Scratchwork: Class Field Theory

One common mistake is to say the ring of integers of $K = \mathbb{Q}(\sqrt{-5})$ is $\mathbb{Z}[\sqrt{-5}]$. In fact it's $\mathbb{Z}[\frac{1+\sqrt{-5}}{2}]$. This example is important because it's the first time we observe the failure of unique factorization in "integers":

$$2 \times 3 = (1 + \sqrt{-5}) \times (1 - \sqrt{-5})$$

Despite being quite well-known, I feel this is the kind of result that needs to be checked very carefully. Number Theory in particular, is known to re-arrange obvious facts in shocking ways:

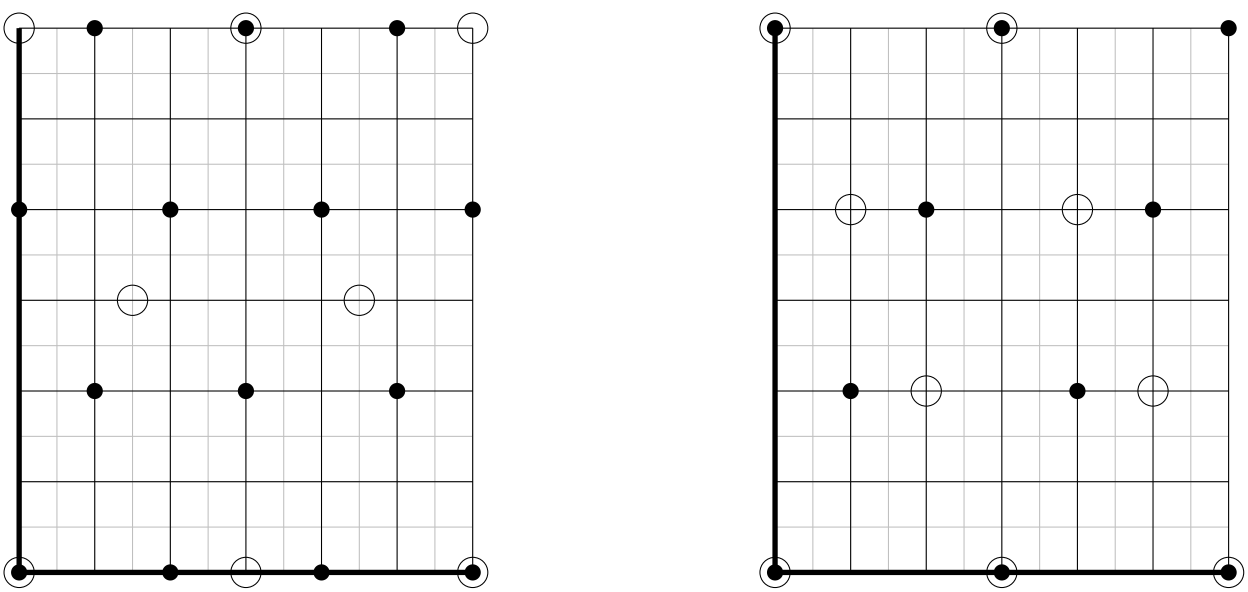
$$\left(\frac{1+\sqrt{-5}}{2} \right)^2 = \frac{1}{4} + \sqrt{-5} - \frac{5}{4} = 2 \times \left(\frac{1+\sqrt{-5}}{2} \right) - 2 \times 1$$

What's so special about the $\sqrt{-5}$ that we obtain a number field with class number $h(K) = 2$?

Ex Factor the numbers $1 \leq n \leq 100$ in each of the two orders, $\mathcal{O}_1 = \mathbb{Z}\left[\frac{1+\sqrt{-5}}{2}\right]$ and $\mathcal{O}_2 = \mathbb{Z}[\sqrt{-5}]$.

Ex Show that the ring of integers of $\mathbb{Q}(\sqrt{-5})$ is $\mathbb{Z}\left[\frac{1+\sqrt{-5}}{2}\right]$.

Let's try to draw the ideal (2).



Also (3) and on the right hand side $(1 + \sqrt{-5})$ and $(1 - \sqrt{-5})$.

That was much harder than it should have been. Btw, do you believe this? This is what happens when we use a calculator and get the correct answer. And it's perfectly good.

```
>>> 5**0.5/2
1.118033988749895
```

10/06 What is the ring of integers anyway?

Def Let $A \subseteq B$ be an extension of rings. An element $b \in B$ is called **integral** over A if it satisfies a monic equation:

$$x^n + a_1 x^{n-1} + \cdots + a_0 = 0$$

with coefficients in $a_i \in A$. The ring B is called **integral** over A if all its elements $b \in B$ are integral over A.

