Scratchwork: $\zeta_K(2)$ with $K = \mathbb{Q}(\sqrt{2})$

For today's warmup problem we show that $x = \sqrt{2} + \sqrt{3}$ is an algebric number. Certainly we have that $\sqrt{2}$ and $\sqrt{3}$ are algebraic numbers, since:

$$(\sqrt{2})^2 - 2 = 0 \text{ and } (\sqrt{3})^2 - 3 = 0$$

and it seems plausible that the sum of two algebraic numbers is an algebraic number, but I can't think of the polynomial. Let's do some trial an error:

- $1 = 1$
- $\sqrt{2} + \sqrt{3} = \sqrt{2} + \sqrt{3}$
- $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$
- $(\sqrt{2} + \sqrt{3})^3 = (2 + 3 \times 3)\sqrt{2} + (3 + 3 \times 2)\sqrt{3} = 11\sqrt{2} + 9\sqrt{3}$
- $(\sqrt{2} + \sqrt{3})^4 = 2 \times 2 + 3 \times 3 + 6 \times 6 + 4 \times (2 + 3) \times \sqrt{6} = 49 + 20\sqrt{6}$

I am not sure if I made an arthmetic error. Let me check these with a computer:

```
>>> ( 5 + 2*6**0.5 ) - ( 2**0.5 + 3**0.5 )**2

-1.7763568394002505e-15

>>> (49 + 20*6**0.5) - ( 2**0.5 + 3**0.5 )**4

-2.842170943040401e-14
```

These decimal errors are just somewhat scary, but at least we obtain statements like:

$$\left|(\sqrt{2} + \sqrt{3})^4 - (49 + 20\sqrt{6})\right| < 10^{-12}$$

in fact the difference is zero. However, that thing we called "$\sqrt{2}$" or "$\sqrt{3}$" was likely something else anyway, with even a small error.

What if we used integers? Let's try representing the $\sqrt{2}$ and $\sqrt{3}$ as 2×2 matrices:

$$\sqrt{2} = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} \text{ and } \sqrt{3} = \begin{bmatrix} 0 & 3 \\ 1 & 0 \end{bmatrix}$$

and these aren't the only representations either. Let's merge these into a single matrix:

$$\sqrt{2} \otimes 1 = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mapsto \left[\begin{array}{cc|cc} 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{array}\right]$$

$$1 \otimes \sqrt{3} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 3 \\ 1 & 0 \end{bmatrix} \mapsto \left[\begin{array}{cc|cc} 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{array}\right]$$

These matrices come out of nowhere:

```
>>> import numpy as np
>>> a = np.array([[0,2,0,0],[1,0,0,0],[0,0,0,2],[0,0,1,0]])
>>> b = np.array([[0,0,3,0],[0,0,0,3],[1,0,0,0],[0,1,0,0]])
```

but they come out with answers related to what we obtained before:

```
>>> np.dot(a+b,a+b)
array([[ 5,  0,  0, 12],
       [ 0,  5,  6,  0],
       [ 0,  4,  5,  0],
       [ 2,  0,  0,  5]])

>>> f = lambda x : np.dot(x,a+b)
>>> f(f(a+b))
array([[ 0, 22, 27,  0],
       [11,  0,  0, 27],
       [ 9,  0,  0, 22],
       [ 0,  9, 11,  0]])

>>> f(f(f(a+b)))
array([[ 49,   0,   0, 120],
       [  0,  49,  60,   0],
       [  0,  40,  49,   0],
       [ 20,   0,   0,  49]])
```

Running these tensor product comutations backwards, are we sure this map is true?

$$\left[\begin{array}{cc|cc} 49 & 0 & 0 & 120 \\ 0 & 49 & 60 & 0 \\ \hline 0 & 40 & 49 & 0 \\ 20 & 0 & 0 & 49 \end{array}\right] \mapsto \left(49 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + 20 \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 3 \\ 1 & 0 \end{bmatrix}\right)^{\otimes 2}$$

I was able to find this answer because I know the answer already and I'm making up the rules as I go along. In fact, we have re-construted the **tensor product** and the $\mathbb{Z}$-**module**.

Later, this perfect algebric description should also have a defect, since we'll observe that $\overline{\mathbb{Q}(\sqrt{2}+\sqrt{3})} = \mathbb{R}$ and wonder how that is happening.

Here is more code:

```
>>> f1 = lambda a,b,c,d : a + b*2**0.5 + c*3**0.5 + d*6**0.5
>>> f2 = lambda a,b,c,d : a - b*2**0.5 + c*3**0.5 - d*6**0.5
>>> f3 = lambda a,b,c,d : a + b*2**0.5 - c*3**0.5 - d*6**0.5
>>> f4 = lambda a,b,c,d : a - b*2**0.5 - c*3**0.5 + d*6**0.5
>>> g = lambda a,b,c,d: np.round( f1(a,b,c,d)*f2(a,b,c,d)*f3(a,b,c,d)*f4(a,b,c,d)).astype(int)
>>> [g(a,b,c,d) for a in range(5) for b in range(5) for c in range(5) for d in range(5)]
```

Then we obtain some silly factorizations like this:

$$-23 = (2+\sqrt{2}+\sqrt{3}) \times (2-\sqrt{2}+\sqrt{3}) \times (2+\sqrt{2}-\sqrt{3}) \times (2-\sqrt{2}-\sqrt{3})$$

Let's restrict our attention to subfields $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$. This is also a quadratic extension, with the base field $K=\mathbb{Q}(\sqrt{2})$. By the same token we have another quadratic extension $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{3})]=2$.

