj} x_j \right). \end{aligned}$$

Thus the ith entry of $S \circ T(x_1, \dots, x_n)$ is

$$\left(\sum_{k=1}^{m} a_{ik} b_{k1} \right) x_1 + \cdots + \left(\sum_{k=1}^{m} a_{ik} b_{kn} \right) x_n.$$

So the matrix representing $S \circ T$ has i, j-entry

$$\sum_{k=1}^{m} a_{ik} b_{kj},$$

which is the i, j-entry of AB. Hence AB is the matrix representing $S \circ T$. □

Theorem 14.4. *Matrix multiplication is associative, and matrix multiplication distributes over matrix addition.*

Discussion of proof: First, say A, B, C are matrices of sizes $s \times t$, $t \times m$, $m \times n$ (respectively). Let $R : \mathbb{R}^t \to \mathbb{R}^s$, $S : \mathbb{R}^m \to \mathbb{R}^t$, $T : \mathbb{R}^n \to \mathbb{R}^m$ be the linear transformations associated to these matrices. Then $A(BC)$ is the matrix associated to $R\circ(S\circ T)$, and $(AB)C$ is the matrix associated to $(R\circ S)\circ T$; since $R\circ(S\circ T) = (R\circ S)\circ T$, we have $A(BC) = (AB)C$.

Similarly, say A is a $t\times m$ matrix, and B, C are $m\times n$ matrices; let $R : \mathbb{R}^m \to \mathbb{R}^t$ be the linear transformation associated to A, and let $S, T : \mathbb{R}^n \to \mathbb{R}^m$ be the linear transformations associated to B, C. Then we know $B + C$ is the matrix associated to $S+T$, and $A(B+C)$ the matrix associated to $R\circ(S+T)$. Also, AB is the matrix associated to $R \circ S$, and AC the matrix associated to $R \circ T$. Since, by Theorem 10.2, $R \circ (S + T) = R \circ S + R \circ T$, we have $A(B + C) = AB + AC$. □

§15. Echelon forms and elementary matrices

Here we see that when a matrix A has a certain shape, it is relatively easy to solve an equation $Av = w$, and then we see how to use "elementary matrices" to put a matrix into this sort of shape, called "reduced row echelon form".

Definition. An $m\times n$ matrix is said to be in *row echelon form* if each nonzero row begins with more zeros than the preceeding row (and thus any rows of zeros occur below all nonzero rows). An $m\times n$ matrix is said to be in *reduced row echelon form* if it is in row echelon form, and each leading nonzero entry in any nonzero row is 1.

Discussion: When a matrix A is in reduced row echelon form, it is easy to solve an equation

$$A\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix}$$

for the values of x_i.

For example, consider the equation

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 5 \\ 6 \\ 7 \end{pmatrix}.$$

Clearly we must have $x_3 = 7$; then we must also have $x_2 + 4\cdot 7 = 6$, or equivalently, $x_2 = -22$. So we must also have $x_1 + 2\cdot(-22) + 3\cdot 7 = 5$, or equivalently, $x_1 = 28$.

Let us consider another example:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 5 \\ 6 \\ 7 \end{pmatrix}$$

has no solution since we cannot have $0x_1 + 0x_2 + 0x_3 = 7$. (Thus the linear transformation associated to the above 3×3 matrix is not surjective.)

Finally, let us consider one more example:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

has many solutions, for the equation holds provided $x_4 = 0$, $x_3 = 1$, and $x_1 + 2x_2 = 0$ (and this last equation holds for any $x_2 \in \mathbb{R}$ provided we have $x_1 = -2x_2$). (Thus the linear transformation associated to the above 3×4 matrix is not injective.)

Given any matrix A, we will see that we can left-multiply A by "elementary matrices" to produce a matrix EA in reduced row echelon form. We will also see that a product E of elementary matrices represents a bijective linear transformation, and that consequently, with v, w column matrices, the equation $Av = w$ is solvable for v exactly when $EAv = Ew$ is solvable for v. Also, using Theorem 12.2, we will be able to conclude that the linear transformation associated to A is injective exactly when the linear transformation associated to EA is, and the linear transformation associated to A is surjective exactly when the linear transformation associated to EA is.

The elementary matrices correspond to the elementary operations we used earlier to solve a system of linear equation. Before defining elementary matrices in general, let us consider an example.

