

These are compact notes. For more details, you may consult the relevant parts of my lecture notes on *Number rings* on the school [website](#).

In algebraic number theory, we ‘solve’ polynomial equations over domains like $\mathbf{Z}$ or $\mathbf{Q}$.

We start with a concrete example in the spirit of the school: a cubic polynomial equation

$$y^2 = x^3 - 1 \quad (*).$$

This represents a *curve* over the real numbers, and a *Riemann surface* over the complex numbers.

Geometry: use the *homogeneous* cubic equation and look at the projective curve

$$E : Y^2Z = X^3 - Z^3$$

describing the curve in *projective* 2-space. This yields an extra point $O_E = [0 : 1 : 0]$ *at infinity*, and leads to well known pictures over the real (“elliptic curve”) and complex (“torus”) numbers.

Arithmetic question: what are the *rational* solutions (x, y) to $(*)$, having $x, y \in \mathbf{Q}$? Is the obvious point $P = (1, 0)$ the only integral solution to our equation? In this CIMPA School you will learn:

Theorem. *Over every field $K \subset \mathbf{C}$, the set $E(K)$ of projective K -rational solutions has a natural abelian group structure in which any three collinear points in $E(K)$ add up to O_E .*

This group structure is algebraic, and actually arises over any field K and any elliptic curve E/K .

One may explicitly give an elliptic curve E/K by a Weierstrass equation $y^2 = x^3 + ax + b$ with $a, b \in K$, provided the discriminant $-4a^3 - 27b^2 \in K$ of the cubic polynomial is non-zero. (For K of characteristic 2 or 3 a slightly more general equation is needed.)

Theorem. *The elliptic curve E defined by $y^2 = x^3 - 1$ has $E(\mathbf{Q}) = \{O_E, P\} \cong \mathbf{Z}/2\mathbf{Z}$.*

You will be able to prove this after the school. It is a special case of the following theorem.

Mordell’s theorem. *For every elliptic curve $E/\mathbf{Q}$, the group $E(\mathbf{Q})$ is finitely generated.*

The same is true over a general *number field* K , i.e., a finite extension of $\mathbf{Q}$. Most proofs over $\mathbf{Q}$ naturally end up proving this more general **Mordell-Weil theorem**.

Your birthday provides you with a personal elliptic curve — put $a = \text{month}$, $b = \text{day}$ and consider

$$E_{a,b} : y^2 = x^3 + ax + b.$$

Challenge question 1: determine your point group $E_{a,b}(\mathbf{Q})$ by the end of the school! (This is part of the elliptic curves course, not of the algebraic number theory course.)

We start with a more modest result illustrating the use of number rings.

Theorem 1. *The only solution in integers to the equation $y^2 = x^3 - 1$ is $(x, y) = (1, 0)$.*

We work in the ring $\mathbf{Z}[i]$ of Gaussian integers, which is a *principal ideal domain* (PID) with unit group $\mathbf{Z}[i]^* = \langle i \rangle$ of order 4 (see exercise 1). Suppose $x, y \in \mathbf{Z}$ satisfy

$$x^3 = y^2 + 1 = (y + i)(y - i).$$

Now $y + i$ and $y - i$ have difference $2i$, and they must be coprime as x cannot be even: look mod 4. As PID's have unique prime factorisation, we deduce that $y + i$ and $y - i$ are both cubes in $\mathbf{Z}[i]$. Solving $y + i = (a + bi)^3 = (a^3 - 3ab^2) + (3a^2b - b^3)i$ we find $b = \pm 1$ and $3a^2 - 1 = \pm 1$, hence $a = 0 = y$ and $(x, y) = (1, 0) = P$. $\square$

This proof uses the non-obvious fact that the ring $\mathbf{Z}[i]$ of Gaussian integers is a PID, just like $\mathbf{Z}$. Unfortunately, not all subrings of number fields are so well-behaved — they may have non-principal ideals, and also infinite unit groups. Algebraic number theory tells us how to work such *number rings*, and to effectively control these two fundamental problems.

We may define a number field K (in many ways) by a *monic* irreducible polynomial $f \in \mathbf{Z}[X]$, as

$$K = \mathbf{Q}[X]/(f) = \mathbf{Q}(\alpha) \quad \text{with } \alpha = X \bmod (f).$$

It is the field of fractions of the *ring of integers* $\mathcal{O}_K = \{x \in K : f_{\mathbf{Q}}^x \in \mathbf{Z}[X]\}$ of K .

