

# 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:

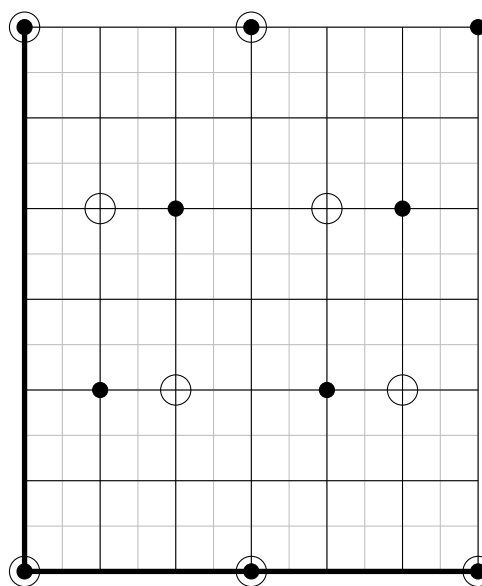
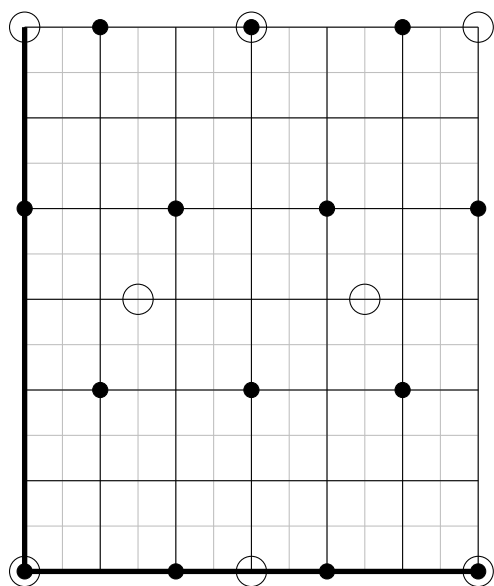
$$\left(\frac{1 + \sqrt{-5}}{2}\right)^2 = \frac{1}{4} + \sqrt{-5} - \frac{5}{4} = 2 \times \left(\frac{1 + \sqrt{-5}}{2}\right) - 2 \times 1$$

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,  $\mathcal{O}_1 = \mathbb{Z}[\frac{1+\sqrt{-5}}{2}]$  and  $\mathcal{O}_2 = \mathbb{Z}[\sqrt{-5}]$ .

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

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** Finitely 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  $2 \times 2$  matrices using a straightforward device:

$$a + b\sqrt{-5} \mapsto \begin{bmatrix} a & b \\ 5b & a \end{bmatrix}$$

As a  $2 \times 2$  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  $3 \times 3$ .

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \mapsto \begin{bmatrix} \begin{vmatrix} e & f \\ h & i \end{vmatrix} & \begin{vmatrix} d & f \\ g & i \end{vmatrix} & \begin{vmatrix} d & e \\ g & h \end{vmatrix} \\ \begin{vmatrix} a & b \\ h & i \end{vmatrix} & \begin{vmatrix} a & c \\ g & i \end{vmatrix} & \begin{vmatrix} b & c \\ g & h \end{vmatrix} \\ \begin{vmatrix} a & b \\ e & f \end{vmatrix} & \begin{vmatrix} a & c \\ d & f \end{vmatrix} & \begin{vmatrix} b & c \\ d & e \end{vmatrix} \end{bmatrix}$$

Wikipedia returns this formula for the  $2 \times 2$  and  $3 \times 3$  adjoint matrix.<sup>1</sup> and Linear Algebra formula exist in abundance. We never use them.

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

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?

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

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  $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ .

<sup>1</sup>[https://en.wikipedia.org/wiki/Adjugate\\_matrix](https://en.wikipedia.org/wiki/Adjugate_matrix)

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

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

**Proof** This follows immediately from the exact sequence:

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

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.  $\square$

**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

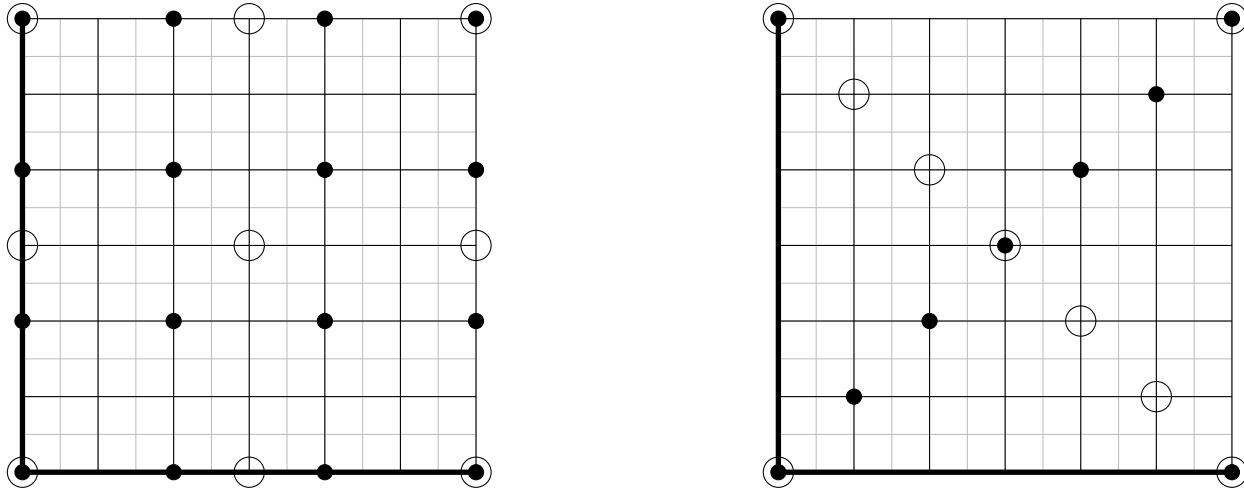
---

<sup>2</sup>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.

10/18 Let's try to fix the error from last week.

- $(2) = 2\mathbb{Z} \oplus 2\sqrt{-5}\mathbb{Z}$
- $(3) = 3\mathbb{Z} \oplus 3\sqrt{-5}\mathbb{Z}$
- $(1 + \sqrt{-5}) = (1 + \sqrt{-5})\mathbb{Z} \oplus (5 - \sqrt{-5})\mathbb{Z}$
- $(1 - \sqrt{-5}) = (1 - \sqrt{-5})\mathbb{Z} \oplus (5 + \sqrt{-5})\mathbb{Z}$

We may as well write these ideals as  $(2, 0) \oplus (0, 2)$ ,  $(3, 0) \oplus (0, 3)$ ,  $(1, 1) \oplus (5, -1)$  and  $(1, -1) \oplus (5, 1)$ .



A quick look at this diagram shows that the LCM of 2 and 3 is 6. But this is also the LCM of  $1 + \sqrt{-5}$  and  $1 - \sqrt{-5}$  is 6. This tells us our bookkeeping methods need to get supplemented quite a bit.

How and why do continued fractions occur? Did we get all the mileage we can out of such a construction? If we complain these objects are useless, maybe it's possible to design a better one.

Let's try an example over  $\mathbb{Z}$ . Hoping, maybe it can be extended to  $\mathbb{Z}[\sqrt{-5}]$ . We can show that since  $\pi < 5$  there is no GCD in this domain. Euclidean geometry doesn't just finish... what's left of that?

**Thm** Let  $\theta$  and  $Q > 1$  be real.<sup>3</sup> There is an integer such that  $0 < q < Q$  and  $||q\theta|| < Q^{-1}$ .

*Proof #1 ...*

*Proof #2 ...*

<sup>3</sup>What's coming is yet another very thorough check of the construction of  $\mathbb{R}$ . It's supposed to look and feel like a ruler, more or less. Was the thing you measured even flat?? Did you have all the numbers in between 2 and 3?

