Math Notes

Jeremy Kelly
www.anthemion.org
February 21, 2019

Contents

1 Whole numbers

The **natural numbers** $\mathbb{N}$ contain all non-negative integers, and sometimes zero. This set may be represented with $\mathbb{N}_0$ or $\mathbb{N}^0$ if zero is included, or with $\mathbb{N}_1$, $\mathbb{N}^*$, $\mathbb{N}^+$, or $\mathbb{N}_{>0}$ if it is not.

$\mathbb{Z}$ is the set of all **integers**. A number is **even** if it is equal to $2m$ for some integer m:

$$\mathbb{Z}_{\text{even}} = \{2m : m \in \mathbb{Z}\}$$

Theorem: Multiplying an even number by any integer produces another even number.

Proof: If a is even, and if b is another integer:

$$ab = 2mb = 2n$$

$n = mb$ is another integer, so ab is even.

Corollary: If a^2 is even, then a must be even. More generally, if ab is even, and if a and b are both integers, then one or both must be a multiple of two, so one or both must be even.

Corollary: If a^2 is odd, then a must be odd, since an even a would have produced an even a^2.

A number is **odd** if it is equal to $2m + 1$ for some integer m:

$$\mathbb{Z}_{\text{odd}} = \{2m + 1 : m \in \mathbb{Z}\}$$

Theorem: The square of any odd number is also odd.

Proof: If a is odd:

$$\begin{aligned} a^2 &= 4m^2 + 4m + 1 \\ &= 2(2m^2 + 2m) + 1 \\ &= 2n + 1 \end{aligned}$$

$n = 2m^2 + 2m$ is another integer, so a^2 is odd.

1.1 Divisibility and congruence

More generally, an integer a is **divisible** by integer d if:

$$a = md$$

for some integer m. This divisibility relation is asserted with:

$$a|d$$

If a and b are integers, then a is **congruent** to b **modulo** d if $a-b$ is divisible by d. This is a special type of *equivalence* between a and b that exists in the *context* defined by the **modulus** d. It can be written:

$$a \equiv b \pmod{d}$$

This implies that a and b have the same integer **remainder** r when divided by d, so that:

$$a = md + r$$

$$b = nd + r$$

for some integers m and n. The congruence defines a system of **modular arithmetic**, which supports common operations over a limited number domain.

Theorem: If $a \equiv b \pmod{d}$ and $e \equiv f \pmod{d}$, then:

$$a + e \equiv b + f \pmod{d}$$

and

$$ae \equiv bf \pmod{d}$$

Proof: There must exist integers m and n such that:

$$a - b = md \quad \text{and} \quad e - f = nd$$

Therefore:

$$(a - b) + (e - f) = md + nd$$
$$(a + e) - (b + f) = (m + n)d$$

showing that $(a + e)$ is congruent to $(b + f)$.

Using the same integers m and n:

$$a = b + md \quad \text{and} \quad e = f + nd$$

so:

$$\begin{aligned} ae &= (b + md)(f + nd) \\ &= bf + bnd + fmd + mnd \\ &= bf + (bn + fm + mn)d \end{aligned}$$

$(bn + fm + mn)$ is an integer, so ae is congruent to bf.

2 Rational and real numbers

The **rational numbers** $\mathbb{Q}$ are those that can be represented as a fraction m/n for some integer m, and some non-zero integer n.

By assigning different non-zero integers to p, a single rational number $q = pm/pn$ can be presented in many different ways. In general, given integers m, n, s, and t:

$$\frac{m}{n} = \frac{a}{b} \quad \text{if and only if} \quad mb = an$$

A rational number $q = m/n$ is expressed in **lowest form** if m and n have no common divisor other than one. One or both of m and n must therefore be odd, because if both were even, they would have a common divisor of two.

Theorem: $\sqrt{2}$ is not a rational number.

Proof: Assume that rational number a exists, such that $a^2 = 2$. If $a = m/n$ in lowest form, then either m or n must be odd. By extension, m^2 or n^2 must be odd. Because:

$$\frac{m^2}{n^2} = 2$$
$$m^2 = 2n^2$$

m^2 and m must be even, and n^2 and n odd. This implies $m = 2p$ for some integer p, so that:

$$4p^2 = 2n^2$$
$$2p^2 = n^2$$

However, this implies that n^2 and n are also even. This has been ruled out, so a cannot exist.

If m and n are non-zero integers, and if $a = m/n$, then:

$$a^{-1} = n/m$$

is the **multiplicative inverse** of a, and:

$$a \cdot a^{-1} = 1$$

When adding rational numbers, each term can be multiplied by the denominators in other terms to produce a **common denominator**. In particular, if a, b, c, and d are integers, and if b and d are non-zero:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}$$

The **real numbers** $\mathbb{R}$ include all rational numbers, plus other points on the number line that cannot be expressed rationally. A real number that is not rational is **irrational**. Such a number cannot be represented with a finite number of decimal digits, since decimal numbers are rational numbers with implicit power-of-ten denominators.