Your birthday provides you with a personal cubic field — put $a = \text{month}$, $b = \text{day}$ and consider $K_{a,b} = \mathbf{Q}[X]/(X^3 + aX + b)$.

In case f happens to be reducible or too nasty, feel free to swap the sign of a , or swap a and b !

Challenge question 2: find $\mathcal{O}_{K_{a,b}}$ and its basic invariants defined below by the end of the course!

The ring of integers $\mathcal{O}_K$ is the *maximal order* of K . The *equation order* $\mathbf{Z}[\alpha] = \mathbf{Z}[X]/(f)$ used to define K is of *finite* index in $\mathcal{O}_K$, and we have the **fundamental equality**

$$\Delta(f) = [\mathcal{O}_K : \mathbf{Z}[\alpha]]^2 \cdot \Delta_K \in \mathbf{Z}.$$

Here $\Delta(f) = \prod_{i < j} (\alpha_i - \alpha_j)^2 \in \mathbf{Z}$ is the discriminant of the polynomial $f = \prod_{i=1}^n (X - \alpha_i)$, defined in terms of its *complex* roots, and $\Delta_K \in \mathbf{Z}$ is the discriminant of K (or actually $\mathcal{O}_K$).

Examples. For $f = X^2 + 1$, the Gaussian number field $K = \mathbf{Q}(i)$ has $\mathcal{O}_K = \mathbf{Z}[i]$ and $\Delta_K = -4$. For $f = X^2 + 5$, the number field $K = \mathbf{Q}(\sqrt{-5})$ has $\mathcal{O}_K = \mathbf{Z}[\sqrt{-5}]$ and $\Delta_K = -20$. For $f = X^2 - 5$, the number field $K = \mathbf{Q}(\sqrt{5})$ has $\mathcal{O}_K = \mathbf{Z}[(1 + \sqrt{5})/2]$ and $\Delta_K = 5$.

The ring $\mathcal{O}_K$ is a *Dedekind domain* in which every ideal $I \neq 0$ is a *unique* product of prime ideals. This may fail for the equation order $\mathbf{Z}[\alpha]$, which has *singular primes* dividing $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$. Elements $x \neq 0$ in $\mathcal{O}_K$ are products of irreducible elements, but these can be very non-unique, even if one takes the presence of *units* in $\mathcal{O}_K$ into account. There are two basic **finiteness theorems**.

Theorem 2. The equivalence classes of non-zero $\mathcal{O}_K$ -ideals under the equivalence relation

$$I \sim J \iff xI = yJ \quad \text{for elements } x, y \in K^*$$

naturally form a **finite abelian group** under multiplication, the **class group** $Cl(\mathcal{O}_K) = Cl_K$ of K .

The class group of the ring of integers $\mathcal{O}_K$ is trivial if and only if $\mathcal{O}_K$ is a PID. In case the class group is non-trivial, we are forced to work with ideals, and the unit group becomes highly relevant.

Theorem 3. The unit group $\mathcal{O}_K^*$ has a finite cyclic torsion subgroup μ_K , and for f having r real and s complex conjugated pairs of roots, $\mathcal{O}_K^*/\mu_K$ is a free abelian group of **finite rank** $r + s - 1$.

This course does not focus on the (non-constructive) proofs of these results, but on *algorithms* to actually compute the ring $\mathcal{O}_K$, its unit group $\mathcal{O}_K^*$ and the class group Cl_K , and to work with them.

Examples. The ring $\mathbf{Z}[i]$ has trivial class group and cyclic unit group $\mathbf{Z}[i]^* = \langle i \rangle$ of order 4.
The ring $\mathbf{Z}[\sqrt{-5}]$ has a class group of order 2 and unit group $\mathbf{Z}[\sqrt{-5}]^* = \langle -1 \rangle$ of order 2.
The ring $\mathbf{Z}[\alpha]$ with $\alpha = (1 + \sqrt{5})/2$ has trivial class group and unit group $\mathbf{Z}[\alpha]^* = \langle -1 \rangle \times \langle \alpha \rangle$.

