Excursions in Computing Science:
Week 4. Two-dimensional Numbers and Turtles

T. H. Merrett[*]
McGill University, Montreal, Canada

May 4, 2009

I. Prefatory Notes

1. We've described a rotation as a product of matrix and vector,

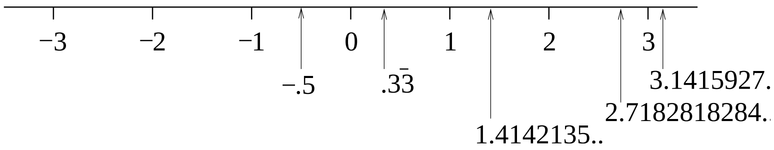
$$R.\vec{v} = \begin{pmatrix} c & -s \\ s & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

and a double rotation as a product of two matrices.

$$R_\phi R_\theta = \begin{pmatrix} c & -s \\ s & c \end{pmatrix}_\phi \begin{pmatrix} c & -s \\ s & c \end{pmatrix}_\theta$$

Can these be replaced by just numbers?

2. Numbers so far are 1-dimensional.



A quarter-turn (rotation by $\pi/2$) rotates it by a right angle into the—unknown. E.g.

$$R_{\pi/2} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Two quarter-turns turn 1 into -1

$$R_{\pi/2} R_{\pi/2} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$$

3. On the line, we can do this by

$$-1 \times x = -x$$

for any x including $x = 1$.

In the (unknown) two dimensions

$$(R_{\pi/2})^2 \begin{pmatrix} 1 \\ 0 \end{pmatrix} = -\begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

So maybe

$$R_{\pi/2} = \sqrt{-1}$$

How can we write $R_{\pi/2}$ (or R_θ) as a number?

4. Try $R_\theta = \cos\theta + \sqrt{-1}\sin\theta$, e.g.,

$$\begin{aligned} R_{\pi/2} &= \sqrt{-1} \\ R_\pi &= R_{\pi/2}R_{\pi/2} = (R_{\pi/2})^2 = -1 \\ R_\phi R_\theta &= (c + \sqrt{-1}s)_\phi (c + \sqrt{-1}s)_\theta \\ &= c_\phi c_\theta - s_\phi s_\theta + \sqrt{-1}(c_\phi s_\theta + s_\phi c_\theta) \end{aligned}$$

Compare this last with

$$\begin{pmatrix} c & -s \\ s & c \end{pmatrix}_\phi \begin{pmatrix} c & -s \\ s & c \end{pmatrix}_\theta = \begin{pmatrix} c_\phi c_\theta - s_\phi s_\theta & -(c_\phi s_\theta + s_\phi c_\theta) \\ c_\phi s_\theta + s_\phi c_\theta & c_\phi c_\theta - s_\phi s_\theta \end{pmatrix}$$

5. So rotations are (weird) numbers.

What about vectors?

$$\begin{pmatrix} c & -s \\ s & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} cx - sy \\ sx + cy \end{pmatrix}$$

$$\text{Try } \begin{pmatrix} x \\ y \end{pmatrix} = x + \sqrt{-1}y$$

$$(c + \sqrt{-1}s)(x + \sqrt{-1}y) = cx - sy + \sqrt{-1}(sx + cy)$$

Bingo!

6. $\sqrt{-1}$ is important, if unimaginable.

We'll call it i for "imagine that!".

The best we can do is think of it as a right-angle departure from the known numbers to the unknown.

Think of i = rot90: $(\text{rot90})^2$ = rot180 = -1.

(We could call it $\perp$ and write $\perp$ in place of $\sqrt{-1}$ from now on, but that would make it harder for you to read conventional notation.)

(There are in fact *two* conventions. The second convention is to write j for $\sqrt{-1}$. This is used by engineers, perhaps because i also means electric current. i is used by mathematicians and scientists. MATLAB supports both conventions.)

We'll call these two-dimensional numbers "2-numbers" from now on, to keep it short. If we need to, we'll call the old, one-dimensional numbers "1-numbers".

We could call the two components "horizontal" and "vertical", respectively, but that would be unconventional and also confusing later when we use 2-numbers in ways that no longer physically mean horizontal and vertical. So we will stick to convention and call the components "real" and "imaginary", pejorative though that is.

7. These “2-numbers” have the *same formal properties* as the “1-numbers”:

+, × – closed
– commutative $a + b = b + a$, $a \times b = b \times a$
– associative $(a + b) + c = a + (b + c)$, $(a \times b) \times c = a \times (b \times c)$
– have identities 0 (+), 1 (×)

+ each element has an inverse $a + a' = 0 = a' + a$

× each element except 0 has an inverse $a \times a' = 1 = a' \times a$

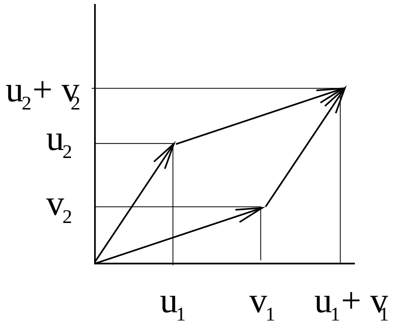
+, × × is distributive over +: $a \times (b + c) = a \times b + a \times c$

The above are the “field axioms”. 2-numbers and 1-numbers each exemplify what mathematicians call a “field”. (This is quite different from what physicists call a “field”, and neither has anything to do with what a farmer calls a “field”.)

The fact that 2-numbers have the same formal properties as 1-numbers makes them familiar and easy to use. It also justifies our calling them both “numbers”.

