# AWS_2_Number_Fields

March 5, 2026

# 1 Number fields

## 1.1 Question 1: Number field basics

In this question, we will become acquainted with some of the basic functions relating to number fields, and use them to compute the class number.

The most straightforward way to define a number field is by a defining polynomial. Below we define a polynomial ring and name its generator `x`, and then define a number field and name its generator `a`.

[2]:

```
P<x> := PolynomialRing(Rationals());
coeffs := [ 361, 266, 98, -46, -2, -2, 2, -2, 1 ];
f := P!coeffs; f;
K<a> := NumberField(f); // NumberField(coeffs) also works!
K;
```

```
x^8 - 2*x^7 + 2*x^6 - 2*x^5 - 2*x^4 - 46*x^3 + 98*x^2 + 266*x + 361
Number Field with defining polynomial x^8 - 2*x^7 + 2*x^6 - 2*x^5 - 2*x^4 -
46*x^3 + 98*x^2 + 266*x + 361 over the Rational Field
```

Magma has all of the number field invariants you are used to using, and the function is usually called what you think it is. The section of the handbook on number fields describes many of these functions in detail, and is a good place to look if you are confused.

We can compute the ring of integers of `K` using `MaximalOrder` or `Integers`; we can compute the discriminant with `Discriminant`. Why do `Discriminant(K)` and `Discriminant(ZK)` give different answers?

[0]:

```
ZK := MaximalOrder(K);
Discriminant(K);
Discriminant(ZK);
```

Magma can also compute the unit group in the ring of integers. It should have rank $r_1 + r_2 - 1$, where $r_1$ is the number of real embeddings of $K$, and $r_2$ the number of conjugate pairs of complex embeddings. Check this is true for the field `K`.

[0]:

```

```

Now we will test the class number formula. Let $\zeta_K$ be the Dedekind zeta function associated to $K$. Then the class number formula states that

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}\cdot(2\pi)^{r_2}\cdot \mathrm{Reg}(K)\cdot h_K}{\omega_K\cdot\sqrt{|\Delta_{\mathcal{O}_K}|}}.$$

The quantity $\mathrm{Reg}(K)$ is called the **regulator**. The other quantities are $h_K$ the class number, and $\omega_K$ the number of roots of unity contained in $K$. Magma allows us to compute values of the zeta function to high precision:

[0]:

```
L := LSeries(K);
Evaluate(L,2);
```

Choose a value of $s$ close to 1. Using `Evaluate(L,s)` and other Magma functions, find an approximation to the class number $h_K$.

[0]:

```
R := RealField(30);
pi := Pi(R);
```

While the class number formula does seem magical, it does not actually save much time versus computing class groups in the usual manner, since the regulator is about as hard to compute as the class group!

Using the command `IdealsUpTo` to gather many ideals of the number field, and `IsPrincipal` to test their powers, make a guess about the isomorphism class of the class group of $K$.

(Yes, this process is slower and more cumbersome than Magma's function `ClassGroup`, but that has been optimised significantly, so we shouldn't expect to match its speed! And in any case, it is good practice to know how to compute something many ways, both for mathematical development, and as a check that algorithms are working correctly!)

[0]:

```

```

**Extension:** The L-series $L$ associated to $K$ can be factorised as

$$\zeta_K(s) = \prod_{\rho} L(\rho,s)^{\dim(\rho)},$$

where $\rho$ runs over the irreducible complex representations of $\mathrm{Gal}(K/\mathbb{Q})$. Using Magma's `ArtinRepresentations` functionality and the LMFDB database, identify these factors, and express the value $\zeta_K(2)$ in terms of as many known constants as you can. Check your expression against the numerical value returned by Magma.

[0]:

```

```

### 1.2 Question 2: Constructing interesting representations with class field theory

Class field theory describes abelian extensions of number fields, i.e. those fields whose Galois groups are abelian. By iterating constructions from class field theory, we can compute number fields whose Galois groups are **solvable**. Included in this class are some number fields associated to elliptic curves. We will construct the 2-torsion representation associated to the elliptic curve

$$E\colon y^2 + y = x^3 + x^2 - 769x - 8470$$

which has conductor 19. The image of this representation is this group $\mathrm{GL}_2(\mathbb{F}_2)$, a non-abelian group of order 6. Its composition series is

$$C_1 \lhd C_3 \lhd \mathrm{GL}_2(\mathbb{F}_2)$$

and so we should be able to compute an extension $L/\mathbb{Q}$ with $\mathrm{GL}_2(\mathbb{F}_2)$ as its Galois group by first computing an field extension of $\mathbb{Q}$ with Galois group $C_2 \simeq \mathrm{GL}_2(\mathbb{F}_2)/C_3$, and then an extension of *that* field with Galois group $C_3 \simeq C_3/C_1$. We will proceed in an ad hoc manner, but all of the choices we make can be precisely justified with class field theory.

Standard results about representations coming from elliptic curves tells us that $L/\mathbb{Q}$ is ramified, at most, only at $p = 2$ and $p = 19$; let us first construct a field with Galois group $C_2$ (a quadratic field), ramified at some subset of our primes. There are five choices of quadratic field with these ramification properties. Use Magma's `QuadraticField` function to pick $\mathbb{Q}(\sqrt{-19})$.