2.1 Exponents and roots

The square of a real number is always positive. Therefore, for any real x, the **absolute value**:

$$|x| = \sqrt{x^2}$$

More generally, any even-numbered exponent produces a positive number. Therefore, if an even-numbered root is applied to some value:

$$a^2 = m$$

the result can be either positive *or* negative:

$$a = \pm\sqrt{m}$$

Theorem: If a and b are positive real numbers, then:

$$\sqrt[n]{ab} = \sqrt[n]{a} \cdot \sqrt[n]{b}$$

Proof: There must exist $s = \sqrt[n]{a}$ and $t = \sqrt[n]{b}$. Because $s^n = a$ and $t^n = b$, it follows that:

$$ab = s^n t^n = (st)^n$$

Therefore:

$$\sqrt[n]{ab} = st = \sqrt[n]{a} \cdot \sqrt[n]{b}$$

In general, if a is a real number:

$$a^{m+n} = a^m a^n$$

and:

$$(a^m)^n = a^{mn}$$

From these rules, it follows that:

$$a^0 = 1 \quad \text{and} \quad a^{-n} = \frac{1}{a^n} \quad \text{and} \quad a^{m/n} = \sqrt[n]{a^m}$$

2.2 Inequalities

Given an inequality, such as:

$$a < b$$

multiplying both sides by a negative number $m < 0$ *reverses* the inequality:

$$ma > mb$$

Geometrically, this inverts the number line positions of both a and b relative to zero, and possibly scales their distances from zero. Because of this, it can be difficult to simplify inequalities. Consider the situation where a, b, c, and d are numbers, and:

$$\frac{ax}{bx + c} < d$$

It is necessary to remove $bx + c$ from the denominator, but it is not known yet whether that expression is positive or negative, so *both* possibilities must be considered. Starting with the case where $bx + c$ is positive, it is immediately seen that:

$$x > \frac{-c}{b}$$

if b is positive. Returning to the original inequality:

$$\begin{aligned} ax &< d(bx + c) \\ &< bdx + cd \\ ax - bdx &< cd \\ (a - bd)x &< cd \end{aligned}$$

If $a - bd$ is also positive:

$$x < \frac{cd}{a - bd}$$

This may or may not agree with the assumption that $bx + c > 0$. If it does, then this example has defined an **interval** for x:

$$\frac{-c}{b} < x < \frac{cd}{a - bd}$$

If it does *not*, both conclusions must be discarded, and the case where $bx + c < 0$ must be evaluated instead.

An interval's **endpoints** may be included or excluded. An **open** interval excludes both endpoints:

$$a < x < b$$

A **half-open** or **half-closed** interval includes one and excludes the other:

$$a \leq x < b$$

A **closed** interval includes both:

$$a \leq x \leq b$$

3 Quadratic equations

The **square of the sum**:

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

The **square of the difference**:

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

The **difference of squares**:

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

Applying the last of these:

$$\begin{aligned} (a + b + c)(a + b - c) &= ((a + b) + c)((a + b) - c) \\ &= (a + b)^2 - c^2 \end{aligned}$$

Similarly:

$$\begin{aligned}(a+b+c)(a-b-c) &= (a+(b+c))(a-(b+c)) \\ &= a^2-(b+c)^2\end{aligned}$$

and:

$$\begin{aligned}(a+b-c)(a-b+c) &= (a+(b-c))(a-(b-c)) \\ &= a^2-(b-c)^2\end{aligned}$$

A **quadratic equation** is a second-degree equation of the form:

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

with $a \neq 0$. The **reduced form** sets $p=b/a$ and $q=c/a$, so that:

$$x^2+px+q=0$$

Because:

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

the reduced form is solved by **completing the square**, so that $a=x$ and $b=p/2$. This involves subtracting q and adding $(p/2)^2$:

$$\begin{aligned}x^2+2\left(\frac{p}{2}\right)x+\left(\frac{p}{2}\right)^2 &= \left(\frac{p}{2}\right)^2-q \\ \left(x+\frac{p}{2}\right)^2 &= \frac{p^2}{4}-q \\ x+\frac{p}{2} &= \pm\sqrt{\frac{p^2}{4}-q} \\ x &= -\frac{p}{2}\pm\sqrt{\frac{p^2}{4}-q}\end{aligned}$$

When $p^2/4-q$ is greater than zero, this produces two solutions. When it is zero, one solution is produced. When it is negative, there is no real-number solution.

Because $p=b/a$ and $q=c/a$, the general form of a quadratic equation is solved with:

$$\begin{aligned}x &= -\frac{b}{2a}\pm\sqrt{\frac{b^2}{4a^2}-\frac{c}{a}} \\ &= \frac{-b\pm\sqrt{b^2-4ac}}{2a}\end{aligned}$$

The **discriminant**:

$$D=b^2-4ac$$

As before, when D is positive, the equation has two solutions. When it is zero, there is one solution. When it is negative, there is no real-number solution.

4 Polynomials

A **polynomial** is an expression that adds, subtracts, or multiplies variables, but does *not* divide them. By extension, all variable exponents must be *positive*. Constant values called **coefficients** can also be added, subtracted, multiplied, or divided.

The **degree** of a term in some polynomial is the sum of the exponents of the variables within that term. The degree of the polynomial as a whole is the highest degree of any of its terms.