8. Adding 2-numbers

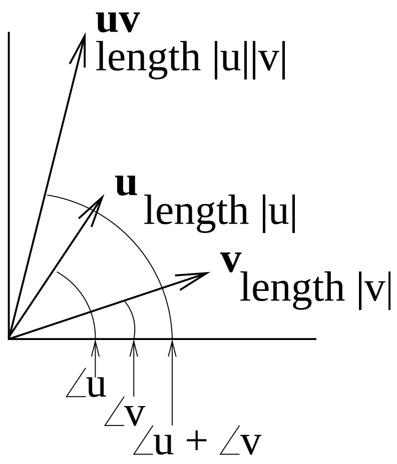
$$\begin{aligned} u + v &= (u_1 + iu_2) + (v_1 + iv_2) \\ &= u_1 + v_1 + i(u_2 + v_2) \end{aligned}$$



9. Multiplying 2-numbers

$$\begin{aligned} uv &= (u_1 + iu_2)(v_1 + iv_2) \\ &= u_1v_1 - u_2v_2 + i(u_1v_2 + u_2v_1) \\ \text{Try } v &= \mid u \mid (\cos \angle u + i \sin \angle u) =\mid u \mid (c + is) \\ u &= \mid v \mid (\cos \angle v + i \sin \angle v) =\mid v \mid (c' + is') \\ \mid u \mid &= +\sqrt{u_1^2 + u_2^2} \\ \mid v \mid &= +\sqrt{v_1^2 + v_2^2} \\ \text{Now } u_1v_1 - u_2v_2 &= \mid u \mid\mid v \mid (cc' - ss') =\mid u \mid\mid v \mid \cos(\angle u + \angle v) \\ u_1v_2 + u_2v_1 &= \mid u \mid\mid v \mid (cs' + sc') =\mid u \mid\mid v \mid \sin(\angle u + \angle v) \\ \text{Compare } \begin{pmatrix} c & -s \\ s & c \end{pmatrix} \begin{pmatrix} c' & -s' \\ s' & c' \end{pmatrix} &= \begin{pmatrix} cc' - ss' & -(cs' + sc') \\ (cs' + sc') & cc' - ss' \end{pmatrix} \end{aligned}$$

where the first matrix is $\text{rot}_{\angle u}$, the second is $\text{rot}_{\angle v}$, and the resulting matrix is $\text{rot}_{\angle u + \angle v}$:



Since multiplying these 2-numbers by each other just sums their angles, i.e., the resultant 2-number has an angle which is the sum of the angles of the two elements in the product, the 2-numbers behave just like exponentials.

We can try writing

$$\begin{aligned} u &= \mid u \mid e^{i\angle u} \\ v &= \mid v \mid e^{i\angle v} \\ uv &= \mid u \mid\mid v \mid e^{i(\angle u+\angle v)} \end{aligned}$$

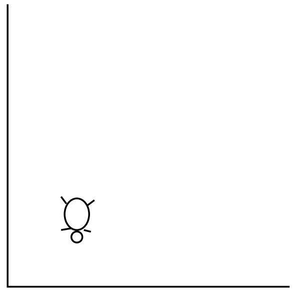
(whatever e is: it doesn't really matter to us).

10. Turtle graphics.

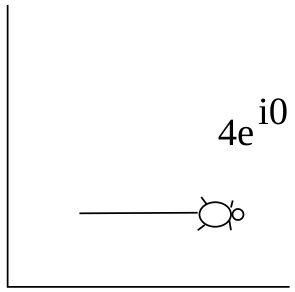
If computers are the wave of the future,
graphics is the surfboard Apologies to [Nel78]

Let's draw a house.

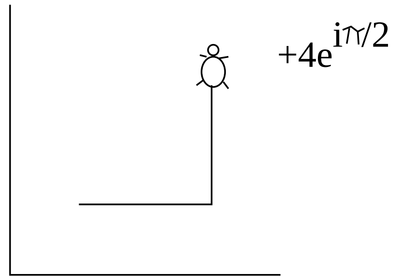
Start.



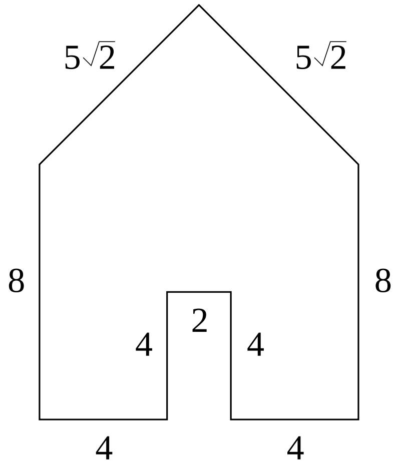
Turn $\pi/2$; Go 4. $4e^{i0}$



Turn $\pi/2$; Go 4.	$+4e^{i\pi/2}$



Turn $-\pi/2$; Go 2.	$+2e^{i0}$
Turn $-\pi/2$; Go 4.	$+4e^{-i\pi/2}$
Turn $\pi/2$; Go 4.	$+4e^{i0}$
Turn $\pi/2$; Go 8.	$+8e^{i\pi/2}$
Turn $\pi/4$; Go $5\sqrt{2}$.	$+5\sqrt{2}e^{i3\pi/4}$
Turn $\pi/2$; Go $5\sqrt{2}$.	$+5\sqrt{2}e^{i5\pi/4}$
Turn $\pi/4$; Go 8.	$+8e^{i3\pi/2}$



Note: the turtle ends up in the same position and orientation, and the "total turtle turning", TTT, is 2π.