Discussion: We revisit our initial example of §9, written as a matrix equation.

$$\begin{pmatrix} 1 & 2 & 3 \\ 5 & -1 & 2 \\ 2 & 3 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3 \\ 13 \\ 0 \end{pmatrix}.$$

We can "eliminate" the $(2,1)$-entry of the 3×3 matrix by multiplying the equation on the left by

$$\begin{pmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

to get

$$\begin{pmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 5 & -1 & 2 \\ 2 & 3 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 13 \\ 0 \end{pmatrix},$$

or equivalently,

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -11 & -13 \\ 2 & 3 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3 \\ -2 \\ 0 \end{pmatrix}.$$

Next, we eliminate the $(3,1)$-entry of the new 3×3 matrix by multiplying our new matrix equation on the left by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2 & 0 & 1 \end{pmatrix}$$

to get

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 0 & -11 & -13 \\ 2 & 3 & -1 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2 & 0 & 1 \end{pmatrix}\begin{pmatrix} 3 \\ -2 \\ 0 \end{pmatrix},$$

or equivalently,

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -11 & -13 \\ 0 & -1 & -7 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3 \\ -2 \\ -6 \end{pmatrix}.$$

Now we multiply row 3 of our matrix equation by -1 by multiplying the equation on the left by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

to get

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -11 & -13 \\ 0 & 1 & 7 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}\begin{pmatrix} 3 \\ -2 \\ -6 \end{pmatrix} = \begin{pmatrix} 3 \\ -2 \\ 6 \end{pmatrix}.$$

Now we swap rows 2 and 3 by left-multiplying by the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

to get

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 7 \\ 0 & -11 & -13 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3 \\ 6 \\ -2 \end{pmatrix}.$$

Next, we eliminate the $(3,2)$-entry of the new 3×3 matrix by left-multiplying the matrix equation by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 11 & 1 \end{pmatrix}$$

to get

$$\begin{pmatrix}1 & 2 & 3\\ 0 & 1 & 7\\ 0 & 0 & 64\end{pmatrix}\begin{pmatrix}x\\ y\\ z\end{pmatrix}=\begin{pmatrix}3\\ 6\\ 64\end{pmatrix}.$$

Finally, we left-multiply our new matrix equation by

$$\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1/64\end{pmatrix}$$

to get

$$\begin{pmatrix}1 & 2 & 3\\ 0 & 1 & 7\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}x\\ y\\ z\end{pmatrix}=\begin{pmatrix}3\\ 6\\ 1\end{pmatrix}.$$

We can easily solve this last equation: We must have $z=1$, and so we must have $y+7\cdot 1=6$, or equivalently, $y=-1$, and so we must have $x+2\cdot(-1)+3\cdot 1=3$, or equivalently, $x=2$.

Definition. Fix a positive integer m; we define 3 types of elementary linear transformations on $\mathbb{R}^m$, and we describe the $m\times m$ matrices that represent these.

For $1\le k\le m$, $1\le \ell\le m$, define $S_{k\ell}:\mathbb{R}^m\to\mathbb{R}^m$ to be the linear transformation that swaps the kth and ℓth entries of a vector in $\mathbb{R}^m$; so

$$S_{k\ell}(x_1,\dots,x_m)=(x_1',\dots,x_m') \text{ where } x_i'=\begin{cases}x_i & \text{if } i\ne k,\ell,\\ x_\ell & \text{if } i=k,\\ x_k & \text{if } i=\ell.\end{cases}$$

Thus the matrix $E_{k\ell}$ representing $S_{k\ell}$ has (i,j)-entry

$$\begin{cases}1 & \text{if } i=j, i\ne k,\ell,\\ 1 & \text{if } (i,j)=(k,\ell) \text{ or } (i,j)=(\ell,k),\\ 0 & \text{otherwise.}\end{cases}$$

Notice that $S_{k\ell}=S_{\ell k}$.

