A linear algebra exercise

Frits Beukers, Ronald van Luijk, Raimundas Vidunas

February 4, 2002

1 The problem

Anyone who has ever composed a written test on linear algebra knows that it often taken considerable effort to make the 'numbers come out right'. In fact, this problem may even be harder than the linear algebra problem itself. A particular subject where this problem arises, is eigenvalues of symmetric matrices. Usually we consider only matrices with integral coefficients. We know that 4×4-matrices tend to become too laborious. Since 2×2-matrices are not very exciting we have to confine ourselves to 3×3-matrices. We know that there are 3 real eigenvalues in this case. We cannot let the poor students solve irreducible cubic equations, so we might see to it that the eigenvalues are integers, which the students can recognize by inspection. Moreover, computing the eigenvalue equation of an arbitrary symmetric 3×3-matrix may be a little too stressful. So we choose our matrix to have a simple shape, say

$$M_{a,b,c} = \begin{pmatrix} 0 & a & b \\ a & 0 & c \\ b & c & 0 \end{pmatrix}$$

But now we created a problem for ourselves. How to choose integers a, b, c such that the symmetric matrix $M_{a,b,c}$ has three integral eigenvalues ?

The eigenvalue equation reads

$$\lambda^3 - (a^2 + b^2 + c^2)\lambda - 2abc = 0$$

If $a = 0$ for example and we choose b, c such that $b^2 + c^2 = u^2$ for some integer u (e.g. $b = 3, c = 4, u = 5$), then our eigenvalue equation reads

$$(\lambda - u)(\lambda + u)\lambda = 0.$$

If $a = \pm b$ and a, c are such that $c^2 + 8a^2 = u^2$ for some integer u (e.g. $a = 3, c = 7, u = 11$), then our eigenvalue equation becomes

$$(\lambda \pm c)(\lambda - (\pm c + u)/2)(\lambda - (\pm c - u)/2) = 0.$$

Note that the eigenvalue equation is symmetric in a, b, c. So we see that the above ideas yield solutions with the property that $abc = 0$ or $(a^2 - b^2)(a^2 -$

$c^2)(b^2-c^2)=0$. To make our linear algebra problem a little interesting we would like the numbers a, b, c to be non-zero and with distinct absolute values. Hence we have the following question.

Question Do there exist non-zero integers a, b, c, with distinct absolute values, such that

$$X^3-(a^2+b^2+c^2)X-2abc$$

has three integral zeros X?

This is precisely Problem 10 on page 413 of Nieuw Archief 1 (2000). There it was posed as an open problem and two of the co-authors showed in different ways that there does exist an infinite number of solutions. In the next section we sketch the construction of three infinite families.

2 Three solutions

If we let x, y and z denote the eigenvalues of the given matrix $M_{a,b,c}$, then the characteristic polynomial of $M_{a,b,c}$ equals

$$\lambda^3-(a^2+b^2+c^2)\lambda-2abc=(\lambda-x)(\lambda-y)(\lambda-z).$$

Hence we want to find integers a, b, c, x, y, z, such that this polynomial equation holds. Comparing coefficients, we find the equations

$$\begin{aligned} x+y+z&=0, \\ xy+yz+zx&=-a^2-b^2-c^2, \\ xyz&=2abc. \end{aligned} \tag{1}$$

These equations describe a two-dimensional surface S in five-dimensional projective space $\mathbb{P}^5$. We look for points with integral or, what amounts to the same, rational coordinates. Instead of looking for individual rational points we shall look for so-called rational curves on S, i.e. polynomials in one variable which satisfy (1). Note that this surface, which is of degree 6, actually lies in projective four-space, as it is contained in the hypersurface given by $x+y+z=0$.

Closer scrutiny by Ronald van Luijk has shown that S is birationally equivalent to a so-called singular K3-surface. As a consequence the surface S has a large number of interesting properties, but we shall not go into this here.

In the remainder of this section we describe three approaches to find an infinite number of rational solutions.

From the discussion in the previous section we know that there are infinitely many solutions with $a=0, x=0$. Namely $z=-y$ and $y^2=b^2+c^2$. This is the projective equation of a unit circle C. We choose t arbitrarily and intersect S with the hyperplane $x=ta$ in $\mathbb{P}^5$. The intersection is a curve of degree 6, but we know that it always contains the conic C as a factor. Hence the remainder of the intersection should be a curve of degree 4. This becomes even more apparent if we take $x = ta$ in (1), take $a = 1$ to go to affine coordinates, and eliminate c, z. We find