Seems like a lot of effort to find new classes of integers. $(\sqrt{-5})^2 + 5 = 0$ so that $\sqrt{-5}$ is integral over $\mathbb{Z}$. Any element of $\mathbb{Q}(\sqrt{-5})$ is the root of a quadratic over $\mathbb{Q}$, at least.

$$(a + b\sqrt{-5})^2 = a^2 + 5b^2 + 2\sqrt{-5}\,ab = 2a(a + b\sqrt{-5}) + (-a^2 + 5b^2)$$

Don't you think this algebra is tedious? So let's have this other definition of integrality:

Thm Finintely many elements $b_1, \dots, b_n \in B$ are all integral over A if and only if the ring $A[b_1, \dots, b_n]$ viewed as an A-module is finitely generated.

Here's another non-constructive argument that you only need a quadratic: $(a+b\sqrt{-5})^2 \in (a+b\sqrt{-5})\,\mathbb{Q} \oplus 1\,\mathbb{Q}$, so there must be a quadratic relation. Modern algebra is frustratingly succinct but at least we didn't have to solve anything.

We can represent elements of $\mathbb{Q}(\sqrt{-5})$ as 2×2 matrices using a straightforward device:

$$a + b\sqrt{-5} \mapsto \left[\begin{array}{cc} a & b \\ 5b & a \end{array} \right]$$

As a 2×2 matrix we could use the **Cayley-Hamilton theorem** we have that I and A and A^2 must have a relation over $\mathbb{Q}$. This machinery is a bit over-powerful if we only solve Pell-type equations with it. In fact, it makes no sense to use adjoint matrices until 3×3.

$$\left[\begin{array}{ccc} a & b & c \\ d & e & f \\ g & h & i \end{array} \right] \mapsto \left[\begin{array}{ccc} \left| \begin{array}{cc} e & f \\ h & i \end{array} \right| & \left| \begin{array}{cc} d & f \\ g & i \end{array} \right| & \left| \begin{array}{cc} d & e \\ g & h \end{array} \right| \\ & & \\ \left| \begin{array}{cc} a & b \\ h & i \end{array} \right| & \left| \begin{array}{cc} a & c \\ g & i \end{array} \right| & \left| \begin{array}{cc} b & c \\ g & h \end{array} \right| \\ & & \\ \left| \begin{array}{cc} a & b \\ e & f \end{array} \right| & \left| \begin{array}{cc} a & c \\ d & f \end{array} \right| & \left| \begin{array}{cc} b & c \\ d & e \end{array} \right| \end{array} \right]$$

Wikipedia returns this formula for the 2×2 and 3×3 adjoint matrix.[1] and Linear Algebra formula exist in abundance. We never use them.

$$A^* = I(\text{tr}A) - A \quad (2 \times 2) \quad \text{or} \quad A^* = \frac{1}{2}\big((\text{tr}A)^2 - \text{tr}(A^2)\big) - A(\text{tr}A) + A^2 \quad (3 \times 3)$$

It seems awfully odd we don't check the cubic case. We might use a computer, in my opinion this merely occludes all the middle steps. If these calculations were so easy, how come we don't follow-up?

$$x^2 + ax + b = 0 \to x = -\frac{-a + \sqrt{a^2 - 4b}}{2}$$

When does $a^2 - 4b = -5$? Then $a^2 \equiv -1 \pmod 4$. Thankfully I'm wrong $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$, however $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

[1] https://en.wikipedia.org/wiki/Adjugate_matrix

Anyways, Euclids algorithm fails miserably and we have nothing to replace it with.[2] Terrifyingly, Neukirch's approach is to merge Dirichet's Unit Theorem and the finiteness of class number into a single theorem:

Thm The group $\mathsf{CH}(\overline{\mathcal{O}})^0$ is compact.

Proof This follows immediately from the exact sequence:

$$0 \mapsto H/\Gamma \to \mathsf{CH}(\overline{\mathcal{O}})^0 \to \mathsf{CH}(\mathcal{O}) \to 0$$

I might choose $K = \mathbb{Q}(x)/(x^3 - x - 1)$ or $K = \mathbb{Q}(\sqrt{8})$ or something like that, Neukirch is already nudging us towards Arakelov geometry. □

Ex (Hard) Let $K = \mathbb{Q}(\sqrt{5})$ show that $\zeta_K(-1) = \frac{1}{30}$ and $\zeta_K(2) = \frac{2\sqrt{5}}{375}\pi^4$.

References

[1] Henri Cohen **Computational Number Theory in Relation with L-Functions** `arXiv:1809.10904`

[2] And unlike many number theorists, I do not feel the presence of a computer obviates the need to do things for myself with my own two hands.