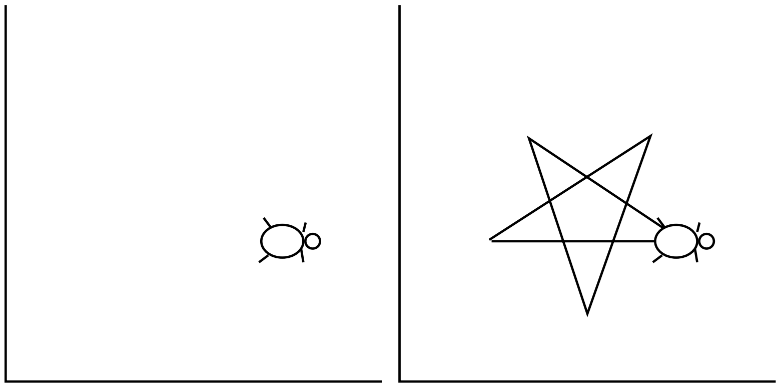
$$4e^{i0} + 4e^{i\pi/2} + 2e^{i0} + 4e^{-i\pi/2} + 4e^{i0} + 8e^{i\pi/2} + 5\sqrt{2}e^{i3\pi/4} + 5\sqrt{2}e^{i5\pi/4} + 8e^{i3\pi/2} = 0$$

11. Closed figures.

Is TTT $= 2\pi$ always?

Let's try $4\pi/5$ 5 times:

$$e^{i4\pi/5} + e^{i8\pi/5} + e^{i12\pi/5} + e^{i16\pi/5} + e^{i20\pi/5}$$



TTT $= 4\pi$ and note that the turtle winds up where it started and in the same orientation:

$$e^{i4\pi/5} + e^{i8\pi/5} + e^{i12\pi/5} + e^{i16\pi/5} + e^{i20\pi/5} = 0.$$

12. Summary

(These notes show the trees. Try to see the forest!)

- i (Imagine it!) (or $\perp$ or $\sqrt{-1}$ or j) is some weird 2nd dimension.
- $i\times$ rotates a 2-number through $\pi/2$
- $i \times i\times$ rotates a 2-number through π, i.e. $\mathit{number}\!\rightarrow -\mathit{number}$
- 2-numbers, $a + ib$ or $a + \perp b$, behave formally exactly like 1-numbers: both satisfy the "field axioms"
- $(\cos\theta + i\sin\theta)\times$ (or $(\cos\theta + \perp \sin\theta)\times$) rotates a 2-number through θ
- $(c + is)(c' + is')\times$ (or $(c + \perp s)(c'\!+ \perp s')\times$) rotates a 2-number through $\angle(c, s) + \angle(c's')$ ...
- ... so this suggests we write $\cos\theta + i\sin\theta$ as $e^{i\theta}$, for some e, just for convenience
- $ae^{i\theta} + a'e^{i\theta'} + ..$ models turtle graphics (except that the turtle makes relative turns, but the angles $\theta, \theta', ..$ are absolute orientations).
- Total Turtle Turning TTT, returning to same position and orientation, is an integer multipls of 2π, and
$$\sum_{k=1}^{m} e^{i2k\pi/m} = 0$$

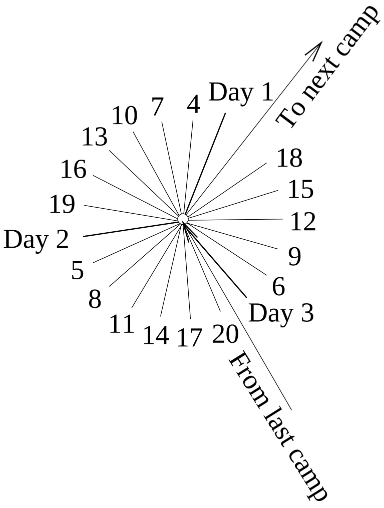
II. The Excursions

You've seen lots of ideas. Now *do* something with them!

1. For some 1-number, e, (and we do not need to know just now what its value is), $\cos\theta + i\sin\theta = e^{i\theta}$. We need two arguments to show this: a) the expression $\cos\theta + i\sin\theta$ behaves as though it were something raised to the power θ; b) i must also be in this power. What are the arguments? From this, what is the relationship among the five important "numbers", $0, 1, e, i, \pi$?
(Note. An *expression* is a combination of mathematical symbols, including operators and variables, for which a value can be calculated once values are chosen for the variables.)
2. Use MATLAB to plot e^{ix} (`exp(i*x)`). Compare this with a plot of $\cos(x) + i \times \sin(x)$.

3. Find a running copy of the programming language Logo (politely ask your kid sibling for a go) and explore "turtle graphics". Describe the graphics operators in terms of 2-numbers. Look up "turtle geometry" [AdS81]. What is the turtle's take on general relativity? (Logo not only has neat graphics for Grade 3 use, it also is a superb programming language. Explore all of it!)

4. A colony of the army ant species Eciton burchellii bivouacs for a period of three weeks, while eggs become pupae, and radiates outward daily in search of food [Mof06]. Their 20 days of hunting (followed by the 21st day, in which they set off for a new bivouac a couple of kilometers distant) cover a region of about 80 m. radius as shown:



Describe this pattern using 2-numbers.
How would you include the path along which the ants arrive from their previous bivouac on day 0?

5. 2-numbers can represent both points and straight lines in two dimensions. The representation of a line is the difference between the representations of the end points,

$$L = P_f - P_s$$

where P_s is the starting point of the line and P_f is the finishing point. (Thus the line, L, has a length and a direction. It does *not* have a position: the line from $P_s + c$ to $P_f + c$ has the same representation as the line from P_s to P_f.)

