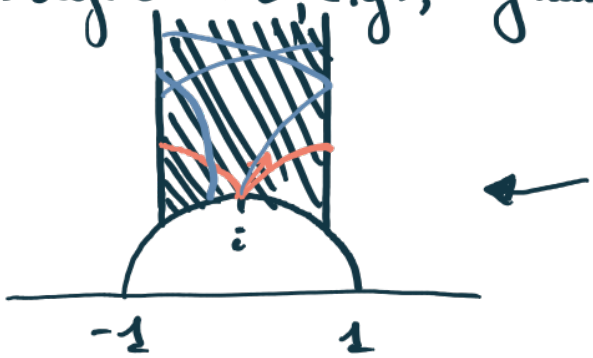
1) Short introduction

1.1 - Who am I?

- Background is in homogeneous dynamics, e.g., dynamics on $SL_2(\mathbb{Z}) \backslash SL_2(\mathbb{R})$



1.2 - Who is Federico Vicela?

- A PhD-student of Nicolas Monod, working on representations of totally disconnected groups.

1.3 - Structure of course / literature

We follow lecture notes by Philippe Michel. These can be found on the moodle website.

2) Exercise classes & exam

- Weekly problem sessions. The problem sessions are for you to ask q's.
- The exam will be 50% exercises compiled from the exercise sheets, 25% proofs and examples from the lecture, 25% new-ish questions for those that run out of problems to think about.
- Exercise sheets include programming tasks. They help with making abstract concepts concrete and let us "sample" data to help with intuition. No programming in exam.

3 - A glimpse of the content of the course:

3.1 - Problems of interest / Diophantine equations:

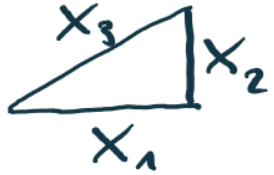
A Diophantine equation, named so after Diophantus of Alexandria, is an equation of the form

$$P(X_1, \dots, X_n) = 0 \qquad P \in \mathbb{Z}[X_1, \dots, X_n],$$

where we are interested in the integral zeroes, i.e., $\underline{x} \in \mathbb{Z}^n$ s.t. $P(\underline{x}) = 0$.

Examples:

(1) Pythagorean triples $P = X_1^2 + X_2^2 - X_3^2$



[There are (infinitely many) non-trivial solutions, e.g. $(3,4,5)$, (primitive) primitive

$(6,8,10)$: (non-primitive)

$6^2 + 8^2 - 10^2 = (2\cdot 3)^2 + (2\cdot 4)^2 - (2\cdot 5)^2 = 2^2 \underbrace{(3^2 + 4^2 - 5^2)}_{=0}$]

(2) $P = X_1^2 - 2X_2^2$

⌜There are no non-trivial solutions. Indeed, $x_1^2 = 2x_2^2$ with $x_i \neq 0$ for some $i = 1, 2$, then $x_1 x_2 \neq 0$ and therefore

$$2 = \frac{x_1^2}{x_2^2} = \left(\frac{x_1}{x_2}\right)^2$$

is a square of a rational number $\frac{x_1}{x_2} \in \mathbb{Q}$ ↯ ⌟

(3) $P = X_1^2 - 4X_2^2$

⌜The are non-trivial solutions, there are only four primitive solutions:

$$\{(2,1), (2,-1), (-2,1), (-2,-1)\}$$

⌟

(4) Pell-equation / Pell-Fermat equation: Let $N \in \mathbb{N} = \{1,2,3,\dots\}$,

$$P = x^2 - Ny^2 - 1.$$

If N is a square, i.e., $N = n^2$ for some $n \in \mathbb{N}$, then there are only two solutions: $\{(1,0),(-1,0)\}$. Let $m,k \in \mathbb{N}$, then

$$(m+k)^2 - m^2 = 2mk + k^2 \geq 3.$$

Note that $x^2 - n^2y^2$ is a difference between two squares. Therefore, if $x \neq \pm ny$, then

$$|P(x_1,x_2)| \geq 2.$$

If N is not a square, then P has infinitely many solutions (due to Lagrange). Notice that primitivity is not a problem in this case because the solutions lie on a hyperbola (show picture)