## 11/14 Let's try to parse these definitions from Chapter III

**Def** A *prime*  $\mathfrak{p}$  of an algebraic number field  $K$  is a class of equivalent valuation of  $K$ .

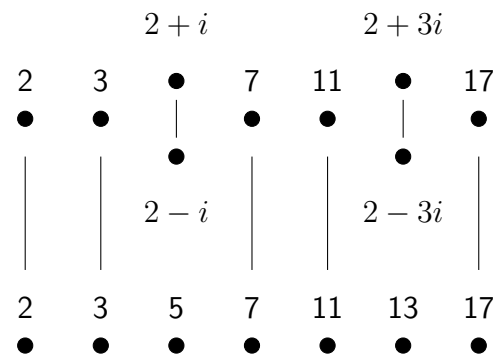
- the non-archimedian equivalence classes are called *finite primes*.
- the archmedian equivalence classes are called *infinite primes*.

This is the start of a bunch of jargon that we have to learn, but we grin and bear it.

$\mathbb{Q}(\sqrt{2})$  has **two** infinite places  $|a + b\sqrt{2}|_1 = |a + b\sqrt{2}|$  and  $|a + b\sqrt{2}|_2 = |a - b\sqrt{2}|$ .

$\mathbb{Q}$  has only **one** infinite place,  $|a| = |-a| = a$  when  $a > 0$ .<sup>4</sup>

The primes in the number field  $\mathbb{Q}(i)$  can be arranged in a sort of number line.



There are two primes over 5 in  $\mathbb{Q}$  we have  $\mathfrak{p}_1 = 2 + i$  and  $\mathfrak{p}_2 = 2 - i$  with  $\mathfrak{p}_1|5$  and  $\mathfrak{p}_2|5$ .

Now the book says we can assign a (canonical) homomorphism  $v_{\mathfrak{p}} : K^{\times} \rightarrow \mathbb{R}$  and all the absolute values solve something like unique factorization:

**Prop** For any  $a \in K^{\times}$  we have  $|a|_{\mathfrak{p}} = 1$  for almost all  $\mathfrak{p}$ . Also,  $\prod_{\mathfrak{p}} |a|_{\mathfrak{p}} = 1$

Any surprises there, that no number is the product of infinitely many primes? We could construct those thing as well, with enough imagination. The object might even be realistic in some ways.

How do fractions work over number fields, such as  $\mathbb{Q}(i)$  or  $\mathbb{Q}(\sqrt{-5})$  or  $\mathbb{Q}(\sqrt{2})$ ? Is it safe to assume they work exactly the same way?

- $J(\mathcal{O})$  is the group of fractional ideals of  $K$
- $P(\mathcal{O})$  is the group of principal fractional ideals of  $K$
- $Pic(\mathcal{O}) = J(\mathcal{O})/P(\mathcal{O})$  is the **ideal class group** of  $K$

I really need to get an undergraduate algebra textbook because I'm rusty on all of this. A definition like this means that perhaps we could have a fractional ideal in a number field, that's not principal. Indeed  $|Cl_{\mathbb{Q}(\sqrt{-5})}| = 2$ . That result doesn't mean much at the moment, until we do more it's just a bunch of talk.

<sup>4</sup>This is a great time to start wondering if  $\mathbb{Q}$  is even the most natural construct. We count things, don't we? And we talk about fairness and proportion? Yet, do fractions really describe the way we allocate goods, or (mentally) divide things into parts? Are **positive** and **negative** really the only two signs a value can have...?

E.g.  $[a - b] = (a, b)/(1, -1)$  as vectors in  $\mathbb{R}^2$ .