For $1\le k\le m$, $1\le\ell\le m$, and $\alpha\in\mathbb{R}$, $\alpha\ne 0$, define $S_{k\ell}(\alpha):\mathbb{R}^m\to\mathbb{R}^m$ to be the linear transformation that adds α times entry ℓ to entry k; so

$$S_{k\ell}(\alpha)(x_1,\dots,x_m)=(x_1',\dots,x_m') \text{ where } x_i'=\begin{cases}x_i & \text{if } i\ne k,\\ \alpha x_\ell+x_k & \text{if } i=k.\end{cases}$$

Thus the matrix $E_{k\ell}(\alpha)$ representing $S_{k\ell}(\alpha)$ has (i,j)-entry

$$\begin{cases}1 & \text{if } i=j,\\ \alpha & \text{if } (i,j)=(k,\ell),\\ 0 & \text{otherwise.}\end{cases}$$

For $1 \leq k \leq m$ and $\alpha \in \mathbb{R}$, $\alpha \neq 0$, we define $S_k(\alpha) : \mathbb{R}^n \to \mathbb{R}^m$ to be the linear transformation that multiplies entry k by α; thus

$$S_k(\alpha)(x_1, \dots, x_m) = (x'_1, \dots, x'_m) \text{ where } x'_i = \begin{cases} x_i & \text{if } i \neq k, \\ \alpha x_k & \text{if } i = k. \end{cases}$$

Thus the matrix $E_k(\alpha)$ representing $S_k(\alpha)$ has (i, j)-entry

$$\begin{cases} 1 & \text{if } i = j \neq k, \\ \alpha & \text{if } i = j = k, \\ 0 & \text{if } i \neq j. \end{cases}$$

Theorem 15.1. *An $m \times n$ matrix A (with real entries) can be left-multiplied by suitable elementary matrices $B_0, \dots, B_k$ so that $B_k \cdots B_0 A$ is in reduced row echelon form.*

Discussion of proof: We present an algorithm to accomplish this.

First, consider column 1 of A. If column 1 of A consists of zeros, then there is nothing we need to do to this column. Suppose column 1 has a nonzero entry in row ℓ; then we left-multiply A by an elementary matrix B_0 to swap the first row of A with row ℓ (if $\ell = 1$ then $B_0 = I$). Then we left-multiply by an elementary matrix B_1 to make the $1,1$-entry of $B_0 A$ be 1. Now we left-multiply $B_1 B_0 A$ by elementary matrices $B_2, \dots, B_m$ to eliminate the 1st entries in all rows below row 1 of $B_1 B_0 A$. Thus $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ is the first column of $(B_m \cdots B_1 B_0)A$. So column 1 and row 1 of this new matrix meet the conditions for reduced row echelon form.

Repeat the process described above, but focus on column 2 of $(B_m \cdots B_1 B_0)A$, ignoring row 1; then proceed to column 3 (ignoring rows 1 and 2); etc. In this way we find elementary matrices $B_k, \dots, B_0$ to that $(B_k \cdots B_0)A$ is in reduced row echelon form. $\square$

Discussion: Suppose A is is reduced row echelon form. Then we can left-multiply A by a sequence of elementary matrices whose product is B so that BA is also in reduced row echelon form with the additional property that if row k is nonzero with its leading nonzero coefficient in column ℓ, then the other entries in column ℓ are zeros. For instance, say

$$A = \begin{pmatrix} 1 & 3 & 5 & 9 \\ 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then with

$$B_0 = \begin{pmatrix} 1 & -5 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

we get

$$B_0A = \begin{pmatrix} 1 & 3 & 0 & -26 \\ 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Continuing, let

$$B_1 = \begin{pmatrix} 1 & 0 & 26 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix};$$

then

$$B_1B_0A = \begin{pmatrix} 1 & 3 & 0 & 0 \\ 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Finally, setting

$$B_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -7 \\ 0 & 0 & 1 \end{pmatrix},$$

we get

$$B_2B_1B_0A = \begin{pmatrix} 1 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Discussion: Suppose A is in reduced row echelon form with the additional property that any column with the leading nonzero entry of some row has zeros as its other entries, and suppose and no row's leading nonzero entry lies in column ℓ. Then A represents a linear transformation that is not injective: For instance, suppose

$$A = \begin{pmatrix} 1 & 0 & 5 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Thus

$$A\begin{pmatrix} 5 \\ 3 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 5 \\ 3 \\ 0 \end{pmatrix} \text{ and } A\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 5 \\ 3 \\ 0 \end{pmatrix}.$$

Discussion: Say A is an $m \times n$ matrix in row echelon form. So each nonzero row begins with more zeros than the preceding row, so row i begins with at least $i-1$ zeros, or row i is a row of n zeros. If A has a row of zeros then A represents a linear transformaion that is not surjective: For instance, suppose

$$A = \begin{pmatrix} 1 & 3 & 5 \\ 0 & 1 & 7 \\ 0 & 0 & 0 \end{pmatrix}.$$

Then

$$A\,(\,x//y//z\,) = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

has no solutions.