Also note $x^2 - Ny^2 = (x+\sqrt{N}y)(x-\sqrt{N}y)$, i.e., for any solution $(x_1,x_2) \in \mathbb{Z}^2$ of $P=0$ we have

$$x_1 + \sqrt{N}x_2 \in \mathbb{Z}[\sqrt{N}]^\times \hookrightarrow \mathbb{Q}(\sqrt{N}) \cong \mathbb{Q}[X]/(X^2-N)$$

(5) Sums of k squares:

Theorem (Fermat)

Let $n \in \mathbb{N}$, then $n = x^2 + y^2$ $(x, y \in \mathbb{N} \cup \{0\})$ if and only if either n is a square or

$$n = m^2 p_1 \cdots p_k,$$

where $m \in \mathbb{N}$ and $p_i \in \mathbb{N}$ are distinct primes satisfy $p_i \equiv 1, 2 \bmod (4)$

these are the primes which are of the form $p_i = x^2 + y^2$

Theorem (Legendre)

Let $n \in \mathbb{N}$, then $n = x^2 + y^2 + z^2$ $(x, y, z \in \mathbb{N} \cup \{0\})$ if and only if n is not of the form

$$n = 4^a (8b + 7) \qquad (a, b \in \mathbb{N} \cup \{0\}).$$

Theorem (Lagrange)

Let $n \in \mathbb{N}$, then $n = x^2 + y^2 + z^2 + t^2$ $(x, y, z, t \in \mathbb{N} \cup \{0\})$

(6) Fermat's equation: Generalizing Pythagorean triples:

$$P_n = X_1^n + X_2^n - X_3^n \qquad (n \geq 2)$$

$(1,0,1)$ $(5,0,5)$
$(0,1,1)$

Fermat's Last Theorem (Wiles '94)

If $n \geq 3$, then $P_n = 0$ has no non-trivial solutions.

We will discuss the case $n=3$ (mostly) in the exercises.

3.2 - Algebra

Recall that in the Pell equation example we encountered the field

$$\mathbb{Q}(\sqrt{N}) \hookleftarrow \mathbb{Z}[\sqrt{N}] \hookleftarrow \mathbb{Z}[\sqrt{N}]^\times,$$

and rings of this/similar shape will play an important role in the course.

Definition

An extension of $\mathbb{Q}$ is a field K containing $\mathbb{Q}$ as a subfield $(\mathbb{Q} \hookrightarrow K)$.

An element $x \in K$ is called algebraic over $\mathbb{Q}$ if there is $P \in \mathbb{Q}[X]$ s.t. $P(x) = 0$. The extension $K|\mathbb{Q}$ is an algebraic extension if every element of K is algebraic over $\mathbb{Q}$. A number field is an algebraic extension $K|\mathbb{Q}$ s.t. $\dim_{\mathbb{Q}} K < \infty$.

Examples: $K=\mathbb{Q}$

$K=\mathbb{Q}(\sqrt{-1})=\mathbb{Q}+\mathbb{Q}\sqrt{-1}\cong \mathbb{Q}[X]/(X^2+1)$

$K=\mathbb{Q}(\sqrt{5})\cong \mathbb{Q}[X]/(X^2-5)$

$K=\mathbb{Q}(e^{2\pi i/3})\cong \mathbb{Q}[X]/(X^2+X+1)$

$K=\mathbb{Q}(\sqrt[3]{2})$

Definition

Let $K|\mathbb{Q}$ a number field. Then $x \in K$ is integral if there is a monic polynomial $(X^n + a_{n-1}X^{n-1} + \dots + a_0 =) P \in \mathbb{Z}[X]$ such that

$$P(x) = 0.$$

The integral elements of K form a subring $\mathcal{O}_K \subseteq K$, which we call the ring of integers in K

These rings are the main focus of this class.