Given m and n in $\mathbb{N}_0$, and $n \leq m$, the **binomial coefficient**:

$$\binom{m}{n}=\frac{m!}{n!(m-n)!}$$

This gives the number of distinct ways that n elements can be selected from m elements, without regard to order. Each of these ways is called a **combination**.

5 Distances and angles

If P and Q are points in a plane, the distance from P to Q is given by $\mathrm{d}(P,Q)$. This value is always positive, or zero, if $P=Q$.

Given points P, Q, and M:

$$\mathrm{d}(P,Q) \leq \mathrm{d}(Q,M)+\mathrm{d}(M,P)$$

This is called the **triangle inequality**.

$\overline{PQ}$ is the *line segment* between distinct points P and Q. If M is also a point:

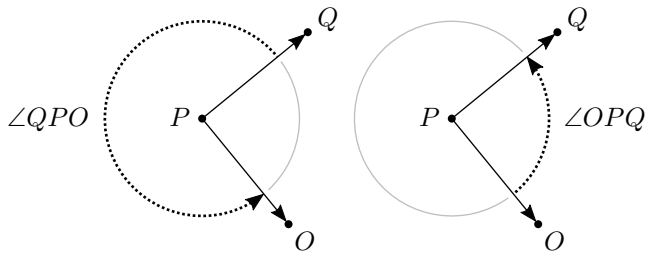
$$\mathrm{d}(P,Q)=\mathrm{d}(P,M)+\mathrm{d}(M,Q)$$

if and only if M is found on $\overline{PQ}$. If $0 \leq c \leq \mathrm{d}(P,Q)$, there is exactly one point M on $\overline{PQ}$ such that:

$$\mathrm{d}(P,M)=c$$

$\overrightarrow{PQ}$ is the *ray* that begins at P and passes through Q. The starting point P is the **vertex** of the ray.

Two rays with a common vertex, such as $\overrightarrow{PO}$ and $\overrightarrow{PQ}$, define a pair of **angles**. One angle $\angle QPO$ is measured from $\overrightarrow{PQ}$ to $\overrightarrow{PO}$. Another angle $\angle OPQ$ is measured from $\overrightarrow{PO}$ to $\overrightarrow{PQ}$. The angles are always measured *counterclockwise*:



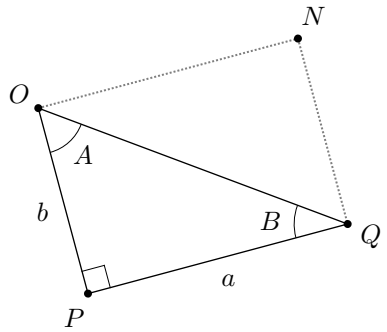
If $\overrightarrow{PO}$ is equivalent to $\overrightarrow{PQ}$, either angle can be interpreted as a **zero angle**, or as a **full angle**. If $\overrightarrow{PO}$ and $\overrightarrow{PQ}$ are exactly *opposite*, so that they point in different directions along the same line, two **straight angles** are formed. The **measure** of angle A, as distinct from the configuration of rays that *forms* the angle, is given by $\mathrm{m}(A)$.

A circle centered on the vertex is divided by the rays into two **arcs**. A disc centered on the vertex is divided into two **sectors**.

5.1 Triangles

Any distinct points O, P, and Q form three segments $\overline{OP}$, $\overline{PQ}$, and $\overline{QO}$. If the points are not collinear, the segments form a **triangle** $\triangle OPQ$. If two of the segments are perpendicular, a **right triangle** is formed. The perpendicular segments are the **legs** of the triangle. The third side, which is always longer, is called the **hypotenuse**.

Consider points N, O, P, and Q, with no three points on the same line. If $\angle OPQ$ is a right angle, if $\overline{ON}$ is parallel to $\overline{PQ}$, and if $\overline{OP}$ is parallel to $\overline{NQ}$, the four segments form a **rectangle**:



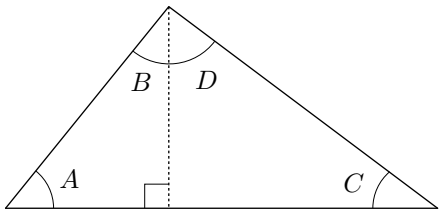
Dividing the rectangle diagonally forms two right triangles. Because the legs of either triangle are equal in length to those of the other, the triangles are congruent. In particular, $\angle POQ$ is equivalent to $\angle NQO$, and $\angle PQO$ is equivalent to $\angle NOQ$. Similarly, the triangles have the same area.

If $\overline{PQ}$ has length a, and $\overline{PO}$ has length b, the rectangle has area ab. The triangles divide this area equally, so *any* right triangle with legs of length a and b has area $ab/2$.

The four right angles of the rectangle have a total measure of 360°. The triangles divide this evenly as well, so, if the acute angles are labeled A and B, then:

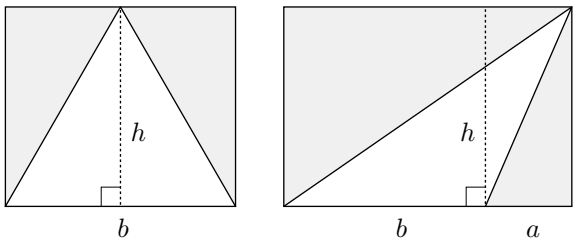
$$\mathrm{m}(A) + \mathrm{m}(B) = 90^\circ$$

for *any* right triangle. Moreover, any triangle can be divided into two right triangles by placing a line that is perpendicular to the longest side:



Assume this produces acute angles A and B on one side, and C and D on the other. Because $\mathrm{m}(A) + \mathrm{m}(B)$ and $\mathrm{m}(C) + \mathrm{m}(D)$ both equal 90°, the angle measures of *any* triangle sum to 180°.