§16. Surjectivity, Injectivity, and Inverses

Definition. For A an $n \times n$ matrix, say A is *invertible* if there exists an $n \times n$ matrix B so that $BA = I_n = AB$; in this case we call B the *inverse* of A, and is often denoted A^{-1}.

Theorem 16.1. *Suppose B is a product of $m \times m$ elementary matrices; then B represents a bijective linear transformation $S : \mathbb{R}^m \to \mathbb{R}^m$, and B is invertible. Thus if A is an $m \times n$ matrix, then $Av = w$ is solvable for v if and only if $BAv = Bw$ is solvable for v.*

Discussion of proof: We know that the composition of bijective maps is again bijective, and the composition of linear transformations is a linear transformation; thus we need verify that each of the three types of elementary linear transformations is bijective.

Recall that $S_{k\ell}$ is the elementary transformation that swaps the kth and ℓth entries; so if we apply $S_{k\ell}$, the kth and ℓth entries are swapped back to their original positions. Thus $S_{k\ell} \circ S_{k\ell}(v) = v$ for any $v \in \mathbb{R}^m$; so $S_{k\ell}$ is its own inverse, and $S_{k\ell}$ is bijective.

For $\alpha \in \mathbb{R}$, $S_{k\ell}(\alpha)$ is the elementary transformation that adds α times the ℓth entry of a vector to the kth entry of the vector. Thus $S_{k\ell}(\alpha) \circ S_{k\ell}(\alpha)$ is the identity map, and hence $S_{k\ell}(\alpha)$ is bijective.

Finally, for $\alpha \in \mathbb{R}$, $\alpha \neq 0$, $S_k(\alpha)$ is the elementary transformation that multiplies the kth entry of a vector by α. Thus $S_k(1/\alpha) \circ S_k(\alpha)$ is the identity map, and hence $S_k(\alpha)$ is bijective.

Thus S is a bijective linear transformation, so S^{-1} exists and is a bijective linear transformation. Let B' be the matrix representing S^{-1}. Then since $S^{-1} \circ S = S \circ S^{-1} = \iota$, the identity map on $\mathbb{R}^m$, we have $B'B = BB' = I_m$. Hence B is invertible.

Since B is invertible, the equation $Av = w$ is equivalent to the equation $BAv = Bw$. $\square$

There are some immediate consequences of the above theorem.

Theorem 16.2. *Suppose $T : \mathbb{R}^n \to \mathbb{R}^m$ is a linear transformation.*

(1) If $m > n$ then T is not surjective.
(2) If $m < n$ then T is not injective.
(3) Suppose $m = n$; then T is injective if and only if T is surjective.

Discussion of proof: Let A be the $m \times n$ matrix representing T, and let B be a product of $m \times m$ elementary matrices so that BA is in reduced row echlelon form.

Let $S : \mathbb{R}^m \to \mathbb{R}^m$ be the linear transformation represented by B; recall that since B is a product of elementary matrices, S is bijective.

(1) Suppose $m > n$. We know row n of BA must begin with at least $n-1$ zeros; since $m > n$, row m must begin with at least n zeros. But each row of BA has exactly n entries, so row m must be a row of zeros. Hence

$$BA \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

has no solution, which means $S \circ T$ is not surjective.

(2) Suppose $m < n$. Then

$$A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

is equivalent to a system of m linear equations in n variables. From experience (and discussed more thoroughly in Appendix 16A), such a system either has no solutions or more than one solution. Since $x_1 = \cdots = x_n = 0$ is one solution, the system must have more than one solution. Hence T, the linear transformation represented by A, cannot be injective.

(3) Suppose $m = n$. First, suppose BA has $k \geq 1$ rows of zeros. Then

$$BA \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

has no solution, and hence T is not surjective. Also,

$$BA \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

is equivalent to a (consistent)system of $n-k$ linear equations in n unknowns, and hence it has more than one solution. Thus T is not injective.

Now suppose BA has no rows of zeros. Then because BA is in reduced row echelon form, the nth row of BA begins with $n-1$ zeros, and its nth entry must be 1. Thus the $(n-1)$st row of BA begins with at least $n-1$ zeros, but cannot begin with as many zeros as row n; hence the $(n-1)$st row of BA begins with $n-2$ zeros, and its $(n-1)$st entry must be 1. Continuing, we find

$$BA = \begin{pmatrix} 1 & * & * & \cdots & * & * \\ 0 & 1 & * & \cdots & * & * \\ 0 & 0 & 1 & \cdots & * & * \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

(where $*$ denotes an unknown entry). Thus given any $(c_1, \dots, c_n) \in \mathbb{R}^n$,

$$BA \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$$

has a unique solution. Therefore BA represents a bijective linear transformation, and hence so does A.

Thus when $m = n$, either T is niether surjective nor injective, or T is bijective. Hence T is injective if and only if T is surejective. $\square$

In the Exercises you prove the following.

Theorem 16.3. *Suppose A is an $n \times n$ matrix representing the linear transformation $T : \mathbb{R}^n \to \mathbb{R}^n$, and suppose T is bijective. There there exists an $n \times n$ matrix B so that $BA = I = AB$.*

Somewhat similarly, we also have

Theorem 16.4. *Suppose A, B are $n \times n$ matrices so that $BA = I$. Then $AB = I$.*

Discussion of proof: Let $S, T : \mathbb{R}^n \to \mathbb{R}^n$ be the linear transformations represented by B, A (respectively). Thus $BA = I$ represents $S \circ T$, meaning $S \circ T$ is ι, the identity map on $\mathbb{R}^n$. In particular, this means $S \circ T$ is injective, and hence T is injective. By Theorem 16.2, this means T is bijective. Thus T^{-1} exists, and

$$\begin{aligned} T^{-1} &= \iota \circ T^{-1} \\ &= (S \circ T) \circ T^{-1} \\ &= S \circ (T \circ T^{-1}) \\ &= S \circ \iota \\ &= S. \end{aligned}$$

Since AB represents $T \circ S$ and

$$T \circ S = T \circ T^{-1} = \iota,$$

we must have $AB = I$. $\square$

§16A. Appendix: Linear transformations from $\mathbb{R}^n$ to $\mathbb{R}^m$ when $m < n$

Suppose $T : \mathbb{R}^n \to \mathbb{R}^m$ is a linear transformation represented by the matrix A, and suppose $m < n$. Let B be a product of elementary matrices so that BA is in row echelon form. Thus with $S : \mathbb{R}^m \to \mathbb{R}^m$ the linear transformation represented by B, we know S is bijective and hence T is injective if and only if $S \circ T$ is injective. Also, we know BA represents $S \circ T$. Here we discuss why $m < n$ implies that $S \circ T$ is not injective (and hence T is not injective).

Let c_{ij} be the i, j-entry of BA (meaning the entry in row i and column j of BA). Note that since BA is in row echelon form, $c_{ij} = 0$ whenever $i > j$. Then with $\underline{0}$ the $m \times 1$ matrix of zeros, the matrix equation

$$BA \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \underline{0}$$

is equivalent to the system of m equations

$$\begin{aligned} c_{11}x_1 + c_{12}x_2 + c_{13}x_3 + \cdots + c_{1m} + \cdots + c_{1n}x_n &= 0 \\ c_{22}x_2 + c_{23}x_3 + \cdots + c_{2m} + \cdots + c_{2n}x_n &= 0 \\ c_{33}x_3 + \cdots + a_{3m} + \cdots + c_{3n}x_n &= 0 \\ &\vdots \\ c_{mm}x_m + \cdots + c_{1n}x_n &= 0 \end{aligned}$$