Example. As $X^2 + 5$ has two distinct roots ± 1 modulo 3, the maps $\mathcal{O} = \mathbf{Z}[\sqrt{-5}] \Rightarrow \mathbf{F}_3$ defined by

$$a + b\alpha \mapsto a \pm b \pmod{3},$$

have as their kernel the prime ideals $\mathfrak{p}_3 = (3, \alpha - 1)$ and $\mathfrak{q}_3 = (3, \alpha + 1)$ of $\mathcal{O}$ over 3. Similarly,

$\mathfrak{p}_7 = (7, \alpha - 3)$ and $\mathfrak{q}_7 = (7, \alpha + 3)$ are the primes $\mathcal{O}$ over 7. All of these primes are non-principal.

The $\mathcal{O}$ -ideal $I = (21)$ factors uniquely as a product $\mathfrak{p}_3\mathfrak{q}_3\mathfrak{p}_7\mathfrak{q}_7$ of primes in $\mathcal{O}$, but the element

$$21 = 3 \cdot 7 = (4 + \sqrt{-5})(4 - \sqrt{-5}) = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

'factors' in three truly **different** ways into irreducible elements in $\mathbf{Z}[\sqrt{-5}]$. These come from rearrangements of the product of $(3) = \mathfrak{p}_3\mathfrak{q}_3$ and $(7) = \mathfrak{p}_7\mathfrak{q}_7$ as

$$(4 + \sqrt{-5}) = \mathfrak{q}_3\mathfrak{p}_7 \text{ and } (4 - \sqrt{-5}) = \mathfrak{p}_3\mathfrak{q}_7,$$

and

$$(1 + 2\sqrt{-5}) = (1 + 2\alpha) = \mathfrak{q}_3\mathfrak{q}_7 \text{ and } (1 - 2\sqrt{-5}) = (1 - 2\alpha) = \mathfrak{p}_3\mathfrak{p}_7$$

As the order of the class group $Cl(\mathcal{O})$ is 2, *any* product of 2 non-principal $\mathcal{O}$ -ideals is principal!

Challenge question 2 amounts to the following problem for your personal cubic field $K_{a,b}$.

KEY PROBLEM: given a number field $K = \mathbf{Q}[X]/(f) = \mathbf{Q}(\alpha)$, find the ring $\mathcal{O}_K$ in which to do arithmetic in K , the unit group $\mathcal{O}_K^*$ and the class group Cl_K .

Suppose that K is given by an irreducible polynomial $f = f_{\mathbf{Q}}^{\alpha} \in \mathbf{Z}[X]$ having r real roots and s complex conjugate pairs of roots, and degree $n = r + 2s$.

The polynomial discriminant $\Delta(f)$ can be computed using resultants. A special case is

$$\Delta(X^3 + aX + b) = -4a^3 - 27b^2.$$

The proofs of Theorems 2 and 3 using the geometry of numbers are not directly constructive, but they give essential information.

Theorem 3. Every ideal class in Cl_K contains an ideal of norm at most the Minkowski bound

$$M_K = (4/\pi)^s \frac{n!}{n^n} \sqrt{|\Delta_K|}.$$

The *norm* of a non-zero $\mathcal{O}_K$ -ideal I is defined as the index $[\mathcal{O}_K : I] = \#(\mathcal{O}_K/I)$.

It follows that the class group Cl_K is generated by prime ideals in $\mathcal{O} = \mathcal{O}_K$ of norm at most M_K .

We compute Cl_K by factoring all *rational* primes up to its Minkowski bound in $\mathcal{O}$, selecting the primes in $\mathcal{O}$ below that bound that we find, and generate all *relations* between them in Cl_K .

EXERCISES

1. Show that $\mathbf{Z}[i]$ admits *division with remainder* (definition?), and deduce that $\mathbf{Z}[i]$ is a PID.
2. Show that for x an element of a number field K , we have $kx \in \mathcal{O}_K$ for some integer $k \geq 1$.
3. Define what it means for elements of a number ring to be *irreducible* and *prime*, and show that $4 + \sqrt{-5}$ and $1 + 2\sqrt{-5}$ are irreducible elements in $\mathcal{O} = \mathbf{Z}[\sqrt{-5}]$ that are not prime.
4. Find all solutions in integers to the equation $y^2 = x^3 - 4$.
5. Show that the sign of the discriminant of a monic separable polynomial $f \in \mathbf{Z}[X]$ having s pairs of complex conjugate roots is $(-1)^s$.
6. Find all solutions in integers to the equation $y^2 = x^3 - 19$.