The **height** or **altitude** of a triangle is the perpendicular distance from one side, called the **base**, to the opposite vertex, known as the **apex**. If a triangle is fit within a rectangle so that its base aligns on one side, one of two general configurations will be formed:



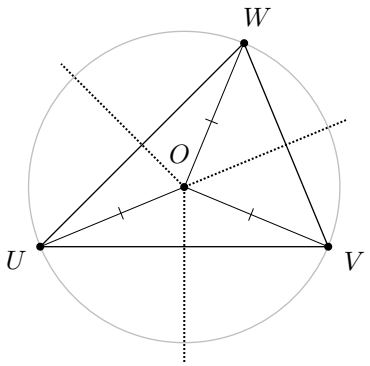
Assume the triangle has height h and a base of length b. If the apex is somewhere *over* the base, the rectangle will have sides of length b and h, and area bh. The segment that defines the height divides the rectangle into two parts, each containing two congruent right triangles, one within the original triangle, and one outside it. The area of the original triangle is therefore $bh/2$.

If the apex is *not* over the base, the base of the rectangle will be larger by some length a. The original triangle divides the rectangle diagonally into two larger right triangles, each with area $(a+b)h/2$. As before, the area of the original triangle:

$$\frac{(a+b)h}{2} - \frac{ah}{2} = \frac{bh}{2}$$

Therefore, the area of *any* triangle is equal to $bh/2$.

Given a triangle of points U, V, and W, perpendicular bisectors can be added to segments $\overline{UV}$ and $\overline{VW}$, and these will necessarily meet at some point O:



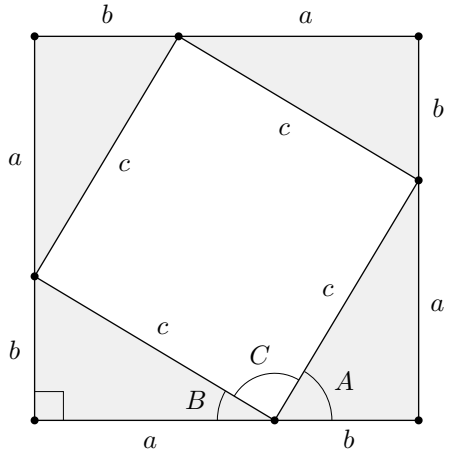
As will be seen, every point on a perpendicular bisector is equidistant from the segment endpoints, so $\mathrm{d}(\overline{VO}) = \mathrm{d}(\overline{UO})$. By the same logic, $\mathrm{d}(\overline{WO}) = \mathrm{d}(\overline{VO})$, so that $\mathrm{d}(\overline{WO}) = \mathrm{d}(\overline{UO})$ as well. This means that the perpendicular bisector of $\overline{WU}$ *also* passes through O, which is called the **circumcenter** of the triangle. This point is also the center of the circle that **circumscribes** the triangle.

5.2 The Pythagorean theorem

Given a right triangle with legs of length a and b, and hypotenuse of length c:

$$a^2 + b^2 = c^2$$

Proof: Consider the following construction:



Four congruent right triangles have been arranged to form a square with sides of length $a+b$ and area $(a+b)^2$. $\mathrm{m}(A) + \mathrm{m}(B) = 90^\circ$, so C is 90°, and another square is formed inside. The smaller square has area c^2, which is necessarily equal to the area of the larger square less that of the triangles. Each triangle has area $ab/2$, so:

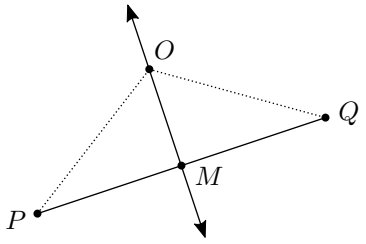
$$\begin{aligned}(a+b)^2 - 4\Big(\frac{ab}{2}\Big) &= c^2 \\ a^2 + 2ab + b^2 - 2ab &= c^2 \\ a^2 + b^2 &= c^2\end{aligned}$$

Corollary: If P and Q are distinct points, and if O is some third point in the plane, then:

$$\mathrm{d}(P,O) = \mathrm{d}(Q,O)$$

if and only if O is found on the **perpendicular bisector** of $\overline{PQ}$, this being the perpendicular line that passes through the middle of a segment.