(Note that some c_{ii} could be zero, and then we must have $c_{\ell\ell} = 0$ for all $\ell > i$ since BA is in row echelon form.) Since $m < n$, either some variable x_k does not appear in any of the equations, or (at least) one of the equations has more than one non-zero coefficient. In either case, the system has infinitely many solutions: In the first instance, one can set x_k to any value, and the other variables x_i to 0 and have a solution to the system. In the second instance, one solves the system beginning with a solution to the mth equation, and then using those values, proceeds to solve the $m-1$st equation, which includes at least one more variable than the mth equation; then using all those values, one proceeds to solve the $m-2$nd equation, which includes at least one more variable. If the mth equation includes more than one variable (meaning more than one variable has a non-zero coefficient), then this equation has more than one solution, and the process of back-substitution leads to more than one solution to the system. Otherwise, at some point in the process of back-substitution one encounters an equation with (at least) two variables not already encountered; so one finds more than one solution to this equation, and hence the process yields more than one solution to the system. Consequently, the equation

$$BA \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \underline{0}$$

has more than one solution, which means the linear transformation $S \circ T$ represented by BA is not injective, and as discussed above, this means T is not injective.

This argument is far from elegant. In §27, we use theory about vector spaces and linear transformations to give a much simpler proof that when $m < n$, a linear transformation $T : \mathbb{R}^n \to \mathbb{R}^m$ is not injective.

§17. Augmented matrices: a computational device

We can use augmented matrices to abbreviate matrix equations.

Discussion: Consider

$$\begin{pmatrix} 1 & 2 \\ 5 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3 \\ 13 \end{pmatrix}.$$

We can abbreviate this equation using the so-called augmented matrix

$$\widetilde{A} = \begin{pmatrix} 1 & 2 & | & 3 \\ 5 & -1 & | & 13 \end{pmatrix}.$$

We left-multiply by

$$B_0 = \begin{pmatrix} 1 & 0 \\ -5 & 1 \end{pmatrix}$$

to get

$$B_0\widetilde{A} = \begin{pmatrix} 1 & 2 & | & 3 \\ 0 & -11 & | & -2 \end{pmatrix}.$$

Then with $B_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1/11 \end{pmatrix}$,

$$B_1B_0\widetilde{A} = \begin{pmatrix} 1 & 2 & | & 3 \\ 0 & 1 & | & 2/11 \end{pmatrix}.$$

Finally, with $B_2 = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$, we get

$$B_2B_1B_0\widetilde{A} = \begin{pmatrix} 1 & 0 & | & 29/11 \\ 0 & 1 & | & 2/11 \end{pmatrix}.$$

This last matrix is an abbreviation for the equation

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 29/11 \\ 2/11 \end{pmatrix},$$

or equivalently, $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 29/11 \\ 2/11 \end{pmatrix}$.

Note that we cannot always reduce the left-hand side of an augmented matrix to the identity matrix; this occurs when there are either no solutions or infinitely many solutions to an equation. For instance, with

$$\widetilde{A} = \begin{pmatrix} 1 & -3 & | & 1 \\ 7 & -21 & | & 1 \end{pmatrix},$$

we have

$$\begin{pmatrix} 1 & 0 \\ -7 & 1 \end{pmatrix} \widetilde{A} = \begin{pmatrix} 1 & -3 & | & 1 \\ 0 & 0 & | & -6 \end{pmatrix};$$

this represents the equation

$$\begin{pmatrix} 1 & -3 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ -6 \end{pmatrix}$$

or equivalently the system

$$\begin{aligned} x - 3y &= 1 \\ 0 &= -6 \end{aligned}$$

which has no solution.

Somewhat similarly, with

$$\widetilde{A} = \begin{pmatrix} 1 & -1 & 1 & | & 1 \\ 1 & 1 & 2 & | & 0 \end{pmatrix}$$

we have

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \widetilde{A} &= \begin{pmatrix} 1 & -1 & 1 & | & 1 \\ 0 & 2 & 1 & | & -1 \end{pmatrix}, \\ \begin{pmatrix} 1 & 0 \\ 0 & 1/2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \widetilde{A} &= \begin{pmatrix} 1 & -1 & 1 & | & 1 \\ 0 & 1 & 1/2 & | & -1/2 \end{pmatrix}. \end{aligned}$$

Thus the solutions to the system

$$\begin{aligned} x - y + z &= 1 \\ x + y + 2z &= 0 \end{aligned}$$

are the solutions to

$$\begin{aligned} x - y + z &= 1 \\ y + \frac{1}{2}z &= -\frac{1}{2}, \end{aligned}$$

and these solutions are $y + \frac{1}{2}z = -\frac{1}{2}$, or $y = -\frac{1}{2} - \frac{1}{2}z$, and $x - y + z = 1$, or $x = 1 + y - z = \frac{1}{2} - \frac{3}{2}z$.