Given a starting point, P_s, and a line L, we can find the finishing point,

$$P_f = P_s + L$$

Armed with this information, find out where to dig for the following treasure, buried on an island which has an oak tree, a pine tree and a gallows [Gam47]. The instructions you found, stuck into a musty old book in your elderly relative's attic, say

(a) starting at the gallows, go to the pine tree, make a left right-angle turn, walk the same distance again, and mark the spot;

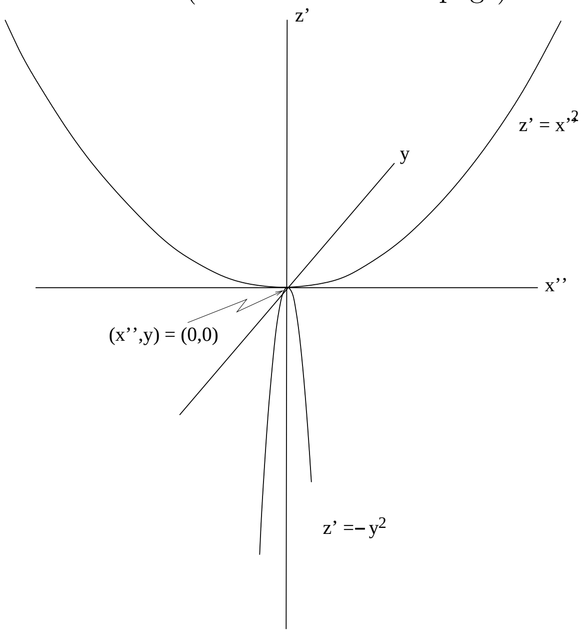
(b) starting again at the gallows, go to the oak tree, make a right right-angle turn, walk the same distance again, and mark that spot, too;

(c) halfway between the marked spots, dig for the treasure.

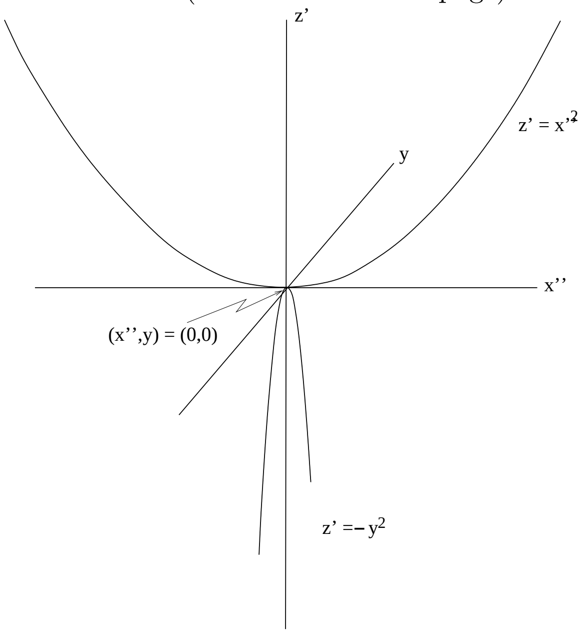
However, when you get to the island, there is no longer any sign of the gallows.

6. Think about the following two chains of transformations of a parabola, $z = x^2$, and its “shadow” parabola in the perpendicular plane, $z = -y^2$. Relate the final equations for z in each case to $z = ax^2 + bx + c$, and discover the formulas for the “roots”, i.e., the values of x and y when $z = 0$.

Chain 1 (read down to next page)

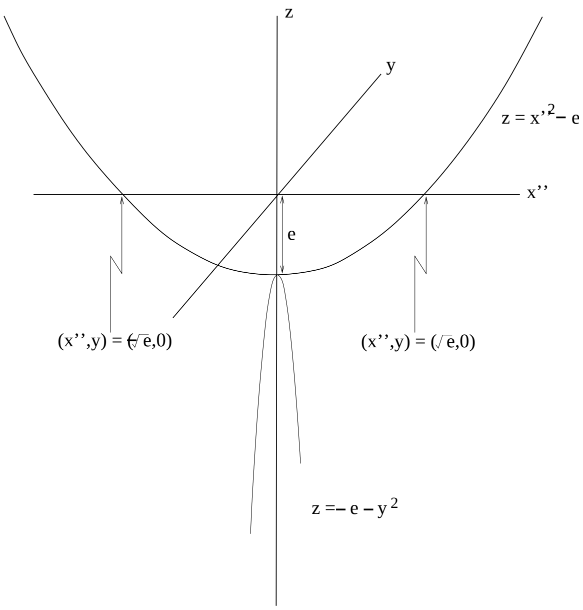


Chain 2 (read down to next page)

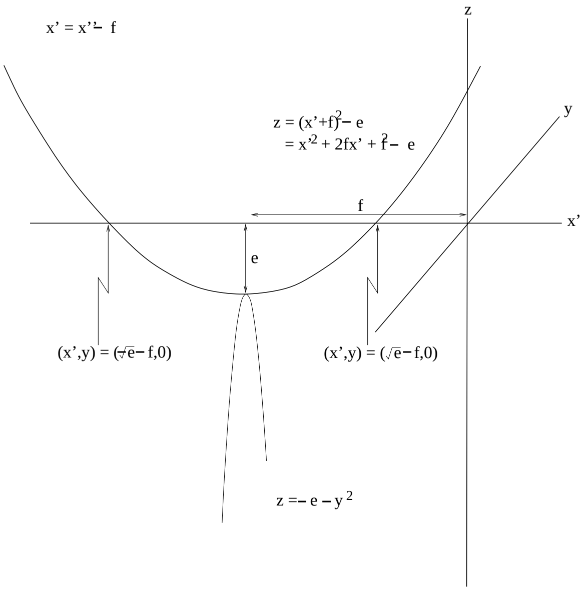


Chain 1 (cont.: read downwards)