$$t^2y^2(t+y)^2 - 4b^2(t^2+ty+y^2) + 4b^2(1+b^2) = 0. \tag{2}$$

This can be considered as a family of fourth degree curves X_t with parameter t, or alternatively, as a fourth degree curve with coefficients in $\mathbb{Q}(t)$. The coordinates of the curve are b, y. A short calculation shows that the curve has two singular points, namely $(b, y) = (0, 0), (0, -t)$. From the geometry of curves we know that such an algebraic curve has genus 1. The points on genus one curves have an abelian group structure which we can now exploit. First we look for a number of obvious points on X_t. They come from the straightforward solutions we found in the previous section. First the point with $b = -a = -1$ and $c = y$. A brief calculation shows that $y = -t + 2/t$ and the corresponding point is $(b, y) = (-1, -t + 2/t)$. We denote this point by O. Another point is found by taking $c = 1, y = -b$. We then find the point $(b, y) = (t - 2/t, -t + 2/t)$, which we denote by P. General theory of elliptic curves tells us that we can take O as the neutral element of a commutative addition law on X_t. Doing so, a straightforward, but tedious, computation shows that $2P$ is now given by the point

$$(b, y) = \left(\frac{-t^6 - 4t^4 + 4}{t^6 - 8t^4 + 20t^2 - 12}, \frac{2t^6 - 12t^4 + 16t - 8}{t^7 - 8t^5 + 20t^3 - 12t} \right).$$

After clearing the denominators this gives us the solution

$$\begin{aligned}
a &= t(t^6 - 8t^4 + 20t^2 - 12)\\
b &= -t(t^6 - 4t^4 + 4)\\
c &= (t^2 - 2)(t^6 - 6t^4 + 8t^2 - 4)\\
x &= t^2(t^6 - 8t^4 + 20t^2 - 12)\\
y &= 2t^6 - 12t^4 + 16t^2 - 8\\
z &= -t^8 + 6t^6 - 8t^4 - 4t^2 + 8
\end{aligned}$$

By computing higher multiples nP of P we could in principle find an infinite number of such parametrisations. However, the degrees of the polynomials involved increase like n^2 and become unwieldy very soon.

There is another remark we can make concerning (2). The singular point $(b, y) = (0, -t)$ is a double point and the equation of its two tangents is easily seen to be

$$4(1 - t^2)b^2 + (y + t)^2t^4 = 0.$$

Now replace t by $(s + 1/s)/2$ so that $4(1 - t^2) = -(s - 1/s)^2$. The equation of the tangents now factors as

$$\left((y + t)t^2 - b(s - 1/s)\right)\left((y + t)t^2 + b(s - 1/s)\right).$$

Take one of the tangents. At the point $(b, y) = (0, -t)$ it has triple intersection with X_t. So the tangent intersects in only one more point. After straightforward, but again tedious, computation we find the following points after clearing denominators:

$$
\begin{aligned}
a &= 2s(s^6-5s^4+11s^2+1)(s^6+11s^4-5s^2+1)\\
b &= 4s(s-1)(s+1)(s^2+1)^3(s^2+2s-1)(s^2-2s-1)\\
c &= (s-1)(s+1)(s^6-4s^5+3s^4+8s^3+3s^2-4s+1)\\
&\quad \times(s^6+4s^5+3s^4-8s^3+3s^2+4s+1)\\
x &= (s^2+1)(s^6-5s^4+11s^2+1)(s^6+11s^4-5s^2+1)\\
y &= -(1+s^2)(s^6-4s^5+3s^4+8s^3+3s^2-4s+1)\\
&\quad \times(s^6+4s^5+3s^4-8s^3+3s^2+4s+1)\\
z &= -16s^2(s-1)^2(s+1)^2(s^2+1)(s^2-2s-1)(s^2+2s-1)
\end{aligned}
$$

A third possibility to find a rational curve on S is to look for bad fibers of the family of curves X_t, i.e. look for those values of t for which X_t acquires an extra singularity. An irreducible fourth degree curve with three singular points has genus 0, in other words, it is a rational curve. Unfortunately, the bad fibers of the family X_t all turn out to be reducible with components not defined over $\mathbb{Q}$. However, it is possible to construct another family of genus one curves on S by intersecting it with the family of hyperplanes $a-b+t(c+z)=0$. Note that $a-b=0$, $z=-c$ also correponds to a straightforward solution from the first section. It turns out that the special hyperplane $a-b-2(c+z)=0$ intersects S in a conic plus a fourth degree curve with three singularities. Rational parametrisation of the latter curve yields the solution

$$
\begin{aligned}
a &= (4u-7)(u+2)(u^2-6u+4)\\
b &= (5u-6)(5u^2-10u-4)\\
c &= -(3u^2-4u+4)(u^2-4u+6)\\
x &= 2(3u^2-4u+4)(4u-7)\\
y &= -(u+2)(5u-6)(u^2-4u+6)\\
z &= (u^2-6u+4)(5u^2-10u-4)
\end{aligned}
$$

When we substitute $u=3$ in the latter parametrisation, we get $a=-125$, $b=99$ and $c=-57$ with eigenvalues 190, -135 and -55. By a computer search, we find that this is the second smallest example, when ordered by $\max(|a|,|b|,|c|)$. The smallest has $a=26$, $b=51$ and $c=114$.