Proof: Assume that $\mathrm{d}(P,O)$ does equal $\mathrm{d}(Q,O)$. A line can be drawn that both contains O and is perpendicular to the line containing $\overline{PQ}$, but this may or may not bisect the segment. If M is the point on $\overline{PQ}$ through which the line passes:



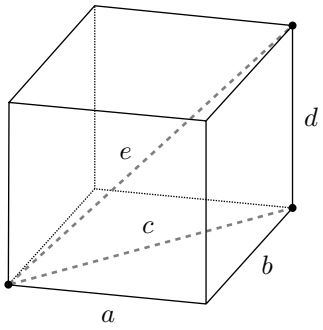
then, by the Pythagorean theorem:

$$\begin{gathered}\mathrm{d}(P,O)^2 = \mathrm{d}(Q,O)^2 \\ \mathrm{d}(P,M)^2 + \mathrm{d}(M,O)^2 = \mathrm{d}(Q,M)^2 + \mathrm{d}(M,O)^2\end{gathered}$$

$$\mathrm{d}(P,M)^2 = \mathrm{d}(Q,M)^2$$
$$\mathrm{d}(P,M) = \mathrm{d}(Q,M)$$

Therefore, M is in the middle of the segment, and the line containing O is the bisector. Conversely, if O is on the perpendicular bisector, the reverse argument shows that $\mathrm{d}(P,O) = \mathrm{d}(Q,O)$.

The Pythagorean theorem can easily be extended to three dimensions. A 3D displacement can be decomposed into a 2D displacement followed by a 1D displacement:



If the 2D displacement has orthogonal components a and b, then the length in that plane $c = |\sqrt{a^2 + b^2}|$. The 1D displacement is orthogonal to the 2D displacement, so another right triangle is formed. If the 1D displacement has length d, and if the total length is e:

$$c^2 + d^2 = e^2$$

Therefore:

$$a^2 + b^2 + d^2 = e^2$$

6 Isometries

A **constant** mapping is one that associates every value with a single, unvarying output:

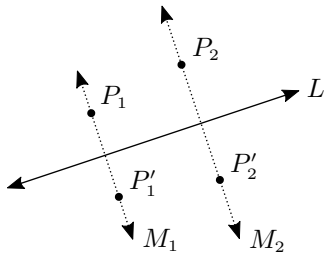
$$F(V) = c$$

for all V in the domain. An **identity** is one that associates every value with itself, so that:

$$F(V) = V$$

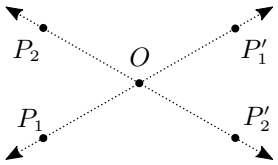
for all V.

Consider a line L, and another line M that is perpendicular to L, and that contains point P. If P' is another point on M that is the same distance from L:



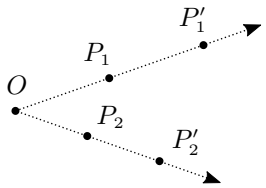
then $P \mapsto P'$ is the **reflection through the line** L.

Consider points O and P. If a line passes through these points, and if point P' is the same distance from O on the other side:



then $P \mapsto P'$ is the **reflection through the point** O.

Points O and P also produce a ray that has O as its vertex. If point P' is also found on this ray:

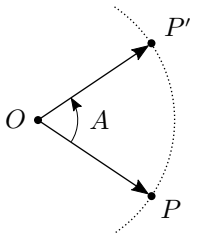


and if:

$$\mathrm{d}(O,P') = r \cdot \mathrm{d}(O,P)$$

then $P \mapsto P'$ is the **dilation** by r relative to O.

It is also possible to draw a circle that contains P, with O as its center. If P' is another point on this circle, and if counterclockwise angle $\angle POP'$ has measure $\mathrm{m}(A)$:



then $P \mapsto P'$ is the **rotation** by A relative to O. Rotation by 180° relative to O is equivalent to *reflection* through O. Rotation by 360° is equivalent to the *identity*.

Points U and V can be made to define a **vector**, which has a direction and a length, but no position. If points P and P' produce the same vector as U and V, then $P \mapsto P'$ is the **translation** by that vector.

Given a mapping F of the plane onto itself, a **fixed point** of F is any P such that $F(P) = P$. If F is an identity, all points are fixed. If F is the reflection through a point O, then O is the one and only fixed point. If F is the reflection through a line L, the fixed points are all the points on L.

Mapping F is an **isometry** if and only if, for all points O and P:

$$\mathrm{d}(F(O), F(P)) = \mathrm{d}(O, P)$$

Isometries are said to be **distance-preserving**. Reflection through a point, reflection through a line, rotation, and translation are all isometries.

Theorem: If F is an isometry, the image of the line segment $\overline{PQ}$ under F is another line segment, from $F(P)$ to $F(Q)$.

Proof: If P and Q are distinct points, their distance must be greater than zero. Because F is an isometry, the distance from $P' = F(P)$ to $Q' = F(Q)$ must also be greater than zero, so P' and Q' are distinct points. In general, for point M:

$$\mathrm{d}(P, Q) = \mathrm{d}(P, M) + \mathrm{d}(M, Q)$$

if and only if M is found on $\overline{PQ}$. The isometry requires that:

$$\mathrm{d}(P', Q') = \mathrm{d}(P, Q)$$
$$\mathrm{d}(P', M') = \mathrm{d}(P, M)$$
$$\mathrm{d}(M', Q') = \mathrm{d}(M, Q)$$

so that:

$$\mathrm{d}(P', Q') = \mathrm{d}(P', M') + \mathrm{d}(M', Q')$$

Therefore, every point M on $\overline{PQ}$ maps to a point M' on $\overline{P'Q'}$. By itself, this does not prove that the image is a line segment, only that it is *contained* by a segment. However, a similar argument shows that every point M' on $\overline{P'Q'}$ is mapped by a point M on $\overline{PQ}$.