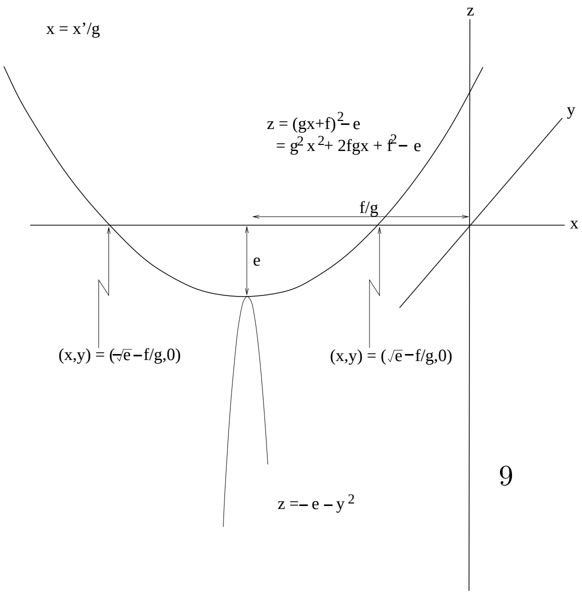
$z = z' - e$



$x' = x'' - f$

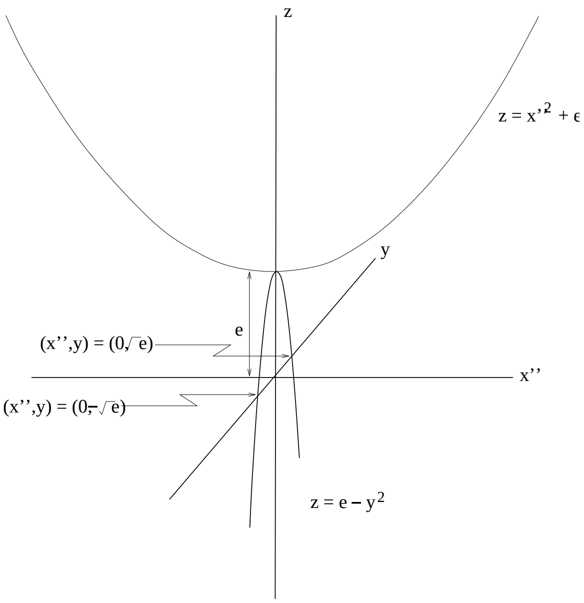

z
y
$z = (x'+f)^2 - e$
$= x'^2 + 2fx' + f^2 - e$
f
x'
e
$(x',y) = (-\sqrt{e} - f,0)$
$(x',y) = (\sqrt{e} - f,0)$
$z = -e - y^2$

$x = x'/g$

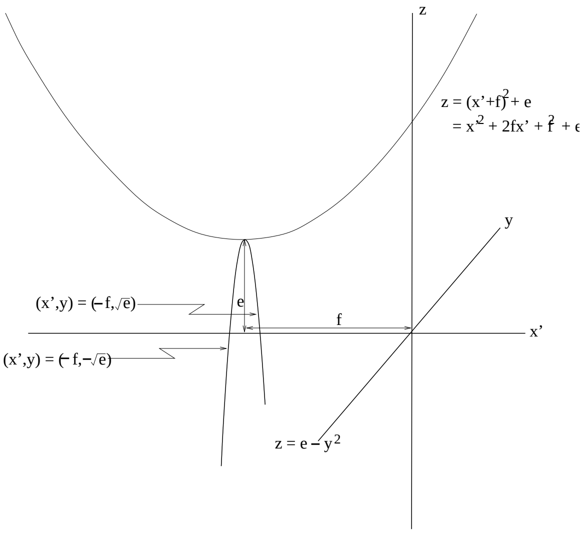

z
y
$z = (gx+f)^2 - e$
$= g^2 x^2 + 2fgx + f^2 - e$
f/g
x
e
$(x,y) = (-\sqrt{e} - f/g,0)$
$(x,y) = (\sqrt{e} - f/g,0)$
$z = -e - y^2$

Chain 2 (cont.: read downwards)

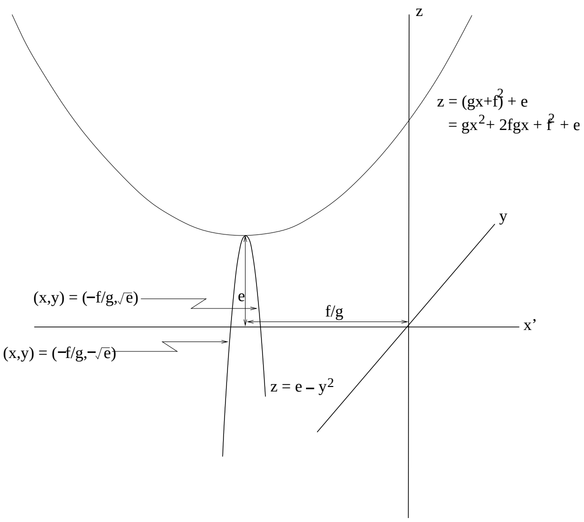
$z = z' + e$



$x' = x'' - f$



$x = x'/g$


z
$z = (gx+f)^2 + e$
$= gx^2 + 2fgx + f^2 + e$
y
$(x,y) = (-f/g,\sqrt{e})$
e
f/g
x'
$(x,y) = (-f/g,-\sqrt{e})$
$z = e - y^2$

7. The parabola $z = x^2$ in the previous excursion is undefined for negative z, but can be extended in direction y at right angles to x with $z = -y^2$. What is the corresponding extension for a circle, $\frac{x^2}{r^2} + \frac{z^2}{r^2} = 1$, or for an ellipse, $\frac{x^2}{a^2} + \frac{z^2}{b^2} = 1$?

8. **Roots of unity.** a) Show that $e^{2\pi i/3}$ and $e^{4\pi i/3}$ are cube roots of 1 as well as 1 itself. Draw these three cube roots as points in the 2-number plane.
b) The "*primitive* cube roots of unity" are those cube roots of 1 that have no power less than the third power which equals 1. Show that $e^{2\pi i/3}$ and $e^{4\pi i/3}$ are primitive cube roots of unity, and 1 is not.
c) Find, and draw, the fourth roots of 1, and say which are primitive.
d) Find, and draw, the fifth, sixth and seventh roots of 1, and say which are primitive. Discuss the patterns you find. For which n are there $n-1$ primitive nth roots of 1? What is the rule for other values of n?