We could ask about the ring of integers, $\mathcal{O}_L$ with $L=\mathbb{Q}(\sqrt{2},\sqrt{3})$ and solve the quadratic equations:

$$x^2+(a_0+a_1\sqrt{2})x+(b_0+b_1\sqrt{2})=0$$

with $x=x_0+x_1\sqrt{2}+x_2\sqrt{3}+x_3\sqrt{6}$ (or the basis of your choice). The discriminant condition determines a variety:

$$\sqrt{(a_0+a_1\sqrt{2})^2-4(b_0+b_1\sqrt{2})}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$$

Even for the extension $[\mathbb{Q}(i):\mathbb{Q}]=2$ I don't remember how this works, why this would obtain the ring of integers $\mathbb{Z}[i]$ (or even that this is closed under addition, that if $a\in\mathbb{Z}[i]$ and $b\in\mathbb{Z}[i]$ then $a+b\in\mathbb{Z}[i]$.

— —

The goal of today's talk is much more modest, to write down the zeta function $\zeta_K(2)$ with $K=\mathbb{Q}(\sqrt{2})$. This barely requires understanding the primes in $\mathbb{Z}[\sqrt{2}]$, since all we care about are the norms and ideal classes. However, naïvely I don't know what those are, just integers and maybe complex conjugates. So a certain amount of trial and error must occur.

Also in elementary school the multiplication and division tables $2\times 3=6$ were *memorized*. And we spent 5 or 6 years in school developing the appropriate notions of number and applying them. High school learning to apply these ideas in general, in college applying this knowledge to other subjects. It suggests that even in 4 years of university we can't learn very much.

Then after all this we complain that $\mathbb{Z}$ wasn't a very good concept of number at all, but we have to build up to that.

4/27 Back to work. We're going to build a zeta function for all integers in $\mathbb{Z}[\sqrt{2}]$. These rings no longer totally agree. If I say "$\mathbb{Q}(\sqrt{2})$ is the set of all quotients of $\mathbb{Z}[\sqrt{2}]$" then we have an equation like this:

$$\frac{m_1+n_1\sqrt{2}}{m_2+n_2\sqrt{2}} = a+b\sqrt{2} \text{ with } (m_1,m_2,n_1,n_2)\in\mathbb{Z}^4 \text{ and } a,b\in\mathbb{Q}$$

In that case we could solve for both a and b and we obtain a map:

$$(m_1,m_2,n_1,n_2)\in\mathbb{Z}^4 \mapsto (a,b) = \left(\frac{m_1m_2+2n_1n_2}{m_2^2-2n_2^2}, \frac{m_1n_2+m_2n_1}{m_2^2-2n_2^2}\right)\in\mathbb{Q}^2$$

These rational numbers could be slopes of line lines. We could arrange all these possible sloes in a circle:

$$\cos^2\theta+\sin^2\theta = (a+b\sqrt{2})^2+(c+d\sqrt{2})^2 = \big(a^2+c^2+2b^2+2d^2\big)+\sqrt{2}\big(2ab+2cd\big) = 1+0\sqrt{2}$$

I needed to consult the definition. The **Dedekind Zeta function** of a number field (such as $K=\mathbb{Q}(\sqrt{2})$) is the sum over integral ideals of K. And I don't quite know enough ring theory to decide what those are. There's a bit of Euclidean geometry there...

$$\zeta_K(s) = \sum_a \frac{1}{N(a)^s}$$

as $(a)=(a_1+a_2\sqrt{2})\subseteq K$ varies over the integral ideals, with $a_1,a_2\in\mathbb{Z}$. An alternative definition is as the product over all primes:

$$\zeta_K(s) = \prod_p \frac{1}{1-N(p)^s}$$

Detailed examinations of these zeta functions exist in the literature, but what matters is our own understanding. Do we know what prime numbers $\mathfrak{p}\in\mathbb{Z}$ look like in this ring? Books do, I don't:

- $(\sqrt{2}+1)(\sqrt{2}-1)=1$ and this means the same prime can apper infinitely many times.
- $(2\sqrt{2}+1)(2\sqrt{2}-1)=7\in\mathbb{Z}$ this means that prime numbers can split in two.

By quadratic reciprocity we know how primes split over this field. However, these two theorems: quadratic reciprocity and sum of two squares theorem, I don't know if I take them for granted:

$$p=x^2+2y^2 \text{ iff } \{x : x^2\equiv 2 \pmod p\}\neq\varnothing \text{ iff } p\equiv\pm1 \pmod 8$$

and this is a fairly well-studied but somewhat random sequence. Every time I learn a new number, it's quite informative:

```
  7,  17,  23,  31,  41,  47,  71,  73,  79,  89,  97,
103, 113, 127, 137, 151, 167, 191, 193, 199, 223, 233,
239, 241, 257, 263, 271, 281, 311
```

These are cute, but every time I get a fact like this, I need to check the logic, and also every time we have even a basic question over $\mathbb{Z}[\sqrt{2}]$ it factors through one like this. What if we try to compute the GCD of 31 and 41:

$$\frac{31}{41} = \frac{7+3\sqrt{2}}{9+5\sqrt{2}}\times\frac{7-3\sqrt{2}}{9-5\sqrt{2}}$$

To me, these multiplication facts are much more interesting than the actual answer. What if we run the Euclidean algorithm on the first two factors:

$$9+5\sqrt{2} = a(7+3\sqrt{2})+b$$

with some "small" a,b. Do we know the answer? We take as a given that the answer can be found, but we don't really know. Do we know an isomorphism:

$$\mathbb{Z}[\sqrt{2}]/(7+3\sqrt{2})\mathbb{Z}[\sqrt{2}]\simeq\mathbb{F}_{31}=\mathbb{Z}/31\mathbb{Z}$$

It's not instantly obvious to me. This is clearly a statement about lattices and requires Euclidean geometry, or Fermat's little theorem.