Corollary: Every isometry preserves the straightness of lines in the domain.

Theorem: If P and Q are distinct, fixed points of isometry F, then every point on the line $\overleftrightarrow{PQ}$ is also a fixed point.

Proof: Assume that point M is somewhere on $\overleftrightarrow{PQ}$. As shown above, if M is also *within* $\overline{PQ}$, its image M' is on $\overline{P'Q'}$:

$$\mathrm{d}(P', Q') = \mathrm{d}(P', M') + \mathrm{d}(M', Q')$$

P is fixed, so it is interchangeable with P', just as Q is interchangeable with Q'. As a result:

$$\mathrm{d}(P, Q) = \mathrm{d}(P, M') + \mathrm{d}(M', Q)$$

M' occupies the same position as M, so every point M on $\overline{PQ}$ is mapped to the same point M'.

If M is *outside* $\overline{PQ}$, it will be found on the P side of $\overleftrightarrow{PQ}$, or on the Q side. If it is on the P side, then P is within segment $\overline{MQ}$, so that:

$$\mathrm{d}(M, Q) = \mathrm{d}(M, P) + \mathrm{d}(P, Q)$$

and:

$$\mathrm{d}(M', Q') = \mathrm{d}(M', P') + \mathrm{d}(P', Q')$$
$$\mathrm{d}(M', Q) = \mathrm{d}(M', P) + \mathrm{d}(P, Q)$$

Therefore, P is within $\overline{M'Q}$, and M' is on $\overleftrightarrow{PQ}$. Furthermore:

$$\mathrm{d}(M, P) = \mathrm{d}(M', P') = \mathrm{d}(M', P)$$

so $M' = M$. A similar argument applies when M is on the Q side of $\overleftrightarrow{PQ}$.

Theorem: If O, P, and Q are distinct, fixed points of isometry F, and if they are not collinear, then F is the identity mapping.

Proof: The points are not collinear, so lines $\overleftrightarrow{OP}$ and $\overleftrightarrow{PQ}$ are distinct. The points are also fixed, so every other point on the lines is fixed. The lines span the plane, so a third line that intersects both can be drawn through any point. The intersections are fixed, so all other points on the third line are fixed. Therefore, every point in the plane is fixed.

6.1 Composing isometries

A series of mappings can be applied *in succession* to produce a **composite**. If mapping G is applied to P, and if mapping F is applied to the result, then:

$$P \mapsto F(G(P))$$

This can also be written:

$$(F \circ G)(P) = F(G(P))$$

Note that the mapping on the *right* side of $F \circ G$ is evaluated first. If F and G are isometries, then their composite is also an isometry.

Composition is *associative*:

$$(F \circ G) \circ H = F \circ (G \circ H)$$

This is seen from the fact that:

$$((F \circ G) \circ H)(P) = (F \circ G)(H(P)) = F(G(H(P)))$$

and:

$$F \circ (G \circ H)(P) = F((G \circ H)(P)) = F(G(H(P)))$$

so the same mappings are applied in the same order. This is essentially a notational detail; it is true because the rightmost operation is chosen at each level. Changing the mapping order, on the other hand, *could* change the result. For example, a translation followed by a rotation is *not* typically equivalent to a rotation followed by a translation.

If a mapping is composed with itself, the composite can be represented with an exponent:

$$F \circ F = F^2$$

By extension, if I is the identity mapping:

$$F^0 = I$$

Mapping G is the **inverse** of F if and only if:

$$F \circ G = G \circ F = I$$

The inverse if F can be represented as F^{-1}. As a result, if:

$$F(P) = Q$$

then:

$$F^{-1}(Q) = P$$

since:

$$F^{-1}(Q) = F^{-1}(F(P)) = I(P) = P$$

In this case, P is the **inverse image** of Q under F.

Theorem: There is only one inverse for a given mapping.

Proof: Assume G and H are both inverses of F. Composition is associative, so:

$$(H \circ F) \circ G = H \circ (F \circ G)$$

Moreover:

$$(H \circ F) \circ G = I \circ G = G$$

and:

$$H \circ (F \circ G) = H \circ I = H$$

so it is always true that $G = H$.

Theorem: Given mappings F and G, the inverse of their composite is equal to the composite of their inverses, in the reverse order:

$$(F \circ G)^{-1} = G^{-1} \circ F^{-1}$$

Proof: It is obviously true that:

$$(F \circ G)^{-1} \circ (F \circ G) = I$$

However, it is also true that:

$$G^{-1} \circ F^{-1} \circ (F \circ G) = G^{-1} \circ (F^{-1} \circ F) \circ G = I$$

so $G^{-1} \circ F^{-1}$ is also the inverse of $F \circ G$.

Theorem: If O, P, and Q are distinct, non-collinear points, and if F and G are isometries where:

$$F(O) = G(O) \qquad F(P) = G(P) \qquad F(Q) = G(Q)$$

then $F = G$.