9. If $v = x + iy =\mid v \mid e^{i\angle v}$ is any 2-number, its *reflection* in the line of 1-numbers is given by a new operation, the *conjugate*, $v^* = (x + iy)^* = x - iy = (\mid v \mid e^{i\angle v})^* =\mid v \mid e^{-i\angle v}$. Suppose $u = c + is = e^{i\angle u}$ is any other 2-number of magnitude $\mid u \mid= 1$, giving the direction of a line, which we will also call u, and convince yourself that uv^*u is the reflection of v in u.
Using this, go on to show that the *projection* of v in u (that is the component of v that lies in the same direction as u) is $(v + uv^*u)/2$, and that the component of v that is perpendicular to this is $(v - uv^*u)/2$. What are the projections of v on the line of 1-numbers and on $\perp$, the line at right angles to it?

10. Two-dimensional numbers support the rotation

$$\begin{pmatrix} c & -s \\ s & c \end{pmatrix}$$

as $c + is$, with $c^2 + s^2 = 1$ The Lorentz shear

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

has $a^2 - b^2 = 1$ How might two-dimensional numbers, i in particular, be used to make this shear look like a rotation?
Does it seem from this that there is a 2-number operator for shear, in the way there is a 2-number operator for rotation (and for reflection and for projection)?

11. a) Show that the eigenvalues of

$$\begin{pmatrix} c & -s \\ s & c \end{pmatrix}$$

are $e^{i\theta}$ and $e^{-i\theta}$, where c is $\cos\theta$ and s is $\sin\theta$, and that the eigenvectors (fixed-point vectors of the transformation) are

$$\begin{pmatrix} 1 \\ i \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 \\ -i \end{pmatrix}$$

b) The appearance of 2-numbers suggests that the eigenvectors must somehow be perpendicular to the two dimensions the rotation takes place in. Indeed, if a third dimension were added, the rotation leaves fixed the vector perpendicular to the plane of rotation.
However, by finding the eigenvalues and eigenvectors of the (2-D) rotation in three dimensions,

$$\begin{pmatrix} c & -s & \\ s & c & \\ & & 1 \end{pmatrix}$$

you can see that the extra dimension suggested by the 2-numbers is not the same as the new third dimension.

12. Find all products of the matrices

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

Do they commute ($xy - yx = 0$)? Do they anticommute ($xy + yx = 0$)? What matrices must be added so that they form a closed set apart from scalar multiples? What are their inverses?

13. Find the inverse of the matrix

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

Hint: try multiplying it by itself and then see if you must adjust anything.

How does this compare with finding the inverse of a rotation matrix?

14. On the field axioms (Note 7):
a) Show that, if 1-numbers and i satisfy the field axioms, then so do 2-numbers.
b) Find two matrices whose product does not commute.
c) Are matrix products associative?
d) Compare uv^T and $v^T u$ for a vector u and a transposed vector v^T. Is this operation closed?
e) Find an operation on 1-numbers which is commutative but not associative.
f) Find an operation on strings, such as "hello " and "world ", which is associative but not commutative. (Note. A *string* is a sequence of characters, often letters and spaces.)
g) Are the field axioms consistent, i.e., do any of them contradict any others? (Other questions one can ask about axioms: Are they independent—can any be derived from others? Are they complete—is anything missing?)

15. These axioms are also given by W. W. Sawyer *A Concrete Approach to Abstract Algebra* [Saw59]. Discuss his demonstration, at the end of the book, that an angle cannot be trisected using only straight lines and lengths ("ruler and compass").

16. What important property of 1-numbers is completely ignored by the field axioms? (Hint. Who is more excellent, the student who got 80% in English and 90% in math, or the student who got 90% in English and 80% in math?)

17. **Field trip** a) Show that arithmetic "**modulo**" 3 is a field. Here are the addition and multiplication tables. Note how 3 is effectively 0 and the numbers "wrap around" from 2 to 0: the idea of **modulo** is to use remainders of the result divided by 3.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

It is actually more intuitive to use −1 instead of 2—note how both play the same role in this arithmetic. So we will rewrite the tables and follow the −1 version for the rest of this excursion.

$+$	0	1	-1
0	0	1	-1
1	1	-1	0
-1	-1	0	1

$\times$	0	1	-1
0	0	0	0
1	0	1	-1
-1	0	-1	1

b) Now look at linear and quadratic polynomials over this field and try to factor the quadratic ones.
Show that there are 27 polynomials of the form $ax^2 + bx + c$ where a, b and c are in the field. Here are some of them. Which ones are missing?
In the line below each polynomial are the "roots" of the polynomial. For linear polynomial equations, $bx + c = 0$, the root, r, satisfies $x - r = 0$, so $r = -c/b$. For quadratic polynomial equations, $ax^2 + bc + c = 0$, the roots, r_1 and r_2, satisfy $(x - r_1)(x - r_2) = 0$ and can be found even in this small field using the quadratic formula we derived in an earlier excursion. Or you can just check them now that they are found.