We can also use this method to find the inverse of a matrix (if this inverse exists). Given a square matrix A, say we want to find A^{-1}. So we want to solve for X the equation

$$AX = I.$$

If A has an inverse, we can left-multiply the augmented matrix $(A|I)$ by elementary matrices until we obtain $(I|B)$, which is an abbreviation for the equation $IX = B$, which is equivalent to $X = B$. So $X = B$ is a solution to the original equation $AX = I$, meaning $B = X = A^{-1}$.

Suppose A is a square matrix but does not have an inverse; then A can be row-reduced to a matrix with bottom row zeros. Thus we can left-multiply the augmented matrix $(A|I)$ to get $(A'|B)$ where A' is in row echelon form with bottom row zeros. Also, B is a product of elementary matrices, and hence is an invertible matrix. The augmented matrix $(A'|B)$ is an abbreviation for the equation $A'X = B$, but $A'X$ represents a linear transformation that is not surjective, while B represents a bijective linear transformation. So the equation $A'X = B$ has no solution, which means $AX = I$ has no solution.

§18. Determinants and volumes

The "determinant" of a matrix measures how the associated linear transformation changes the volume (and orientation) of a basic box. We will look first at how elementary linear transformations change the volume and orientation of a basic box.

Discussion: Consider elementary transformations on $\mathbb{R}^2$, and the box B with vertices $(0,0),(1,0),(0,1),(1,1)$. We know that an injective linear transformation T maps lines to lines, parallel lines to parallel lines, and 0 to 0. Thus to understand what T does to B, we only need to know $T(1,0)$ and $T(0,1)$.

First consider the elementary transformation S_{12}; this maps $(1,0)$ to $(0,1)$, and $(0,1)$ to $(1,0)$. So S_{12} maps B to itself, but since it swaps the sides from $(0,0)$ to $(1,0)$ and from $(0,0)$ to $(0,1)$, we consider the orientation of the box to have changed. Correspondingly, the determinant of this transformation is defined to be -1.

Next consider the elementary transformation $S_{12}(\alpha)$ where $\alpha \in \mathbb{R}$. This maps $(1,0)$ to itself, and $(0,1)$ to $(\alpha,1)$; so the base of B is left fixed, but $S_{12}(\alpha)$ skews B into a parallelogram, whose height is 1. The orientation is left unchanged; correspondingly, the determinant of this transformation is defined to be 1.

Finally consider the elementary transformation $S_1(\alpha)$, $\alpha \in \mathbb{R}$, $\alpha \neq 0$. So this maps $(1,0)$ to $(\alpha,0)$, and $(0,1)$ to itself. So the orientation of B is preserved, but its base now has length α. Correspondingly, the determinant of this transformation is defined to be α.

Definition. Let A be a square matrix. We define the *deteminant*, $\det A$ (sometimes denoted $|A|$), inductively:

If $A = (a)$ is 1×1, $\det A = a$.

If $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ is 2×2, $\det A = a_{11}a_{22} - a_{12}a_{21}$.

Say $n > 2$ and $A = (a_{ij})$ is $n \times n$. Let $A_{k\ell}$ denote the $(n-1)\times(n-1)$ matrix we obtain by eliminating from A row k and column ℓ. Then we define

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

Discussion: With

$$A = \begin{pmatrix} 3 & 5 & -7 \\ 1 & 2 & 4 \\ 6 & -1 & 9 \end{pmatrix},$$

we have

$$\begin{aligned}\det A &= \begin{vmatrix} 3 & 5 & -7 \\ 1 & 2 & 4 \\ 6 & -1 & 9 \end{vmatrix} \\ &= 3 \cdot \begin{vmatrix} 2 & 4 \\ -1 & 9 \end{vmatrix} - 5 \cdot \begin{vmatrix} 1 & 4 \\ 6 & 9 \end{vmatrix} + (-7) \cdot \begin{vmatrix} 1 & 2 \\ 6 & -1 \end{vmatrix} \\ &= 3(18+4) - 5(9-24) - 7(-1-12) \\ &= 232.\end{aligned}$$

Facts. For any k $(1 \le k \le n)$,

$$\det A = \sum_{\ell=1}^{n} (-1)^{\ell-k} a_{k\ell} \det A_{k\ell},$$

and for any ℓ $(1 \le \ell \le n)$,

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

These facts can be deduced from another extremely useful fact:

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

(presuming A, B are square matrices of the same size).