Proof: As will be seen, every isometry has an inverse. Composition with F^{-1} produces:

$$(F^{-1} \circ F)(O) = (F^{-1} \circ G)(O)$$
$$(F^{-1} \circ F)(P) = (F^{-1} \circ G)(P)$$
$$(F^{-1} \circ F)(Q) = (F^{-1} \circ G)(Q)$$

so that:

$$O = (F^{-1} \circ G)(O)$$
$$P = (F^{-1} \circ G)(P)$$
$$Q = (F^{-1} \circ G)(Q)$$

$F^{-1} \circ G$ is an isometry, and it is fixed at three non-collinear points, so it is the identity, and G is the inverse of F^{-1}. There is a one-to-one relationship between mappings and their inverses, so $F = G$. Alternatively:

$$F^{-1} \circ G = I$$
$$F \circ F^{-1} \circ G = F \circ I$$
$$G = F$$

This can be used to show that certain composites are equivalent. For example, if H is reflection through a vertical line, and if V is reflection through a horizontal line, it is easily seen that $H \circ V = V \circ H$ for any three points. Therefore, it is true for all points.

Theorem: Given points P, Q, P', and Q', with:

$$\mathrm{d}(P,Q) = \mathrm{d}(P',Q')$$

there is an isometry F such that $F(P) = P'$ and $F(Q) = Q'$.

Proof: There is obviously a translation T such that:

$$T(P) = P' \quad \text{and} \quad T^{-1}(P') = P$$

T^{-1} is an isometry, so:

$$\mathrm{d}(P,Q) = \mathrm{d}(T^{-1}(P'), T^{-1}(Q')) = \mathrm{d}(P, T^{-1}(Q'))$$

There is also a rotation R around P that maps Q to any point that is the same distance from P. T and R are both isometries, so $F = T \circ R$.

Theorem: If P and Q are distinct points that are fixed under isometry F, then F is the identity, or it is the reflection through line $\overleftrightarrow{PQ}$.

Proof: Assume that M is a point on the perpendicular bisector of $\overline{PQ}$, and $F(M) = M'$. If $M' = M$, then three non-collinear points are fixed under F, so it is the identity.

If $M' \neq M$, then F is another mapping. M is on the bisector, so:

$$\mathrm{d}(P,M) = \mathrm{d}(M,Q)$$

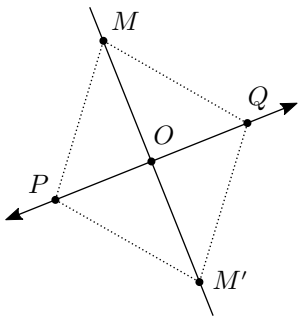
Because F is an isometry:

$$\mathrm{d}(P',M') = \mathrm{d}(M',Q')$$

P and Q are fixed, so:

$$\mathrm{d}(P,M') = \mathrm{d}(M',Q)$$

As shown earlier, this implies that M' is also on the perpendicular bisector of $\overline{PQ}$:



Let O be the point at which the bisector crosses $\overline{PQ}$. Its distance from P or Q is invariant under F, so it is also fixed, allowing:

$$\mathrm{d}(M,O) = \mathrm{d}(M',O)$$

M' is therefore the reflection of M through $\overleftrightarrow{PQ}$. A reflection is its own inverse, so if R is the reflection through this line, then $R^{-1} = R$, and:

$$R(M) = M' \qquad R(M') = M$$

$R \circ F$ is an isometry that leaves P and Q fixed. Additionally:

$$R(F(M)) = R(M') = M$$

so $R \circ F$ also leaves M fixed. It is therefore the identity, and:

$$F = R^{-1} = R$$

Theorem: If point O is fixed under isometry F, then F is the identity, or it is a rotation, or it is a rotation composed with a reflection through some line containing O.

Proof: Consider distinct point P, with $F(P) = P'$. If $P' = P$, then two points are fixed, and F is the identity or the reflection through $\overleftrightarrow{OP}$.

If $P' \neq P$, it is still true that:

$$\mathrm{d}(O,P) = \mathrm{d}(O,P')$$

since O is fixed. Therefore, there is a rotation R such that $R(P) = P'$ and:

$$R^{-1}(P') = R^{-1}(F(P)) = P$$

As a result, P is fixed under $R^{-1} \circ F$, as is O. This implies that $R^{-1} \circ F$ is the identity, or a reflection L through $\overleftrightarrow{OP}$.

If $R^{-1} \circ F$ is the identity, then F is the rotation R. If it is L, then:

$$\begin{aligned} R^{-1} \circ F &= L \\ R \circ R^{-1} \circ F &= R \circ L \\ F &= R \circ L \end{aligned}$$

Theorem: If no point is fixed under isometry F, then F is a translation, or a translation composed with a rotation,

or a translation composed with both a rotation and a reflection through some line.

Proof: Consider a point P such that $F(P) = P'$. There must exist a translation such that $T(P) = P'$ and:

$$T^{-1}(P') = T^{-1}(F(P)) = P$$

so P is fixed under $T^{-1} \circ F$. This composite is an isometry, so it is the identity, or a rotation, or a rotation composed with a reflection through some line. Therefore F is a translation composed with one of these mappings.

Corollary: Every isometry has an inverse.