a			0					1		
		c	0	1	-1		c	0	1	-1
	b	0	0	1	-1	b	0	x^2	$x^2 + 1$	$x^2 - 1$
								0,0	$-\surd, \surd$	$1, -1$
		1	x	$x + 1$	$x - 1$		0	$x^2 + x$	$x^2 + x + 1$	$x^2 + x - 1$
			0	-1	1			$0, -1$	1,1	$1 - \surd, 1 + \surd$
		-1	$-x$	$-x + 1$	$-x - 1$		-1	$x^2 - x$	$x^2 - x + 1$	$x^2 - x - 1$
			0	1	-1			0,1	$-1, -1$	$-1 - \surd, -1 + \surd$

c) Note that a new element, $\surd$, has appeared. This is short for either $\sqrt{2}$ or $\sqrt{-1}$, whichever you prefer: they are both the same in this field. Try squaring either one to see.
Not only $\surd$ but all six possible combinations of $\surd$ with the field elements 0, 1, -1 also appear. Show that these, together with the elements 0, 1, -1 themselves, also form a field. This new field is called an *extension* of the original field. A notation for the two fields is F_3 and $F_3[\surd]$.
d) To show that x^3 is meaningful, even in a field in which $3 = 0$, here are all possible powers of x. Check them carefully. Note that x^3 does not give us anything new over F_3, but over $F_3[\surd]$ we must go to x^8 before we start repeating. Which elements of $F_3[\surd]$ are *generators* of $F_3[\surd]$, in the sense that their powers up to 8 generate all elements of $F_3[\surd]$ except 0?

x	0	1	-1	$\surd$	$-\surd$	$1 + \surd$	$-1 - \surd$	$1 - \surd$	$-1 + \surd$
x^2	0	1	1	-1	-1	$-\surd$	$-\surd$	$\surd$	$\surd$
x^3	0	1	-1	$-\surd$	$\surd$	$1 - \surd$	$-1 + \surd$	$1 + \surd$	$-1 - \surd$
x^4	0	1	1	1	1	-1	-1	-1	-1
x^5	0	1	-1	$\surd$	$-\surd$	$-1 - \surd$	$1 + \surd$	$-1 + \surd$	$1 - \surd$
x^6	0	1	1	-1	-1	$\surd$	$\surd$	$-\surd$	$-\surd$
x^7	0	1	-1	$-\surd$	$\surd$	$-1 + \surd$	$1 - \surd$	$-1 - \surd$	$1 + \surd$
x^8	0	1	1	1	1	1	1	1	1

e) Show from the above that every element of $F_3[\surd]$, and also of F_3, has a cube root in the respective field. Show also that there are no further square roots we can find over F_3.
So if there are any cubic polynomials, $x^3 + ax^2 + bx + c$, which cannot be factored linearly over $F_3[\surd]$ (that is factored completely into linear factors with coefficients, i.e., roots, in $F_3[\surd]$), we are faced with a new situation.
(The cubic equation formula for ordinary numbers

$$x = -\frac{p}{3u} + u - \frac{a}{3}$$

where

$$u^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

and

$$p = b - \frac{a^3}{3}, q = c + \frac{2a^3 - 9ab}{27}$$

will not help us because of those multiples of 3 on the denominators: remember $3 = 0$ in F_3 as well as in $F_3[\surd]$.)

Indeed, there are eight such cubic polynomials (well, 16, if we include all their negatives): $x^3 - x + 1$, $x^3 - x - 1$, $x^3 + x^2 - 1$, $x^3 - x^2 + 1$, $x^3 + x^2 + x - 1$, $x^3 - x^2 + x + 1$, $x^3 + x^2 - x + 1$, and $x^3 - x^2 - x - 1$.

Find *all* the cubic polynomials with coefficients in F_3. How many are there? Find the roots of all except the eight (well, 16) above. Note that cubic polynomials such as $x^3 + 1$ can be factored completely into linear factors in F_3 although it cannot in the fields of ordinary numbers.

f) In the new situation we forewarned, above, we cannot use "radicals" to factor cubic polynomials.

(The word "radical" is from "radix" in Latin, which means "root": radicals are also people who like to get to the root of things. To avoid confusion with "roots" of polynomials, we use "radical" to refer to square roots, cube roots, and so on, of the elements of the field. Note that in the fields of ordinary numbers, we can use radicals to factor any quadratic, cubic or quartic polynomial, by the formulas given in an earlier excursion (quadratic), this excursion (cubic), and in Week_iii (quartic).)

We can, however, solve all eight of these cubics *formally.* By this we mean, imagine a root, say r, of, say $x^3 - x + 1$ and note that, because we have invented r to be a root, $r^3 - r + 1 = 0$. So of course $r^3 = r - 1$ and we can express all further powers of r using only r and r^2.

If we extend F_3 to $F_3[r]$, we will be adding 24 more elements to make the total of 27 including 0, 1 and -1: $F_3[r]$ will contain all 27 elements of the form $ur^2 + vr + w$ for u, v and w chosen from 0, 1 and -1. We can get them all, except 0, from the powers of r: verify the following eleven.

r^3	r^4	r^5	r^6	r^7	r^8	r^9	r^{10}	r^{11}	r^{12}	r^{13}
$r - 1$	$r^2 - r$	$-r^2 + r - 1$	$r^2 + r + 1$	$r^2 - r - 1$	$-r^2 - 1$	$r + 1$	$r^2 + r$	$r^2 + r - 1$	$r^2 - 1$	-1

Show that there are 26 different powers of r. On the other hand, if q is a (formal) root of $x^3 - x - 1$, show that there are only 13 different powers of q: q is not a generator but r is.

Here are the first three powers of half of the 24 non-F_3 elements of $F_3[r]$. Verify them. Show that they provide three different roots for each of four of the cubic polynomials we identified above as not having radical factors. What is the simple change needed to find the other 12 and so roots of the other four cubic polynomials?

x	r	$r + 1$	$r - 1$	r^2	$r^2 + 1$	$r^2 - 1$
x^2	r^2	$r^2 - r + 1$	$r^2 + r + 1$	$r^2 - r$	$-r + 1$	$-r^2 - r + 1$
x^3	$r - 1$	r	$r + 1$	$r^2 + r + 1$	$r^2 + r - 1$	$r^2 + r$

x	$r^2 + r$	$r^2 - r$	$r^2 + r + 1$	$r^r + r - 1$	$r^2 - r + 1$	$r^2 - r - 1$
x^2	$-r^2 + r + 1$	$-r^2 - 1$	$r^2 - 1$	$-r - 1$	$r^2 + r$	$-r$
x^3	$r^2 - r$	$r^2 - 1$	$r^2 - r + 1$	$r^2 - r - 1$	r^2	$r^2 + 1$

g) We could not solve eight of the cubics over F_3 by radicals simply because there are not enough radicals. We cannot write down a general formula using radicals to give the roots of quintic polynomials over the fields of ordinary numbers either. This is surprising and the

reasons are subtle. We must wait until Week 8c to understand them.
Find out about the people who solved the quadratic, cubic and quartic polynomials over the fields of ordinary numbers, and about the long and unsuccessful effort to do the same for the quintic.