Discussion: An honest proof of the fact that $\det(AB) = (\det A)(\det B)$ is beyond the scope of this course. However, we can give some intuition about why this is true. Given $n \times n$ matrices A, B, these represent linear transformations from $\mathbb{R}^n$ to $\mathbb{R}^n$, and AB represents the composition of these linear transformations.

Say A represents $T : \mathbb{R}^n \to \mathbb{R}^n$. We know that T maps lines to lines (or points), and so T maps a fundamental unit box to a parallelopiped.

When $n = 2$, T maps the box with vertices $(0,0)$, $(1,0)$, $(0,1)$ and $(1,1)$ to a parallelogram with vertices $T(0,0)$, $T(1,0)$, $T(0,1)$ and $T(1,1)$; sometimes (when T is not injective) this "parallelogram" is actually just a line segment, or the point $(0,0)$. When $n > 2$, the situation is similar.

So $\det A$ tells us how T distorts distances and changes orientation.

For instance, $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ represents the linear transformation $T : \mathbb{R}^2 \to \mathbb{R}^2$ defined by $T(x,y) = (y,x)$, and $\det T = -1$. So (without being precise and giving all relevant definitions) this map T changes our usual orientation on $\mathbb{R}^2$.

As another instance, when $A = \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}$, A represents $T : \mathbb{R}^2 \to \mathbb{R}^2$ defined by $T(x,y) = (5x, y)$; $\det T = 5$ and T stretches vectors by a factor of 5 along the x-axis.

Another instance: when $A = \begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix}$, A represents $T : \mathbb{R}^2 \to \mathbb{R}^2$ defined by $T(x, y) = \big(x + 2y, 3(x + 2y)\big)$. So T maps all vectors to the line

$$L = \{\alpha(1, 2) : \ \alpha \in \mathbb{R}\ \},$$

and so T collapses any box to a line segment, which has 2-dimensional volume 0. Also, $\det T = 0$.

We know that when we compose 2 linear transformations T, S given by the matrices A, B, the composition $T \circ S$ is given by AB. We can measure how $T \circ S$ distorts distances and changes orientation by measuring first what S does in this regard, followed by what T does.

We can left-multiply a matrix A by an elementary permutation matrix $E_{k\ell}$ to swap rows k and ℓ of A; similarly, right-multiplying A by $E_{k\ell}$ swaps columns k and ℓ. Using this observation together with the fact that $\det(BA) = \det(AB) = (\det B)(\det A)$ one can deduce (with some effort) the other formulas for computing $\det A$.

Theorem 18.1. *Say A is an $n \times n$ matrix. Then $\det A \neq 0$ is equivalent to A being invertible. Thus for $T : \mathbb{R}^n \to \mathbb{R}^n$ a linear transformation represented by A, T is bijective if and only if $\det A \neq 0$.*

Discussion of proof: We have seen that we can left-multiply A by a product B of elementary matrices so that BA is in reduced row echelon form. When A is not invertible, we have seen that BA has a row of zeros, and hence $\det(BA) = 0$. Since B is a product of elementary matrices, each of whose determinants is nonzero, $\det B \neq 0$; remembering that $\det(BA) = (\det B)(\det A)$, we see $\det A = 0$.

When A is invertible, there is an $n \times n$ matrix B so that $BA = I$; thus $\det(BA) = (\det B)(\det A) = 1$ and hence $\det A \neq 0$.

Now suppose $T : \mathbb{R}^n \to \mathbb{R}^n$ is a linear transformation represented by A. By Theorem 16.3, if T is bijective then A is invertible. Conversely, suppose A is invertible; let $S : \mathbb{R}^n \to \mathbb{R}^n$ be the linear transformation represented by A^{-1}. Then $A^{-1}A = I$ represents $S \circ T$, and $AA^{-1} = I$ represents $T \circ S$. Hence $S \circ T$ is the identity map; since the identity map is injective, this means T is injective. Also, $T \circ S$ is the identity map; since the identity map is surjective, this means T is surjective. Thus if A is invertible, T is bijective. □