Proof: Every isometry with three or more non-collinear fixed points is the identity. Every isometry with fewer than three is the reflection through some line, or a rotation composed with such a reflection, or a translation composed with both of these, one, or neither. All these mappings have inverses, so their composite has an inverse as well.

6.2 Congruence

A sets of points S is **congruent** to another set S' if an isometry F exists such that the image $F(S)$ is equal to S'.

Theorem: Any two circles with the same radius are congruent.

Proof: Consider circles $C(r, O)$ and $C(r, O')$ with radius r and centers O and O'. There is a translation T such that $T(O) = O'$. T is an isometry, so if point P has distance r from O, $T(P)$ is the same distance from O', and all points in the first circle are mapped to points in the second. A similar argument shows that all points on the second circle are mapped to the first.

Theorem: Any two segments with the same length are congruent.

Proof: Consider segments $\overline{PQ}$ and $\overline{MN}$ with the same length. There is a translation T such that $T(M) = P$ and:

$$\mathrm{d}(P, T(N)) = \mathrm{d}(P, Q)$$

Therefore, there is a rotation R around P such that $R(T(N)) = Q$, and the composite isometry $R \circ T$ maps M and N to P and Q. As shown earlier, the image of a line segment under an isometry is another line segment, so $\overline{PQ}$ and $\overline{MN}$ are congruent.

Theorem: If triangles $\triangle PQM$ and $\triangle P'Q'M'$ have sides with the same lengths:

$$\begin{aligned} \mathrm{d}(P, Q) &= \mathrm{d}(P', Q') \\ \mathrm{d}(Q, M) &= \mathrm{d}(Q', M') \\ \mathrm{d}(M, P) &= \mathrm{d}(M', P') \end{aligned}$$

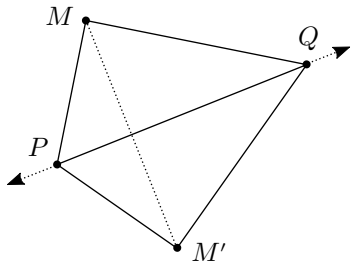
then the triangles are congruent.

Proof: There is a translation that maps P to P', so it is sufficient to prove the case where $P = P'$. Next, there is a rotation that maps Q to Q' while leaving P fixed, so it is sufficient to prove the case where $P = P'$ and $Q = Q'$. Given that the sides match, there are now two possible outcomes, one where $M' = M$, and one where it does not.

If M' does equal M, a composite isometry that maps the first triangle to the second has already been found. In the case where $M \neq M'$:

$$\begin{aligned} \mathrm{d}(P, M) &= \mathrm{d}(P, M') \\ \mathrm{d}(Q, M) &= \mathrm{d}(Q, M') \end{aligned}$$

so points P and Q are found on the perpendicular bisector of segment $\overline{MM'}$:



Reflection through $\overleftrightarrow{PQ}$ maps M to M' while leaving P and Q fixed, so the composite isometry maps $\triangle PQM$ to $\triangle P'Q'M'$.

The same reasoning can be applied to a filled shape by decomposing its interior into a set of line segments. For instance, every point inside triangle $\triangle PQM$ will be found on some segment $\overline{PX}$, with X being a point on side $\overline{QM}$. Similarly, if an angle is defined by rays $\overrightarrow{OP}$ and $\overrightarrow{OQ}$, every point inside the angle will be found on some segment $\overline{XY}$, with X being a point on $\overrightarrow{OP}$, and Y a point on $\overrightarrow{OQ}$.

7 Functions

A **function** or **mapping** associates elements in one set, called the **domain**, with elements in another set, called

the **codomain**. The mapping between domain value V and associated value V' is asserted with:

$$V \mapsto V'$$

If the function is named F, this can also be expressed as:

$$F(V) = V'$$

Given a subset A of the domain, the **image** of A under F is the set of codomain values that are associated with the elements in A. An image may also be described as a **range**, but that term is also used as a synonym for *codomain*.

A **variable** represents a set of numbers or other objects. Depending on the statement that contains the variable, the set may contain a single value, or all the values in an interval, or all the values in the domain of the containing function. If the statement has no solution, the set will be empty. Conversely, the **solution** of some statement is the set of values for which the statement is true.

Within a function, an **independent** variable represents an *input*, and therefore, some or all of the function's domain. It may also be called an **argument** of the function. A **dependent** variable represents the *output* of the function, and therefore, some part of its codomain.

A Miscellanea

An operation is **commutative** if it returns the same result regardless of the order of its arguments:

$$a + b = b + a$$

An operation is **associative** if, when used more than once in a single expression, it returns the same result regardless of the order in which the operations are resolved:

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

One operation is **distributive** with respect to another if an argument of the distributive operation can be copied and distributed among terms in the other argument. Multiplication is distributive with respect to addition:

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

Sources

Basic Mathematics
Serge Lang
1988, Springer Science+Business Media

Wikipedia
https://en.wikipedia.org/wiki
/Natural_number
/Modular_arithmetic
/Polynomial
/Triangle
/Function_(mathematics)
/Variable_(mathematics)
/Dependent_and_independent_variables

This document was typeset with LaTeX. Diagrams were created with Inkscape.