18. a) Show that arithmetic **modulo** 6 is not a field. (Arithmetic modulo 6 is arithmetic limited to the six integers 0, 1, 2, 3, 4 and 5 that are the remainder when any integer is divided by 6. You can write out the addition and multiplication tables as 6 × 6 arrays by doing ordinary arithmetic then writing down the remainder of the result after dividing by 6. Hint: the multiplication table will show you what you need to argue.)
b) For what integers, n, is arithmetic **modulo** n a field?

19. If a set is not closed under an operation, can the operation be associative? Revisit the question of the independence of the field axioms.

20. The integers do not form a field but a "ring": which field axiom must be omitted to describe integers? Are the real numbers a ring? Are there more fields than rings or vice-versa? Show that polynomials (see Week_iii) form a ring. (Note that polynomials include the elements of their field of coefficients as a special case. Why?)

21. **"Symmetric polynomials".** a) Show that symmetric expressions, such as $r_1r_2(r_1+r_2)$ or $2(r_1+r_2)$ or $r_1r_2+r_2r_3+r_3r_1+r_1^2+r_2^2-r_3^2$ or $(r_1-r_2)^2(r_1-r_3)^2(r_2-r_3)^2$, form a ring: a symmetric expression in terms $r_1, r_2, .., r_n$ is any expression that remains unchanged after any permutations of the n terms. (I am using the computer-science word "expression" rather than the mathematical word "polynomial" for these because this excursion will not get far into the mathematics.)
b) Show that the coefficients, $a_0, a_1, .., a_{n-1}$, of a polynomial

$$x^n + a_{n-1}x^{n-1} + .. + a_1x + a_0 = (x-r_1)(x-r_2)..(x-r_n)$$

are symmetric expressions in the roots, $r_1, r_2, .., r_n$.
These are called *elementary* symmetric expressions. For example, for x^3+ax^2+bx+c, $a=-(r_1+r_2+r_3)$, $b=r_1r_2+r_2r_3+r_3r_1$ and $c=r_1r_2r_3$.
c) Look up "Newton's identities", which relate "power sum" symmetric expressions, such as $r_1^2+r_2^2+r3^2$ or $r_1^5+r_2^5$, to the elementary symmetric expressions.
d) Confirm that the "discriminant" of the polynomials Ax^2+Bx+a and x^3+ax^2+bx+c are, respectively, B^2-4AC and $q^2/4+p^3/27$ where $p=b-a^3/3$ and $q=c+(2a^3-9ab)/27$: the discriminant is the function of the roots of the polynomial that goes to zero only when two or more roots are the same, $\sum_{i<j}(r_i-r_j)^2$, e.g., respectively, $(r_1-r_2)^2$, and $(r_1-r_2)^2(r_1-r_3)^2(r_2-r_3)^2$. You will need Newton's identities and some algebra for the second.

22. Look up Leonhard Euler, 1707–83. What are Euler's identity and Euler's number? How did he come across them?

23. Look up Johann Carl Friedrich Gauss, 1777–1855, and his doctoral thesis on the fundamental theorem of algebra [Gau99]. How does he use two-dimensional numbers? Does he refer to $\sqrt{-1}$? Given the completeness of 2-numbers established by Gauss' proof, how likely is it that there are "3-numbers", with the same properties (i.e., satisfying the field axioms) and describing three dimensions? What property(ies) should be changed to describe 3D?
What mathematical progression did Gauss discover at the age of 10?

24. Expand the terms of the expressions describing the two closed figures of Notes 10 and 11,

$$4e^{i0}+4e^{i\pi/2}+2e^{i0}+4e^{-i\pi/2}+4e^{i0}+8e^{i\pi/2}+5\sqrt{2}e^{i3\pi/4}+5\sqrt{2}e^{i5\pi/4}+8e^{i3\pi/2}$$

and

$$e^{i4\pi/5} + e^{i8\pi/5} + e^{i12\pi/5} + e^{i16\pi/5} + e^{i20\pi/5}$$

and show that they each sum to zero in both dimensions.

25. Any part of the lecture that needs working through.

References

[AdS81] H. Abelson and A. di Sessa. *Turtle Geometry.* The M.I.T. Press, Cambridge, Mass, 1981.

[Gam47] George Gamow. *One two three ... infinity: Facts & Speculations of Science.* The Viking Press, New York, 1947.

[Gau99] Carl Friedrich Gauss. *New Proof of the Theorem That Every Algebraic Rational Integral Function In One Variable can be Resolved into Real Factors of the First or the Second Degree.* PhD thesis, Julia Carolina Academy, 1799. English translation by Ernest Fandreyer, Prof. of Mathematics, Fitchburg State College.

[Mof06] Mark W. Moffett. Army ants: Inside the ranks. *National Geographic*, 210(2):138–49, Aug. 2006. Prefaced by Edward O. Wilson *Ants: The Civilized Insect.*

[Nel78] Theodor H. Nelson. *Computer Lib/Dream Machines.* the distributors, 702 South Michigan, South Bend IN 46618, May, 1978.

[Saw59] W. W. Sawyer. *A Concrete Approach to Abstract Algebra.* W. H. Freeman & Co., San Francisco, 1959.