Examples: • $K = \mathbb{Q}$, then $\mathcal{O}_K = \mathbb{Z}$,

• $K = \mathbb{Q}(i)$, then $\mathcal{O}_K = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}.i$,

• $K = \mathbb{Q}(e^{2\pi i/3})$, then $\mathcal{O}_K = \mathbb{Z}[e^{2\pi i/3}]$,

• $K = \mathbb{Q}(\sqrt{5})$, then $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Recall that an ideal $I \lhd R$ (R a ring) is an R-submodule of R, i.e., $\forall x,y \in I \; \forall r \in R$ we have

$$x+y \in I \quad \text{and} \quad r.x \in I.$$

An ideal $I \lhd R$ is a principal ideal if there is $r \in R$ s.t.

$$I = R.r =: (r).$$

The ring R is a principal ideal domain (PID) if

(i) R is a domain (i.e. $\overset{a,b \in R}{ab=0} \Rightarrow a=0$ or $b=0$) and

(ii) every $I \lhd R$ is principal.

Given $I, J \lhd R$, we say that $I \mid J$ if $J \subseteq I$. Note that for $r,s \in R$ we have

$$(r) \mid (s) \Leftrightarrow s \in (r) = R.r \Leftrightarrow r \mid s.$$

Examples of PIDs are $\mathbb{Z}$, $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$, $\mathbb{Z}[e^{2\pi i/3}]$, $K[X]$ (fundamental thm of arith.)

Crucial: PIDs admit unique factorization of ideals by primes.

(Unfortunately not all the rings of integers are PIDs. We will measure how far it is from being one via the class number. Let

$$\mathcal{I}_K = \{I \triangleleft \mathcal{O}_K\}$$

and define

$$\mathcal{I}_K \times \mathcal{I}_K \longrightarrow \mathcal{I}_K, \quad (I,J) \longmapsto I \cdot J = \left\{ \sum_{i=1}^{r} a_i b_i : a_i \in I, b_i \in J, r \in \mathbb{N} \setminus \{0\} \right\}$$

Define a relation on $\mathcal{I}_K$ by

$I \sim J$ if there are $r, s \in \mathcal{O}_K - \{0\}$ s.t. $(r)I = (s)J$.

Then $\sim$ defines an equivalence relation on $\mathcal{I}_K$ compatible w/ the multiplication, i.e., if $I_1 \sim J_1, I_2 \sim J_2$, then

$$I_1 \cdot I_2 \sim J_1 \cdot J_2.$$

Therefore multiplication descends to $\mathcal{I}_K/\sim =: \mathcal{C}\ell(K)$, which turns $\mathcal{C}\ell(K)$ into an abelian monoid with the neutral element being the equivalence class of the principal ideal. Put differently

$$\mathcal{C}\ell(K) = \mathcal{I}_K / \mathcal{P}_K, \text{ where } \mathcal{P}_K = \{I \in \mathcal{I}_K : I \text{ is principal}\}.$$

Note: $\mathcal{O}_K$ is a PID if and only if $Cl(K)$ is trivial.

It will turn out that $Cl(K)$ is a finite abelian group, the class group of K.

The class number $h(K) := |Cl(K)|$ of K measures for us how far $\mathcal{O}_K$ is from being a PID.

Examples: Let $d \neq$ square-free integer, then

- $h(\mathbb{Q}(\sqrt{-d})) = 1 \Leftrightarrow d = 1, 2, 3, 7, 11, 19, 43, 67, 163$
  (conjectured by Gauss, proven by Heegner).
- $h(\mathbb{Q}(\sqrt{-5})) = 2$
- It is unknown whether there are infinitely many $d > 0$ s.t. $h(\mathbb{Q}(\sqrt{d})) = 1$.