More definition. A **replete ideal** of  $K$  is an element of the group

$$J(\overline{\mathcal{O}}) := J(\mathcal{O}) \times \prod_{\mathfrak{p}|\infty} \mathbb{R}_+^\times$$

These “replete ideals” factor into a product of finite and infinite places:

$$\mathfrak{a} = \mathfrak{a}_f \cdot \mathfrak{a}_\infty = \prod_{\mathfrak{p}|\infty} \mathfrak{p}^{\nu_{\mathfrak{p}}} \times \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{\nu_{\mathfrak{p}}}$$

A **replete divisor** (or **Arakelov divisor**) is a formal sum (here  $\nu_p \in \mathbb{Z}$ ) and  $\nu_p \in \mathbb{R}$  for  $p|\infty$  and  $\nu_p = 0$  for almost all  $\mathfrak{p}$ .

$$D = \sum_{\mathfrak{p}} \nu_{\mathfrak{p}} \mathfrak{p}$$

For example, instead of writing the factorization  $105 = 3 \times 5 \times 7$  we could write a divisor:

$$105 = 1 \times (3) + 1 \times (5) + 1 \times (7)$$

here the prime ideals  $(3), (5), (7) \subseteq \mathbb{Q}^\times$ . I’m getting ahead of myself. There is a canonical homomorphism:

$$\text{div} : K^\times \rightarrow \text{Div}(\overline{\mathcal{O}})$$

and we have computed that  $\text{div}(105) = (3) + (5) + (7)$ . Next define the **replete divisor class group** (or **Chow group**):

$$CH^1(\overline{\mathcal{O}}) = \text{Div}(\overline{\mathcal{O}})/P(\overline{\mathcal{O}})$$

next we have the degree map

$$\begin{aligned} \text{deg} &: \text{Div}(\overline{\mathcal{O}}) \rightarrow \mathbb{R} \\ &: D \mapsto \sum_{\mathfrak{p}} \nu_{\mathfrak{p}} \log N(\mathfrak{p}) \end{aligned}$$

abstractly, Neukirch says this is a continuous homomorphism<sup>5</sup> which is going to merge the unit group and the ideal class group:

$$\text{deg} : CH^1(\overline{\mathcal{O}}) \rightarrow \mathbb{R}$$

One of the benefits of this abstraction is that the arithmetic of number fields is going to get very very organized. We can use *exact sequences*:

**Thm** The group  $CH^1(\overline{\mathcal{O}})^0$  is compact.

$$0 \rightarrow H/\Gamma \rightarrow CH^1(\overline{\mathcal{O}})^0 \rightarrow CH^1(\mathcal{O}) \rightarrow 0$$

We need numbers !!!

**Ex** A real quadratic number field  $\mathbb{Q}(\sqrt{d})$  is Euclidean (and therefore class number is 1) if  $d \in \{5, 8, 12, 13, 17, 21, 24, 28, 29\}$ . I doubt anyone has tried it, although we take for granted we could run such a computation on a computer.<sup>6</sup>

**Ex**

- $K = \mathbb{Q}(\sqrt{6})$  has class number  $h = 1$ .
- $K = \mathbb{Q}(\sqrt{-5})$  has class number  $h = 2$ .
- $K = \mathbb{Q}(\sqrt{-23})$  has class number  $h = 3$ .
- $K = \mathbb{Q}(\sqrt{-47})$  has class number  $h = 5$ .

---

<sup>5</sup>over which topology?

<sup>6</sup>We are saying that some square-root computations involving  $\sqrt{d}$  always behave a certain way. How do GCD computations work here? For two ideals we’d have  $\text{gcd}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$ , and  $\text{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$ .

## References

- [1] Helmut Koch **Algebraic Number Theory**
- [2] Jürgen Neukirch **Algebraic Number Theory** (Grundlehren der mathematischen Wissenschaften #322) Springer, 1999.
- [3] Mak Trifković **Algebraic Theory of Quadratic Numbers** (Universitext) Springer, 2013.
- [4] Jarvis Frazer **Algebraic Number Theory** (Universitext) Springer, 2014.
- [5] Daniel Marcus **Number Fields** (Universitext) Springer, 2018.

## References

- [1] Henri Cohen, Karim Belabas **Modular Forms in Pari/GP** arXiv:1810.00547
- [2] Henri Cohen  
**Expansions at Cusps and Petersson Products in Pari/GP** arXiv:1809.10908  
**An Introduction to Modular Forms** arXiv:1809.10907  
**Computational Number Theory in Relation with L-Functions** arXiv:1809.10904