[0]:
```
E := EllipticCurve([0, 1, 1, -769, -8470]);
N := 1; //change me!
K:=QuadraticField(N);
ZK := MaximalOrder(K);
```

Now we will look for an extension of $K$ with Galois group $C_3$ using class field theory. This extension will be ramified, at most, at $p = 2$ and $p = 19$. Magma's class field theory is accessed through `RayClassGroup` and `RayClassField`. Since $K$ is already ramified at 19, let's try only adding 2 and seeing what we get.

[0]:
```
F := RayClassField(2*ZK);
```

It seems that the ray class field of the modulus $\mathfrak{m} = (2)$ has Galois group $C_3$, as we wanted. We can use the command `NumberField` to turn Magma's `FldAb` type into a `FldNum`, which lets us do explicit calculations with it in the normal way. However, this will only return a *relative field*, the degree 3 extension of $K$, so we also need to use `AbsoluteField` to get the full degree 6 extension.

[0]:
```
L := AbsoluteField(NumberField(F));
```

We have found a 2-dimensional representation of $\mathrm{Gal}(L/\mathbb{Q})$ over $\mathbb{F}_2$, but how can we be sure it is the correct one? (If you know about division polynomials of elliptic curves, put that to one side for now!) Another important theorem in the study of Galois representations associated to elliptic curves is the following: if $\rho$ is our representation and $\mathrm{Frob}_p$ is a Frobenius element at $p$ in $\mathrm{Gal}(L/\mathbb{Q})$, then

$$\mathrm{trace}(\rho(\mathrm{Frob_p})) \equiv (1 + p - \#E(\mathbb{F}_p)) \pmod 2$$

(Implicit in the above is that $p$ does not ramify in $\mathrm{Gal}(L/\mathbb{Q})$!)

Verify this equality for sufficiently many primes that you feel happy that we have the correct representation. **Warning**: Magma's `FrobeniusElement` function returns elements of `GaloisGroup(L)`, which is isomorphic (but not necessarily always *equal*) to the result of `AutomorphismGroup(L)`. You will need to either find some way of acting on the field `L` with the Galois group, or write your own Frobenius function that uses the automorphism group.

Some useful parts of the handbook:

- Changing the ring of definition of an elliptic curve
- Automorphism groups of number fields

[0]:

```
A, _, phi := AutomorphismGroup(L);
// phi is a map that takes an element of the abstract automorphism group A
// and returns the actual map on elements of L corresponding to that group element

M := IrreducibleModules(A,GF(2))[2];
rho := Representation(M);
```

Now that we have a grip on the method, repeat these steps to find the 2-torsion representations of the elliptic curves

$$E_1 \colon y^2 + y = x^3 - x$$

$$E_2 \colon y^2 + xy = x^3 - 2x - 1$$

Note, some of the decisions we made during the first example were unjustified, but happened to work. For these examples, you will need to explore several possibilities at each stage.

**Extension:** For some curves, the quadratic extension $K$ we take as the first step in building its 2-torsion representation is real quadratic, for others it is imaginary quadratic. Can you explain this in terms of information about the curve itself? That is, come up with a condition in terms of a curve $E$ that tells you the sign of the discriminant of the quadratic subfield of its 2-torsion representation without having to explicitly compute it. It might help to use the LMFDB, where many properties of many elliptic curves are readily available.

[0]:

```

```

**Extension:** The elliptic curve

$$E \colon y^2 + y = x^3 - x^2$$

has rather a rather small mod 5 representation. Generically, one expects full image, which would be $\mathrm{GL}_2(\mathbb{F}_5)$, a group of order 480. This would mean working in a degree 480 number field, which is far beyond what is feasible to compute with in Magma in any reasonable period of time. The image of *this* curve, however, is the Frobenius subgroup $F_5$ (which you can read all about here). This group is solvable, and so we should be able to construct the field using class field theory. Attempt to do this.

(Editor's note: while this should be possible *in principle*, it might be quite hard to do in practice!)

[0]:

### 1.3 Question 3: Class numbers via subfields

When $F$ is a Galois number field, we might expect to be able to understand it by understanding its subfields. For example, if $F = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ is a biquadratic field with non-trivial subfields $F_1 = \mathbb{Q}(\sqrt{a})$, $F_2 = \mathbb{Q}(\sqrt{b})$, and $F_3 = \mathbb{Q}(\sqrt{ab})$, then we have the classical relation between their class numbers:

$$h(F) = 2^i \cdot h(F_1)h(F_2)h(F_3),$$

where $i \in \mathbb{Z}$.

Now let $F$ be a degree 6 number field with Galois group $S_3$. Using existing databases (e.g. the LMFDB), produce a conjecture for a similar relation between the class number of $F$ and its non-trivial subfields.

[0]:

**Extension:** Relations such as these can be understood in terms of *norm relations*, which are relations in the group algebra $\mathbb{Q}[\mathrm{Gal}(F/\mathbb{Q})]$. Consider this recent paper. Can you find a result that might imply your conjecture? Can you find a norm relation in $\mathbb{Q}[S_3]$ that explains your conjecture?

[0]: