M2R

Géométrie arithmétique

Présentation M2R

Thème : Théorie des nombres et géométrie algébrique
Lieu : Grenoble
Contact : Emmanuel.Peyre @ univ-grenoble-alpes.fr

Thème

Une question presque aussi ancienne que les mathématiques est la suivante (j'utilise des termes modernes pour la décrire

Soit $P \in \mathbb{Z}[T_1, \dots, T_n]$

antiquité ↙ ↘ $\sim$ XIX^e siècle

Décrire les $(t_1, \dots, t_n) \in \mathbb{Z}^n$ tels que $P(t_1, \dots, t_n) = 0$

eg $X^p + Y^p = Z^p$ ("théorème de FERMAT")

XX^e siècle $\Longleftrightarrow$

objet géométrique $\{(t_1, \dots, t_n) \in \mathbb{C}^n \mid P(t_1, \dots, t_n) = 0\}$

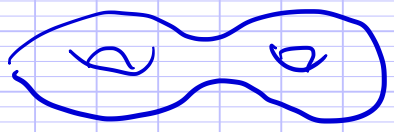
eg $X^p + Y^p = 1 \subset \mathbb{C}^2$

$X^p + Y^p = Z^p \subset \mathbb{P}^2(\mathbb{C})$

courbe complexe C

"surface de RIEMANN"

homéomorphe à



L'archétype des résultats qui montrent ce lien est le

Théorème de FALTINGS

Si $g(C) \geq 2$ le nombre de solutions de l'équation à coordonnées dans $\mathbb{Q}$ est fini.

Le M2 est conçu dans cet esprit

Cours fondamentaux

Algebraic Number Theory ↔ An introduction to algebraic geometry

↔ Arithmetics under the influence of geometry

Cours avancés

Diophantine Approximation for values of special functions

Grassmannians and enumerative geometry

1er semestre :

Valider 2 des cours fondamentaux

2nd semestre

Valider 1 des cours avancés + Stage.

Arithmetics under the influence of geometry

The topic of the lectures is as old as mathematics. One has found a babylonian tablet about 3800 years old containing the formula

$$18541^2 - 12709^2 = 13500^2$$

Diophantes who lived during the 2nd or 3rd century wrote a book containing similar equations of degree 3. You have probably heard of FERMAT's last theorem.

Theorem (FERMAT ~ 1650, WILES, ..., 1995)

Let $n \geq 3$

$\forall a, b, c \in \mathbb{Z}$ $\quad a^n + b^n = c^n \Rightarrow abc = 0$

Inspired by this result EULER conjectured around 1769 that

Conjecture (EULER, 1769)

If $N \geq 4$

$$X_1^N + \cdots + X_{N-1}^N = X_N^N$$

has no solution $(a_1, \ldots, a_n)$ with $a_i > 0$ integers

ELKIES (1988)

$$2682440^4 + 15365639^4 + 18796160^4 = 20615673^4$$

More generally start with a polynomial

$$P(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots X_n]$$

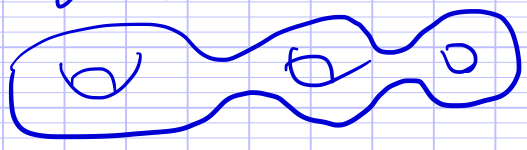
solutions over $\mathbb{Z}^n$
- Is there any?
- Is the number of solutions finite or infinite?

← 20th century →

solutions in $\mathbb{R}^n$ or $\mathbb{C}^n$ defines a « variety » which can be used to define geometrical invariants

geometry can help to answer these question

(genus of a Riemann surface)



$g = 3$

Theorem (FALTINGS)

If the solutions over $\mathbb{C}$ define a Riemann surface of genus $g \geq 2$ then the number of solutions / $\mathbb{Q}$ is finite

Corollary

For $n \geq 4$, the number of primitive solutions (ie with $\gcd(a,b,c) = 1$) of FERMAT equation is finite.

Course content

Informations

Emmanuel.Peyre@univ-grenoble-alpes.Fr

No lecture on Tuesday october 3, 2022

Reference

HINDRY - SILVERMAN : Diophantine geometry : an introduction.

Arithmetics under the influence of geometry

First, let us consider the question:

I How to find solutions

Of course you may think that nowadays the answer is trivial with computers

1) Naïve answer on computers

Let $P_1, \dots, P_m \in \mathbb{Z}[X_1, \dots, X_N]$

We want to study

$$S(P) = \{(x_1, \dots, x_N) \in \mathbb{Z}^N \mid \forall i \in \{1, \dots, m\}, P_i(x_1, \dots, x_N) = 0\}$$

Algorithm

1) $B := 0$
2) for all $(x_1, \dots, x_N) \in \mathbb{Z}^N$ such that $\max(|x_1|, \dots, |x_N|) = B$
   if $\forall i \in \{1, \dots, m\}$ $P_i(x_1, \dots, x_N) = 0$
   Print $(x_1, \dots, x_n)$;
3) $B := B + 1$; go back to 2)

This algorithm will display all the solutions of the equations, ordered by increasing size of the solution

It has only a tiny drow-back: it is based on an infinite loop and never stops

So Imagine you launch it and nothing appears during 3 or 4 days, either

- There is a solution but the smallest solution is given by very large integers
- There is no solution.

Also the program can not tell you whether the number of solutions is finite or not. In fact, long before computers existed it was possible to answer some of these basic questions

2) Questions

As before

Take $P_1, \dots, P_m \in \mathbb{Z}[X_1, \dots, X_N]$

$S(\underline{P}) = \{(x_1, \dots, x_N) \in \mathbb{Z}^N \mid \forall i \in \{1, \dots, m\},\ P_i(x_1, \dots, x_N) = 0\}$

Questions

1) Is $S(\underline{P})$ empty ?
2) Is $S(\underline{P})$ finite ?
3) Is it possible to find all solutions ?
4) How many solutions is there with bounded coordinates ?

...

As I explained during the presentation last week the Babylonians were already able to provide big solutions for a simple equation

3) Back to the babylonians

As I told you this tablet, according to the style of writing is supposed to be 3800 years old. I should stress that the problem with this kind of tablet is that we have no idea of the reason for which it was written,

since it contains « mistakes » one can imagine that it was written by a student as an exercise

Anyway it contains numbers organized in columns each column has an header (exactly like on excel file). I am going to concentrate on the 2nd and 3rd columns, which may be translated (for the 1st lines) as

short side	diagonal
119	169
3367	4825 *
4601	6649
12709	18541
65	97
319	481
2291	3541
799	1249
481	769

* corrected

So for each line if you compute the □ of the diagonal − the □ of the short side you obtain the square of an integer :

$$169^2 - 119^2 = 120^2$$
$$4825^2 - 3367^2 = 3456^2$$
$$6649^2 - 4601^2 = 4800^2$$
$$18541^2 - 12709^2 = 13500^2$$
$$97^2 - 65^2 = 72^2$$
$$481^2 - 319^2 = 360^2$$
$$3541^2 - 2291^2 = 2700^2$$
$$1249^2 - 799^2 = 960^2$$
$$769^2 - 481^2 = 600^2$$

Moreover you may notice that each number on the right hand side of the equation is of the form

$$2^a 3^b 5^c$$

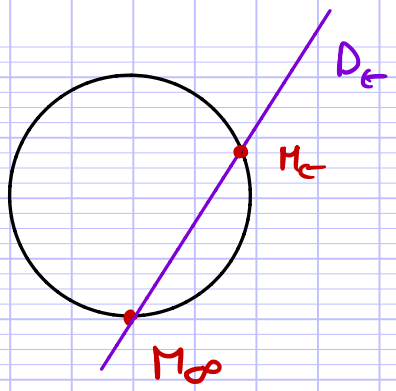
Where 2, 3, 5 are the divisors of 60 which was the base used in babylonian numeral system (which we are still using for measuring time or angles). We can not be completely sure of the method use by the babylonian to get those numbers, but 4] Diophantus gave such a method. In fact, DIOPHANTUS published books which were collections of solved exercises or problems

Problem II.8

Find rational solutions of $X^2 + Y^2 = a^2$ (C)

Of course $X^2 + Y^2 = a^2$ defines a circle of radius a and the equation has an obvious solution

$$M_\infty = (0, -a)$$



Now take a line through M_∞ which is not horizontal:

$$D_t : X = t(Y+a)$$

Then $D_t \cap \mathcal{C}$ contains 2 points

Let us find the coordinates of the intersection

$$t^2(Y+a)^2 + Y^2 = a^2$$

gives $\quad t^2(Y+a)^2 + (Y-a)(Y+a) = 0$

and $\quad (Y+a)\left((t^2+1)Y + (t^2-1)a\right) = 0$

thus $\quad Y = -a \quad$ or $\quad Y = \dfrac{t^2-1}{t^2+1}a$

We get the 2 points of intersection

$$M_\infty = (0,-a) \quad \text{and} \quad M_t = a\left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right)$$

So we get a bijection

$$\mathbb{Q} \cup \{\infty\} \longrightarrow \mathcal{C}(\mathbb{Q}) = \{(x,y) \in \mathbb{Q}^2 \mid x^2+y^2 = a^2\}$$

$$t \longmapsto M_t$$

$$\frac{y+a}{x} \longleftarrow (x,y)$$

Why does it answer the question of finding all pythagorean triples that is all integral solutions of $X^2+Y^2 = Z^2$

Take $a=1$ and write $t = \dfrac{u}{v} \in \mathbb{Q}$, $u,v \in \mathbb{Z}$

Then $M_t = \left(\dfrac{2uv}{u^2+v^2}, \dfrac{u^2-v^2}{u^2+v^2}\right)$ is on $\mathcal{C}$: $X^2+Y^2=1$

In other words

$$(2uv)^2 + (u^2-v^2)^2 = (u^2+v^2)^2$$

is a solution of $X^2+Y^2 = Z^2$

and by taking small numbers for u and v we get all the pythagorean triples found on the babylonian tablet.

u	v	$2uv$	u^2-v^2	u^2+v^2
12	5	120	119	169
64	27	3456	3367	4825
75	32	4800	4601	6649
125	54	13500	12709	18541
9	4	72	65	97
20	9	360	319	481
54	25	2700	2291	3541
32	15	960	799	1249
25	12	600	769	481

More precisely let us say that

Definition

Let A be a commutative ring we say that $(a_1, \dots, a_n) \in A^n$ is primitive if there exists $(u_1, \dots, u_n) \in A^n$ such that

$$u_1 a_1 + \dots + u_n a_n = 1$$

Remark

If A is principal this is equivalent to

$$\gcd(a_1, \dots, a_n) = 1.$$

Proposition

Up to sign and exchanging X and Y, the primitive solutions of

$$X^2 + Y^2 = Z^2$$

in $\mathbb{Z}^3$ are of the form $(2uv, u^2-v^2, u^2+v^2)$ for $(u,v) \in \mathbb{Z}^2$ and $\gcd(u,v) = 1$.

Note that we obtain the non primitive solutions by multiplying x, y, z by a some integer d.

Proof

Let (x, y, z) be a primitive pythagorean triple
We may assume $x \geq 0$, $y \geq 0$ and $z \geq 0$.
The reduction modulo 4 of triple (x, y, z) is a primitive solution $(\bar{x}, \bar{y}, \bar{z})$ of

$$X^2 + Y^2 = Z^2$$

in $(\mathbb{Z}/4\mathbb{Z})^3$. But in $\mathbb{Z}/4\mathbb{Z}$ a square is 0 or 1 and since the solution is primitive at least one of $\bar{x}, \bar{y}, \bar{z}$ is $\neq 0$.

We get that

z is odd

and one of x, y is even and the other odd

By exchanging x and y we may assume that x is even and y odd

Write $x = 2x'$

we get

$$(z - y)(z + y) = 4x'^2$$

But $z - y$ and $z + y$ are even

So $\frac{z-y}{2} \times \frac{z+y}{2} = x'^2$

But if $d \mid \frac{z-y}{2}$ and $d \mid \frac{z+y}{2}$ then $d \mid z$ and $d \mid y$
and $d^2 \mid x'^2 \Rightarrow d \mid x' \Rightarrow d \mid x$
which contradicts the hypothesis

$$\gcd(x, y, z) = 1$$

So $\gcd\left(\frac{z-y}{2}, \frac{z+y}{2}\right) = 0$

Notation

$\mathcal{P}$ set of prime numbers

For $n \in \mathbb{N}$, $n \geq 1$ write

$$n = \prod_{p} p^{v_p(n)}$$

its prime decomposition we may extend it to $\mathbb{Q}$ by

$$\begin{cases} v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b) & \text{if } a, b \in \mathbb{Z} - \{0\} \\ v_p(0) = +\infty \end{cases}$$

End of the proof

For any prime p,

$$\min\left(v_p\left(\frac{x+y}{2}\right), v_p\left(\frac{x-y}{2}\right)\right) = 0$$

and

$$v_p\left(\frac{x+y}{x}\right) + v_p\left(\frac{x-y}{2}\right) \text{ is even}$$

Thus $v_p\left(\frac{x+y}{2}\right)$ and $v_p\left(\frac{x-y}{2}\right)$ are even

But $\frac{x+y}{2} \geq 0$ and $\frac{x-y}{2} \geq 0$

So $\frac{x+y}{2}$ and $\frac{x-y}{2}$ are both squares!

Write $\frac{x+y}{2} = u^2$ and $\frac{x-y}{2} = v^2$

get

$$(x, y, z) = (2uv, u^2 - v^2, u^2 + v^2)$$

Moreover

$$\gcd(u, v) = 1.$$

Note that $u^2 - v^2$ is odd, so u and v are not both odd. $\square$

Let us now consider the general case of a

5 Conics

$q \in \mathbb{Z}[X,Y,Z]$ homogeneous polynomial of degree 2 which defines a non-degenerate quadratic form on $\mathbb{Q}^3$

$$q(X,Y,Z) = aX^2 + bY^2 + cZ^2 + dXY + eYZ + fXZ$$

Remark 1

If $(x,y,z) \in \mathbb{Z}^3$ is a solution of

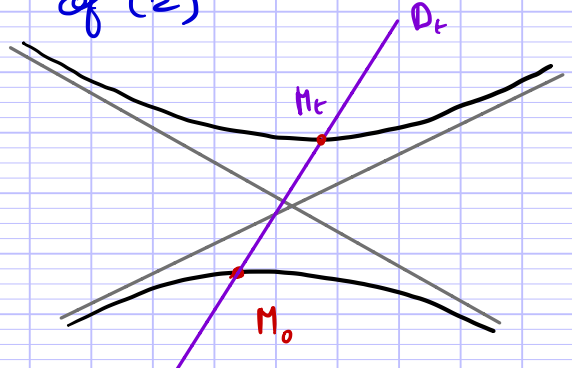
(1) $\quad q(X,Y,Z) = 0$

with $z \neq 0$, then $\left(\frac{x}{z}, \frac{y}{z}\right) \in \mathbb{Q}^2$ is a solution of

(2) $\quad aX^2 + bY^2 + dXY + fX + dY + c = 0$ $\mathcal{C}$

So it is almost the same to find the integral solutions of (1) or the rational solutions of (2)! (Up to a finite number of solutions)

Assume that we know a solution $M_0 = (x_0, y_0) \in \mathbb{Q}^2$ of (2)



Again, we consider D_t a line through M_0

$$D_t : \quad Y - y_0 = t(X - x_0)$$

$\mathcal{C} \cap D_t$ is given by

$$q(X, t(X - x_0) + y_0, 1) \in \mathbb{Q}[t, X] \text{ polynom}$$

of degree 2 in the X variable with x_0 as root and therefore divisible by $X - x_0$. The quotient may be written as

$$P(t)X + Q(t)$$

with P, Q polynoms of degree ≤ 2.
which gives

$$X = -\frac{Q(t)}{P(t)} \qquad Y = t\left(-\frac{Q(t)}{P(t)} - x_0\right) + y_0$$

we get again a bijection from

$$\mathcal{C}(\mathbb{Q}) = \{(x,y) \in \mathbb{Q}^2 \mid Q(x,y,1) = 0\}$$

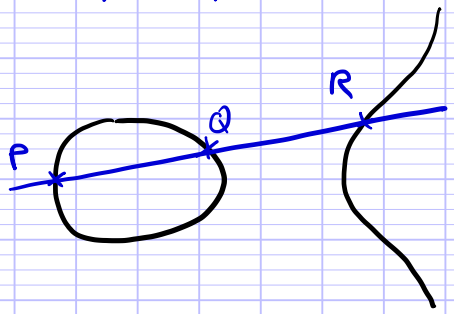
to

$$\mathbb{Q} - \{t \in \mathbb{Q} \mid P(t) = 0\} \cup \{\infty\}.$$

So for a homogeneous equation of degree 2 as soon as one knows a solution, one can easily parametrize the set of solutions
What can we do in degree 3

5) Degree 3

$$\mathcal{C}: \quad y^2 = x^3 + ax + b$$



Let us take <u>two</u> points $P = (x_0, y_0)$, $Q = (x_1, y_1) \in \mathcal{C}(\mathbb{Q})$ and let D be the line through P and Q

$$D: \quad \alpha X + \beta Y + \gamma = 0$$

with $\alpha, \beta, \gamma \in \mathbb{Q}$, $(\alpha, \beta) \neq (0,0)$
get $Y = \frac{-\alpha X - \gamma}{\beta}$ (or $X = \frac{-\beta Y - \gamma}{\alpha}$)

Then $\mathcal{C}(\mathbb{Q}) \cap D$ is given by

$$\left(\frac{-\alpha X - \gamma}{\beta}\right)^2 = X^3 + aX + b$$

which is a polynomial equation of degree 3 with 2 known solutions x_0 and x_1

So this polynom is divisible by $(X - x_0)(X - x_1) \in \mathbb{Q}[X]$

The quotient is a polynom of degree 1 in $\mathbb{Q}[X]$

This gives the coordinates of the 3rd intersection point R

Get $R \in \mathcal{C}(\mathbb{Q})$

NB.

If $P = Q$, take for D the tangent at P to $\mathcal{C}$ (given by

$$2y_0(Y - y_0) = (3x_0^2 + a)(X - x_0)$$

get a polynom divisible by $(X - x_0)^2$)

So we get a law on $\mathcal{C}(\mathbb{Q})$

$$(P, Q) \longmapsto P * Q$$

Question

Using this construction, can we obtain all the points on $\mathcal{C}(\mathbb{Q})$ starting from a finite set of points of $\mathcal{C}(\mathbb{Q})$?

Answer (Conjecture of MORDELL proven by WEIL)

YES! We can.

The proof of this result is not obvious and is one the aim of this course.

Conjecture (After LANG)

Up to a finite set of points all rational solutions of polynomial equations might be obtained using methods similar to the 2 we have just seen.

(To be made more precise later on)

To start with I am going to study more carefully the law $*$

II Elliptic curves

1) Projective space

In the course of Jean FASEL, he will define a particular scheme : the projective scheme, later I shall explain the connexion with the next definition. Right now, I am interested in the points of the projective space

a) Set definition homogeneous coordinates

Definition

For a (commutative) field $\mathbb{K}$, E a $\mathbb{K}$ vector space

$\mathbb{P}(E) = \{$ vector subspaces of dim 1 in $E\}$

is the projective space associated to E

In particular Let $n \in \mathbb{N} = \{n \in \mathbb{Z},\ n > 0\}$

the set of $\mathbb{K}$-points of the projective space $\mathbb{P}^n$ is the set

$$\mathbb{P}^n(\mathbb{K}) = \{\text{vector subspaces of dim } 1 \text{ in } \mathbb{K}^{n+1}\}$$

If $(x_0, \dots, x_n) \in \mathbb{K}^{n+1} - \{0\}$ then it defines a point in the projective space

$$[x_0 : x_1 : \dots : x_n] = \mathbb{K}(x_0, \dots, x_n)$$

the line generated by $(x_0, \dots, x_n)$

If $P = [x_0 : x_1 : \dots : x_n]$ we say that $(x_0, \dots, x_n)$ are homogeneous coordinates for P

2 Homogeneous coordinates are not unique

$$[x_0 : x_1 : \dots : x_n] = [y_0 : y_1 : \dots : y_n]$$

iff $(x_0, \dots, x_n)$ and $(y_0, \dots, y_n)$ are colinear

So homogeneous coordinates define a bijection

$$\mathbb{K}^{n+1} - \{0\} / \mathbb{K}^* \longrightarrow \mathbb{P}^n(\mathbb{K})$$

where $\mathbb{K}^{n+1} - \{0\} / \mathbb{K}^*$ is the set of orbits for the action of $\mathbb{K}^*$ on $\mathbb{K}^{n+1} - \{0\}$ given by

$$\lambda (x_0, \dots, x_n) = (\lambda x_0, \dots, \lambda x_n)$$

We are going to generalize this definition to a particular class of rings.

Definition

A <u>principal ideal ring</u> is a commutative ring in which all ideals are generated by an element

⚠ A principal ideal domain is a principal ideal ring which is integral!

Examples

fields, $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ are all principal ideal rings (if n is not prime $\mathbb{Z}/n\mathbb{Z}$ is not integral).

Definition

If A a ring, A^* is the group of invertible elements in A

A^* acts on the set of primitive elements in A^{n+1} by multiplication of the coordinates

$$\lambda (a_0, \dots, a_n) = (\lambda a_0, \dots, \lambda a_n)$$

We define

$$\mathbb{P}^n(A) = \{ \text{primitive elements in } A^{n+1} \} / A^*$$

N.B.

This is compatible with the definition given for fields.

Remark

This definition is functorial:
If A, B are principal ideal rings
and $\varphi : A \to B$ is a morphism of rings
then if $(a_0, \dots, a_n) \in A^{n+1}$ is primitive
there exists $(u_0, \dots, u_n) \in A^{n+1}$ such that

$$u_0 a_0 + \dots + u_n a_n = 1$$

so $\varphi(u_0)\varphi(a_0) + \dots + \varphi(u_n)\varphi(a_n) = \varphi(1) = 1$
Thus $(\varphi(a_0), \dots, \varphi(a_n))$ is primitive
and $\varphi(A^*) \subset B^*$
Thus φ induces a map
which we also denote by φ

$$\varphi : \mathbb{P}^n(A) \to \mathbb{P}^n(B)$$

Prop

The natural injection

$$\mathbb{P}^n(\mathbb{Z}) \to \mathbb{P}^n(\mathbb{Q})$$

is a bijection.

Proof

First note that

$$(a_0, \dots, a_n) \in \mathbb{Z}^{n+1}$$

is primitive if and only if $\gcd(a_0, \dots, a_n) = 1$

- Let $[x_0 : \dots : x_n] \in \mathbb{P}^n(\mathbb{Q})$
write $x_i = \frac{p_i}{q_i}$ with $p_i \in \mathbb{Z}$, $q_i \in \mathbb{Z} - \{0\}$

Let $q = \operatorname{lcm}(q_i)$ lowest common multiple
then $q x_i \in \mathbb{Z}$ $\quad 0 \le i \le n$
let $d = \gcd(q x_i)$

then

$$[x_0 : \dots : x_n] = \left[\frac{q}{d}x_0 : \dots : \frac{q}{d}x_n\right]$$

But $\frac{q}{d}x_0, \dots, \frac{q}{d}x_n$ are coprime integers and define a point in $\mathbb{P}^n(\mathbb{Z})$.

So the map $\mathbb{P}^n(\mathbb{Z}) \to \mathbb{P}^n(\mathbb{Q})$ is surjective.

- Let $(x_0, \dots, x_n)$ and $(y_0, \dots, y_n)$ be $n+1$-uples of coprime integers such that

$$[x_0 : \dots : x_n] = [y_0 : \dots : y_n] \text{ in } \mathbb{P}^n(\mathbb{Q})$$

then there exist $\lambda = \frac{a}{b} \in \mathbb{Q}^*$, with $a, b \in \mathbb{Z}$ and $\gcd(a,b) = 1$ such that

$$(y_0, \dots, y_n) = \lambda (x_0, \dots, x_n)$$

Thus $b(y_0, \dots, y_n) = a(x_0, \dots, x_n)$

Since $\gcd(a,b) = 1$

we get that

$$a \mid y_i \text{ for } i \in \{0, \dots, n\}$$

But $\gcd(y_0, \dots, y_n) = 1$

and therefore $a \in \{-1, 1\}$

similarly we get $b \in \{-1, 1\}$

and $\lambda \in \mathbb{Z}^*$

Thus $[x_0 : \dots : x_n] = [y_0 : \dots : y_n]$ in $\mathbb{P}^n(\mathbb{Z})$. □

<u>Definition</u>

If $M \in \mathbb{N} - \{0\}$, the reduction map

$$\text{red}_M : \mathbb{P}^n(\mathbb{Q}) \to \mathbb{P}^n(\mathbb{Z}/M\mathbb{Z})$$

is defined as the only map making the diagram

$$\begin{array}{ccc} \mathbb{P}^n(\mathbb{Q}) & \xrightarrow{\text{red}_M} & \mathbb{P}^n(\mathbb{Z}/M\mathbb{Z}) \\ \uparrow & \nearrow & \\ \mathbb{P}_n(\mathbb{Z}) & & \end{array}$$

commutative.

b) Affine atlas

Definition

For any commutative ring A, the set of A-points of the affine space $\mathbb{A}^n$ is

$$\mathbb{A}^n(A) = A^n$$

Remarks

(i) Gives a functor from the category of commutative rings to the category of sets

(ii) If A is a commutative ring and B a commutative A-algebra (which is a ring)

$$\begin{array}{l} \mathrm{Mor}\left(A[x_1, \dots, x_n], B\right) \\ \updownarrow \text{bijection} \\ B^n \end{array}$$

morphisms of A-algebra mapping 1 to 1

(FASEC's course)

Construction

If A is a principal ideal ring and $i \in \{0, 1, \dots, n\}$ we may define a natural map

$$\begin{aligned} j_i : A^n &\longrightarrow \mathbb{P}^n(A) \\ (x_0, x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) &\longmapsto [x_0 : x_1 : \dots : x_{i-1} : 1 : x_{i+1} : \dots : x_n] \end{aligned}$$

which is injective. Its image is

$$\{[x_0 : \dots : x_n] \in \mathbb{P}^n(A) \mid x_i \in A^*\}$$

Therefore we get

Proposition

If $\mathbb{K}$ is a field then the projective space can be covered by affine spaces

$$\mathbb{P}^n(\mathbb{K}) = \bigcup_{i=0}^{n} j_i(\mathbb{K}^n).$$

2 False for $\mathbb{Z}$, true for local rings.

Remark

There is also a map

$$\iota : \mathbb{P}^{n-1}(k) \longrightarrow \mathbb{P}^n(k)$$
$$[x_1 : \dots : x_n] \longmapsto [0 : x_1 : \dots : x_n]$$

We have for a field k ($\coprod$ disjoint union)

$$\mathbb{P}^n(k) = j_0(\mathbb{A}^n(k)) \coprod \iota(\mathbb{P}^{n-1}(k))$$

So we write

$$\mathbb{P}^n = \mathbb{A}^n \coprod \mathbb{P}^{n-1} = \mathbb{A}^n \coprod \mathbb{A}^{n-1} \coprod \dots \coprod \{\ast\}$$

Geometrically we may describe it as:

$$\mathbb{P}^n(k) = \mathbb{A}^n(k) \coprod \{\text{directions of lines in } \mathbb{A}^n(k)\}$$

for each direction of lines in the affine space we add one point at ∞

Terminology

The points in the image of $\mathbb{P}^{n-1}(k)$ in $\mathbb{P}^n(k)$ are called the points at ∞.

c) Action of $PGL_n(k)$

Definition

For a commutative ring A,

$$GL_n(A) = M_n(A)^* = \{M \in M_n(A) \mid \det(M) \in A^*\}$$

$$I_n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_n(A) \qquad A^* I_n \subset GL_n(A)$$

$$PGL_n(A) = GL_n(A) / A^* I_n$$

The natural action of $GL_n(\mathbb{K})$ on $\mathbb{K}^{n+1}$ preserves the dimension of subspaces

If $\mathbb{K}$ is a field $GL_n(\mathbb{K})$ acts on $\mathbb{P}^n(\mathbb{K})$ via

$$g \cdot D = g(D)$$

The action of $\mathbb{K}^* I_n$ is trivial, therefore this induces an action of $PGL_n(\mathbb{K})$ on $\mathbb{P}^n(\mathbb{K})$

Example

If $n = 2$ $\quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{K})$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} [x : y] = [ax + by : cx + dy]$$

(homographies on $\mathbb{P}^1(\mathbb{C})$).

Definition

- If E is a $\mathbb{K}$-vector space, a projective subspace of $\mathbb{P}(E)$ is a subset of the form $\mathbb{P}(F)$ for some $\mathbb{K}$ vector subspace F of E
- If $\dim(E) = n+1$, a projective frame of $\mathbb{P}(E)$ is a $(n+2)$-tuple of points $P_0, \dots, P_{n+1}$ in $\mathbb{P}(E)$ such that for any $i \in \{0, \dots, n+1\}$, $P_0, \dots, P_{i-1}, P_{i+1}, \dots, P_{n+1}$ is not contained in a strict projective subspace of $\mathbb{P}(E)$

Proposition

If $(P_0, \dots, P_{n+1})$ is a projective frame of $\mathbb{P}(E)$, then there exists an isomorphism of vector spaces

$$\varphi : \mathbb{K}^{n+1} \longrightarrow E$$

such that if $(\vec{e}_0, \dots, \vec{e}_n)$ is the usual basis of $\mathbb{K}^{n+1}$, $P_i = \varphi(\mathbb{K} e_i)$ for $i \in \{0, \dots, n\}$ and $P_{n+1} = \varphi\left(\mathbb{K}\left(\sum_{i=0}^{n} e_i\right)\right)$

Moreover this φ is unique up to composition by an homothecy $\lambda \mathrm{Id}_{\mathbb{K}^{n+1}}$.

Proof

Existence

Choose $\vec{f}_i \in P_i$ for $i \in \{0, \dots, n, n+1\}$ (P_i : line in E)

Then $(\vec{f}_0, \dots, \vec{f}_n)$ is not contained in any hyperplane so it is a basis of E

$$\vec{f}_{n+1} = \sum_{i=0}^{n} a_i \vec{f}_i$$

If $a_i = 0$ then $\{\vec{f}_0, \dots, \vec{f}_{i-1}, \vec{f}_{i+1}, \dots, \vec{f}_n, \vec{f}_{n+1}\}$ is in contained in the hyperplane $X_i = 0$

So $a_i \neq 0$ for $i \in \{0, \dots, n\}$

and $(a_1 \vec{f}_1, \dots, a_n \vec{f}_n)$ is a basis of E

Choose $\varphi : \mathbb{K}^{n+1} \to E$ as the unique linear map which maps $\vec{e}_i$ on $a_i \vec{f}_i$.

Unicity

If φ_1 and φ_2 satisfy the conditions we get that

$$\varphi_2(\vec{e}_i) = a_i \varphi_1(\vec{e}_i) \text{ for } i \in \{0, \dots, n\}$$

and

$$\varphi_2\left(\sum_{i=0}^{n} \vec{e}_i\right) = a \varphi_1\left(\sum_{i=0}^{n} \vec{e}_i\right)$$

which implies that

$$a_i = 0 \text{ for } i \in \{0, \dots, n\}$$

So $\varphi_2 = a \varphi_1$. □

2) Algebraic spaces of affine setting

Remark

The idea is to have an "elementary" definition of geometric objects defined by polynomial equations. There is a little problem to do that. Consider the equation

$$X^2 + Y^2 + 1 = 0$$

This equation has no solutions over $\mathbb{R}$ and therefore none over $\mathbb{Q}$. Nevertheless we wish to consider the geometric object defined by this equation and to "think" of it as a curve.

The idea is to use the notion of foncteur and consider the solutions with coordinates not only over $\mathbb{Q}$ but in an arbitrary commutative ring.

Definition

Let A be a commutative ring and let

$$P_1, \dots, P_m \in A[X_1, \dots, X_N]$$

be m polynomials with coefficients in A. Let $I = (P_1, \dots, P_m)$ be the generated ideal. To this family of polynomials we may associate the foncteur V_I from the category of A-algebras to the category of Sets given by

$$V_I(B) = \{(x_1, \dots, x_N) \in B^n \mid \forall P \in I,\ P(x_1, \dots, x_N) = 0\}$$

We say that $V_I(B)$ is the algebraic subset of B^N defined by I.

Convention Unless otherwise stated
any algebra is a ring (most of the time commutative)
any morphism of algebras maps 1 to 1

Remark

(i) To define a functor, I should also describe how it applies to morphisms; in the sequel I shall not do it when it is quite obvious
If $\varphi : B \to C$ is a morphism between commutative A-algebras, then

$$V_I(\varphi) : V_I(B) \longrightarrow V_I(C)$$
$$(x_1, \dots, x_N) \longmapsto (\varphi(x_1), \dots, \varphi(x_N))$$

(ii) Let me explain the connection to the theory of schemes which is the object of Jean FASEC's lectures:
Construction of
a) a category of geometric objects: the category of schemes with
b) a contravariant fully faithful functor from the category of commutative rings to the category of schemes: the spectrum
In other words if A and B are commutative rings, there is a canonical bijection

$$\mathrm{Mor}_{\text{rings}}(B, A) \xrightarrow{1.1} \mathrm{Mor}_{\text{sch}}(\mathrm{Spec}(A), \mathrm{Spec}(B))$$

Terminology
. Let A be a commutative ring
a scheme over A (or A-scheme) is a scheme X equipped with a "structural" morphism

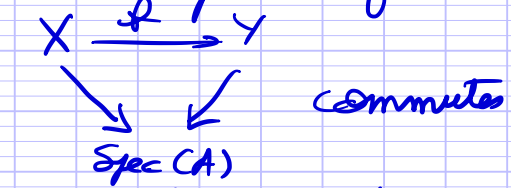
$$\pi : X \to \mathrm{Spec}\, A$$

Example

If B is a commutative A-algebra the natural morphism $A \to B$, $a \mapsto a1$ induces a morphism $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ and $\mathrm{Spec}(B)$ may be seen as a scheme over A

Terminology (continued)

- If X and Y are schemes over A a morphism of A-schemes is a morphism of schemes $f : X \to Y$ such that



- If X is an A-scheme and B a commutative A-algebra then the B-points of X is the set

$$X(B) = \mathrm{Mor}_{\mathrm{Spec}(A)}(\mathrm{Spec}(B), X)$$

This defines a foncteur

Category of commutative A-algebras $\to$ Sets

Example

If I is an ideal in $A[X_1, \dots, X_N]$ let $V_I = \mathrm{Spec}(A[X_1, \dots, X_N]/I)$ then one can check that, for any commutative A-algebra B, there are canonical bijections

$$\{(x_1, \dots, x_N) \in B \mid \forall P \in I,\ P(x_1, \dots, x_N) = 0\}$$

$$\downarrow$$

$$\mathrm{Mor}_{A\text{-alg}}(A[X_1, \dots, X_N]/I, B)$$

$$\downarrow$$

$$\mathrm{Mor}_{\mathrm{Spec}(A)}(\mathrm{Spec}(B), V_I)$$

$$\| $$

$$V_I(B).$$

So what I have defined is a particular case of the foncteur of points associated to a scheme *

Prop. Let me give a few properties of these foncteurs

a) If $I \subset J$ ideals of $A[X_1, \dots, X_N]$ then for any commutative A algebra B

$$V_J(B) \subset V_I(B)$$

b) If I, J are ideals of $A[X_1, \dots, X_N]$

$$V_I(B) \cap V_J(B) = V_{I+J}(B)$$

$I+J$ ideal generated by $I \cup J$

c) With the same notations If B is integral

$$V_I(B) \cup V_J(B) = V_{I \cap J}(B)$$

2 [When B is not integral $V_I(B) \cup V_J(B)$ is not necessarily $V_{I \cap J}(B)$! and $V_I \cup V_J$ is not an algebraic space]

b) Projective setting

Similarly we can define algebraic subsets in the projective setting.

Definition

Let A be a commutative ring

Let $P_1, \dots, P_m$ be homogeneous polynomials in $A[X_0, \dots, X_N]$.

Let $J = (P_1, \dots, P_m) \subset A[X_0, \dots, X_N]$ generated ideal

J_{hom} is the set of homogeneous polynomials in J

Then we may consider

The foncteur from the category of commutative A algebras which are principal ideal rings to the category of sets given by

$$Z_J(B) = \{[x_0 : \dots : x_N] \subset \mathbb{P}^N(B) \mid \forall P \in J_{hom}, P(x_0, \dots, x_N) = 0\}$$

does not depend on the choice of homogeneous coordinates.

We say that $Z_J(B)$ is the algebraic subset of $\mathbb{P}^n(B)$ defined by $P_1, \dots, P_m$ (or J).

Remark

Since the P here are homogeneous which means that there are integers d such that

$$P(TX_0, \dots, TX_N) = T^d P(X_0, \dots, X_N)$$

If $[x_0 : \dots : x_N] = [y_0 : \dots : y_N]$ there exists $\lambda \in B^*$ such that

$$(y_0, \dots, y_n) = \lambda (x_0, \dots, x_n)$$

and

$$P(y_0, \dots, y_N) = \lambda^d P_i(x_0, \dots, x_N)$$

Therefore

$$P(y_0, \dots, y_N) = 0 \iff P(x_0, \dots, x_N)$$

c) HILBERT Nullstellensatz

Let me first give a quick reminder about algebraic closed fields:

Definition

A field K is said to be algebraically closed if it satisfies one of the following equivalent conditions:

(i) The irreducible polynomials in $K[T]$ are the polynomials of degree 1

(ii) Any polynomial $P \in K[T]$ of degree $d \geq 0$ may be written as

$$P = a \prod_{i=1}^{d} (X - \alpha_i) \text{ with } \alpha_1, \dots, \alpha_d \in K \text{ and } a \in K^*$$

(iii) Any polynomial $P \in K[T]$ of degree $d \geq 1$ has a root in K

One important fact is that any field has an algebraic closure

Definition

An algebraic closure of a field K is an extension $\overline{K}$ of K such that

(i) $\overline{K}$ is algebraic over K

(ii) $\overline{K}$ is algebraically closed.

Theorem (Reminder)

If K is a field

a) There exists an algebraic closure $\overline{K}$ of K

b) If K_1 and K_2 are algebraic closures of K then K_1 and K_2 are isomorphic as K-algebra

c) If K is an algebraic closure of K and L an algebraic extension of, there exist a morphism of K-algebras $\varphi : L \to \overline{K}$

Example

If we define $\overline{\mathbb{Q}}$ as the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, that is

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \exists P \in \mathbb{Q}[X] - \{0\}, \ P(\alpha) = 0\}$$

then $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$.

Theorem (HILBERT's Nullstellensatz)

Let $\overline{K}$ be an algebraically closed field

Let I be an ideal of $\overline{K}[X_1, \dots, X_n]$

$$V_I(\overline{K}) = \{(x_1, \dots, x_n) \in \overline{K}^n \mid \forall P \in I, \ P(x_1, \dots, x_n) = 0\}$$

Let $P \in \overline{K}[X_1, \dots, X_n]$ such that

$$\forall (x_1, \dots, x_n) \in V_I(\overline{K}), \ P(x_1, \dots, x_n) = 0$$

Then there exists $m \in \mathbb{N}$ such that $P^m \in I$

Corollary

Let $P_1, \dots, P_m$ be homogeneous polynomials in $\overline{K}[X_0, \dots, X_N]$ such that the corresponding algebraic subset $Z_J(\overline{K}) \subset \mathbb{P}^N(\overline{K})$ is empty. Then there exists $m \in \mathbb{N}$ such that

$$X_i^m \in J = \underbrace{(P_1, \dots, P_m)}_{\text{ideal generated by } P_1, \dots, P_m} \text{ for all } i \in \{0, \dots, N\}$$

Proof

We consider $V_J(\overline{K}) \subset \overline{K}^{N+1}$

The hypothesis is equivalent to

$$\underbrace{V_J(\overline{K})}_{\text{subset of } \overline{K}^{N+1} \text{ defined by } J} \subset \{0\}$$

we apply HILBERT's Nullstellensatz to the X_i. □

Remark

The converse is also true (but obvious): if $X_i^m \in J$ for all $i \in \{0, \dots, N\}$ then for any non-zero K-algebra which is a principal ideal ring

$$Z_J(A) \subset \bigcap_{i=0}^{N} \{[x_0 : \dots : x_N] \in \mathbb{P}^N(A) \mid x_i = 0\} = \emptyset$$

since homogeneous coordinates are primitive so they can't all be 0.

Corollary 2

Let K be a field, $P_1, \dots, P_m \in K[X_0, \dots, X_N]$ be homogeneous polynomials, $\overline{K}$ be an algebraic closure of K and A be a K algebra which is a principal ideal ring. Then $Z_J(A) \neq \emptyset \Rightarrow Z_J(\overline{K}) \neq \emptyset$

Remark

We are going to see that
(a) To test if an algebraic set is empty it is enough to check it over an algebraic closure
(b) To test a polynomial relation on an algebraic set it is enough to check it over an algebraic closure.

I am going to prove HILBERT's Nullstellensatz but it requires several steps.

Proposition

Let A be an integral ring
Let $K = Fr(A)$ be its fraction field
Let L be a field extension of K and assume that L is generated by a finite number of elements as an A-algebra. Then
a] L is a finite extension of K
b] There exists $a \in A - \{0\}$ such that $K = A[a^{-1}]$

Proof

Let S be a finite subset of L which generates L as an A-algebra. We shall proceed by induction on $\#S$.

Initialisation

Assume that all elements in S are algebraic over K (true if $S = \emptyset$)
Then L/K is generated by a finite number of algebraic elements and therefore
$[L:K]$ is finite
Let $(e_i)_{i \in I}$ be a basis of L over K.
the coordinates of the elements of S, of 1 and of the products $e_i e_j$ in the basis give a finite set of elements in

$$K = \left\{ \frac{a}{b}, (a,b) \in A \times A - \{0\} \right\}$$

by taking the product of the denominators of the elements of this set, we get that they belong to $A[a^{-1}]$ for some $a \in A - \{0\}$
The set

$$\left\{ \sum_{i \in I} a_i e_i, \ (a_i)_{i \in I} \in (A[a^{-1}])^I \right\}$$

is then a subalgebra of L over A which contains S. So it is equal to L.
Thus it contains $K e_1$
Since $(e_i)_{i \in I}$ is a basis of L/K we get that
$K = A[a^{-1}]$.

Induction

Let us now assume that $s \in S$ is transcendental over k this means that

$$\begin{array}{ccc} A[X] & \longrightarrow & A[s] \subset L \\ P & \longmapsto & P(s) \end{array}$$

is an isomorphism, and $A[s]$ is an integral ring

Let $E = Fr(A[s])$. E is an $A[s]$ algebra, L is generated by $S - \{s\}$ so we may apply the induction hypothesis: there exist $b \in A[s] - \{0\}$ such that $E = A[s][b^{-1}]$

But then $\exists P \in A[X]$ such that $b = P[s]$

so $E = A[s][P(s)^{-1}]$

Since $A[X] \to A[s]$ is an isomorphism

$Q \longmapsto Q(s)$

$K(X) = Fr(A[X]) \to E = Fr(A[s])$ is an isomorphism

$\frac{R(X)}{Q(X)} \to \frac{R(s)}{Q(s)}$

We get $K(X) = A[X][P(X)^{-1}] \subset K[X][P(X)^{-1}]$

But the set of irreducible polynomials in $K[X]$ is infinite (because K is infinite or K is finite and there are irreducible polynomials of any degree)

Let $Q \in K[X]$ be an irreducible polynomial which does not divide $P(X)$

We get

$$\frac{1}{Q(X)} = \frac{R(X)}{P(X)^m}$$

for some $m \in \mathbb{N}$ and $R(X) \in K[X]$

so $Q(X) \mid P(X)^m$ which is absurd. $\square$

Corollary

Let K be a field, A a finitely generated K-algebra and $\mathfrak{m}$ a maximal ideal in A. Then

a) $[A/\mathfrak{m} : K]$ is finite

b) Let Ω be an algebraically closed extension of K. There exists a morphism of K-algebras

$$\varphi : A \to \Omega$$

such that $\ker(\varphi) = \mathfrak{m}$

Proof

By Theorem 1 applied to $A = K$ and $L = A/\mathfrak{m}$

$[A/\mathfrak{m} : K]$ is finite (and therefore algebraic)

Since Ω is algebraically closed there exists a morphism of K-algebras

$$\overline{\varphi} : A/\mathfrak{m} \to \Omega$$

and if we denote by $\pi : A \to A/\mathfrak{m}$ the projection $\varphi = \overline{\varphi} \circ \pi$ satisfies b).

Corollary 2

Let I be an ideal of $K[X_1, \dots, X_n]$ and $\overline{K}$ an algebraic closure of K. Then

$$V_I(\overline{K}) = \emptyset \Rightarrow 1 \in I$$

Proof

If $I \neq K[X_1, \dots, X_n]$ then there exists a maximal ideal m of $K[X_1, \dots, X_n]$ containing I. By Corollary 1 there exists $\varphi : K[X_1, \dots, X_n] \to \overline{K}$ such that $\ker(\varphi) = m$

Let $x_i = \varphi(X_i)$

For any $P \in I$,

$P(x_1, \dots, x_n) = \varphi(P) = 0$ since $I \subset m = \ker(\varphi)$

So $(x_1, \dots, x_n) \in V_I(\overline{K})$ and $V_I(\overline{K}) \neq \emptyset$. □

Corollary 3

Let K be a field, I an ideal in $K[X_1, \dots, X_n]$ and $\overline{K}$ be an algebraic closure of K

If there exists a non-zero K-algebra A such that

$$V_I(A) \neq \emptyset$$

Then $V_I(\overline{K}) \neq \emptyset$

Proof

If $1 \in I$, $V_I(A) = \emptyset$ for any non-zero algebra A.

□

So, again, to test if an algebraic set is empty it is enough to test it for $\overline{K}$.

Proof of HILBERT's Nullstellensatz

The result is true if $P = 0$

Otherwise let $\hat{I}$ be the ideal in $K[X_1, \dots, X_n, T]$ generated by I and $1 - TP$,

Let $(x_1, \dots, x_m, t) \in V_{\hat{I}}(\bar{K})$
then $(1 - PT)(x_1, \dots, x_m, t) = 0$
so $P(x_1, \dots, x_m)\, t = 1$
So $P(x_1, \dots, x_m) \neq 0$
Since P is 0 on $V_I(\bar{K})$
we get $(x_1, \dots, x_m) \notin V_I(\bar{K})$
There exists $Q \in I$ such that $Q(x_1, \dots, x_m) \neq 0$
This contradicts $(x_1, \dots, x_m, t) \in V_{\hat{I}}(\bar{K})$
So $V_I(\bar{K}) = \emptyset$
so $1 \in \hat{I}$
So there exist $g_0, \dots, g_r \in K[X_1, \dots, X_m, T]$
and $h_1, \dots, h_r \in I$ such that

$$1 = g_0(1 - PT) + g_1 h_1 + \cdots g_r h_r$$

$K[x_1, \dots, x_m][T] / (1 - PT)$
is isomorphic to $K[x_1, \dots, x_m]\left[\frac{1}{P}\right]$
we get

$$1 = \overline{g_1} h_1 + \cdots + \overline{g_r} h_r$$

write $\overline{g_i} = \frac{a_i}{P^m}$ with $a_i \in K[x_1, \dots x_m]$
(We may take the same m)
We get $P^m = \underbrace{a_1 h_1 + \cdots + a_r h_r}_{\in I}$ in $K[x_1, \dots, x_m]$

□

d) From projective equations to affine equations and back

Reminder

$$\begin{aligned} j_0 : \mathbb{A}^N &\longrightarrow \mathbb{P}^N \\ (x_1, \dots, x_n) &\mapsto [1 : x_1 : \cdots : x_n] \end{aligned}$$

Let A be a commutative ring,
$P_0, \dots, P_m \in A[X_0, \dots, X_N]$ be homogeneous polynomials
$J = (P_0, \dots, P_m)$
B be an A-algebra which is a principal ideal ring

$$Z_J(B) \subset \mathbb{P}^N(B) \supset \mathbb{A}^N(B)$$

then

$$Z_J(B) \cap \mathbb{A}^N(B) = V_{J_0}(B)$$

where $J_0 = \{P(1, X_1, \dots, X_N),\ P \in J\}$

Conversely
Let I be an ideal in $A[X_1, \dots, X_N]$
We want to define $J \subset A[X_0, \dots, X_N]$
so that for any B as above
(i) $V_I(B) = Z_J(B) \cap \mathbb{A}^N(B)$
(ii) Z_J minimal for that property
so J has to be maximal

Idea (suggested by HILBERT's Nullstellensatz)
$\tilde{I} = \{P \in A[X_0, \dots, X_N] \mid \exists m \in \mathbb{N},\ P^m(1, X_1, \dots, X_N) \in I\}$
It is an ideal of $A[X_0, \dots, X_N]$
Indeed if $P, Q \in \tilde{I}$
Then there exist $m, n \in \mathbb{N}$ such that

$$P^m(1, X_1, \dots, X_N),\ Q^n(1, X_1, \dots, X_N) \in I$$

By NEWTON's binomial formula

$$(P+Q)^{m+n}(1, X_1, \dots, X_N) \in I$$

So $P + Q \in \tilde{I}$
And you can check that it is stable by multiplication by an element of $A[X_0, \dots, X_N]$

Fact

$$Z_{\tilde{I}}(B) \cap \mathbb{H}^N(B) = V_I(B)$$

Proof

Let $(x_1, \dots, x_N) \in B^N$

if $(x_1, \dots, x_N) \in V_I(B)$

and $P \in \tilde{I}$, pick $m \in \mathbb{N}$ such that $P^m(1, x_N) \in I$

then

$$P(1, x_1, \dots, x_N) = 0$$

so $[1 : x_1 : \dots : x_N] \in Z_{\tilde{I}}(B)$

Conversely if $[1 : x_1 : \dots : x_N] \in Z_{\tilde{I}}(B)$

and $P(x_1, \dots, x_N) \in I$

let $d = \deg(P)$ total degree

and $\tilde{P} = x_0^d P\left(\frac{x_1}{x_0}, \dots, \frac{x_N}{x_0}\right) \in A[x_0, \dots, x_N]$

then $\tilde{P}(1, x_1, \dots, x_N) = P(x_1, \dots, x_N) \in I$

So $\tilde{P} \in \tilde{I}$

Thus $\tilde{P}(1, x_1, \dots, x_n) = 0$

and $P(x_1, \dots, x_n) = c$

so $(x_1, \dots, x_N) \in V_I(B)$ □

Terminology

$Z_{\tilde{I}}(B) - V_I(B)$ are called the points at ∞ of V_I.

N.B.

For efficiency sake, if $I = (P_1, \dots, P_m)$

we shall use

$$\tilde{I} = (\tilde{P}_1, \dots, \tilde{P}_m)$$

although the set we get is not necessarily minimal.

Example

Affine equation

$$Y^2 = X^3 + aX + b$$

projective equation

$$Y^2T = X^3 + aXT^2 + bT^3$$

points at ∞ correspond to $T=0$

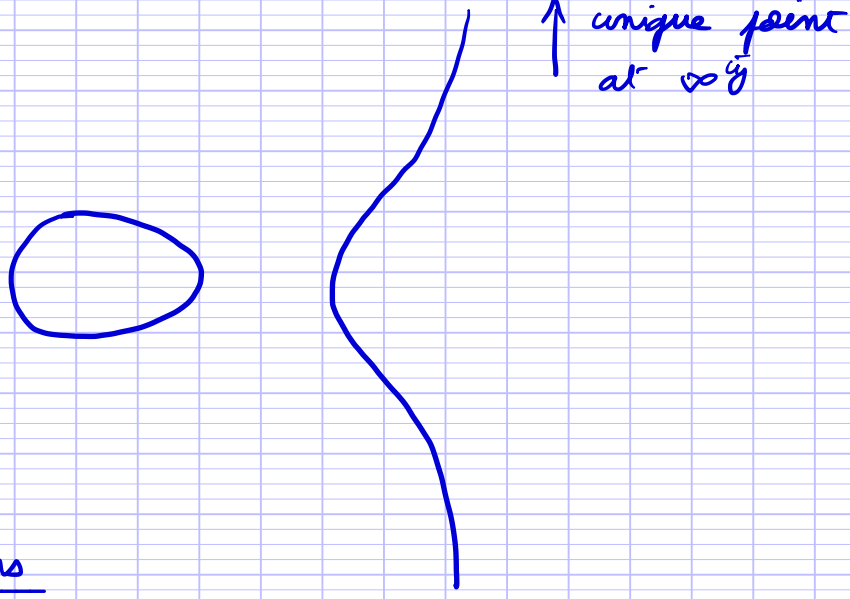
get $X^3 = 0$ so $X=0$

so there is a unique point at ∞ of

$$[0:0:1]$$

T X Y

(which is a triple point as we shall explain)



c) Morphisms

Principle

A morphism between algebraic spaces is a natural transformation which is everywhere defined by rational functions (quotients of polynomials)

Let me give an explicit and precise definition of what I mean by that

Definition (not simple)

Let K be a field, $\overline{K}$ an algebraic closure of K

$P_1, \dots, P_m \in K[X_0, \dots, X_N]$

and $Q_1, \dots, Q_n \in K[X_0, \dots, X_N]$ be homogeneous polynomials; Let $I = (P_1, \dots, P_m)$, $J = (Q_1, \dots, Q_n)$

A morphism $\phi : Z_I \longrightarrow Z_J$ is a

$\cap \qquad\qquad \cap$

$\mathbb{P}_M \qquad\quad \mathbb{P}_N$

natural transformation (ie for any K-algebra B which is a principal ideal ring (K-PIR)

$$\phi_B : Z_I(B) \longrightarrow Z_J(B)$$

such that for any morphism of K-PIRs $B \to C$

$$\begin{array}{ccc} Z_I(B) & \xrightarrow{\phi_B} & Z_J(B) \\ \downarrow & & \downarrow \\ Z_I(C) & \xrightarrow{\phi_C} & Z_J(C) \end{array}$$

commutes) defined as follows:

There exists

- integers $d_1, \dots, d_r$
- homogeneous polynomials of degree d_i

$$R_{i,0}, \dots, R_{i,N} \in K[X_0, \dots, X_m]$$

so that for all $[x_0 : \dots : x_m] \in Z_I(\overline{K})$

if we write $y_i = (R_{i,0}(x_0, \dots, x_m), \dots, R_{i,N}(x_0, \dots, x_m))$

(i) The y_i are collinear in $\overline{K}^{N+1}$

(ii) Not all y_i are 0

(iii) $\phi_{\overline{K}}([x_0 : \dots : x_m]) = \overline{\mathbb{K}}\, y_i$

In general, needs several families $(R_{i,0}, \dots, R_{i,N})$.

Remark

Using HILBERT's Nullstellensatz, the conditions (i), (ii) may be expressed using polynomials:

(i) $\exists\, m \in \mathbb{N}$ such that
$$\left(R_{i,k}R_{j,l} - R_{i,l}R_{j,k}\right)^m \in I$$

(ii) $\exists\, m \in \mathbb{N}$ such that
$$X_i^m \in (P_1, \dots, P_m, R_{i,k},\ 1 \le i \le r,\ 0 \le k \le N)$$

Definition

An isomorphism is a morphism $\varphi : Z_I \to Z_J$ such that there is a morphism $\psi : Z_J \to Z_I$ with $\psi \circ \varphi = Id_{Z_I}$ and $\varphi \circ \psi = Id_{Z_J}$.

Example

Assume $\mathrm{char}(\mathbb{K}) \neq 2$

Consider the projective curve associated to the circle
$$X^2 + Y^2 = 1$$
which corresponds to the homogeneous equation
$$S^1 \qquad X^2 + Y^2 = T^2$$

We have a morphism
$$\varphi : \mathbb{P}^1 \longrightarrow S^1$$
$$[U:V] \longmapsto [U^2+V^2 : 2UV : U^2-V^2]$$

φ is well defined if the characteristic is $\neq 2$:
if $(U^2+V^2,\ 2UV,\ U^2-V^2) = 0$
then $U = 0$ or $V = 0$ and thus $U = V = 0$

Let us prove that it is an isomorphism
$$\psi : S^1 \longrightarrow \mathbb{P}^1$$
$$[T:X:Y] \longmapsto [Y+T : X]$$ not defined for $[1:0:-1]$

$[T:X:Y] \longmapsto [X:Y-T]$ not defined for $[1:0:1]$

Both expressions coïncide on the circle:

$(Y+T)(Y-T) = Y^2 - T^2 = X^2$

Thus if $\mathrm{char}\, \mathbb{K} \neq 2$

$\mathbb{P}^1 \xrightarrow{\sim} S^1$

But we needed 2 polynomial expressions to define the inverse map.

N.B.

If $\mathrm{char}(\mathbb{K}) = 2$, one has

$X^2 + Y^2 - T^2 = (X+Y+T)^2$

Exercise

If $\mathrm{char}(\mathbb{K}) \neq 2$, $q \in \mathbb{K}[T,X,Y]$ a non degenerate isotropic quadratic form

$C: \; q(X,Y,T) = 0$

then there exists an isomorphism

$\mathbb{P}^1 \xrightarrow{\sim} C$.

3) Plane curves

a) Definition, smoothness

Definition

Let K be a field.

A plane curve is an algebraic subset of $\mathbb{P}^2_K$ defined by an homogeneous polynomial

$F \in K[T,X,Y]$ - dcy

The degree of the curve is the degree of P.

We say that the curve is geometrically irreducible if F is irreducible in $\overline{K}[T,X,Y]$.

We keep the notation K, F in the rest of this paragraph

Definition

Let C be the curve defined by F
Let L be a field extension of K
and let $P=[t:x:y] \in C(L)$

- We say that C is <u>smooth at P</u> if
$$\left(\frac{\partial F}{\partial x}(t,x,y), \frac{\partial F}{\partial y}(t,x,y), \frac{\partial F}{\partial z}(t,x,y)\right) = 0$$
- In that case the <u>tangent to C at P</u> is the projective line T defined by the equation
$$\frac{\partial F}{\partial T}(t,x,y)T + \frac{\partial F}{\partial x}(t,x,y)X + \frac{\partial F}{\partial Y}(t,x,y)Y = 0$$
- We say that P is a <u>singular point</u> of C if C is not smooth at P
- We say that C is <u>smooth</u> if $C(\bar{K})$ contains no singular point

Remark

(1) $\frac{\partial F}{\partial T}$, $\frac{\partial F}{\partial x}$ and $\frac{\partial F}{\partial y}$ are homogeneous of degree $d-1$ so the condition
$$\left(\frac{\partial F}{\partial T}(t,x,y), \frac{\partial F}{\partial x}(t,x,y), \frac{\partial F}{\partial y}(t,x,y)\right) = 0$$
does not depend on the choice of homogeneous coordinates.
Note also that the relation
$$F(UT, UX, UY) = U^d F(T,X,Y)$$
implies the relation (by taking the derivative

relative to U :

$$F(T,X,Y) = d\left(T\frac{\partial F}{\partial T}(T,X,Y) + X\frac{\partial F}{\partial X}(T,X,Y) + Y\frac{\partial F}{\partial Y}(T,X,Y)\right)$$

Thus if $P = [t : x : y]$,

$$\left(\frac{\partial F}{\partial T}(t,x,y), \frac{\partial F}{\partial X}(t,x,y), \frac{\partial F}{\partial Y}(t,x,y)\right) = 0 \Rightarrow P \in C(L).$$

Example (Hyperelliptic curve)

Let us consider the projective curve defined by the affine equation

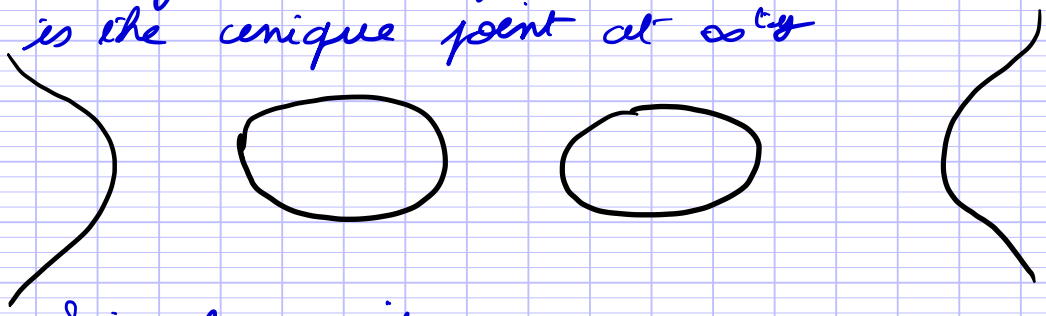
$$Y^2 = P(X)$$

where $P = a_d X^d + \dots + a_0$ with $a_d \neq 0$, $d \geq 2$

Then the projective equation is

$$Y^2 T^{d-2} = a_d X^d + a_{d-1} X^{d-1} T + \dots + a_0 T^d$$

Taking $T = 0$ we get that $(0 : 0 : 1)$ is the unique point at ∞



Singular points

$$\left((d-2)\, y^2 t^{d-3} - a_{d-1} x^{d-1} - \dots - d a_0 t^{d-1}, a_d d x^{d-1} + \dots + a_1 t^{d-1}, 2y t^{d-2}\right) = 0$$

so we get $y = 0$ or $t = 0$

If $y = 0$ then $t \neq 0$ and we may assume $t = 1$

we get $P(x) = P'(x) = 0$

so x is a multiple root of P

If $t = 0$ then $x = 0$ and $y = 1$

and the condition gives $d \geq 4$ or $d = 2$

So the curve is smooth if and only if $d = 3$ and P has no multiple root.

b) Intersection with a projective line

We keep the notation of the previous paragraph

Lemma

Let L be a field extension of K and let $D \subset \mathbb{P}^2_L$ be a projective line given by the equation

$$aT + bX + cY = 0$$

with $(a, b, c) \in L^3$ then

$$D \subset C$$

if and only if

$$aT + bX + cY \mid F$$

Proof

By the Nullstellensatz if $D(K) \subset C(K)$ then there exist $m \in \mathbb{N}$ such that

$$F^m \in (aT + bX + cY)$$

But since $L[T, X, Y]$ is a unique factorization domain, this implies that

$$aT + bX + cY \mid F$$

Remark

If the curve is of degree $d \geq 2$ and geometrically irreducible then this is not possible : the curve can not contain a line

Lemma

Let $P \in \overline{K}[U,V] - \{0\}$ be an homogeneous polynomial of degree d then there exists r elements $[u_i : v_i] \in \mathbb{P}^1(\overline{K})$, pairwise distincts and $m_1, \dots, m_r \in \mathbb{N} - \{0\}$ such that

$$P = \prod_{i=1}^{r} (v_i U - u_i V)^{m_i}$$

Moreover $m_1 + \dots + m_r = d$.

Proof

$P(U,1) \in \overline{K}[U]$ splits

we may write it

$$P(U,1) = a \prod_{i=1}^{k} (U - \alpha_i)^{m_i} \quad \text{with } a \neq 0$$

Then

$$P = a \left(\prod_{i=1}^{k} (U - \alpha_i V) \right) V^{d - m_1 - \dots - m_k}$$

By taking a d-th root of a we get the wanted expression. □

Notation

Let us define the abelian group of <u>divisors of</u> $\mathbb{P}^1_K$

$$\mathrm{Div}(\mathbb{P}^1_K) = \mathbb{Z}^{(\mathbb{P}^1(\overline{K}))}$$

$$= \left\{ (n_P)_{P \in \mathbb{P}^1(\overline{K})} \in \mathbb{Z}^{\mathbb{P}^1(\overline{K})} \;\middle|\; \#\{P \mid n_P \neq 0\} \text{ is finite} \right\}$$

$(n_P)_{P \in \mathbb{P}^1(\overline{K})}$ is denoted by $\sum_{P \in \mathbb{P}^1(\overline{K})} n_P P$

$$\deg : \mathrm{Div}(\mathbb{P}^1_K) \longrightarrow \mathbb{Z}$$

$$(n_P)_{P \in \mathbb{P}^1(\overline{K})} \longrightarrow \sum_{P \in \mathbb{P}^1(\overline{K})} n_P$$

Then we define the divisor of F as

$$\mathrm{div}(F) = \sum_{i=1}^{r} m_i [u_i : v_i] \in \mathrm{Div}(\mathbb{P}^1_K)$$

N.B.

$\deg(\operatorname{div}(F)) = \deg(F)$

Remarks

(i) We get a morphism of monoids from

$\{\text{homogeneous polynomials}\} \longrightarrow \operatorname{Div}(\mathbb{P}^1_{\bar{K}})$

(ii) div is compatible with linear change of variables:

If E is a vector space of dimension 2 / $\bar{K}$

$F : E \to \bar{K}$ a homogeneous polynomial of deg d, we get

$$\operatorname{div}(F) \in \operatorname{Div}(\mathbb{P}^1(E))$$

(iii) $\operatorname{div}(F) = \operatorname{div}(G) \Rightarrow \exists \lambda \in \bar{K}^*,\ G = \lambda F$.

Definition

I assume that $D \nmid C$

Then up to an exchange of coordinates

We may assume D is given by

$$aT + bX + cY = 0$$

with $a \neq 0$ $\quad T = -\frac{b}{a}X - \frac{c}{a}Y$

The intersection $C \cap D$ is given by

$F_{|D}(X,Y) := F\left(-\frac{b}{a}X - \frac{c}{a}Y, X, Y\right) = 0$

$F_{|D}$ is homogeneous of degree $d = \deg(C)$.

We define the <u>intersection counted with multiplicities</u>

$$D \cap C = \operatorname{div}(F_{|D}) \in \operatorname{Div}(D)$$

We write

$$D \cap C = \sum_{P \in D(\bar{K})} m_P(D \cap C)\, P.$$

$m_P(D \cap C)$ is called the multiplicity of intersection of D and C at P.

Remarks

(i) Take $P \in D \subset \mathbb{P}^2(\overline{K})$

Then P corresponds to a line in $\overline{K}^3$

and $D = \mathbb{P}(\tilde{D})$ for $\tilde{D}$ a plane in $\overline{K}^3$

We choose a basis (e_0, e_1, e_2) of $\overline{K}^3$

with $e_0 \in P$, $e_1 \in \tilde{D}$

Then in the coordinates (T, X, Y) given by this basis

$P = [1:0:0]$

and $D : Y = 0$

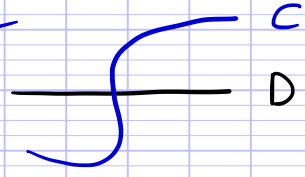
Then $m_P(D \cap C) = v_X(F(T, X, 0))$

$= \max\{m \mid X^m \mid F(T, X, 0)\}$

(ii) if $P \in D$

$m_P(D \cap C) = 0 \iff P \notin C$

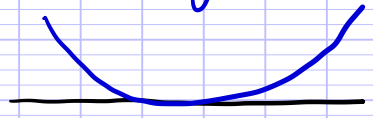
$m_P(D \cap C) = 1$ corresponds to a normal crossing

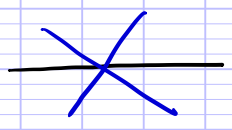


(iii) $m_P(D \cap C) \geq 2$

P is a singular point of C

or D is tangent to C at P





Indeed take a basis (e_0, e_1, e_2)

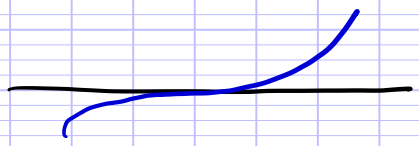
as above. Then

$$F(e_0 + Xe_1) = F(e_0) + X\,dF_{e_0}(e_1) + X^2 Q(T)$$

$m_P(D \cap C) \geq 2$ corresponds to $F(e_0) = 0$

and $dF_{e_0}(e_1) = 0$

(iv) $m_P(\tilde{D}^{e_0} \cap C) = 3$ If P is not singular implies that C is tangent to D and cross the tangent



Terminology

If $m_P(D \cap C)$ for some line D, then one says that P is an inflection point of the curve.

Lemma

Let D be a line in $\mathbb{P}^2(K)$ such that there exists $P_1, \dots, P_{d-1} \in \mathbb{P}^2(K)$ with

$$\deg\left(\operatorname{div}(F_D) - \sum_{i=1}^{d-1} P_i\right) = 1$$

(all intersection points but 1 have coordinates in K)

Then there exists $P_d \in \mathbb{P}^1(K)$ such that

$$\operatorname{div}(F_D) = \sum_{i=1}^{d} P_i$$

Proof

$D : aT + bX + cY = 0$ with $a, b, c \in K$

May assume $a \neq 0$

Then

$$F_D(X,Y) = F\left(-\frac{b}{a}X - \frac{c}{a}Y, X, Y\right) \in K[X,Y]$$

and if we write

$P_i = [t_i : x_i : y_i]$ with $t_i, x_i, y_i \in K$ for $i \in \{1, \dots, d\}$

Then F_D is divisible by

$$\prod_{i=1}^{d-1} (y_i X - x_i Y)$$

and the quotient is a homogeneous polynomial

of degree 1 in $K[X,Y]$ we may write as

$$y_d Y - x_d X$$

and like

$$P_d = \left[-\frac{b}{a} x_d - \frac{c}{a} y_d : x_d : y_d \right] . \quad \square$$

3] Elliptic curves

Reference

A. W. KNAPP, Elliptic curves, Math Notes 40, PRINCETON UNIVERTY PRESS

a] Definition, Weierstrass form

Definition

An elliptic curve over a field K is a smooth plane curve of degree 3 equipped with a point $O \in E(K)$.

A morphism of elliptic curves $\varphi : E \to E'$ is a morphism of algebraic subsets this gives a notion of isomorphisms

Theorem (NAGELL)

Any elliptic curve is isomorphic to an elliptic curve given by an affine equation

$$Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6$$

with $O = [0:0:1]$ the unique point at ∞^y.

If $\mathrm{char}(K) \neq 3$ we may assume that $a_2 = 0$

If $\mathrm{char}(K) \neq 2$ we may assume that $a_1 = a_3 = 0$

Terminology

Such an elliptic curve is said to be in WEIERSTRAß form

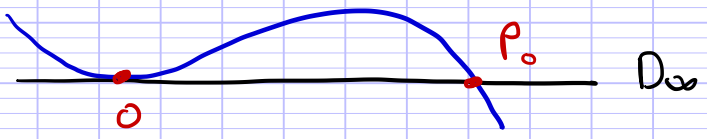
Remark

Assume that E is in WEIERSTRAß form
let D_∞ be the line at ∞ given by $T=0$
then $F_{|D_\infty}(X,Y) = X^3$
so O is an inflection point of E
(this means the isomorphism is not simply a linear change of coordinates. We have to make O one of the inflection point)

Proof

1st step

Let D_∞ be the tangent to E at O
By the last lemma I proved
$\operatorname{div}(F_{|D_\infty}) = 2O + P_0$ with $P_0 \in E(K)$



If $P_0 = O$ then O is already on inflection point
assume $P_0 \neq O$
We want to make O into an inflection point
We are going to use a special transformation of the projective plane : The Cremona tranformation

CREMONA involution

The map $\sigma : [T:X:Y] \to \left[\frac{1}{T} : \frac{1}{X} : \frac{1}{Y}\right]$ defines

an involution on $\mathbb{P}^2(K) - \{[1:0:0], [0:1:0], [0:0:1]\}$
that is $\sigma^2 = Id$ outside $XYT = 0$

N.B.

(i) $\left[\frac{1}{T} : \frac{1}{X} : \frac{1}{Y}\right] = [XY : YT : TX]$
so it is indeed defined outside the 3 points

(ii) The line $T=0$ is mapped to the point $[1:0:0]$
——— $X=0$ ——— $[0:1:0]$
——— $Y=0$ ——— $[0:0:1]$
σ^2 defined outside $XYT=0$

If we choose 3 points on the plane which are not aligned then we can defined a similar transform outside these points
The nice thing is that if we take a plane curve then the restriction of the involution to the curve can be extended in an isomorphism of curves, as we shall see
We have to choose the points carefully
Assume that there exists a point $P_1 \in E(K) - D_\infty$ such that the projective line $D_1 = (O P_1)$ is not tangent to E in P_1.
Then $Div(F_{D_1}) = O + P_1 + P_2$ with $P_2 \in E(K)$
By a linear change of coordinates we may assume
$P_0 = [1:0:0]$, $P_1 = [0:1:0]$ and $P_2 = [0:0:1]$
Since P_1, P_2 and O are aligned and distinct we may further assume that $O = [0:1:1]$
Then $D_\infty : X = Y$

Now let us consider the coefficients of F in that choice of coordinates

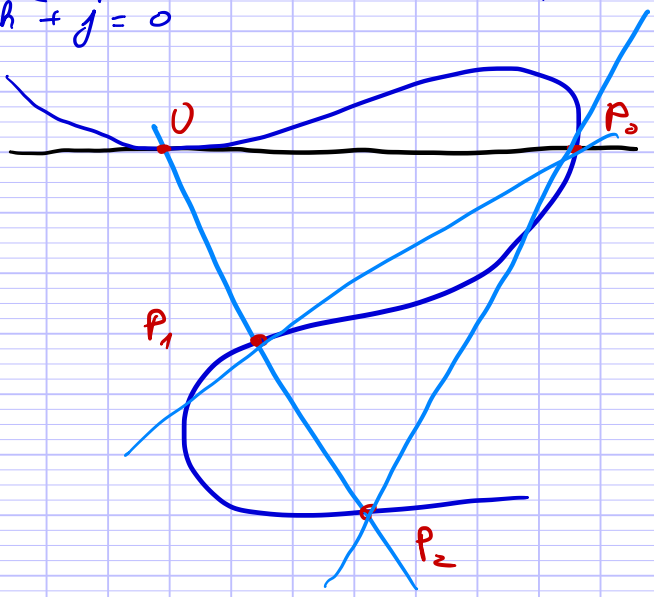
$$F(T,X,Y) = aX^3 + bY^3 + cT^3 + dX^2Y + eXY^2 + fX^2T + gXT^2 + hY^2T + iYT^2 + jXYT$$

Since $P_0, P_1, P_2 \in E(K)$, we get $a = b = c$

$O \in E(K)$ give $d + e = 0$ and

since $\left(\frac{\partial F}{\partial T}(0,1,1), \frac{\partial F}{\partial X}(0,1,1), \frac{\partial F}{\partial Y}(0,1,1)\right) = (f+h+j, 2d+e, d+2e)$

$f + h + j = 0$



Let us apply CREMONA involution with that choice of coordinates

The equation of $\sigma(E)$ is given by

$$F\left(\frac{1}{T}, \frac{1}{X}, \frac{1}{Y}\right) = 0$$

But

$$T^2X^2Y^2 F\left(\frac{1}{T}, \frac{1}{X}, \frac{1}{Y}\right) = dYT^2 + eXT^2 + fY^2T + gY^2X + hX^2T + iX^2Y + jXYT$$

$!!$

$F^\sigma(T,X,Y)$

defines an elliptic curve E^σ, $O^\sigma = \sigma(O) = [1:0:0]$

The tangent to E^σ at O^σ is given by
$dY + cX = 0$ that is $X = Y$.
$F^\sigma_{|D_\infty} = (d+e)XT^2 + (f+h+j)X^2T + (g+i)X^3$
$= (g+i)X^3$
So O^σ is an inflection point of E^σ.
Remains to extend the morphism to the whole of E
The equation of E might be written as
$F(T,X,Y) = XY(dX+eY) + TG(T,X,Y)$
So on E
$[XY : YT : TX] = [XY(dX+eY) : YT(dX+eY) : TX(dX+eY)]$
$= [G(T,X,Y) : Y(dX+eY) : X(dX+eY)]$
well defined in $[0:0:1]$ and $[0:1:0]$.
By exchanging the variables we get a polynomial expression everywhere.

Now I made an hypothesis about the existence of another point on $E(K)$ with some conditions, but in general, such a point may not exist!

Almost general case

Take a line D in $\mathbb{P}^2(K)$ going through O
Assume it is not tangent to E (in particular $D \neq D_\infty$)
Then since $O \in E(K) \cap D$
$F_{|D}$ is divisible by a polynomial of degree 1 vanishing at O.
Let Q be the quotient, if it is not irreducible then we get two points P_1 and P_2 and we may apply the previous construction
We now assume Q is irreducible

After a linear change of variables we may assume that

$O = [0:0:1]$ _ $P_0 = [0:1:0]$

and $D : X = 0$

we may write Q as $a_1 Y^2 + b_1 Y T + c_1 T^2$

with $a_1 Y^2 + b_1 Y + c_1$ irreducible (and $a \neq 0$)

Let $L = K[Y]/(Q(1,Y))$ (quadratic extension of K) and let α and $\bar{\alpha}$ be the two roots of $Q(1,Y)$ in L

Note that $\alpha + \bar{\alpha} = -\frac{b_1}{a_1}$ and $\alpha\bar{\alpha} = \frac{c_1}{a_1}$.

Over L we may use the CRÉMONA transform in the points

$P_0 = [0:1:0]$ $P_1 = [1:0:\alpha]$ and $P_2 = [1:0:\bar{\alpha}]$

which gives the isomorphism φ we are looking for over L

Fact

In fact, φ is defined over K (which means that it is given by polynomials with coefficients in K).

Proof of the fact

Let

$$M = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & \alpha & \bar{\alpha} \end{pmatrix}, \quad \det(M) = \alpha - \bar{\alpha} \neq 0$$

Since Q is irreducible.

$$M^{-1} = \frac{1}{\alpha - \bar{\alpha}} \begin{pmatrix} 0 & \alpha - \bar{\alpha} & 0 \\ -\bar{\alpha} & 0 & 1 \\ \alpha & 0 & -1 \end{pmatrix}$$

Then φ is given the composite map

$$M \circ [x:y:z] \mapsto \left[\frac{1}{x}:\frac{1}{y}:\frac{1}{z}\right] \circ M^{-1}$$

where M denotes the action of Γ on the projective space. Let us compute that

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & \alpha & \bar{\alpha} \end{pmatrix} \cdot \left[\frac{1}{X} : \frac{\alpha-\bar{\alpha}}{-\bar{\alpha}T+Y} : \frac{\alpha-\bar{\alpha}}{\alpha T-Y}\right]$$

$$= \left[\frac{\alpha-\bar{\alpha}}{-\bar{\alpha}T+Y} + \frac{\alpha-\bar{\alpha}}{\alpha T-Y} : \frac{1}{X} : \alpha\frac{\alpha-\bar{\alpha}}{-\bar{\alpha}T+Y} + \bar{\alpha}\frac{\alpha-\bar{\alpha}}{\alpha T-Y}\right]$$

$$= \left[\frac{(\alpha-\bar{\alpha})(\alpha-\bar{\alpha})T}{-\alpha\bar{\alpha}T^2+(\alpha+\bar{\alpha})YT-Y^2} : \frac{1}{X} : \frac{-(\alpha-\bar{\alpha})(\alpha-\bar{\alpha})Y}{-\alpha\bar{\alpha}T^2+\alpha+\bar{\alpha}YT-Y^2}\right]$$

$$(\alpha-\bar{\alpha})(\alpha-\bar{\alpha}) = (\alpha+\bar{\alpha})^2 - 4\alpha\bar{\alpha} = \frac{b_1^2-4a_1c_1}{a_1^2} = \frac{\Delta}{a_1^2}$$

$$-\alpha\bar{\alpha}T^2+\alpha\bar{\alpha}YT-Y^2 = \frac{-1}{a_1}Q$$

get

$$\varphi : [X:Y:Z] \longmapsto \left[\frac{-\Delta T}{a_1 Q} : \frac{1}{X} : \frac{\Delta Y}{a_1 Q}\right]$$

is defined over K. □

End of the proof

Are we sure that there exist a line D through O not tangent to E?

$F = \cancel{aX^3} + \cancel{bY^3} + cT^3 + dX^2Y + \cancel{eXY^2} + fX^2T + gXT^2 + hY^2T + iYT^2 + jXYT = 0$

with $a, b, c, \ldots, j \in K$

We may again assume that $O = [0:0:1]$ and $P_0 = [0:1:0]$

which implies

$F(0,0,1) = b = 0 \qquad F(0,1,0) = a = 0$

and $\frac{\partial F}{\partial X}(0,0,1) = e = 0, \quad \frac{\partial F}{\partial T}(0,0,1) = h \neq 0$

If $P = [1 : x : y] \in E(K)$ the line (OP) is the vertical line $X = xT$

It is tangent to E if

$$\frac{\partial F}{\partial Y}(1, x, y) = 0$$

which gives the equations

$$\begin{cases} dx^2 + 2hy + i + jx = 0 \\ c + fx^2 + gx - hy^2 = 0 \end{cases}$$

given by $F(1, x, y) - y \frac{\partial F}{\partial Y}(1, x, y) = 0$

If $\mathrm{char}(K) = 2$ get 2 possible values for x (since $D_\infty \notin E$, $d \neq 0$)

If $\mathrm{char}(K) \neq 2$ at most 4 possible values for x

If $K \neq \mathbb{F}_2$ and $K \neq \mathbb{F}_3$ We may choose x outside these values.

If K is $\mathbb{F}_2$ or $\mathbb{F}_3$ one may have to apply two CREMONA involutions. I spare you the details

---

Final steps

We now assume that $O = [0 : 0 : 1]$ is an inflection point with $D_\infty : T = 0$

Write again

$$F = aX^3 + bY^3 + cT^3 + dX^2Y + eXY^2 + fX^2T + gXT^2 + hY^2T + iYT^2 + jXYT = 0$$

with $a, b, c, \ldots, j \in K$

$F(0, 0, 1) = b = 0$

$F_{|D_\infty} = aX^3 + dX^2Y + eXY^2 \Rightarrow d = e = 0$

and $a \neq 0$. We may divide F by $-a$

and, by taking one more change of coordinates assume that

$$\frac{\partial F}{\partial T}(0,0,1) = h = 1$$

We get the equation

$$Y^2T + jXYT + iYT^2 = X^3 - fX^2T - hXT^2 - cT^3$$

as wanted

If $\mathrm{char}\,K \neq 2$ taking $Y' = Y + \frac{a_1}{2}X + \frac{a_2}{2}T$ enables to reduce to $a_1 = a_3 = 0$

If $\mathrm{char}\,K \neq 3$ taking $X' = X + \frac{a_2}{3}T$ enables to reduce to $a_2 = 0$ □

Proposition

Let E be an elliptic curve in WEIERSTRAß form

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

Put

$$b_2 = a_1^2 + 4a_2$$
$$b_4 = 2a_4 + a_1a_3$$
$$b_6 = a_3^2 + 4a_6$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

then E is smooth if and only if

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \neq 0$$

Remark

If $\mathrm{char}(K) \notin \{2, 3\}$ then the equation might be reduced to

$$Y^2 = X^3 + aX + b$$

and the condition reduces to

$$27b^2 + 4a^3 \neq 0$$

Proof

When $\mathrm{char}(K) \notin \{2,3\}$

We have seen that E is smooth if and only if the roots of $X^3 + aX + b$ in $\overline{K}$ are $\neq$. Let us compute

$$\Delta(P) = \mathrm{Res}(P,P') = \begin{vmatrix} 1 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 3 & 0 \\ a & 0 & a & 0 & 3 \\ b & a & 0 & a & 0 \\ 0 & b & 0 & 0 & a \end{vmatrix} = \begin{vmatrix} -2a & 0 & 3 \\ -3b & -2a & 0 \\ 0 & -3b & a \end{vmatrix}$$

$$= 4a^3 + 27b^2. \quad \square$$

b) Group structure

In this paragraph, E is an elliptic curve in WEIERSTRÁß form

$$Y^2T + a_1XYT + a_3YT^2 = X^3 + a_2X^2T + a_4XT^2 + a_6T^3$$

$$\| \quad YT(Y + a_1X + a_3T)$$

with $a_1 = a_3 = 0$ if $\mathrm{char}(K) \neq 2$

and $a_2 = 0$ if $\mathrm{char}(K) \neq 3$

F_1 is the corresponding homogeneous polynomial.

Definition

We say 3 points $P, Q, R \in E(K)$ are aligned if there exists a projective line D such that

$$\mathrm{div}(F_D) = P + Q + R$$

Aim

Define a group law on $E(K)$ characterized by the 2 conditions

(i) O is the neutral element

(ii) $P+Q+R=O \Leftrightarrow P, Q, R$ are aligned

Remarks

(i) With these conditions

$$P+Q=O \Leftrightarrow P+Q+O=O$$
$$\Leftrightarrow P, Q, O \text{ are aligned}$$

But since $O=[0:0:1]$

if $P=[1:x_P:y_P]$ and $Q=[1:x_Q:y_Q]$

$P=-Q \Leftrightarrow x_P=x_Q$.

Note that map $-: E \longrightarrow E$

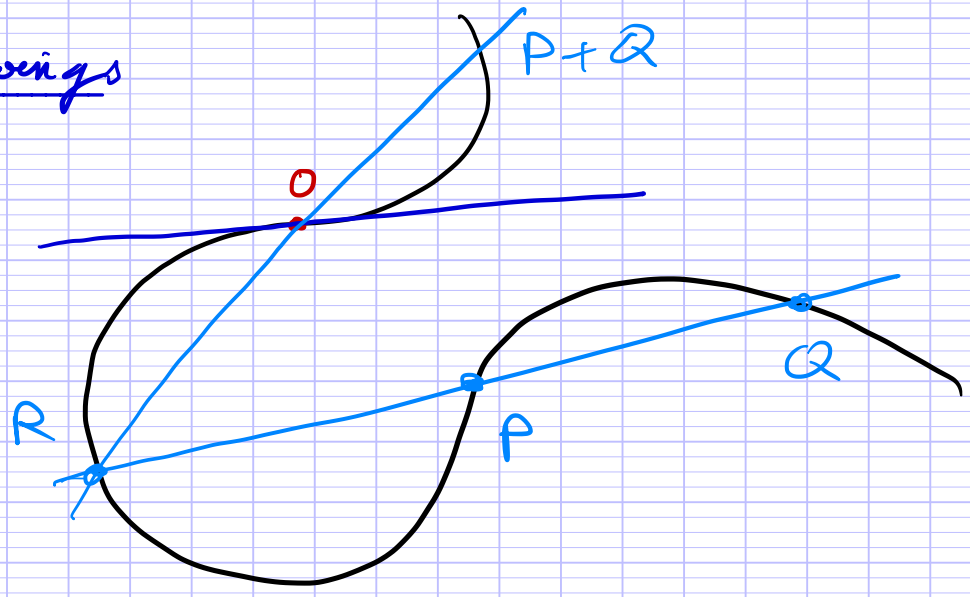
$$[T:X:Y] \longmapsto [T:X:-Y+a_1X+a_3T]$$

Defines an involution of E with $-O=O$ and $P, -P, O$ aligned for any $P \in E(K)$.

(Remember that $a_1=a_3=0$ if $\mathrm{char}(K) \neq 2$)

(ii) $P+Q+R=O \Leftrightarrow R=-(P+Q)$.

Drawings



Notation

In this paragraph, if $P, Q \in E(K)$, we denote by $P * Q$ the unique point of $E(K)$ such that P, Q and $P * Q$ are aligned

Theorem (POINCARÉ)

$$+ : E(K) \times E(K) \longrightarrow E(K)$$
$$(P, Q) \mapsto ((P * Q) * O)$$

defines a commutative group structure on $E(K)$.

Beginning of the proof

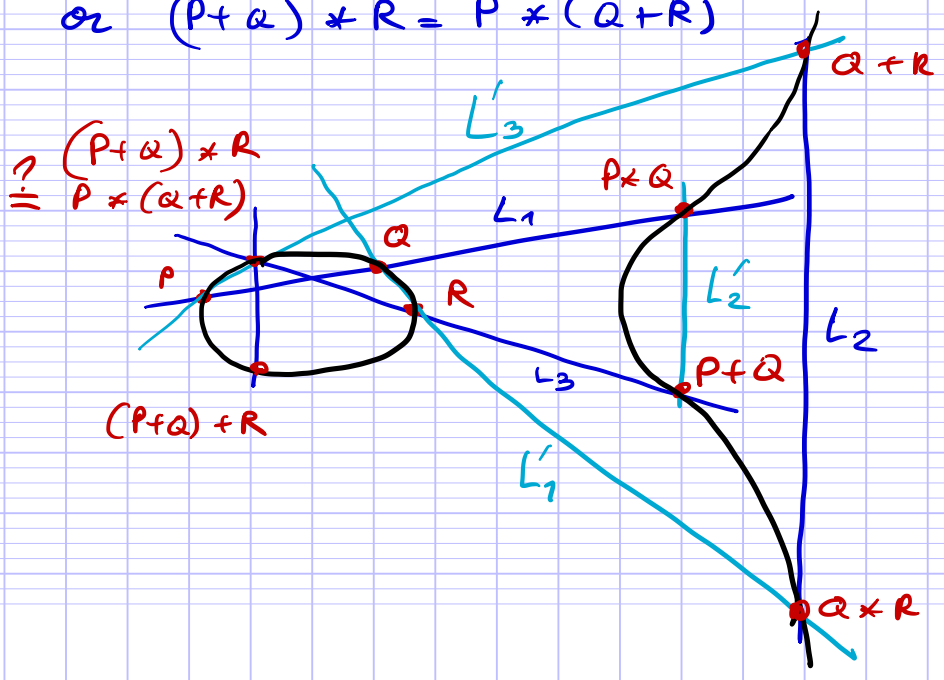
- $P + O = ((P * O) * O) = P$ since P, O and $O * P$ are aligned
- $P + (-P) = O$ since O, P and $-P$ are aligned
- $P + Q = ((P * Q) * O) = ((Q * P) * O) = Q + P$

So the only difficulty is to prove that the law is associative

Remains to prove:

$$(((P * Q) * O) * R) * O = (P * ((Q * R) * O)) * O$$

or $(P + Q) * R = P * (Q + R)$



enough to prove

$\forall P, Q, R, S \in E(K) \quad (P * Q) * (R * S) = (P * R) * (Q * S)$

implies

$P * (Q+R) = ((P * Q) * Q) * (O * (Q * R)) = ((P * Q) * O) * (Q * (Q * R))$

We have to consider the following nine points on the curve

P, Q, R, S

$P * Q$, $P * R$

$Q * S$, $R * S$

$(P * Q) * (R * S) \overset{?}{=} (P * R) * (Q * S)$

These 8 first points are all on

- The elliptic curve E
- The union of 3 lines

$L_1 = (PQ) \ni P * Q$

$L_2 = (RS) \ni R * S$

$L_3 = ((P * R)(Q * S))$

- The union of 3 lines

$L'_1 = (PR) \ni P * R$

$L'_2 = (QS) \ni Q * S$

$L'_3 = ((P * Q)(R * S))$

$(P * R) * (Q * S) \in E(K) \cap (L_1 \cup L_2 \cup L_3)$

$\overset{?}{=}$

and $(P * Q) * (R * S) \in E(K) \cap (L'_1 \cup L'_2 \cup L'_3)$

Reminder

$E \cap$ 3 lines contains, if we count multiplicities, exactly 9 points

So this determines $(P * R) * (Q * S)$ (resp. $(P * Q) * (R * S)$) as the ninth point of intersection

It suffices to show that these two intersections are the same

Remark

$L_1 \cup L_2 \cup L_3$ (resp. $L'_1 \cup L'_2 \cup L'_3$) is an algebraic set defined by the product F_2 (resp. F_3) of three linear forms

So they are plane curves of degree 3

In other words, we have three plane curves of degree 3 going through 8 points. What can we say about the set of such curves

Let us consider the equations of plane curves of degree 3:

$$F(T,X,Y) = aX^3 + bY^3 + cT^3 + dX^2Y + eXY^2 + fX^2T + gXT^2 + hY^2T + iYT^2 + jXYT$$

The algebraic set defined by F does not change if we multiply F by a non zero constant

So we get an element

$$[F] = [a:b:c:d:e:f:g:h:i:j] \in \mathbb{P}^9(K)$$

The condition

$$P = [t:x:y] \in Z_F(K)$$

is given by

$$x^3a + y^3b + t^3c + x^2y\,d + xy^2e + x^2tf + xt^2g + y^2th + yt^2i + xyt\,j = 0$$

(with t, x, y given and $a, b, c, \dots, j$ as variables)

So the set of F of degree 3 such that $Z_F(K)$ contains 8 points is given by the intersection of 8 projective hyperplanes in $\mathbb{P}^8(K)$

If the equations of these eight hyperplanes are linearly independant then this set is a projective line in $\mathbb{P}^3(K)$
If this is the case then the equations of the 3 planes curves above are linearly dependant; let us denote them by F_1, F_2, F_3
Since F_1 and F_2 are linearly independant (since the sets they define are $\neq$) we can write

$$F_3 = \alpha F_1 + \beta F_2$$

and $Z_{F_1}(K) \cap Z_{F_2}(K) \subset Z_{F_3}(K) \cap Z_{F_1}(K)$.
We get (by exchanging F_2 and F_3)

$$Z_{F_1} \cap Z_{F_2}(K) = Z_{F_1} \cap Z_{F_3}(K)$$

and therefore

$$(P*Q)*(R*S) = (P*R)*(Q*S)$$

Problem

Are the equations of the 8 hyperplanes linearly independant ?

As written, false if 2 of the points coincide!
Let us check that more carefully :

1st case "general case"

the 8 points are distinct
($\Rightarrow$ among P, Q, R, S no three are aligned)
Then (P, Q, R, S) is a projective frame of $\mathbb{P}^3(K)$
Therefore, by a linear change of variable, we may assume

$P = [1:0:0]$

$Q = [0:1:0]$

$R = [0:0:1]$

$S = [1:1:1]$

$P*Q = [1:x_1:0]$ with $x_1 \neq 0$

$P*R = [1:0:y_1]$ with $y_1 \neq 0$

$Q*S = [1:x_2:1]$ with $x_2 \notin \{0,1\}$ (otherwise $P*R = Q*S$)

$R*S = [1:1:y_2]$ with $y_2 \notin \{0,1\}$ (otherwise $P*Q = R*S$)

Let us now consider the matrix

T^3	X^3	Y^3	XYT	XT^2	YT^2	X^2Y	XY^2	
1	0	0	0	0	0	0	0	P
0	1	0	0	0	0	0	0	Q
0	0	1	0	0	0	0	0	R
1	1	1	1	1	1	1	1	S
1	x_1^3	0	0	x_1	0	0	0	$P*Q$
1	0	y_1^3	0	0	y_1	0	0	$P*R$
1	x_2^3	1	x_2	x_2	1	x_2^2	x_2	$Q*S$
1	1	y_2^3	y_2	1	y_2	y_2	y_2^2	$R*S$

It is enough to prove that this matrix is invertible. We are going to do elementary transformation on this matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & x_1 \neq 0 & 0 & 0 & 0 \\ 0 & 0 & y_1 \neq 0 & 0 & 0 \\ x_2 & 0 & 1-x_2 & x_2(x_2-1) \neq 0 & 0 \\ y_2 & 1-y_2 & 0 & 0 & y_2(y_2-1) \neq 0 \end{bmatrix}$$

We get the 8 linear forms are linearly independant. and thus
$(P+Q)*R = P*(Q+R)$ as wanted.

I shall now give several proof for the other cases :

Over $\mathbb{C}$

The map

$$E(\mathbb{C})^4 \longrightarrow E(\mathbb{C})$$
$$(P,Q,R,S) \longmapsto (P*Q)*(R*S)$$

is continuous as the map

$$(P,Q,R,S) \longmapsto (P*R)*(Q*S)$$

So

$F = \{(P,Q,R) \in E(\mathbb{C})^3 \mid (P*Q)*(R*S) = (P*R)*(Q*S)\}$

is closed. But the set

$\{(P,Q,R) \in E(\mathbb{C})^3 \mid \#\{P,Q,R,S,P*Q,P*R,Q*S,R*S\} = 8\}$

is a dense open set in $E(\mathbb{C})^3$ contained in F

Therefore

$$E(\mathbb{C})^3 = F.$$

Over a field K of characteristic 0

$$E : y^2 = x^3 + ax + b$$

Let $K_0 = \mathbb{Q}(a_1, a_3, a_2, a_4, a_6) \subset K$

Then E is defined over K_0

Since K_0 is a finitely generated extension of $\mathbb{Q}$, there exists a morphism of fields

$$\sigma : K_0 \hookrightarrow \mathbb{C}$$

which induces

$$\overline{\sigma} : K_0 \hookrightarrow \mathbb{C}$$

since the result is true over $\mathbb{C}$ it is true over $\overline{K_0}$
and by Hilbert's Nullstellensatz,
it is true over $\overline{K}$.

* Using algebraic geometry over arbitrary fields

E is geometrically irreducible.

Thus $E \times E \times E \times E$ is (geometrically) irreducible

$F = \{(P,Q,R,S) \in E^4 \mid (P*Q)*(R*S) = (P*R)*(Q*S)\}$

is a closed subset of E^4 (for Zariski topology)

as is

$G = \{(P,Q,R,S) \in E^4 \mid \#\{P,Q,R,S,P*Q,P*R,Q*S,R*S\} < 8\}$

and $G \neq E^4$

since $E^4 = F \cup G$ and is irreducible

$= F$ (definition of irreducible) $*$

Computations

If two of the points are equal

Let T be the tangent to E at this point S

and let (L_1, L_2, L_3) be one of the triple of lines going through all the points

then

- either one of the line is T
- or two of the lines go through the point S

In both case if F_2 is the product of the linear forms defining the lines, we get

$$d_S F_2(\hat{T}) = 0$$

where $T = \mathbb{P}(\hat{T})$. We get a new linear condition on the coefficients of the homogeneous polynomials of degree 3 (details left as exercise)

[Let us for example assume $P = Q$, with
$\#\{P, Q, R, S, P*Q, P*R, Q*S, R*S\} = 7$
After a linear change of variables,
we may assume
$P = Q = [1:0:0]$
The tangent to E at P is $Y = 0$
$R = [0:0:1]$
$S = [1:1:1]$
$P*Q = [1:x_1:0]$ with $x_1 \neq 0$
$P*R = [1:0:y_1]$ with $y_1 \neq 0$
$Q*S = [1:x_2:x_2]$ with $x_2 \notin \{0,1\}$
$R*S = [1:1:y_2]$ with $y_2 \notin \{0,1\}$
which gives the matrix

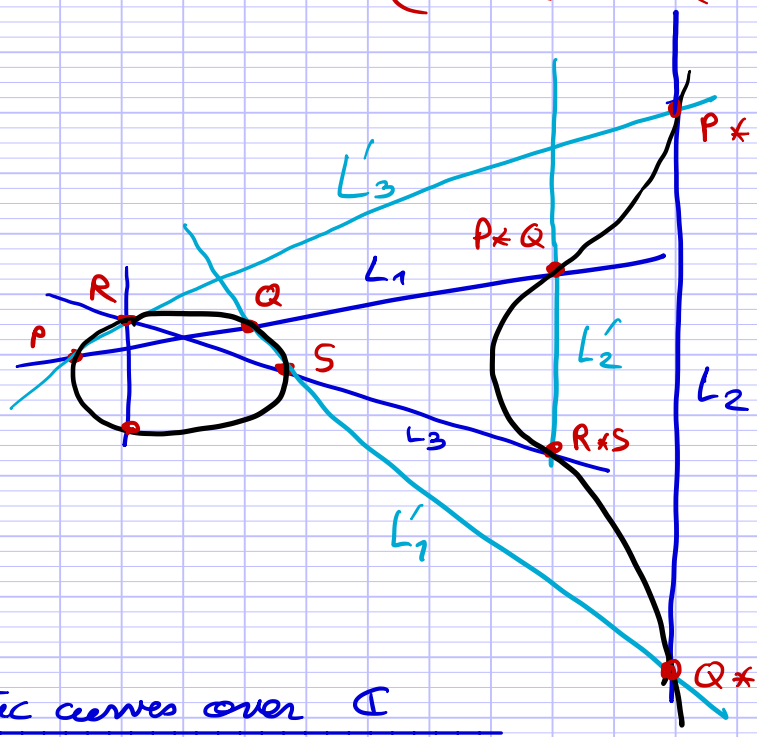
T^3	XT^2	Y^3	XYT	X^2T	YT^2	Y^2X	XY^2	
1	0	0	0	0	0	0	0	P
0	1	0	0	0	0	0	0	$2P$
0	0	1	0	0	0	0	0	R
1	1	1	1	1	1	1	1	S
1	x_1	0	0	x_1^2	0	0	0	$P*Q$
1	0	y_1^3	0	0	y_1	0	0	$P*R$
1	x_2	x_2^3	x_2^2	x_2^2	x_2	x_2^3	x_2^3	$Q*S$
1	1	y_2^3	y_2	1	y_2	y_2	y_2^2	$R*S$

and then

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & x_1^2 \neq 0 & 0 & 0 & 0 \\ 0 & 0 & y_1 \neq 0 & 0 & 0 \\ x_2^2 & 0 & x_2(1-x_2) & x_1^2(x_2-1) \neq 0 & x_2^2(x_2-1) \\ y_2 & 1-y_2 & 0 & 0 & y_2(y_2-1) \neq 0 \end{bmatrix}$$

By symmetry, this works also if $P = R$ or $Q = S$ or $R = S$.]

$(P*Q)*(R*S) \overset{?}{=} (P*R)*(Q*S)$



c) Elliptic curves over $\mathbb{C}$

This will be a reminder for those of you we took a course on Riemann surfaces

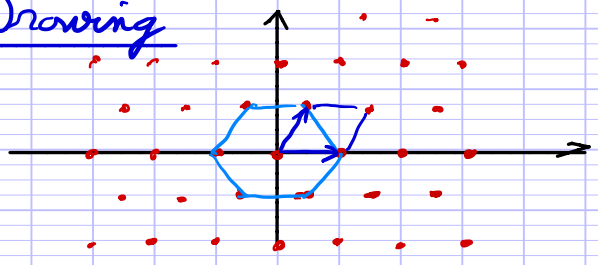
Definition

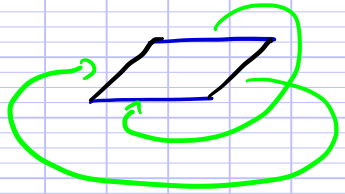
A torus is a Riemann surface obtained as a quotient

$$T = \mathbb{C}/\Lambda$$

where $\Lambda \subset \mathbb{C}$ is a lattice, that is a subgroup generated by a basis of the $\mathbb{R}$-vector space $\mathbb{C}$.

Drawing





Remark

Taking (e_1, e_2) as a basis we may assume it is direct, that is $\tau = e_2/e_1$ satisfies $\mathrm{Im}(\tau) > 0$. Then

$$\begin{aligned} \mathbb{C}/\Lambda &\longrightarrow \mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau \\ \overline{z} &\longmapsto \overline{z/e_1} \end{aligned}$$

is an isomorphism, so we may assume that $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, with $\mathrm{Im}(\tau) > 0$.

Proposition / Definition

The series

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda - \{0\}} \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}$$

converges uniformly on any compact subset of $\mathbb{C} - \Lambda$ and defines a meromorphic function on $\mathbb{C}$ which is Λ-periodic and even

$$\wp'(z) = \sum_{\lambda \in \Lambda} \frac{-2}{(z-\lambda)^3}$$

The set of poles is Λ, each pole has order 2.

Proof

- $$\left| \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right| = \left| \frac{(\lambda + z - \lambda)(\lambda - z + \lambda)}{\lambda^2 (z-\lambda)^2} \right|$$

$$= \left| z \, \frac{2\lambda - z}{\lambda^2 (z-\lambda)^2} \right| \leq |z| \, \frac{2|\lambda| + |z|}{|\lambda|^2 (|\lambda| - |z|)^2}$$

$$\leq 10\,|z| \, \frac{1}{|\lambda|^3}$$

if $|z| \leq R$ and $|\lambda| \geq 2R$.

- $|\cdot|$ and $\|x+\tau y\| = \max(|x|,|y|)$ define equivalent norms

So

$$\sum_{|\lambda|\geq 2R} \frac{1}{|\lambda|^3} \leq C \sum_{(m,n)\neq(0,0)} \frac{1}{\max(m,n)^3} = 8C \sum_n \frac{n}{n^3} < +\infty$$

The fact that $\wp$ is meromorphic, the formula for $\wp'$ and the description of the poles follows from a standard theorem on series of meromorphic functions.

By definition it is even and $\wp'$ is Λ-periodic

So for any $\lambda \in \Lambda$ $\wp(z+\lambda) - \wp(z)$ is constant

for $\lambda = 1$ or τ

$$\wp(-\tfrac{1}{2}) = \wp(\tfrac{1}{2})$$

and

$$\wp(-\tfrac{\tau}{2}) = \wp(\tfrac{\tau}{2})$$

So $\wp$ is Λ periodic. □

Remark

$\mathcal{G}$ induces a meromorphic function

$$\wp : T = \mathbb{C}/\Lambda \longrightarrow \mathbb{P}^1(\mathbb{C})$$

with a unique pole of order 2 at $\overline{0}$.

Definition

For any integer $j \geq 3$, put

$$G_j(\Lambda) = \sum_{\lambda \in \Lambda - \{0\}} \frac{1}{\lambda^j}$$

Remark

Since $\Lambda = -\Lambda$, $G_j(\Lambda) = 0$ if j is odd.

Proposition

$$\wp(z) = \frac{1}{z^2} + \sum_{k \geq 1} (2k+1) G_{2k+2}(\Lambda) z^{2k}$$

Proof

If $\lambda \neq 0$

$$\frac{1}{(z-\lambda)^2} = \frac{1}{\lambda^2} \sum_{k \in \mathbb{N}} (k+1) \left(\frac{z}{\lambda}\right)^k - \frac{1}{\lambda^2} = \sum_{k \geq 1} (k+1) \frac{z^k}{\lambda^{k+2}}$$

and the n-th coefficient of the LAURENT series of a sum of a series is given by the sum of the n-th coefficient of the terms of the series. □

Theorem

$$\forall z \in \mathbb{C} - \Lambda, \quad \wp'(z)^2 = 4\wp(z)^3 - 60 G_4(\Lambda) \wp(z) - 140 G_6(\Lambda)$$

Proof

Let us look at the first coefficients of the LAURENT series of the difference at 0.

$$\wp(z) = \frac{1}{z^2} + 3 G_4(\Lambda) z^2 + 5 G_6(\Lambda) z^4 + O(z^6)$$

$$\wp'(z) = -\frac{2}{z^3} + 6 G_4(\Lambda) z + 20 G_6(\Lambda) z^3 + O(z^5)$$

$$\wp'(z)^2 = \frac{4}{z^6} - 24 G_4(\Lambda) \frac{1}{z^2} - 80 G_6(\Lambda) + O(z^2)$$

$$-4\wp(z)^3 = -\frac{4}{z^6} - 36 G_4(\Lambda) \frac{1}{z^2} - 60 G_6(\Lambda) + O(z^2)$$

So

$$\wp'^2 - 4\wp^3 + 60 G_4(\Lambda) \wp + 140 G_6(\Lambda)$$

is a Λ-periodic meromorphic function with no pole in $\mathbb{C} - \Lambda$ nor 0 (or Λ) and which

takes the value 0 en 0.
Thus it is bounded entire function,
and therefore equal to 0. □

Conclusion
The map

$$z \longmapsto (\wp(z), \wp'(z))$$

induces an isomorphism $\overline{\varphi}$ of Riemann surfaces

$$T = \mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$$

where E is the elliptic curve defined by the affine equation

$$y^2 = 4X^3 - 60\, G_4(\Lambda) X - 140\, G_6(\Lambda)$$

which maps $\overline{0}$ to 0 (the point at ∞)

Remark
$\wp$ and $\wp'$ are analytic but not algebraic
(not given by polynomials)

Fact
$\overline{\varphi}$ is an isomorphism of groups.

Proof
Take $z, z_0 \in \mathbb{C}$.
We have to prove that the points
$(\wp(z+z_0), -\wp'(z+z_0))$, $(\wp(z), \wp'(z))$ and $(\wp(z_0), \wp'(z_0))$
are aligned
So consider the function

$$z \longmapsto D_{z_0}(z) = \begin{vmatrix} \wp(z+z_0)-\wp(z_0) & \wp(z)-\wp(z_0) \\ -\wp'(z+z_0)-\wp'(z_0) & \wp'(z)-\wp'(z_0) \end{vmatrix}$$

it is meromorphic and Λ periodic with possible poles at 0 and $-z_0$

In 0 the Laurent series starts with

$$\big(\wp(z+z_0)-\wp(z_0)\big)\big(\wp'(z)-\wp'(z_0)\big)+\big(\wp'(z+z_0)+\wp'(z_0)\big)\big(\wp(z)-\wp(z_0)\big)$$
$$=\Big(\wp'(z_0)\,z+\tfrac{1}{2}\wp''(z_0)z^2+\tfrac{1}{6}\wp'''(z_0)z^3\Big)\times\Big(-\frac{2}{z^3}\Big)$$
$$+\Big(2\wp'(z_0)+\wp''(z_0)\,z+\tfrac{1}{2}\wp'''(z_0)z^2\Big)\times\Big(\frac{1}{z^2}-\wp(z_0)\Big)+O(z)$$
$$=\frac{1}{6}\wp'''(z_0)-2\wp'(z_0)\wp(z_0)+O(z)$$

But the relation

$$\wp'^2=4\wp^3-60\,G_4(\Lambda)\,\wp-140\,G_6(\Lambda)$$

gives

$$2\wp''\wp'=12\wp'\wp^2-60\,G_4(\Lambda)\wp'$$

and $\quad 2\wp''=12\wp^2-60\,G_4(\Lambda)$

Thus $\quad \wp'''=12\,\wp\wp'$

we get In 0 $\quad D(z)=O(z)$

In $-z_0$: Take $z'=z+z_0 \quad z'_0=-z_0$

$$D_{z_0}(z)=\begin{vmatrix} \wp(z')-\wp(z'_0) & \wp(z'+z'_0)-\wp(z'_0) \\ -\wp(z')+\wp'(z'_0) & \wp(z'+z'_0)+\wp'(z'_0) \end{vmatrix}$$
$$=D_{z'_0}(z')$$

so D_{z_0} has no poles $\quad D_{z_0}=0$. □

Notation

If A is an abelian group

The n-torsion of A is

$$A[n]=\{a\in A \mid na=0\}$$

the torsion subgroup is $A_{tors}=\bigcup_{n\in\mathbb{N}-\{0\}} A[n]$.

Corollary

If K is a number field and E an elliptic curve over K, for any $n > 0$ $E(K)[n]$ is isomorphic to a subgroup of

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

Proof

Choose an embedding

$$\sigma : K \hookrightarrow \mathbb{C}$$

it gives $E(K) \hookrightarrow E(\mathbb{C}) \xrightarrow{\sim} \mathbb{C}/\Lambda$

but if $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ is the projection

$$\begin{aligned} \mathbb{C}/\Lambda[n] &= \{ \bar{z} \in \mathbb{C}/\Lambda \mid n\bar{z} = \bar{0} \} \\ &= \pi\{ z \in \mathbb{C} \mid nz \in \Lambda \} \\ &= (\tfrac{1}{n}\Lambda)/\Lambda \end{aligned}$$

we get

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^2 &\xrightarrow{\sim} \mathbb{C}/\Lambda[n] \\ (\bar{a}, \bar{b}) &\longmapsto (a\tfrac{1}{n} + b\tfrac{\tau}{n}) \end{aligned}$$

□

d) Mordell-Weil's theorem

which is actually a conjecture of MORDELL proven by WEIL.

Theorem [MORDELL, WEIL] for elliptic curves.

Let K be a number field, let E be an elliptic curve on K. Then the group $E(K)$ is finitely generated

Aim

Prove this theorem before the end of the semester.

Remark

By the structure theorem of finitely generated abelian groups, there exist a unique $r \in \mathbb{N}$ and a unique family of integers

$$2 \leq d_1 \mid d_2 \mid \dots \mid d_m$$

and an isomorphism

$$E(K) \simeq \mathbb{Z}^r \times \prod_{i=1}^{m} \mathbb{Z}/d_i\mathbb{Z}$$

r is called the rank of the elliptic curve

In fact there is a deeper theorem

Theorem [B. MAZUR, 1978]

Over $\mathbb{Q}$, $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups:

$\mathbb{Z}/d\mathbb{Z}$ for $d \in \{1, \dots, 10, 12\}$

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2d\mathbb{Z}$ for $d \in \{1, 2, 3, 4\}$.

Remark

Generalization by L. MÉREL (1996)

for any number field K, the number of possibilities for $E(K)_{tors}$ is finite!

Open problem

Is the rank of an elliptic curve over a given number field bounded?

Even over $\mathbb{Q}$ we really do not know.

Current known record

2006 [N. ELKIES], explicit elliptic curve / $\mathbb{Q}$ with rank ≥ 28. You can find the

coefficients on the net.

We do not get have the tools to prove MORDELL-WEIL theorem; but, before we turn to other topics, I would like to explain the generalization of MORDELL-WEIL theorem to higher dimensions:

c) Algebraic groups

Remark

If E is an elliptic curve over a field K

$$K' \longmapsto E(K')$$

defines a functor from the category of extension of K to the category of groups.

Algebraic groups generalizes that.

Definition

An algebraic group is an algebraic set G (in fact, a scheme) over a commutative ring A equipped with morphisms

$m : G \times G \to G$ the group law

$e : pt \longrightarrow G$ (ie $e \in G(A)$) neutral element

$\iota : G \longrightarrow G$ inverse

such that the following diagrams commutes

(i)
$$\begin{array}{ccc} G \times G \times G & \xrightarrow{m \times Id_G} & G \times G \\ {\scriptstyle Id_G \times m}\downarrow & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{m} & G \end{array}$$

associativity

(ii)
$$\begin{array}{ccc} G & \xrightarrow{(Id_G, e)} & G\times G \\ {\scriptstyle (e, Id_G)}\downarrow & \searrow^{Id_G} & \downarrow{\scriptstyle m} \\ G\times G & \xrightarrow{m} & G \end{array}$$
neutral element

(iii)
$$\begin{array}{ccc} G & \xrightarrow{(Id_G, i)} & G\times G \\ {\scriptstyle (i, Id_G)}\downarrow & \searrow & \downarrow{\scriptstyle m} \\ G\times G & \xrightarrow{m} & G \end{array}$$
inverse.

It is commutative if the diagram

(iv)
$$\begin{array}{ccc} G\times G & \xrightarrow{\leftrightarrow} & G\times G \\ & {\scriptstyle m}\searrow \quad \swarrow{\scriptstyle m} & \\ & G & \end{array}$$
commutes

Remark
With those notations for any commutative A-algebra C, $G(C)$ is a group
we get a foncteur
commutative A algebras $\longrightarrow$ groups
$C \longmapsto G(C)$.

Examples
a) Additive group
$G_a = \mathbb{A}^1_{\mathbb{Z}}$
with $m : \mathbb{A}^1_{\mathbb{Z}} \times \mathbb{A}^1_{\mathbb{Z}} \to \mathbb{A}^1_{\mathbb{Z}}$
$(x, y) \longmapsto x+y$
$0 \in \mathbb{A}^1(\mathbb{Z})$

$\iota : \mathbb{A}^1_{\mathbb{Z}} \longrightarrow \mathbb{A}^1_{\mathbb{Z}}$
$x \longmapsto -x$

Note that
$\mathbb{G}_a(\mathbb{C})$ is the additive group $\mathbb{C}$

b) Multiplicative group
$\mathbb{G}_{m,\mathbb{Z}}$ defined by the equation $XY = 1$ with

$$\mathbb{G}_{m,\mathbb{Z}} \times \mathbb{G}_{m,\mathbb{Z}} \longrightarrow \mathbb{G}_{m,\mathbb{Z}}$$
$$(x,y), (x',y') \longmapsto (xx', yy')$$

[$xy = 1$ and $x'y' = 1 \Rightarrow xx'yy' = 1$]

$1 = (1,1) \in \mathbb{G}_{m,\mathbb{Z}}$ neutral element

inverse $\mathbb{G}_{m,\mathbb{Z}} \longrightarrow \mathbb{G}_{m,\mathbb{Z}}$
$(x,y) \longmapsto (y,x)$

Note that
$\mathbb{C}^* \xrightarrow{\sim} \mathbb{G}_m(\mathbb{C})$
$x \longmapsto (x, x^{-1})$

Remark
In fact, may like $\mathbb{G}_{m,\mathbb{Z}} = \operatorname{Spec}(\mathbb{Z}[T,T^{-1}])$
since $\mathbb{Z}[T,T^{-1}] \xrightarrow{\sim} \mathbb{Z}[X,Y]/(XY-1)$

c) Linear group
$\mathrm{GL}_{n,\mathbb{Z}}$ defined by

$$T \det\left((X_{ij})_{\substack{1 \le i \le n \\ 1 \le j \le n}}\right) = 1$$

polynomial in n^2+1 variable

multiplication

$$\mathrm{GL}_{n,\mathbb{Z}} \times \mathrm{GL}_{n,\mathbb{Z}} \longrightarrow \mathrm{GL}_{n,\mathbb{Z}}$$
$$\left((X_{ij},T), (X'_{ij},T')\right) \longmapsto \left(\left(\sum_{k=1}^{n} X_{ik} X'_{kj}\right), TT'\right)$$

Well-defined because $\det(MM') = \det(M)\det(M')$ in the ring $\mathbb{Z}[X_{i,j},\ 1 \le i,j \le n]$

$1 = ((\delta_{ij}), 1) \in Gl_{n,\mathbb{Z}}(\mathbb{Z})$

and the inverse

$$\iota : Gl_{n,\mathbb{Z}} \longrightarrow Gl_{n,\mathbb{Z}}$$
$$((X_{ij}), T) \longmapsto (T\,{}^t com(X_{ij}),\ \det(X_{ij}))$$

Note that

$$Gl_{n,\mathbb{Z}}(\mathbb{C}) \xrightarrow{\sim} Gl_n(\mathbb{C})$$

Remark

In fact

$$Gl_{n,\mathbb{Z}} = Spec\left(\mathbb{Z}[X_{i,j}, 1 \le i,j \le n], \frac{1}{\det((X_{i,j})_{\substack{1 \le i \le n \\ 1 \le j \le n}})}\right)$$

f] Abelian varieties

Definition

An abelian variety is an abelian smooth projective geometrically irreducible algebraic group

Example

If $E_1, \dots, E_m$ are elliptic curves over a field K,

$E_1 \times \dots \times E_m$ is an abelian variety over K

Remark

Later we shall see less obvious examples.

Theorem (MORDELL-WEIL) (general form)
Let A be an abelian variety over a number field K. Then the group $A(K)$ is finitely generated

Up to now we have seen how to produce solutions; but how can one proves that there is no solution? This will be a short chapter:

III How to prove that there are no solutions?

1) Obvious obstructions

Using the functoriality

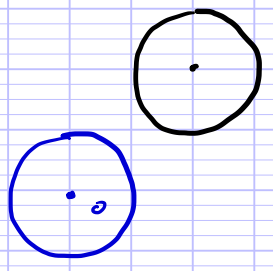
a) Real solutions

If V is an algebraic set over $\mathbb{Q}$
$V(\mathbb{Q}) \subset V(\mathbb{R})$
if $V(\mathbb{R}) \neq \emptyset$ then $V(\mathbb{Q}) = \emptyset$

Examples

a) $X^2 + Y^2 + Z^2 = 0$ in $\mathbb{P}^2(\mathbb{Q})$
$x^2+y^2+z^2 = 0 \Rightarrow (x,y,z) = (0,0,0)$
so $V(\mathbb{R}) = \emptyset$ and $V(\mathbb{Q}) = \emptyset$

b) $\begin{cases} X^2 + Y^2 - T^2 = 0 \\ X^2 + Y^2 - 4XT - 4YT + 7T^2 = 0 \end{cases}$



$\cap$ du cercle de centre O et de rayon 1 avec le cercle de centre $(2,2)$ et de rayon 1.

Remark

It follows from a theorem of TARSKI & SEIDENBERG (1936) there is an algorithm to decide wether $V(\mathbb{R}) \neq \emptyset$

b) Reduction modulo N

α) Affine setting

Let $P_1, \dots, P_m \in \mathbb{Z}[X_1, \dots, X_N]$
and $I = (P_1, \dots, P_m)$
For any $M \geq 2$, there is a reduction map

$$V_I(\mathbb{Z}) \longrightarrow V_I(\mathbb{Z}/M\mathbb{Z})$$

so if $V_I(\mathbb{Z}/M\mathbb{Z}) = \phi$, then $V_I(\mathbb{Z}) = \phi$

Example

$X^2 - Y^2 = 2$
Reduce modulo 4
in $\mathbb{Z}/4\mathbb{Z}$ squares are 0 and 1
so differences of squares are 0, 1, 3

Remark

Also works for

$$38253\,X^2 - 7661\,Y^2 = 36774$$

β) Projective setting

Let $P_1, \dots, P_m \in \mathbb{Z}[X_0, \dots, X_N]$ be homogeneous polynomials and

$$I = (P_1, \dots, P_m)$$

Reminder

There is a reduction map

$$Z_I(\mathbb{Q}) \to Z_I(\mathbb{Z}/M\mathbb{Z})$$

for any integer $M \geq 2$

So if there is no <u>primitive</u> solution to $P_i(X_0, \dots, X_N) = 0$ for $i \in \{1, \dots, m\}$ in $(\mathbb{Z}/M\mathbb{Z})^{N+1}$

then

$$Z_I(\mathbb{Q}) = \emptyset$$

Example

We consider the homogeneous equation

$$X^2 + Y^2 - 3T^2 = 0$$

Let (x, y, t) be a primitive solution
Let us look in $\mathbb{Z}/3\mathbb{Z}$
we get $x^2 + y^2 = 0$
If $x \neq 0$ or $y \neq 0$ we get that -1 is a square in $\mathbb{Z}/3\mathbb{Z}$ absurd
So $x = y = 0$
But then let us look in $\mathbb{Z}/9\mathbb{Z}$
From what we have just seen
$\overline{3} \mid x$ and $\overline{3} \mid y$
Thus $x^2 = y^2 = 0$
So $3t^2 = 0$
Thus $3 \mid t$ & there is no primitive solution in $(\mathbb{Z}/9\mathbb{Z})^3$
So no solutions in $\mathbb{P}^2(\mathbb{Q})$!

So these are the 2 obvious obstructions to the existence of a rational solution

Remark

Using the conjecture of Weil proven by Deligne in 1974, about the number of points of algebraic sets over finite fields, it is possible to prove that there exists

an explicit M_0 such that

$$Z_I(\mathcal{X}_{/M_0\mathbb{Z}}) \neq \phi \Leftrightarrow \forall M \geq 2,\ Z_I(\mathcal{X}_{/M\mathbb{Z}}) \neq \phi.$$

So a natural question is wether the converse is true : if there is a point over $\mathbb{R}$ and over $\mathbb{Z}/M\mathbb{Z}$ for any $M \geq 2$, is there a rational solution, that is a solution over $\mathbb{Q}$? This is called

2] HASSE principle and weak approximation

HASSE principle

An algebraic set Z in $\mathbb{P}^N_{\mathbb{Q}}$ is said to satisfy the HASSE principle if the following implication is true

$$(Z(\mathbb{R}) \neq \phi \text{ and } \forall M \geq 2,\ Z(\mathbb{Z}/M\mathbb{Z}) \neq \phi) \Rightarrow Z(\mathbb{Q}) \neq \phi$$

Theorem (HASSE-MINKOWSKI)

It is true for quadrics defined by non degenerate quadratic forms

I am not going to give the proof but there is a complete proof quite easy to read in

Reference

J.-P. SERRE Cours d'arithmétique.

One can refine that statement : assume that we have solution modulo M does it comes by reduction modulo M from a solution over $\mathbb{Q}$? If we have a solution over $\mathbb{R}$, is it a limit of solutions over $\mathbb{Q}$?

Weak approximation

Let $Z \subset \mathbb{P}^N_K$ be an algebraic set

We say that it satisfies weak approximation if the following is true:

- For any non empty open subset U of $Z(\mathbb{R})$
- any $M \geq N$ and any $x_0 \in \bigcap_{M|M'} \mathrm{im}\left(Z(\mathbb{Z}/M'\mathbb{Z}) \to Z(\mathbb{Z}/M\mathbb{Z})\right)$

there exists

$x \in Z(\mathbb{Q}) \cap U$ which reduces to x_0 modulo M.

Theorem (≠ HASSE-MINKOWSKI)

True for quadrics defined by non-degenerate quadratic forms

Idea of the proof (this is only a quick sketch)

If $Z(\mathbb{R}) = \emptyset$ or there is M such that $Z(\mathbb{Z}/M\mathbb{Z}) = \emptyset$ the result is true

(If $Z(\mathbb{Z}/M\mathbb{Z}) = \emptyset$ for any multiple M' of M $Z(\mathbb{Z}/M'\mathbb{Z}) = \emptyset$)

otherwise we know by HASSE-MINKOWSKI theorem that $Z(\mathbb{Q}) \neq \emptyset$

Pick $P \in Z(\mathbb{Q}) \subset \mathbb{P}^N(\mathbb{Q})$

Then the projective lines in $\mathbb{P}^N(\mathbb{Q})$ going through P are in 1 to 1 correspondence with $\mathbb{P}(\mathbb{Q}^{N+1}/P)$

and for each such line L

- either $L \subset Z(\mathbb{Q})$
- or $L \cap Z$ contains exactly one other points of Z.

we get a "function"

$$\mathbb{P}^{N-1}(\mathbb{Q}) \dashrightarrow Z(\mathbb{Q}) \quad \text{not defined everywhere.}$$

$$\cup \qquad\qquad \cup$$

$$U(\mathbb{Q}) \overset{1:1}{\longleftrightarrow} V(\mathbb{Q})$$

where $\mathbb{P}^{N-1} - U$ (resp $Z - V$) are smaller algebraic subsets (U and V are open for ZARISKI topology).

But $V(\mathbb{R})$ is dense in $Z(\mathbb{R})$

and $V(\mathbb{Q}_p)$ ——— in $Z(\mathbb{Q}_p)$

(where $\mathbb{Q}_p$ = completion of $\mathbb{Q}$ for $|\cdot|_p$)

We are reduced to prove weak approximation for $\mathbb{P}^{N-1}_{\mathbb{Q}}$ for which it [follows from the fact that if W is an open cone in $\mathbb{R}^{N+1}$ and if Λ is the translate of a lattice in $\mathbb{R}^{N+1}$ then $\Lambda \cap W \neq \emptyset$.] is an exercise □

But HASSE himself knew this was not always true!

3) A Counter-example to HASSE principle

a) Sums of 2 squares in $\mathbb{Z}$

Proposition that you probably already know

Let

$$n = \varepsilon \prod_{p \in \mathcal{P}} p^{v_p(n)} \in \mathbb{Z} - \{0\}$$

Then n is the sum of two squares if and only if

- $\varepsilon = 1$

and - $\forall p \in \mathcal{P}$, $p \equiv 3 \ [4] \Rightarrow v_p(n)$ is even.

Proof

The ring $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$ is euclidean for $N : \mathbb{Z}[i] \to \mathbb{N}$
$a + bi \mapsto a^2 + b^2$

Indeed if $x + yi \in \mathbb{C}$ then $x - \lfloor x + \frac{1}{2} \rfloor \leq \frac{1}{2}$
$y - \lfloor y + \frac{1}{2} \rfloor \leq \frac{1}{2}$ so
$N(x + yi - (\lfloor x + \frac{1}{2} \rfloor + \lfloor y + \frac{1}{2} \rfloor i)) \leq \frac{1}{2}$
so if $a, b \in \mathbb{Z}[i]$, $b \neq 0$ there exists $q \in \mathbb{Z}[i]$ such that $N(\frac{a}{b} - q) \leq \frac{1}{2}$
and thus $N(a - bq) < N(b)$

In particular $\mathbb{Z}[i]$ is a principal ideal domain
$\mathbb{Z}[i]^* \subset \{a + bi \mid a^2 + b^2 = 1\}$
$= \{1, -1, i, -i\} \subset \mathbb{Z}[i]^*$

Now let the set of the sum of two squares is $S = N(\mathbb{Z}[i])$
In particular it is stable by multiplication

Lemma

Let $p \in \mathbb{P}$ then $p \in S \iff p = 2$ or $p \equiv 1 \ [4]$

Proof

- Modulo 4 $a^2 + b^2 \in \{0, 1, 2\}$
so if $p \equiv 3 \ [4]$, $p \notin S$
give $\Rightarrow$
- Converse
$2 = 1^2 + 1^2$ $2 \in S$
If $p \equiv 1 \ [4]$
then $(-1)^{\frac{p-1}{2}} = 1$ So -1 is a square in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

Therefore
$$\mathbb{Z}[i]/(p) \simeq \mathbb{Z}/p\mathbb{Z}[T]/(T^2+1)$$
is not a field
So p is not irreducible in $\mathbb{Z}[i]$
We may write
$$p = z_1 z_2$$
with $z_1, z_2 \notin \mathbb{Z}[i]^*$
so $p^2 = N(p) = N(z_1) N(z_2)$
Since $z_1, z_2 \notin \mathbb{Z}[i]^*$ $N(z_1) \neq 1$ and $N(z_2) \neq 1$
We get
$$p = N(z_1) \in S \qquad \square$$

<u>End of the proof of the proposition</u>

$\Leftarrow$ any square is in S
So if $\varepsilon = 1$ and $\forall p \in \mathcal{P}$, $p \equiv 3\ [4] \Rightarrow v_p(n)$ even
$$n = \prod_{p \equiv 3\ [4]} \left(p^{\frac{v_p(n)}{2}}\right)^2 \times \prod_{\substack{p \equiv 1\ [4] \\ \text{or } p=2}} p^{v_p(n)} \in S.$$

$\Rightarrow$ Let $p \in \mathcal{P}$ with $p \equiv 3\ [4]$
and $n \in S$
Let us prove by induction on $v_p(n)$
that $v_p(n)$ is even
- True if $v_p(n) = 0$
- Assume the result for $k < v_p(n)$ and $v_p(n) \geq 1$
Since $p \equiv 3\ [4]$ (-1) is not a square in $\mathbb{F}_p$
So $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[T]/(T^2+1)$ is a field
So p is irreducible in $\mathbb{Z}[i]$
write $n = N(z) = z\bar{z}$ in $\mathbb{Z}[i]$
$p \mid z\bar{z}$ so $p \mid z$ or $p \mid \bar{z}$ (p irreducible)

But if $p \mid z$, $p \mid \bar{z}$ (and similarly if $p \mid \bar{z}$, $p \mid z$)
($z = p\alpha \Rightarrow \bar{z} = p\bar{\alpha}$)
We get that $p^2 \mid n$
and $\frac{n}{p^2} = N\left(\frac{z}{p}\right) \in S$
by induction $v_p(n) - 2$ is even
$v_p(n)$ is even. □

b) The counter-example

Consider the surface given by the equation
(1) $\quad Y^2 + Z^2 = (3 - X^2)(X^2 - 2)$
Does it have a rational point?
As usual we are going to make this equation homogeneous to reduce the problem to integral solutions. However in that case if I take directly the surface defined in $\mathbb{P}^3$ by the corresponding equation, I get a surface which is not smooth
So instead I am going to see coordinates

$$Y, Z, T, U, V$$

and the equation
(2) $\quad Y^2 + Z^2 = T^2(3V^2 - U^2)(U^2 - 2V^2)$
which is homogeneous in (T, Y, Z)
if $\left(\frac{u}{v}, \frac{y}{\epsilon}, \frac{z}{\epsilon}\right)$ is solution of (1)
then
$((\epsilon, v^2 y, v^3 z), (u, v))$ is solution of (2)
and we may assume first (u, v) (multiply ϵ by $\gcd(u, v)$) and then (ϵ, y, z) primitive.

2 En fait dans $\mathbb{P}(G(2) + G)$

* Solutions over $\mathbb{R}$.

Over $\mathbb{R}$ a number is the sum of 2 squares if and only if it is positive

equivalent to $x^2 \in [2,3]$

(we can't have $x^2 < 2$ and $x^2 > 3$)

* Solutions over $\mathbb{Z}/p^n\mathbb{Z}$, for $p \neq 2$

Taking $u = v = 1$ we get the équation

$$y^2 + z^2 + 2t^2 = 0$$

But if $p \neq 2$ any quadratic form in at least 3 variables is isotropic over $\mathbb{F}_p$

We may then lift a solution modulo p to $\mathbb{Z}/p^n\mathbb{Z}$ (using Hensel's lemma).

* Solutions over $\mathbb{Z}/2^n\mathbb{Z}$

Over $\mathbb{Z}/8\mathbb{Z}$ we may take.

$u = 0$, $v = 1$ which gives

$$y^2 + z^2 - 2t^2 = 0$$

Which has a primitive solution $(1,1,1)$ which can be lifted to $\mathbb{Z}/2^n\mathbb{Z}$ for $n \geq 3$

(because an odd number is a square modulo 2^n if and only if it is modulo 8.

* Solutions over $\mathbb{Z}$

Assume we have a solution

$(x,y,t), (u,v)$ with $\gcd(x,y,t) = \gcd(u,v) = 1$

then

$n = t^2(3v^2 - u^2)(u^2 - 2v^2)$ is the sum of 2 $\square$

which means that

(i) $n > 0$

(ii) $\forall p \in \mathcal{P}$, $p \equiv 3 \ [4] \Rightarrow v_p(n)$ even

But if these conditions are satisfied for n
they are also satisfied by
$$(3v^2-u^2)(u^2-2v^2)$$
which therefore, is also the sum of two squares
But then this implies that
$$\frac{u^2}{v^2} \in [2,3] \quad (\mathbb{R} \text{ condition})$$
then
$$3v^2-u^2 \geq 0$$
and $u^2-2v^2 \geq 0$ divides the sum
and $\gcd(3v^2-u^2, u^2-2v^2) \mid v^2$
and therefore
$$\gcd(3v^2-u^2, u^2-2v^2) = \gcd(u^2, v^2) = 1$$
since $\gcd(u,v)=1$.
If p is a prime number such that $p \equiv 3 \ (4)$
then
$$v_p(3v^2-u^2) + v_p(u^2-2v^2) \equiv 0 \ (2)$$
but one of them is 0
Thus both of them are even
$\forall p \in \mathcal{P}$, $p \equiv 3 \ (4) \Rightarrow v_p(3v^2-u^2)$ and $v_p(u^2-2v^2)$ are even

Conclusion
$3v^2-u^2$ and u^2-2v^2 are both the sum of two squares!

But modulo 4 a square is 0 or 1
So the sum of two squares is $\neq -1$ modulo 4.
Let us look at the possible values

modulo 4

u^2	v^2	$3v^2-u^2$	u^2-2v^2
1	0	−1	1
0	1	3	−2
1	1	2	−1

So $3u^2-v^2$ and u^2-2v^2 can not be both the sum of two squares!
Therefore

$$y^2+z^2=(3-x^2)(x^2-2)$$

has no solutions in $\mathbb{Q}^3$.

Remark

In 1970, at the International Congress of Mathematicians in NICE, MANIN gave a method to produce counter-examples to HASSE principle and the weak approximation. It turned out that all the counter-examples known at that time could be explained using this method. So it is quite natural to ask whether there exists counter-examples which can not be explained that way. It took some time to get an answer to that question. D. HARARI & A. SKOROBOGATOV in 2001 gave an example which can not be explained using MANIN's method.

IV Counting the solutions

If we consider an equation like

$$X^2+Y^2=1$$

there are simple solutions, like

$(1,0)$ is solution as well as

$\left(\frac{60900}{60901}, \frac{349}{60901}\right)$.

We would like to measure the complexity of a given solution (For example to have an estimate of the size of the memory needed to store it on a computer)

1) Exponential heights over $\mathbb{Q}$

Let us fix a norm

$$\|\cdot\|_\infty : \mathbb{R}^{N+1} \longrightarrow \mathbb{R}_{\geq 0}$$

Then we may define a function

$$H : \mathbb{P}^N(\mathbb{Q}) \longrightarrow \mathbb{R}_{>0}$$

by $H([x_0 : \dots : x_N]) = \|(x_0, \dots, x_N)\|_\infty$

if $(x_0, \dots, x_N)$ is a primitive element in $\mathbb{Z}^{N+1}$

Indeed, if

$$[x_0 : \dots : x_N] = [y_0 : \dots : y_N]$$

with $(x_0, \dots, x_N)$ and $(y_0, \dots, y_N) \in \mathbb{Z}^{N+1}$

both primitive

then $\exists \lambda \in \mathbb{Q}$ such that

$$(x_0, \dots, x_N) = \lambda (y_0, \dots, y_N)$$

write λ as $\frac{a}{b}$ with $a \in \mathbb{Z}$, $b \in \mathbb{Z} - \{0\}$

and $\gcd(a,b) = 1$

then $(bx_0, \dots, bx_N) = (ay_0, \dots, ay_N)$

and

$$|b| = |b| \gcd(x_0, \dots, x_N) = \gcd(bx_0, \dots, bx_N) = \gcd(ay_0, \dots, ay_N) = |a|$$

Therefore $\lambda \in \{-1, 1\}$ and

$$\|(x_0, \dots, x_N)\|_\infty = \|(y_0, \dots, y_N)\|_\infty .$$

Definition

$H : \mathbb{P}^N(\bar{\mathbb{Q}}) \to \mathbb{R}_{>0}$ is called the exponential height associated to the norm $\|\cdot\|_\infty$

Example

If we take $\|(x_0, \dots, x_N)\|_\infty = \sup_{0 \le i \le N} |x_i|$

then $H([1 : 0 : 1]) = 1$

whereas $H([6091 : 349 : 60900]) = 60901$.

Remark

By definition

$$\#\{P \in \mathbb{P}^N(\bar{\mathbb{Q}}) \mid H([x_0 : \dots : x_N]) \le B\}$$
$$\le \#\{(x_0, \dots, x_N) \in \mathbb{Z}^{N+1} \mid \|(x_0, \dots, x_N)\|_\infty \le B\}$$

is finite we shall see more precise estimates in a moment.

More generally

Definition

Let V be an algebraic projective set defined / $\bar{\mathbb{Q}}$ and let

$$\phi : V \to \mathbb{P}^N$$

be a morphism of algebraic sets

then we may define an exponential height

$$H_\phi : V(\bar{\mathbb{Q}}) \to \mathbb{R}_{>0}$$

as $H_\phi = H \circ \phi$.

Notation

X a set with a map $H : X \to \mathbb{R}_{>0}$

we define

$$X_{H \leq B} = \{ x \in X \mid H(x) \leq B \}.$$

Remark

If ϕ is injective, then

$V(\mathbb{Q})_{H \leq B}$ is finite

and we may consider its cardinal

$$\# V(\mathbb{Q})_{H \leq B}.$$

Natural questions

How does the set $V(\mathbb{Q})_{H \leq B}$ look like as $B \to +\infty$?

This is a domain of active research.

Let me just consider a simple example

2) Points of bounded height in $\mathbb{P}^N(\mathbb{Q})$

Proposition

$$\# \mathbb{P}^n(\mathbb{Q})_{H \leq B} = \frac{\mathrm{Vol}(\overline{B}_{\|\cdot\|_\infty}(0,1))}{2\zeta_{\mathbb{Q}}(n+1)} B^{n+1} + O(B^n \log(B))$$

where $\overline{B}_{\|\cdot\|_\infty}(0,1) = \{ y \in \mathbb{R}^{N+1} \mid \|y\|_\infty < 1 \}$ and Vol is the usual euclidean volume.

Proof

First, as we have seen, any point in $\mathbb{P}^n(\mathbb{Q})$ that is any 1-dimensional vector subspace of $\mathbb{Q}^{n+1}$ contains exactly 2 primitive

elements in $\mathbb{Z}^{n+1}$ and the sum of these 2 elements is 0. Therefore

$$\#\mathbb{P}^n(\mathbb{Q})_{H\le B} = \frac{1}{2}\#\left\{(x_0,\dots,x_n)\in\mathbb{Z}^{n+1} \;\middle|\; \begin{array}{l}\gcd(x_0,\dots,x_N)=1\\ \|(x_0,\dots,x_n)\|_\infty \le B\end{array}\right\}$$

1st step

For a very short while let us forget about the gcd condition. How can we estimate

$$M(B) = \#\left\{(x_0,\dots,x_N)\in\mathbb{Z}^{N+1} \;\middle|\; \|(x_0,\dots,x_n)\|_\infty \le B\right\}$$

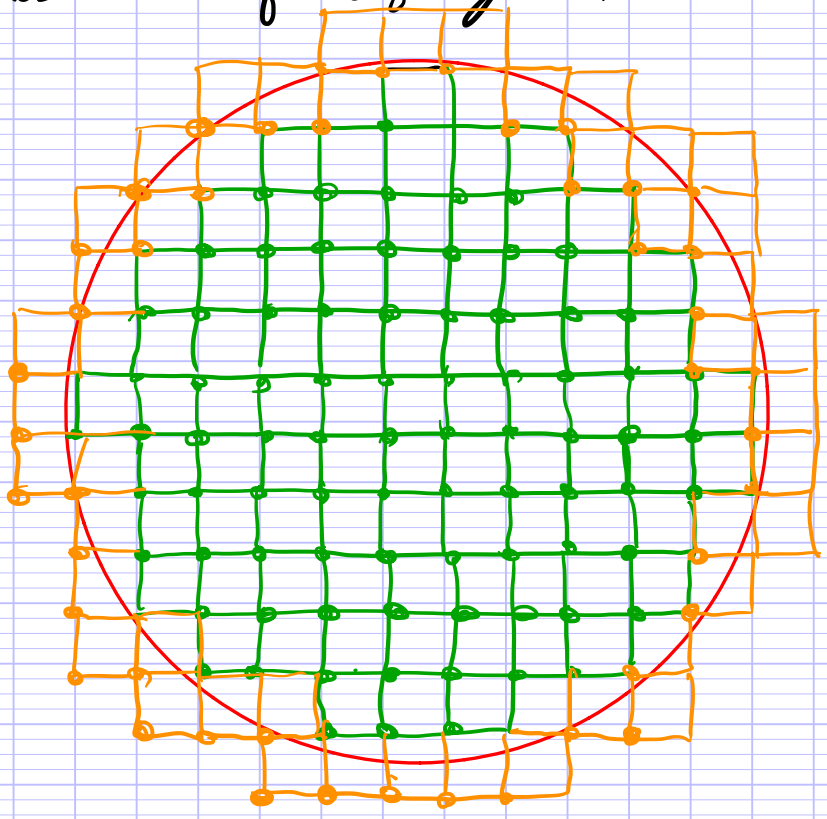
If you think in terms of RIEMANN integration it ought to be similar to the volume of the ball of center 0 and radius B.

More precisely,

Let

$$B_0 = [0,1[^{n+1} \subset \mathbb{R}^{n+1}$$

and for $x\in\mathbb{R}^{n+1}$ $B_x = B_0 + x$ the translate of B_0 by x.



Then
$\mathcal{B}_x \subset \overline{B}_{\|\cdot\|_\infty}(0,B) \Rightarrow x \in \overline{B}_{\|\cdot\|_\infty}(0,B) \Rightarrow \mathcal{B}_x \cap \overline{B}_{\|\cdot\|_\infty}(0,B) \neq \emptyset$
and therefore
$$\mathrm{Vol}\Big(\bigcup_{\mathcal{B}_x \subset \overline{B}_{\|\cdot\|_\infty}(0,B)} \mathcal{B}_x\Big) \leq \#\{x \in \mathbb{Z}^{n+1} \mid \|x\|_\infty \leq B\} \leq \mathrm{Vol}\Big(\bigcup_{\mathcal{B}_x \cap \overline{B}_{\|\cdot\|_\infty}(0,B) \neq \emptyset} \mathcal{B}_x\Big)$$
Mais
$$\bigcup_{\mathcal{B}_x \subset \overline{B}_{\|\cdot\|_\infty}(0,B)} \mathcal{B}_x \subset \overline{B}_{\|\cdot\|_\infty}(0,B) \subset \bigcup_{\mathcal{B}_x \cap \overline{B}_{\|\cdot\|_\infty}(0,B) \neq \emptyset} \mathcal{B}_x$$
But $\mathcal{B}_0$ is compact
and therefore
$$\delta = \mathrm{diam}(\mathcal{B}_0) = \sup_{y,y' \in \mathcal{B}_0} (\|y - y'\|_\infty) < +\infty$$

If $\mathcal{B}_x \cap \overline{B}_{\|\cdot\|_\infty}(0,B) \neq \emptyset$ and $y \in \mathcal{B}_x$
then $\|y\| \leq B + \delta$
and if $\mathcal{B}_y \cap (\mathbb{R}^{n+1} - \overline{B}_{\|\cdot\|_\infty}(0,B)) \neq \emptyset$ and $y \in \mathcal{B}_x$
then $\|y\| \geq B - \delta$
We get that for any $B \geq 1$
$$\Big|\#\{x \in \mathbb{Z}^{n+1} - \{0\} \mid \|x\|_\infty \leq B\} - B^{n+1}\mathrm{Vol}(\overline{B}_{\|\cdot\|}(0,1))\Big|$$
$$\leq \mathrm{Vol}\big(\overline{B}_{\|\cdot\|}(0,1)\big)\big((B+\delta)^{n+1} - (B-\delta)^{n+1}\big)$$
$$\leq C\, B^n \quad \text{for some } C > 0.$$
If we put $\ell = \min_{x \in \mathbb{Z}^{n+1} - \{0\}} \|x\|_\infty$ and
$$M^*(B) = \#\{x \in \mathbb{Z}^{n+1} - \{0\} \mid \|x\|_\infty \leq B\}$$
we have proven there exists $C > 0$ such that
$$\big|M^*(B) - B^{n+1}\mathrm{Vol}(\overline{B}_{\|\cdot\|}(0,1))\big| \leq C\, B^n,$$
for any $B \geq 1$.
But, since 0 removed the origin
$$M^*(B) = 0 \text{ if } B < \ell$$
so the result is also valid for $B < 1$:
$$\forall\, B \in \mathbb{R}_+,\ \big|M^*(B) - B^{n+1}\mathrm{Vol}(\overline{B}_{\|\cdot\|_\infty}(0,1))\big| \leq C B^n.$$

2nd step

Let us now deal with the gcd condition:

Basic idea

$$\#\left\{(x_0,\dots,x_n)\in\mathbb{Z}^{n+1} \;\middle|\; \begin{cases} \gcd(x_0,\dots,x_n)=1 \\ \|(x_0,\dots,x_n)\|_\infty \le B \end{cases}\right\}$$

$$= \#\{x\in\mathbb{Z}^{n+1}-\{0\} \mid \|x\|_\infty \le B\}$$

but then we have to remove those for which all coordinates are divisible by p

$$-\sum_{p\in\mathcal{P}} \#\{x\in(p\mathbb{Z})^{n+1}-\{0\} \mid \|x\|_\infty \le B\}$$

But then if all coordinates are divisible by the product of 2 ≠ primes, we removed them twice.

$$+\sum_{\substack{p_1,p_2\in\mathcal{P}\\ p_1\neq p_2}} \#\{x\in(p_1p_2\mathbb{Z})^{n+1}-\{0\} \mid \|x\|_\infty \le B\}$$

...

this leads to a finite alternate sum, because if $d > B$ then

$$\#\{x\in(d\mathbb{Z})^{n+1}-\{0\} \mid \|x\|_\infty \le B\} = 0.$$

Definition

The Moebius function: $\mu : \mathbb{N}-\{0\} \longrightarrow \{-1,0,1\}$

$$\mu(n) = \begin{cases} (-1)^{\sum_{p\in\mathcal{P}} v_p(n)} & \text{if } \forall p\in\mathcal{P},\ v_p(n)\le 1 \\ 0 & \text{otherwise} \end{cases}$$

Properties

(i) μ is multiplicative

$\forall a, b \in \mathbb{N}-\{0\}$, $\gcd(a,b)=1 \Rightarrow \mu(ab)=\mu(a)\mu(b)$

(ii) If p is prime

$$\mu(p^k) = \begin{cases} 1 & \text{if } k=0 \\ -1 & \text{if } k=1 \\ 0 & \text{otherwise} \end{cases}$$

(iii)

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{otherwise} \end{cases}$$

The only thing we need to prove is the third property. I shall use the following lemma

Lemma

If f and g are multiplicative functions then their convolution product

$$f * g\,(n) = \sum_{kl=n} f(k)\, g(l)$$

is multiplicative as well.

Proof

If $\gcd(a,b)=1$ then

$$\{k \mid a\} \times \{l \mid b\} \longrightarrow \{d \mid ab\}$$
$$(k,l) \longmapsto kl$$

is bijective; its inverse being given by

$$(\gcd(d,a), \gcd(d,b)) \longleftarrow d$$

So $f*g(ab) = \sum_{d \mid ab} f(d)\, g\left(\frac{ab}{d}\right)$

$$= \sum_{\substack{l \mid a \\ l \mid b}} f(kl)\, g\left(\frac{a}{k}\,\frac{b}{l}\right)$$

$$= \sum_{\substack{k \mid a \\ \ell \mid b}} f(k) f(\ell)\, g\left(\frac{a}{k}\right) g\left(\frac{b}{\ell}\right)$$

since f and g are multiplicative and $\gcd(a,b) = 1$

$$= \left(\sum_{k \mid a} f(k)\, g\left(\frac{a}{k}\right) \right) \left(\sum_{\ell \mid b} f(\ell)\, g\left(\frac{b}{\ell}\right) \right)$$

$$= f * g(a)\ f * g(b) \ . \quad \square$$

Proof of (iii)

The constant function 1 is multiplicative

So, by the Lemma $1 * \mu$ as well

Thus

$$1 * \mu(n) = \prod_{p \in \mathcal{P}} 1 * \mu(p^{\nu_p(n)})$$

But

$$1 * \mu(p^k) = \sum_{0 \le \ell \le k} \mu(p^\ell) = \sum_{0 \le \ell \le \min(1,k)} \mu(p^\ell)$$

$$= \begin{cases} 1 & \text{if } k = 0 \\ 0 & \text{otherwise} \end{cases}$$

So

$$1 * \mu(n) = \delta_{1,k} = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases} . \quad \square$$

Let us go back to the 2nd step of the proof:

End of the proof of the 2nd step

$$\#\left\{ (x_0, \dots, x_n) \in \mathbb{Z}^{n+1} \;\middle|\; \begin{cases} \gcd(x_0, \dots, x_n) = 1 \\ \|(x_0, \dots, x_n)\|_\infty \le B \end{cases} \right\}$$

$$= \sum_{d \ge 1} \delta_{1,d}\ \#\left\{ (x_0, \dots, x_n) \in \mathbb{Z}^{n+1} \;\middle|\; \begin{cases} \gcd(x_0, \dots, x_n) = d \\ \|(x_0, \dots, x_n)\|_\infty \le B \end{cases} \right\}$$

$$= \sum_{d \geq 1} \sum_{k \mid d} \mu(k) \# \left\{ (x_0, \dots, x_n) \in \mathbb{Z}^{n+1} \;\middle|\; \begin{array}{l} \gcd(x_0, \dots, x_n) = d \\ \|(x_0, \dots, x_n)\|_\infty \leq B \end{array} \right\}$$

$$= \sum_{k \geq 1} \mu(k) \# \left\{ (x_0, \dots, x_n) \in \mathbb{Z}^{n+1} - \{0\} \;\middle|\; \begin{array}{l} k \mid \gcd(x_0, \dots, x_n) \\ \|(x_0, \dots, x_n)\|_\infty \leq B \end{array} \right\}$$

$$= \sum_{k \geq 1} \mu(k) \# \left\{ (x_0, \dots, x_n) \in (k\mathbb{Z})^{n+1} - \{0\} \mid \|(x_0, \dots, x_n)\|_\infty \leq B \right\}$$

$$x_i' = \frac{x_i}{k}$$

$$= \sum_{k \geq 1} \mu(k) \# \left\{ (x_0', \dots, x_n') \in \mathbb{Z}^{n+1} - \{0\} \mid \|(x_0, \dots, x_n)\|_\infty \leq \frac{B}{k} \right\}$$

$$= \sum_{k \geq 1} \mu(k) M^*\left(\frac{B}{k}\right) = \sum_{1 \leq k \leq \frac{B}{\ell}} \mu(k) M^*\left(\frac{B}{k}\right)$$

Now we combine the 2 steps

Final step

$$\left| \sum_{1 \leq k \leq \frac{B}{\ell}} \mu(k) M^*\left(\frac{B}{k}\right) - \sum_{k \geq 1} \mu(k) \mathrm{Vol}\left(\overline{B}_{\|\cdot\|_\infty}(0,1)\right) \left(\frac{B}{k}\right)^{n+1} \right|$$

$$\leq C \underbrace{\sum_{1 \leq k \leq \frac{B}{\ell}} \left(\frac{B}{k}\right)^n}_{\text{the series converges}} + C' \sum_{k > \frac{B}{\ell}} \left(\frac{B}{k}\right)^{n+1}$$

$$\begin{cases} = O(B \log(B)) \text{ if } n = 1 \\ = O(B^n) \text{ if } n > 1 \end{cases} \qquad O\left(B^{n+1} \frac{1}{B^n}\right)$$

It remains to compute

$$\left(\sum_{k \geq 1} \frac{\mu(k)}{k^{n+1}} \right) \times \zeta_{\mathbb{Q}}(n+1) = \sum_{k \geq 1} \frac{\mu(k)}{k^{n+1}} \times \sum_{\ell \geq 1} \frac{1}{\ell^{n+1}}$$

$$= \sum_{\substack{k \geq 1 \\ \ell \geq 1}} \frac{\mu(k)}{(k\ell)^{n+1}}$$

$$= \sum_{d \geq 1} \left(\sum_{k \mid n} \mu(k) \right) \frac{1}{d^{n+1}} = 1$$

So

$$\#\,\mathbb{P}^n(\mathbb{Q})_{H\le B} = \frac{\mathrm{Vol}(B_{\|\cdot\|_\infty}(0,1))}{2\,\zeta_{\mathbb{Q}}(n+1)}\,B^{n+1} + \begin{cases} O(B\log(B)) & \text{if } n=1 \\ O(B^n) & \text{if } n>1 \end{cases}$$

as wanted. □

I am now going to extend the construction of heights to arbitrary number fields. In order to do that, I am going to use results of algebraic number theory. These results are part of the lectures of SARA CHECCOLI. Therefore I am going to state them without proofs.

3) Number theory in a nutshell

a) Multiplicative structure

References

P. SAMUEL. Théorie algébrique des nombres. HERMANN (1967)

S. LANG. Algebraic Number Theory. SPRINGER (1970)

Notations

K number field, that is a finite field extension of $\mathbb{Q}$

O_K the ring of integers of K, that is the integral closure of $\mathbb{Z}$ in K

$O_K = \{\alpha \in K \mid \exists P \in \mathbb{Z}[X], \text{ monic}, P(\alpha)=0\}$ (dominant coefficient is 1)

Proposition 1

O_K is a DEDEKIND domain: which means that

a) It is an integral domain

b) integrally closed
c) noetherian
d) any nonzero prime ideal is maximal

Notations

A fractional ideal of K is a sub $\mathcal{O}_K$-module α in K such that there exists $d \in \mathcal{O}_K$, $d\alpha \subset \mathcal{O}_K$

$\mathcal{I}(K)$ = set of nonzero fractional ideals of K

Examples

- If $x \in K^*$, $(x) = \mathcal{O}_K x$ is a fractional ideal, such a fractional ideal is said to be principal
- If $\alpha, \beta \in \mathcal{I}(K)$ the product $\alpha\beta$ which is the $\mathcal{O}_K$-module generated by products xy with $x \in \alpha$ and $y \in \beta$ is a fractional ideal.

Notations (continued)

$\mathcal{P}(K)$ = set of nonzero principal fractional ideals

$\mathrm{Val}_f(K) = \mathrm{Spec}(\mathcal{O}_K) - \{(0)\}$ set of nonzero prime ideals of $\mathcal{O}_K$

Theorem 1

The product defines a group structure on $\mathcal{I}(K)$ and any $\alpha \in \mathcal{I}(K)$ may be uniquely written as

$$\alpha = \prod_{\mathfrak{p} \in \mathrm{Val}_f(K)} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)}$$

where $\{\mathfrak{p} \in \mathrm{Val}_f(K) \mid v_{\mathfrak{p}}(\alpha) \neq 0\}$ is finite

Remarks

In other words

$$\bigoplus_{\mathfrak{p}\in Val_f(K)} \mathbb{Z} \longrightarrow \mathcal{J}(K)$$

$$(a_{\mathfrak{p}})_{\mathfrak{p}\in Val_f(K)} \longrightarrow \prod_{\mathfrak{p}\in Val_f(K)} \mathfrak{p}^{a_{\mathfrak{p}}}$$

is an isomorphism of groups

Prop

- $v_{\mathfrak{p}}(ab) = v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}(b)$
- $a \subset b \Leftrightarrow \forall \mathfrak{p} \in Val_f(K)\ v_{\mathfrak{p}}(b) \leq v_{\mathfrak{p}}(a)$

which implies

- $v_{\mathfrak{p}}(a \cap b) = \max(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(b))$
- $v_{\mathfrak{p}}(a+b) = \min(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(b))$.

which generalizes the formula you know for the gcd and lcm.

Remarks

We may restrict to principal ideals and we get a morphism

For any $\mathfrak{p} \in Val_f(K)$

$$v_{\mathfrak{p}} : K^* \longrightarrow \mathbb{Z}$$

So that

- $(x) = \prod_{\mathfrak{p}\in Val_f(K)} \mathfrak{p}^{v_{\mathfrak{p}}(x)}$
- $x \mid y$ (i.e. $(y) \subset (x)$) $\Leftrightarrow \forall \mathfrak{p} \in Val_f(K),\ v_{\mathfrak{p}}(x) \leq v_{\mathfrak{p}}(y)$
- $v_{\mathfrak{p}}(xy) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(y)$
- $v_{\mathfrak{p}}(x+y) \geq \min(v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y))$ with $=$ if $v_{\mathfrak{p}}(x) \neq v_{\mathfrak{p}}(y)$.

Theorem 2

The group $\mathcal{J}(K)/\mathcal{P}(K)$ is finite.
It is called the ideal class group of K
(I shall denote it $\mathcal{C}\ell(\mathcal{O}_K)$).

Notations (continued)

$\#\mathrm{Mor}_{\text{field}}(K, \mathbb{C}) = [K : \mathbb{Q}]$ by Galois theory
and we have an action of $\mathbb{Z}/2\mathbb{Z}$ on this
set via $\sigma \mapsto \overline{\sigma} : x \mapsto \overline{\sigma(x)}$
$\mathrm{Val}_\infty(K)$ is the set of orbits in $\mathrm{Mor}_{\text{field}}(K, \mathbb{C})$
for this action.

N.B.

$\sigma = \overline{\sigma} \Leftrightarrow \sigma(K) \subset \mathbb{R}$
which explains the

Terminology

$v \in \mathrm{Val}_\infty(K)$ is said to be real
if the cardinal of the orbit is one,
complex otherwise

Notations (continued)

$\mathrm{Val}(K) = \mathrm{Val}_f(K) \amalg \mathrm{Val}_\infty(K)$
is called the set of places of K
A place v is said to be
- finite (or non-archimedean) if $v \in \mathrm{Val}_f(K)$
- infinite (or archimedean) otherwise

it is then either real or complex.
r_1 is the number of real places
r_2 the number of complex places

One has $r_1 + 2r_2 = [K:\mathbb{Q}]$

If $v \in Val_\infty(K)$ is the orbit of σ one defines

$$|\cdot|_v : K \longrightarrow \mathbb{R}_{>0} \quad \text{if } v \text{ is real}$$
$$x \longmapsto |\sigma(x)|$$

$$|\cdot|_v : K \longrightarrow \mathbb{R}_{>0} \quad \text{if } v \text{ is complex}$$
$$x \longmapsto |\sigma(x)|^2$$

2 In the complex case

$$|x+y|_v^{1/2} \leq |x|_v^{1/2} + |y|_v^{1/2}$$

but we do not have the usual triangular inequality!

We get a morphism

$$\begin{aligned} G_K^* &\xrightarrow{\log} \prod_{v \in Val_\infty(K)} \mathbb{R} \quad \left(= \mathbb{R}^{r_1+r_2}\right) \\ x &\longmapsto (\log |x|_v)_{v \in Val_\infty(K)} \end{aligned}$$

$$\begin{aligned} pr : \prod_{v \in Val_\infty(K)} \mathbb{R} &\longrightarrow \mathbb{R} \\ (x_v)_{v \in Val_\infty(K)} &\longrightarrow \sum_{v \in Val_\infty(K)} x_v \end{aligned}$$

$L = Im(\log)$

$\mu(K) = \{ x \in K \mid \exists n \geq 1,\ x^n = 1 \}$ roots of unity in K.

Theorem 3

a) $\ker(\log) = \mu(K)$ which is a finite group.

b) L is a lattice in $\ker(pr)$

(which means that it is a subgroup generated by a basis of the real vector space $\ker(pr)$).

If we combine the various theorems, we get the following conclusion:

Conclusion (structure of K^*)

One has 2 exact sequences

$$1 \to G_K^* \to K^* \xrightarrow{\oplus v_v} \bigoplus_{v \in \mathrm{Val}_f(K)} \mathbb{Z} \to \underbrace{Cl(G_K)}_{\text{finite}} \to 1$$

and

$$1 \to \mu(K) \to G_K^* \xrightarrow{\log} L \to 0$$

$$L \downarrow S \quad \mathbb{Z}^{r_1+r_2-1}$$

Exercise

Make this explicit for

$K = \mathbb{Q}(i)\ \mathbb{Q}(\sqrt{2})\ \mathbb{Q}(i\sqrt{5})$.

Corollary (which we are going to use in the proof of MORDELL-WEIL theorem)

Let $S \subset \mathrm{Val}_f(K)$ be a finite set of finite places

Then

$$\ker\left(K^*/K^{*2} \xrightarrow{\oplus \bar{v}_v} \bigoplus_{v \in \mathrm{Val}_f(K)-S} \mathbb{Z}/2\mathbb{Z}\right)$$

is finite.

Proof

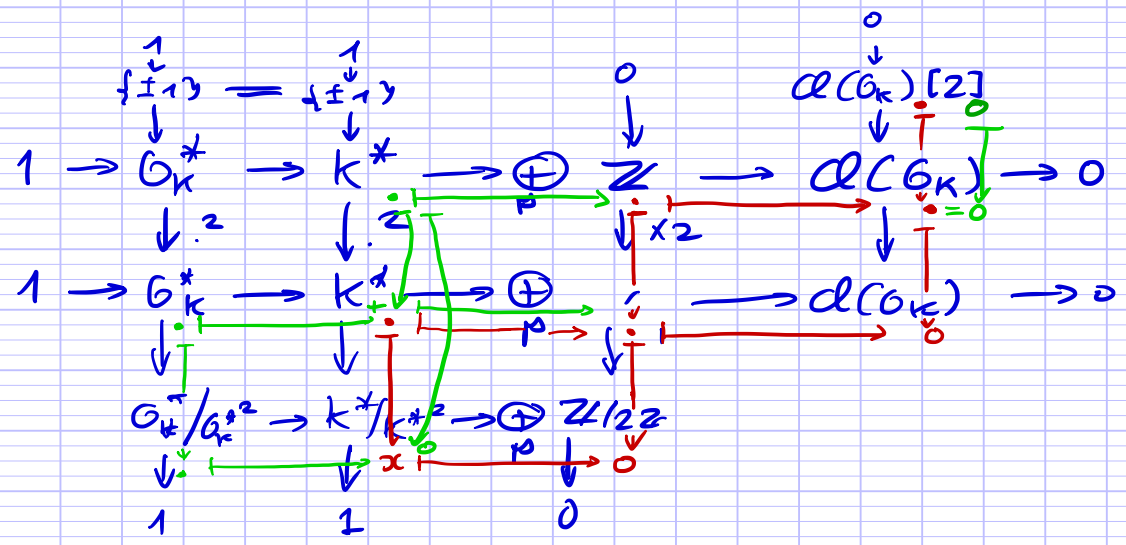
It is enough to prove it for $S = \phi$ since

$$0 \to \underbrace{\ker\left(K^*/K^{*2} \xrightarrow{\oplus \bar{v}_p} \bigoplus_{v \in \mathrm{Val}_f(K)} \mathbb{Z}/2\mathbb{Z}\right)}_{\text{finite}} \to \underbrace{\ker\left(K^*/K^{*2} \xrightarrow{\oplus \bar{v}_v} \bigoplus_{v \in \mathrm{Val}_f(K)-S} \mathbb{Z}/2\mathbb{Z}\right)}_{\text{finite}} \xrightarrow{\oplus \bar{v}_v} \underbrace{\bigoplus_{v \in S} \mathbb{Z}/2\mathbb{Z}}_{\text{finite}}$$

finite $\Longrightarrow$ finite

In the case when $S = \phi$

We use the structure theorem which gives the following exact sequence and we consider the square maps. We get a diagram and we do a little diagram chase

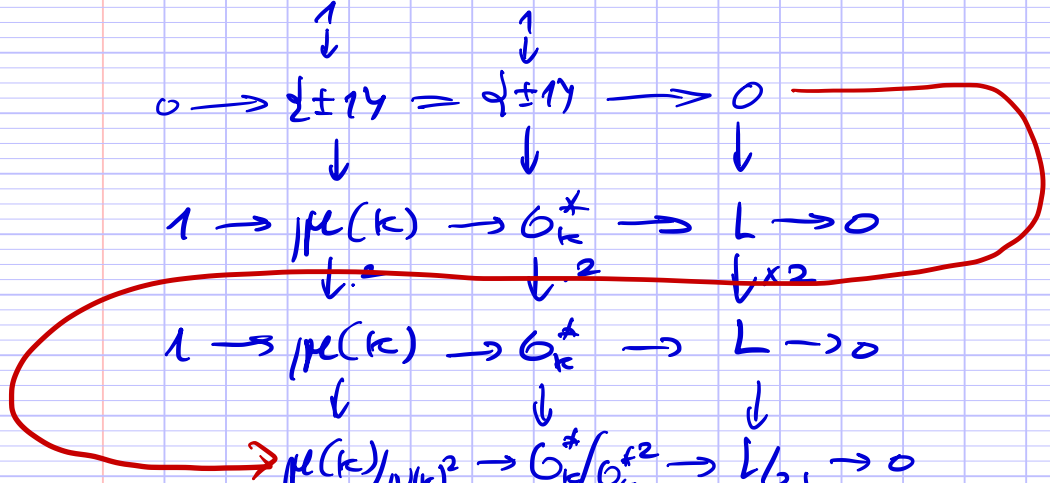


We get an exact sequence

$$1 \to G_K^*/G_K^{*2} \to \ker\left(K^*/K^{*2} \to \bigoplus_{v \in \mathrm{Val}_f(K)} \mathbb{Z}/2\mathbb{Z}\right) \to \underbrace{Cl(G_K)[2]}_{\text{finite}} \to 0$$

It remains to check that G_K^*/G_K^{*2} is finite

But then we use the other exact sequence



In that case we may use the snake lemma

We get an exact sequence

$$1 \to \underbrace{\mu_\infty(K)/\mu_\infty(K)^2}_{\text{finite}} \to G_K^*/G_K^{*2} \to \underbrace{L/2L}_{\text{finite}} \to 0$$

so G_K^*/G_K^{*2} is finite. □

b) An application: the weak MORDELL-WEIL theorem

Let me state this theorem

Theorem

Let E be an elliptic curve over a number field K, then the group

$$E(K)/2E(K)$$

is finite.

Steps of the proof

We may assume E is in Weierstrass form

$$E: \quad Y^2 = X^3 + aX + b$$

Remark

If we take $Y' = u^3 Y$ and $X' = u^2 X$ we get that E is isomorphic to

$$Y'^2 = X'^3 + (u^4 a) X' + (u^6 b)$$

Therefore we may assume $a, b \in \mathcal{O}_K$

The proof is 3 step

1st step

If K'/K is a finite extension of field

$$\ker(E(K)/2E(K) \longrightarrow E(K')/2E(K'))$$

is finite. Therefore we may reduce to the case where $X^3 - aX + b$ is split

$$E: Y^2 = (X-\alpha)(X-\beta)(X-\gamma)$$

with $\alpha, \beta, \gamma \in K$

2nd step

In the latter case we construct

$$E(K)/2E(K) \xrightarrow{(\varphi_\alpha, \varphi_\beta)} K^*/K^{*2} \times K^*/K^{*2}$$

3rd step

If $\mu \in Val_p(K)$ is such that $v_\mu(\Delta) = 0$ then $E(K)/2E(K) \longrightarrow K^*/K^{*2} \times K^*/K^{*2} \xrightarrow{v_\mu} (\mathbb{Z}/2\mathbb{Z})^2$ is 0

then we can apply the previous corollary: $E(K)/2E(K)$ is finite

Let us start with the 1st step:

Proposition

Let E be an elliptic curve over K, $\mathrm{char}(K)=0$, let K'/K be a finite extension then

$$\ker\left(E(K)/2E(K) \longrightarrow E(K')/2E(K')\right)$$

is finite.

Proof

By replacing K by its Galois (or normal) closure over K, we may assume that K'/K is a Galois extension

Then

$Gal(K'/K)$ acts on $E(K')$

via:

$\forall \sigma \in Gal(K'/K)$ $\sigma([x:y:t]) = [\sigma(x):\sigma(y):\sigma(t)]$

(In fact it acts on $\mathbb{P}^n(K')$)

Lemma

$$\mathbb{P}^n(K')^{Gal(K'/K)} = \mathbb{P}^n(K)$$

($\mathbb{P}^n(K)$ means that it is the image of $\mathbb{P}^n(K)$ in $\mathbb{P}^n(K')$)

Proof of the lemma

- $\mathbb{P}^n(K) \subset \mathbb{P}^n(K')^{Gal(K'/K)}$ by definition of the action
- The problem is to prove the converse.

Let $[x_0 : \dots : x_n] \in \mathbb{P}^n(K')^{Gal(K'/K)}$

By permuting the coordinates, if necessary, we may assume that $x_0 \neq 0$

Since $\forall \sigma \in Gal(K'/K)$, $[\sigma(x_0) : \dots : \sigma(x_n)] = [x_0 : \dots : x_n]$

we get $\forall \sigma \in Gal(K'/K), \forall i \in \{1, \dots, n\}$ $\dfrac{\sigma(x_i)}{\sigma(x_0)} = \dfrac{x_i}{x_0}$

or $\forall \sigma \in Gal(K'/K), \forall i \in \{1, \dots, n\}$ $\sigma\left(\dfrac{x_i}{x_n}\right) = \dfrac{x_i}{x_n}$

But $K'^{Gal(K'/K)} = K$

So $\forall i \in \{1, \dots, n\}$ $\dfrac{x_i}{x_n} \in K$

$$[x_0 : \dots : x_n] = \left[1 : \frac{x_1}{x_0} : \dots : \frac{x_n}{x_0}\right] \in \mathbb{P}^n(K).$$

Proof of the proposition (continued)

- Let $x \in \ker\left(E(K)/2E(K) \to E(K')/2E(K')\right)$

Let $P_x \in E(K)$ represent x.

and let $Q_x \in E(K')$ be such that $P_x = 2Q_x$

(since $x_{K'} = 0$ in $E(K')/2E(K')$)

We define

$$\lambda_x : Gal(K'/K) \to E(K')$$
$$\sigma \longmapsto \sigma(Q_x) - Q_x.$$

Note that

$$2\lambda_x(\sigma) = 2\sigma(Q_x) - 2Q_x$$
$$= \sigma(P_x) - P_x = 0$$

So $\lambda_x(\sigma) \in E(K')[2]$ for any $\sigma \in Gal(K'/K)$.

Take $x, x' \in E(K)/2E(K)$ be such that

$$\lambda_x = \lambda_{x'}$$

Then

$$\forall \sigma \in Gal(K'/K) \quad \sigma(Q_x) - Q_x = \sigma(Q_{x'}) - Q_{x'}$$

or $\forall \sigma \in Gal(K'/K) \quad \sigma(Q_x - Q_{x'}) = Q_x - Q_{x'}$

Therefore $Q_x - Q_{x'} \in E(K')^{Gal(K'/K)} = E(K)$

$$P_x - P_{x'} = 2Q_x - 2Q_{x'} = 2(Q_x - Q_{x'}) \in 2E(K).$$

Therefore $x = x'$

So $\lambda_x = \lambda_{x'} \Rightarrow x = x'$.

We get

$$\#\ker(E(K)/2E(K) \to E(K')/2E(K')) \leq \#(E(K')[2])^{Gal(K'/K)}$$

$$\leq 4^{[K':K]} \quad (\text{cf. CC}) \qquad \square$$

Remark

Interpretation in terms of Galois cohomology

$$0 \to E(\bar{K})[2] \to E(\bar{K}) \xrightarrow{\times 2} E(\bar{K}) \to 0$$

is exact this gives a long exact sequence

$$0 \to E(K)[2] \to E(K) \xrightarrow{\times 2} E(K) \to H^1(Gal(\bar{K}/K), E(\bar{K})[2])$$
$$\to H^1(Gal(\bar{K}/K), E(\bar{K})) \cdots$$

So $E(K)/2E(K) \hookrightarrow H^1(Gal(\bar{K}/K), E(\bar{K})[2])$

we get a commutative diagram

$$\begin{array}{ccccc}
0 & & & & 0 \\
\downarrow & & & & \downarrow \\
\ker(E(K)/2E(K) \to E(K')/2E(K')) & \longrightarrow & & & H^1(Gal(K'/K), E(K')[2]) \\
\text{injective} & & & & \\
\downarrow & & & & \downarrow \\
0 \longrightarrow E(K)/2E(K) & \longrightarrow & & & H^1(Gal(\bar{K}/K), E(\bar{K})[2]) \\
\downarrow & & & & \downarrow \\
0 \longrightarrow E(K')/2E(K') & \longrightarrow & & & H^1(Gal(\bar{K}/K'), E(\bar{K})[2])
\end{array}$$

exact by general results on Galois cohomology

We now turn to the 2nd step:

Idea

$$E(K)/2E(K) \longrightarrow E(\bar{K})/2E(\bar{K}) = \ker \gamma$$

Using the computation of the last proof, we get

$$E(K)/2E(K) \hookrightarrow \underset{\text{cont}}{\mathrm{Hom}}(Gal(\bar{K}/K), E(K)[2])$$

$$x \longmapsto \lambda_x$$

$$\downarrow \simeq \text{ By hypothesis}$$

$$(\mathbb{Z}/2\mathbb{Z})^2$$

But Kummer theory shows that

$$K^*/K^{*2} \xrightarrow{\sim} \mathrm{Hom}(Gal(\bar{K}/K), \mathbb{Z}/2\mathbb{Z})$$

$$[x] \longmapsto (\sigma \mapsto \sigma(y)/y) \text{ if } x = y^2 \text{ in } \bar{K}$$

So

$$E(K)/2E(K) \hookrightarrow \left(K^*/K^{*2}\right)^2$$

I am going to construct it explicitely

We assume that E is given by

$$E : Y^2 = (X-\alpha)(X-\beta)(X-\gamma)$$

α, β, γ roots of $X^3 + aX + b$

Since $\mathcal{O}_K$ is integrally closed, $\alpha, \beta, \gamma \in \mathcal{O}_K$.

we define

$$\varphi_\alpha : E(k) \longrightarrow k^*/k^{*2}$$

$$P \longmapsto \begin{cases} (x-\alpha)k^{*2} & \text{if } P=[1:x:y] \text{ if } y\neq 0 \\ (\alpha-\beta)(\alpha-\gamma)k^{*2} & \text{if } P=[1:\alpha:0] \\ k^{*2} & \text{if } P=0 \end{cases}$$

φ_β, φ_γ are defined similarly by permuting α, β and γ

Lemma

$\varphi_\alpha, \varphi_\beta, \varphi_\gamma$ are group morphisms

Proof

By definition

$$\varphi_u(0) = 1$$

If $P=[1:x:y]$ $\varphi_\alpha(-P) = \varphi_\alpha(P) = \varphi_\alpha(P)^{-1}$

It remains to prove that

$$P_1+P_2+P_3=0 \Rightarrow \varphi_\alpha(P_1)\varphi_\alpha(P_2)\varphi_\alpha(P_3)=1$$

Already proven if $0 \in \{P_1, P_2, P_3\}$

We assume that $P_i = [1:x_i:y_i]$

1st case : $[1:\alpha:0] \notin \{P_1, P_2, P_3\}$

Let $Y=pX+q$ be the equation of the line through P_1, P_2 and P_3

Then

$$(X-\alpha)(X-\beta)(X-\gamma) - (pX+q)^2 = (X-x_1)(X-x_2)(X-x_3)$$

Taking $X=\alpha$ we get

$$(x_1-\alpha)(x_2-\alpha)(x_3-\alpha) = (p\alpha+q)^2 \in k^{*2}.$$

That is $\varphi_\alpha(P_1)\varphi_\alpha(P_2)\varphi_\alpha(P_3)=1$.

2nd case

$P_1 = [1 : \alpha : 0] \Rightarrow [1 : \alpha : 0] \notin \{P_2, P_3\}$ since $0 \notin \alpha\{\beta, \gamma\}$

$(X-\alpha)(X-\beta)(X-\gamma) - (pX+q)^2 = (X-\alpha)(X-x_2)(X-x_3)$

$\Rightarrow (X-\alpha) \mid (pX+q)$ in $k[X]$

that is $p\alpha + q = 0$ and $pX + q = p(X-\alpha)$

So $(X-\alpha)(X-\beta)(X-\gamma) - p^2(X-\alpha)^2 = (X-\alpha)(X-x_2)(X-x_3)$

Dividing by $(X-\alpha)$, and taking $X = \alpha$ we get

$(\alpha-\beta)(\alpha-\gamma) = (\alpha-x_2)(\alpha-x_3)$

ie $\varphi_\alpha(P_1) = \varphi_\alpha(P_2)\,\varphi_\alpha(P_3)$. □.

Remark

φ_α induces $\overline{\varphi_\alpha} : E(k)/2E(k) \to k^*/k^{*2}$.

Lemma 2

$P = [1 : x : y] \in 2E(k)$

$\Leftrightarrow (x-\alpha), (x-\beta)$ and $(x-\gamma) \in k^2$ (might be 0).

Proof

$\Rightarrow$ follows from Lemma 1.

$\Leftarrow$ Assume $(x-\alpha), (x-\beta)$ and $(x-\gamma)$ are □

Write $\begin{cases} (x-\alpha) = c_\alpha^2 \\ (x-\beta) = c_\beta^2 \\ (x-\gamma) = c_\gamma^2 \end{cases}$

We want to find P' such that $P = 2P'$

Since $2P' = P \neq 0$ we have $P' = [1 : x' : y']$ with $y' \neq 0$.

So we have to find p, q, x' such that

$(X-\alpha)(X-\beta)(X-\gamma) - (pX+q)^2 = (X-x)(X-x')(X-x')$

that is $(X-x)(X-x')(X-x') + (pX+q)^2$ has roots α, β, γ

Using these relations this might be written as

$$\begin{cases} (p\alpha+q)^2 = c_\alpha^2(\alpha-x')^2 \\ (p\beta+q)^2 = c_\beta^2(\beta-x')^2 \\ (p\gamma+q)^2 = c_\gamma^2(\gamma-x')^2 \end{cases}$$

So we are to solve one of the following linear systems

$$\begin{cases} p\alpha+q \pm (c_\alpha x' - c_\alpha \alpha) = 0 \\ p\beta+q \pm (c_\beta x' - c_\beta \beta) = 0 \\ p\gamma+q \pm (c_\gamma x' - c_\gamma \gamma) = 0 \end{cases}$$

which has a (unique) solution if

$$\begin{vmatrix} 1 & \alpha & \pm c_\alpha \\ 1 & \beta & \pm c_\beta \\ 1 & \gamma & \pm c_\gamma \end{vmatrix} \neq 0$$

$$\Leftrightarrow \pm \underbrace{(\beta-\alpha)}_{\neq 0} c_\gamma \pm \underbrace{(\alpha-\gamma)}_{\neq 0} c_\beta \pm \underbrace{(\gamma-\beta)}_{\neq 0} c_\alpha \neq 0$$

(at most one is 0)

Takes at least 2 distinct values

So we may find a solution (p, q, x')

Then taking $y' = -(px'+q)$ and $P' = [1 : x' : y']$

$P = 2P'$. □

Proposition

$\varphi_\alpha \times \varphi_\beta : E(K)/2E(K) \longrightarrow K^*/K^{*2} \times K^*/K^{*2}$

is injective.

Proof

Take $P = [1 : x : y]$ such that $\varphi_\alpha([P]) = \varphi_\beta([P]) = 1$

Case 1

$x \notin \{\alpha, \beta\}$

then $x-\alpha$ and $x-\beta$ are squares

as $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$

$x-\gamma$ is a square as well

By lemma 2, $P \in 2E(K)$

Case 2 $x = \alpha$ ($x = \beta$ is similar)

Then $(\alpha-\beta)$ and $(\alpha-\gamma)(\alpha-\beta)$ are squares

(Remember the definition of $\varphi_\alpha([1:\alpha:0])$)

So $(\alpha-\gamma)$ is a square as well

By lemma 2 $P \in 2E(K)$. □

3rd step

Proposition

We have $\Delta = (\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2$

If $\mathfrak{p} \in Val_f(K)$ satisfies $v_\mathfrak{p}(\Delta) = 0$

then

$$E(K)/2E(K) \longrightarrow K^*/K^{*2} \xrightarrow{v_\mathfrak{p}} \mathbb{Z}/2\mathbb{Z}$$

(the composite is the zero map)

Proof

So formula for $\Delta = Res(P, P')$ follows from the Problem on resultants.

Remember: $\alpha, \beta, \gamma \in G_K$

so $v_\mathfrak{p}(\alpha-\beta), v_\mathfrak{p}(\beta-\gamma), v_\mathfrak{p}(\gamma-\alpha) \geq 0$

so we get

$$v_\mathfrak{p}(\alpha-\beta) + v_\mathfrak{p}(\beta-\gamma) + v_\mathfrak{p}(\gamma-\alpha) = 0$$

if $P = 0$ or $P \in \{[1:\alpha:0], [1:\beta:0], [1:\gamma:0]\}$

the result is true by definition of $\varphi_\alpha, \varphi_\beta$

Assume $P = [1:x:y]$ with $y \neq 0$

Then let me put

$a = v_p(x-\alpha)$, $b = v_p(x-\beta)$, $c = v_p(x-\gamma)$

Since $(x-\alpha)(x-\beta)(x-\gamma) = q^2$,

$a+b+c \equiv 0 \ (2)$

- If $a < 0$, then

$$v_p(x-\beta) = v_p(\underbrace{x-\alpha}_{v_p<0} + \underbrace{\alpha-\beta}_{v_p\geq 0}) = v_p(x-\alpha) = a$$

So $a = b = c$ and we get

$3a \equiv 0 \ (2) \Rightarrow a \equiv 0 \ (2)$

- If $a > 0$ then

$b = v_p(x-\beta) = 0$ and $c = v_p(x-\gamma) = 0$

So $a \equiv 0 \ (2)$

- Otherwise $a = 0$

In any case $a \equiv 0 \ (2)$ (similarly $b \equiv 0 \ (2)$) □

End of the proof of the theorem

- $\ker\left(E(K)/2E(K) \longrightarrow (K^*/K^{*2})^2\right) = \{0\}$
- $\mathrm{Im}\left(E(K)/2E(K) \to (K^*/K^{*2})^2\right) \subset \underbrace{\ker\left((K^*/K^{*2})^2 \to \bigoplus_{v_p(\Delta)=0} (\mathbb{Z}/2\mathbb{Z})^2\right)}_{\text{finite by corollary}}$

so $E(K)/2E(K)$ is finite. □

---

c) Absolute values

Definition

Let K be a field.

An absolute value on K is a map

$$|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0}$$

such that

(i) $\forall x \in K \ |x| = 0 \Leftrightarrow x = 0$
(ii) $\forall x, y \in K \ |xy| = |x|\,|y|$
(iii) $\forall x, y \in K \ |x+y| \leq |x| + |y|$

This absolute value is said to be <u>ultra metric</u> or non archimedean if it satisfies
(iii') $\forall x, y \in K, \ |x+y| \leq \max(|x|, |y|)$

<u>Examples</u>

a) Any field : the <u>trivial absolute value</u>

$$|x| = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{otherwise} \end{cases}$$

b) If $|\cdot|$ is an absolute value and $\lambda < 1$
$|\cdot|^\lambda$ is also an absolute value
(since $x \mapsto x^\lambda$ is concave
$x^\lambda \geq x$ for $x \in [0,1]$
So $\left(\frac{x}{x+y}\right)^\lambda + \left(\frac{y}{x+y}\right)^\lambda \geq 1$ for $x, y \in \mathbb{R}_{>0}$
which implies
$(x+y)^\lambda \leq x^\lambda + y^\lambda$.)

c) If K/k is a field extension
and $|\cdot|$ an absolute value on K
then $|\cdot|_{|k}$ is an absolute value on k

d) Over $\mathbb{R}$:
$|x|_\infty = \sup(x, -x)$ usual absolute value
is archimedean.

If $p \in \mathbb{P}$ prime number

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

ultra-metric absolute value

e] Over a number field K

$v \in Val(K)$

- If $v \in Val_\infty(K)$ defined by $\sigma : K \to \mathbb{C}$

$x \mapsto |\sigma(x)|$ is an absolute value (which depends only on v).

If $v = \mathfrak{p} \in Val_f(K)$ for any $C > 1$

$$x \longmapsto \begin{cases} C^{-v_{\mathfrak{p}}(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

defines an ultra-metric absolute value on K

In fact this applies to any Dedekind ring:

f] P irreducible polynomial in $k[T]$

$$k(T) \longrightarrow \mathbb{R}_{\geq 0}$$

$$F = \frac{N}{D} \longmapsto \begin{cases} C^{v_P(D) - v_P(N)} & \text{if } F \neq 0 \\ 0 \text{ if } F = 0 \end{cases}$$

is an absolute value as is

$$F = \frac{N}{D} \longmapsto \begin{cases} C^{\deg(N) - \deg(D)} \\ 0 \text{ if } F = 0 \end{cases}$$

Definition

An absolute value $|\cdot|$ defines a topology on K via the distance

$$d(x,y) = |x - y|$$

Proposition

Absolute values $|\cdot|_1$ et $|\cdot|_2$ define the same topology of K if and only if there exist $\lambda \in \mathbb{R}_{>0}$ such that

$$\forall x \in K, \quad |x|_1 = |x|_2^\lambda$$

Definition

Two absolute values are said to be equivalent if and only if they define the same topology

A place of K is an equivalence class of absolute values

Theorem [OSTROWSKI]

Any non-trivial absolute value on $\mathbb{Q}$ is equivalent either to the usual absolute value $|\cdot|$ or one of the p-adic values $|\cdot|_p$.

Corollary

Any non-trivial absolute value on a number field K is isomorphic to one defined in example 2.

Remark

In other words, $\mathrm{Val}(K)$ could be defined as the set of non-trivial places of K (or non-discrete topologies defined by absolute values on K)

Definition

If $v \in \mathrm{Val}(K)$, K_v is the completion of K for the topology defined by v.

Remark

Take $|\cdot|$ representing v, K_v may be constructed as the quotient of the ring of Cauchy sequences with values in K by the ideal of sequences converging to 0.

Examples

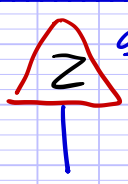
If $K = \mathbb{Q}$, we have canonical isomorphisms
- $\mathbb{Q}_\infty = \mathbb{R}$ completion for $|\cdot|_\infty = |\cdot|$
- $\mathbb{Q}_p = \mathbb{Q}_v$ if v is defined by $p \in \mathcal{P}$

(Note that $|p^n|_p \xrightarrow[n \to +\infty]{} 0$)

Normalization

Let K be a number field, and $v \in \mathrm{Val}(K)$ then
- if v is real (reminder) defined by $\sigma : K \to \mathbb{R}$
$$|\cdot|_v = |\sigma(x)|$$
- if v is complex defined by $\sigma : K \to \mathbb{C}$
$$|\cdot|_v = |\sigma(x)|^2$$
- if v is non-archimedean defined by non zero prime ideal $\mathfrak{p}$
$$|x|_v = N(\mathfrak{p})^{-v_{\mathfrak{p}}(x)}$$
where $N(\mathfrak{p}) = \# \mathbb{F}_{\mathfrak{p}}$ where $\mathbb{F}_{\mathfrak{p}}$ is the finite field $\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_K / \mathfrak{p}$.

Remarks



a) If v is complex, $|\cdot|_v$ is not an absolute value but $|\cdot|_v^{1/2}$ is

b) In all cases the corresponding topology is generated by the balls

$$B_v(a, r) = \{x \in K \mid |x-a|_v < r\}$$

c) $|\cdot|_v$ extends to K_v by continuity

Definition

If v is ultra metric

$$\mathcal{O}_v = \{y \in K_v \mid |y|_v \leq 1\}$$

is a subring of K_v called the ring of integers in K_v.

Proposition

$\mathcal{O}_v$ is a local ring, its maximal ideal is

$$\mathfrak{m}_v = \{y \in K_v \mid |y|_v < 1\}$$

and the residue field

$$\mathbb{F}_v = \mathcal{O}_v / \mathfrak{m}_v$$ is canonically isomorphic to the finite quotient $\mathbb{F}_p = \mathcal{O}_K / \mathfrak{p}$, where $\mathfrak{p}$ is the prime ideal corresponding to v

More generally the canonical morphism of rings

$$\mathcal{O}_K / \mathfrak{p}^n \longrightarrow \mathcal{O}_v / \mathfrak{m}_v^n$$

is an isomorphism and $\mathcal{O}_v$ is isomorphic to $\varprojlim_n \mathcal{O}_K / \mathfrak{p}^n$ (see the problem given in exercise session for the case of $\mathbb{Z}_p$).

Remark

- The isomorphism comes from the maps

$$\mathcal{O}_v \longrightarrow \mathcal{O}_v / \mathfrak{m}_v^n \xleftarrow{\sim} \mathcal{O}_{\mathfrak{p}} / \mathfrak{p}^n$$

- It is an isomorphism of topological rings

Notation

If K'/K is a finite field extension
w a place of K', v a place of K
$|\cdot|'$ an absolute value in w
We say that $v \mid w$ if $|\cdot|'_{|K}$ defines v.
(We also say that v is the restriction of w to K)

Prop

If K'/K is a finite field extension,
$v \in Val(K)$, $w \in Val(K')$ such that $v \mid w$
then
$$\forall y \in K'_w, \quad |y|_w = |N_{K_w/K_v}(y)|_v .$$

Proposition [Product formula]

Let K be a number field
$$\forall x \in K^*, \quad \prod_{v \in Val(K)} |x|_v = 1$$

This formula justify the choice of normalizations I have made.

Proof (sketch)

- When $K = \mathbb{Q}$, any number $x \in \mathbb{Q}^*$ may be written as $\varepsilon \prod_{p \in \mathcal{P}} p^{v_p(x)}$ with $\varepsilon \in \{-1, 1\}$ then

$$\prod_{v \in Val(\mathbb{Q})} |x|_v = \prod_{p \in \mathcal{P}} p^{v_p(x)} \times \prod_{p \in \mathcal{P}} \left| \prod_{p \in \mathcal{P}} p^{v_p(x)} \right|_p$$

$$= \prod_{p \in \mathcal{P}} p^{v_p(x)} \times \prod_{p \in \mathcal{P}} p^{-v_p(x)} = 1$$

Tensor product

Let E and F be two vector spaces over a field K, then $E \otimes F$ is a K vector space with a bilinear map

$$E \times F \to E \otimes F$$
$$(x, y) \mapsto x \otimes y$$

which is universal: for any K vector space G and any bilinear map

$$\varphi : E \times F \to G$$

there exists a unique K linear map

$$\overline{\varphi} : E \otimes F \to G$$

such that $E \times F \xrightarrow{\varphi} G$ commute

$$E \times F \searrow E \otimes F \xrightarrow{\overline{\varphi}} G$$

If $(e_i)_{i \in I}$ is a basis of E and $(f_j)_{j \in J}$ a basis of F then

$(e_i \otimes f_j)_{(i,j) \in I \times J}$ is a basis of $E \otimes F$.

If R is a commutative K algebra and A is a K-algebra then

$R \otimes_K A$ is an R algebra in which the product is defined by

$$(\lambda \otimes a)(\mu \otimes b) = (\lambda\mu \otimes ab)$$

Example

$$R \otimes \mathcal{M}_n(K) \simeq \mathcal{M}_n(R).$$

- In general, for a number field K if $v \in Val(\mathbb{Q})$, one may prove that as a $\mathbb{Q}_v$ algebra

$$\underbrace{K \otimes_{\mathbb{Q}} \mathbb{Q}_v}_{\text{extension of scalars to } \mathbb{Q}_v} \simeq \underbrace{\prod_{w|v} K_w}_{\text{product of algebras}}$$

But if A is a finite dimensional algebra over a field k, and $a \in A$

$$N_{A/k}(a) = \det(m_a) \qquad m_a : A \to A,\ x \mapsto ax$$

We get

$$\forall x \in K,\ N_{K/\mathbb{Q}}(x) = \prod_{w|v} N_{K_w/\mathbb{Q}_v}(x) \text{ in } \mathbb{Q}_v$$

Taking norms we get

$$|N_{K/\mathbb{Q}}(x)|_v = \prod_{w|v} |N_{K_w/\mathbb{Q}_v}(x)|_w$$

$$= \prod_{w|v} |x|_w$$

↑ choice of normalizations

So

$$\prod_{w \in Val(K)} |x|_w = \prod_{v \in Val(\mathbb{Q})} \prod_{w|v} |x|_w$$

$$= \prod_{v \in Val(\mathbb{Q})} |N_{K/\mathbb{Q}}(x)|_v = 1 \quad \square$$

↑ since we have proven the result for $\mathbb{Q}$.

4) Heights over a number field

Definition

Let V a projective algebraic set and let $\phi : V \to \mathbb{P}^N_K$ be a morphism

For any $v \in Val(K)$, we fix

$$\|\cdot\|_v : K_v^{N+1} \longrightarrow \mathbb{R}_{\geq 0}$$

such that

(i) $\forall x \in K_v^{N+1}$, $\|x\|_v = 0 \iff x = 0$

(ii) $\forall \lambda \in K_v$, $\forall x \in K_v^{N+1}$ $\|\lambda x\|_v = |\lambda|_v \|x\|_v$

(iii) a) If v is ultrametric

$\forall x, y \in K_v^{N+1}$, $\|x+y\|_v \leq \max(\|x\|_v, \|y\|_v)$

b) If v is real

$\forall x, y \in K_v^{N+1}$ $\|x+y\|_v \leq \|x\|_v + \|y\|_v$

c) If v is complex

$\forall x, y \in K_v^{N+1}$ $\|x+y\|_v^{1/2} \leq \|x\|_v^{1/2} + \|y\|_v^{1/2}$

(We say that $\|\cdot\|_v$ is a v-adic norm on K_v^{N+1}).

Moreover we assume that for all $v \in Val(K)$ except in a finite set

$$\|(x_0, \dots, x_N)\|_v = \max_{0 \leq i \leq N} |x_i|_v .$$

Then for any $x \in V(K)$, its exponential height is given by

$$H(x) = \prod_{v \in Val(K)} \|(x_0, \dots, x_N)\|_v$$

if

$$\phi(x) = [x_0 : \dots : x_N] \text{ with } (x_0, \dots, x_N) \in K^{N+1}$$

The corresponding logarithmic height is given by

$$h(x) = \log(H(x)).$$

Remarks

a) Well defined :

* outside a finite set of places

$$\|(x_0,\dots,x_n)\|_v = \max_{0\le i\le n}(|x_i|_v)$$

and if $x_i \neq 0$, $\{v \in Val(K) \mid |x_i|_v \neq 1\}$ is finite

so $\{v \in Val(K) \mid \|(x_0,\dots,x_n)\|_v \neq 1\}$ is finite.

* if $\phi(x) = [y_0 : \dots : y_N]$

there exists $\lambda \in K^*$, such that $(y_0,\dots,y_N) = \lambda(x_0,\dots,x_N)$

Then

$$\prod_{v\in Val(K)} \|(y_0,\dots,y_N)\|_v = \prod_{v\in Val(K)} \|\lambda(x_0,\dots,x_N)\|_v$$

$$= \left(\prod_{v\in Val(K)} |\lambda|_v\right) \prod_{v\in Val(K)} \|(x_0,\dots,x_N)\|_v$$

$$= \prod_{v\in Val(K)} \|(x_0,\dots,x_N)\|_v$$

By the product formula

b) If $K = \mathbb{Q}$ and

$$\|(x_0,\dots,x_N)\|_p = \max_{0\le i\le N}(|x_i|_p) \text{ for any } p \in \mathcal{P}$$

then

$(x_0,\dots,x_N)$ is a primitive element in $\mathbb{Z}^{N+1}$

which gives $\gcd(x_0,\dots,x_N) = 1$

$$\|(x_0,\dots,x_N)\|_p = \max_{0\le i\le N}(|x_i|_p)$$

$$= p^{-\min_{0\le i\le N}(v_p(x_i))} = 1$$

So

$$H([x_0 : \dots : x_N]) = \prod_{v\in Val(K)} \|(x_0,\dots,x_N)\|_v = \|(x_0,\dots,x_N)\|_\infty.$$

So the definition for number fields does generalize the one given for rational numbers.

A height depends on the choice of the norms but how much ?

Proposition

If H and H' are heights on V associated to a morphism $\phi : V \to \mathbb{P}^N_{\bar{\mathbb{Q}}}$ then there exists constants $0 < C_1 < C_2$ such that

$$\forall P \in V(K), \quad C_1 H(P) \leq H'(P) \leq C_2 H(P)$$

In other words, $|h(x) - h'(x)|$ is bounded.

Lemma

For any $v \in \mathrm{Val}(K)$ the projective space $\mathbb{P}^n(K_v)$ is compact

Proof

- It is separated.
- Take $\|(x_0, \dots, x_n)\|_v = \max_{0 \leq i \leq n} |x_i|_v$

Then if $P = [x_0 : \dots : x_n] \in \mathbb{P}^n(K_v)$ take i_0 such that $|x_{i_0}| = \max_{0 \leq i \leq n} |x_i|_v$

$$P = \left[\frac{x_0}{x_{i_0}} : \dots : \frac{x_n}{x_{i_0}}\right] \quad \text{with} \quad \left\|\left(\frac{x_i}{x_{i_0}}, \dots, \frac{x_n}{x_{i_0}}\right)\right\|_v = 1$$

In other words

$$\{ y \in K_v^{n+1} \mid \|y\|_v = 1 \} \twoheadrightarrow \mathbb{P}^n(K_v)$$

is surjective, it is also continuous as restriction of continuous function

But $\{ y \in K_v^{n+1} \mid \|y\|_v = 1 \} \subset_{\text{closed}} \{ y \in K_v^{n+1} \mid \|y\|_v \leq 1 \}$

But

$$\{ y \in K_v^{n+1} \mid \|y\|_v \leq 1 \} = \{ y \in K_v \mid |y|_v \leq 1 \}^{n+1}$$

et

$$\{ y \in K_v \mid |y|_v \leq 1 \} = \begin{cases} [0,1] & \text{if } v \text{ is real} \\ \{ z \in \mathbb{C} \mid |z| \leq 1 \} & \text{if } v \text{ is complex} \\ \mathcal{O}_v & \text{if } v \text{ is ultra metric} \end{cases}$$

If v is ultra-metric $\mathcal{O}_v \simeq \varprojlim_n \mathcal{O}_K/\mathfrak{p}^n \subset \prod_n \underbrace{\mathcal{O}_K/\mathfrak{p}^n}_{\text{finite hence compact}}$ □ (closed)

compact by TYCHONOFF's thm.

Proof of the proposition

Say that H is defined by a family $(\|\cdot\|_v)_{v\in Val(K)}$ and H' by $(\|\cdot\|'_v)_{v\in Val(K)}$

Then for any place v of K, we may define

$$\frac{\|\cdot\|'_v}{\|\cdot\|_v} : \mathbb{P}^n(K_v) \longrightarrow \mathbb{R}_{>0}$$
$$[y_0 : \dots : y_n] \longmapsto \frac{\|(y_0,\dots,y_n)\|'_v}{\|(y_0,\dots,y_n)\|_v}$$

since the quotient does not depend on the choice of homogeneous coordinates.

This function is continuous since the composite

$$\mathbb{K}_v^{n+1} - \{0\} \to \mathbb{P}^n(K_v) \to \mathbb{R}_{>0}$$

is. Therefore it admits a maximum and a minimum which gives $0 < c_{1,v} < c_{2,v}$ such that

$$\forall\, y \in \mathbb{K}_v^{N+1} \qquad c_{1,v}\|y\|_v \le \|y\|'_v \le c_{2,v}\|y\|_v$$

but $\|\cdot\|_v = \|\cdot\|_v$ for all v outside a finite set so we may take $c_{1,v} = c_{2,v} = 1$ outside this finite set and put

$$C_1 = \prod_{v\in Val(K)} c_{1,v} \quad \text{and} \quad C_2 = \prod_{v\in Val(K)} c_{2,v}. \ \square$$

Of course it also depends on the choice of the morphism ϕ and this leads to heights the quotients of which are NOT bounded. I am going to describe a particular case

Proposition

Let $f : \mathbb{P}^m_K \to \mathbb{P}^n_K$ be a morphism defined by

$$f([x_0 : \cdots : x_m]) = [P_0(x_0, \ldots, x_m) : \cdots : P_n(x_0, \ldots, x_m)]$$

where $P_0, \ldots, P_n \in K[X_0, \ldots, X_m]$ are homogeneous polynomials of degree d; let $\phi : V \to \mathbb{P}^m_K$ me a morphism of al algebraic sets, let $(\|\cdot\|_v)_{v \in Val(K)}$ $(\text{resp. } (\|\cdot\|'_v)_{v \in Val(K)})$ be a family of v-adic norms for K^{m+1} $(\text{resp. } K^{m+1})$ and let H and H' be the corresponding heights then there exist constants $0 < C_1 < C_2$ such that

$$\forall x \in V(K) \quad C_1 \leq \frac{H'(x)}{H(x)^d} \leq C_2$$

Proof

By the last proposition we may assume that

$$\|(y_0, \ldots, y_m)\|_v = \max_{0 \leq i \leq m} |y_i|_v$$

and $\|(y_0, \ldots, y_n)\|'_v = \max_{0 \leq i \leq n} |y_i|_v$

If $P = \sum_{\underline{\alpha} \in \mathbb{N}^m} a_{\underline{\alpha}} \underline{X}^{\underline{\alpha}} \in K[X_0, \ldots, X_m]$

we write

$$\|P\|_v = \max_{\underline{\alpha} \in \mathbb{N}^m} |a_{\underline{\alpha}}|_v$$

Note that

$$\|P\|_v \leq 1 \text{ for almost all } v \in Val(K)$$

(which means outside a finite set).

Since P_i is homomgeneous of degree d

$$P_i = \sum_{\sum_{i=0}^m \alpha_i = d} a_{\underline{\alpha}} \prod_{i=0}^m X_i^{\alpha_i}$$

and thus

$$|P_i(y_0, \ldots, y_m)|_v \leq C_{d,m,v} \|P\|_v \max_{0 \leq i \leq m} (|y_i|_v)^d \quad \left(C_{d,m,v} = 1 \text{ if } v \text{ archimedean}\right)$$

$$\leq C_{d,m,v} \|P\|_v \|(y_0, \ldots, y_m)\|^d$$

so we get $H'(x) \leq \left(\prod_v C_{d,n,v} \|P\|_v\right) H(x)^d$.

Let us now prove the lower bound
Since the P_i's define a morphism, we have that
$\forall\ x=[x_0:\dots:x_m]\in \mathbb{P}^m(\bar{K})$, $(P_0(x_0,\dots,x_m),\dots,P_n(x_0,\dots,x_m))\neq 0$
By HILBERT's Nullstellensatz, this implies that there exists N such that

$$X_i^N \in (P_0,\dots,P_n) \text{ for all } i\in\{0,\dots,m\}$$

So we may write

$$X_i^N = Q_{i,0}P_0+\dots+Q_{i,n}P_n \text{ for } i\in\{0,\dots,m\}$$

By writing each $Q_{i,j}$ as a sum of homogeneous polynomials, we see that we may assume that $Q_{i,j}$ is homogeneous of degree $N-d$.
So if we take $(y_0,\dots,y_m)\in K_v^{m+1}$
and put $z_i=P_i(y_0,\dots,y_m)$ for $i\in\{0,\dots,n\}$
we get ($\leftarrow$ 1 if v finite)

$$|y_i|_v^N \leq C_{N,m,v}\max_{0\leq j\leq N}\|Q_{i,j}\|\max_{0\leq i\leq m}(|y_i|_v)^{N-d}\max_{0\leq i\leq n}(|z_i|_v)$$

So

$$\|(y_0,\dots,y_m)\|_v^d \leq C_v\,\|(z_0,\dots,z_n)\|_v$$

for all $v\in \mathrm{Val}(K)$ with $C_v=1$ for almost all $v\in\mathrm{Val}(K)$. Take $C_1=\prod_{v\in\mathrm{Val}(K)} C_v^{-2}$. □

5| Finiteness theorem

Notation

Let $P\in\mathbb{P}^n(\bar{\mathbb{Q}})$ write $P=[y_0:\dots:y_n]$
Then $\mathbb{Q}(P)=\mathbb{Q}[y_i/y_j,\ 0\leq i,j\leq n,\ y_j\neq 0]$
is called the field of definition of P.

The degree of P is

$$\deg(P) = [\mathbb{Q}(P) : \mathbb{Q}]$$

and we define

$$H_N^{norm}(P) = H_N(P)^{1/[\mathbb{Q}(P):\mathbb{Q}]}$$

where $H_N : \mathbb{P}^n(\overline{\mathbb{Q}}) \to \mathbb{R}_{\geq 0}$ is the usual height with $\|(y_0, \dots, y_n)\|_v = \max_{0 \leq i \leq n} |y_i|_v$ for all places v.

Remark

In fact if $y_{i_0} \neq 0$ $\quad \mathbb{Q}(P) = \mathbb{Q}\left[\frac{y_0}{y_{i_0}}, \dots, \frac{y_n}{y_{i_0}}\right]$

Theorem [NORTH COTT]

Let $d \in \mathbb{N}$ and $B \in \mathbb{R}_{\geq 0}$; the set

$$\{ P \in \mathbb{P}^n(\overline{\mathbb{Q}}) \mid \deg(P) = d \ \& \ H_n(P) \leq B \}$$

($H_n(P)$ over $\mathbb{Q}(P)$)

is finite.

Remark

SCHANUEC provides an explicit estimate for

$$\#\{ P \in \mathbb{P}^n(K) \mid H_n(P) \leq B \}$$

for any number field K, but the result of NORTHCOTT is stronger, since we are considering all the points in all number fields of degree d over $\mathbb{Q}$

Sketch of the proof

We want to reduce to the case of the projective space over $\mathbb{Q}$, for which the result is known (and easy to prove).

If $K \subset \overline{\mathbb{Q}}$ $\quad G_K = Gal(\overline{\mathbb{Q}}/K) = \underset{K\text{-alg}}{Aut}(\overline{\mathbb{Q}})$

How can we characterize the points in $\mathbb{P}^n(\overline{\mathbb{Q}})$ such that $\deg(P)$ is d? I remind you that there is an action

$$G_{\mathbb{Q}} \text{ acts on } \mathbb{P}^n(\overline{\mathbb{Q}})$$

via $\sigma([x_0 : \cdots : x_n]) = [\sigma(x_0) : \cdots : \sigma(x_n)]$

If $P = [x_0 : \cdots : x_n] \in \mathbb{P}^n(K)$ for a # field K, (which implies $\mathbb{Q}(P) \subset K$)

then G_K acts trivially on P

and therefore the cardinal of the orbit

$\#\, G_{\mathbb{Q}} \cdot P \mid [G_{\mathbb{Q}} : G_K] = [K : \mathbb{Q}]$

Conversely if $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$

Let G_P be the stabilizer of P in $G_{\mathbb{Q}}$

Then $\sigma \in G_P \Leftrightarrow \sigma P = P \Leftrightarrow \sigma_{|\mathbb{Q}(P)} = \mathrm{Id}_{\mathbb{Q}(P)}$

Thus $G_P = G_{\mathbb{Q}(P)}$.

$$\deg(P) = [\mathbb{Q}(P) : \mathbb{Q}] = [G_{\mathbb{Q}} : G_{\mathbb{Q}(P)}] = \#\, G_{\mathbb{Q}} \cdot P$$

So we want to find the orbits in $\mathbb{P}^n(\overline{\mathbb{Q}})$ which are of cardinal d. To describe that let us consider the set of subsets of $\mathbb{P}^n$ of cardinal d which we want to describe as an algebraic set. More precisely

The symmetric group $\mathfrak{S}_d$ acts on $(\mathbb{P}^n)^d$ by permuting the components

$$S^d\mathbb{P}^n = (\mathbb{P}^n)^d / \mathfrak{S}_d$$

corresponds to d-uples in which we forget the ordering.

[Remark

a) Construction of quotients (idea)

Affine case $X = \mathrm{Spec}(A)$ with an action of

a finite group G, $G \subseteq A$
A function on the quotient

$$\begin{array}{ccc} X/G & \xrightarrow{f} & \mathbb{A}^1_k \\ \uparrow & \nearrow & \\ X & & \end{array}$$

corresponds to a function on X which is G equivariant :

$$\forall \sigma \in G, \quad f(\sigma^{-1}(x)) = f(x)$$

So the 1st idea to construct the quotient is

$$X/G = \operatorname{Spec}(A^G)$$

(b) If $S^d \mathbb{P}^n$ is defined as an algebraic set, we have

$$\left(S^d \mathbb{P}^n(\bar{\mathbb{Q}})\right)^{G_{\mathbb{Q}}} = S^d \mathbb{P}^n(\mathbb{Q})$$

then if $x \in \mathbb{P}^n(\bar{\mathbb{Q}})$ has an orbit of cardinal d ($\# G_{\mathbb{Q}} \cdot x = d$) then this orbit is an element of

$$\left(S^d \mathbb{P}^1(\bar{\mathbb{Q}})\right)^{G_{\mathbb{Q}}} = S^d \mathbb{P}^n(\mathbb{Q})$$

We are reduced to prove the finiteness for points of bounded height in $S^d \mathbb{P}^1(\mathbb{Q})$.]

Example

$$S^2\mathbb{P}^1 = \mathbb{P}^1 \times \mathbb{P}^1 / \mathfrak{S}_2 \xrightarrow{\varphi} \mathbb{P}^2$$

$$\{[u_1 : v_1], [u_2, v_2]\} \longmapsto [u_1 u_2 : u_1 v_2 + v_1 u_2 : v_1 v_2]$$

homogeneous of degree 1 in (u_1, v_1) and (u_2, v_2)
symmetric $(u_1, v_1) \leftrightarrow (u_2, v_2)$

So we may define $S^2\mathbb{P}^1$ as $\mathbb{P}^2$ using the above map

If $K/\mathbb{Q}$ is a quadratic extension

$\mathrm{Gal}(K/\mathbb{Q}) = \{\mathrm{Id}_K, \sigma\}$

If $[u:v] \in \mathbb{P}^1(K)$ $\qquad\qquad \mathbb{P}^2(\mathbb{Q})$

$\{[u:v], [\sigma(u):\sigma(v)]\} \longmapsto [u\sigma(u) : u\sigma(v) + v\sigma(u) : v\sigma(v)]$

$\qquad\qquad\qquad\qquad\qquad\qquad\quad \| \qquad\quad \| \qquad\qquad \| \qquad\quad \|$

$\qquad\qquad\qquad\qquad\qquad\qquad\quad N_{K/\mathbb{Q}}(u) \qquad \mathrm{Tr}_{K/\mathbb{Q}}(u\sigma(v)) \qquad N_{K/\mathbb{Q}}(v).$

Proof (continued)

- Let us construct a morphism

$$(\mathbb{P}^n)^d \longrightarrow \mathbb{P}^N$$

for some $N \in \mathbb{N}$ which is invariant under $\mathfrak{S}_d$ and give an injective map

$$(\mathbb{P}^n(\bar{\mathbb{Q}})^d)/\mathfrak{S}_d \hookrightarrow \mathbb{P}^N(\bar{\mathbb{Q}})$$

Take coordinates $X_{i,j}$, $0 \le j \le n$ for the i^{th} component of the product and define

$$\prod_{i=1}^{d} \left(\sum_{j=0}^{n} X_{i,j}\, Y_j\right) = \sum_{(j_1,\dots,j_d)\in\{0,\dots,n\}^d} \prod_{i=0}^{d} X_{i,j_i}\, Y_{j_i}$$

$$= \sum_{k_0+\cdots+k_n=d} Q_{k_0,\dots,k_n}(X_{i,j}) \prod_{j=0}^{n} Y_j^{k_j}$$

$$\psi \quad (\mathbb{P}^n)^d \longrightarrow \mathbb{P}^N$$

$$([x_{i,0}:\cdots:x_{i,n}]) \longmapsto \left(Q_{\underline{k}}(x_{i,j})\right)_{\sum_{i=0}^{n} k_i = d}$$

* This is well defined

- $Q_{k_0,\dots,k_n}(X_{i,j})$ is homogeneous of degree 1 in each set of variables
- if $Q_{\underline{k}}(x_{i,j}) = 0$ for all $\underline{k}$ then $\prod_{i=1}^{d}\left(\sum_{j=0}^{n} x_{i,j}\, Y_j\right)$ in $K[Y_0,\dots,Y_n]$ which is an integral ring, thus one of the terms

has to be 0

$\exists\, i \in \{1,\dots,d\}$, $\sum_{j=0}^{n} x_{i,j} Y_j = 0$

that is $(x_{i,0},\dots,x_{i,n}) = 0$ ↯ absurd

since $(x_{i,0},\dots,x_{i,n})$ are homogeneous coordinates

* invariant under the permutation of components in $(\mathbb{P}^n)^d$.

so it induces a map

$$\overline{\Psi} : (\mathbb{P}^n(\bar{Q}))^d / \mathfrak{S}_d \longrightarrow \mathbb{P}^N(\bar{Q})$$

* This map is injective:

If $\overline{\Psi}([x_{i,j}]) = \overline{\Psi}([y_{i,j}])$

so there exist $\lambda \in K^*$ such that

$$\prod_{i=1}^{d} \left(\sum_{j=0}^{n} x_{i,j} Y_j\right) = \lambda \prod_{i=1}^{d} \left(\sum_{j=0}^{n} y_{i,j} Y_j\right)$$

Since $\bar{Q}[Y_0,\dots,Y_n]$ is factorial, there exist $\sigma \in \mathfrak{S}_d$ and $(\lambda_1,\dots,\lambda_d) \in (K^*)^d$ such that

$$\sum_{j=0}^{n} x_{i,j} Y_j = \lambda_i \left(\sum_{j=0}^{n} y_{\sigma(i),j} Y_j\right) \text{ for } i \in \{1,\dots,d\}$$

then $[x_{i,0} : \dots : x_{i,n}] = [y_{\sigma(i),0} : \dots : y_{\sigma(i),n}]$ for $i \in \{1,\dots,d\}$

and $[x_{i,j}] = [y_{i,j}]$ in $\mathbb{P}^n(\bar{Q})^d / \mathfrak{S}_d$

* Let us assume that $P \in \mathbb{P}^n(\bar{Q})$

such that $\#\mathcal{G}_Q \cdot P \; d$

let $[P]$ be the point of $(\mathbb{P}^n(\bar{Q}))^d / \mathfrak{S}_d$ defined by the subset $\mathcal{G}_Q \cdot P = \{\sigma(P),\ \sigma \in \mathcal{G}_Q\}$

then for any $g \in \mathcal{G}_Q$

$$g(\mathcal{G}_Q \cdot P) = \mathcal{G}_Q \cdot P$$

therefore

$$g\left(\overline{\Psi}([P])\right) = \overline{\Psi}(P)$$

We get that

$$\overline{\Psi}([P]) \in \mathbb{P}^N(\bar{Q})^{\mathcal{G}_Q} = \mathbb{P}^N(Q).$$

Now let us describe the height.

Assume $x_{i,j} \in K$,

for any $(j_1, \dots, j_d) \in \{0, \dots, n\}^d$, and any $v \in \mathrm{Vol}(K)$

$$\left| \prod_{i=1}^{d} x_{i,j_i} \right|_v \leq \prod_{i=1}^{d} \|(x_{i,0}, \dots, x_{i,n})\|_v$$

So we get

$$H_K(\overline{\Psi}([x_{i,j}])) \leq C \prod_{i=1}^{d} H_{N_K}([x_{i,0} : \dots : x_{i,n}])$$

But if $\sigma \in G_{\mathbb{Q}}$ and $[x_0 : \dots : x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$

$$H^{\mathrm{norm}}([x_0 : \dots : x_n]) = H^{\mathrm{norm}}(\sigma[x_0 : \dots : x_n])$$

(Reminder $H^{\mathrm{norm}}([x_0 : \dots : x_n]) = H_n([x_0 : \dots : x_n])^{1/\deg(P)}$)

So if $\deg(P) = d$ and K is the galois closure of $\mathbb{Q}(P)$

$$H_N(\overline{\Psi}([P])) = H_N^{\mathrm{norm}}(\overline{\Psi}([P])) = H_K(\overline{\Psi}([P]))^{\frac{1}{[K:\mathbb{Q}]}}$$

$$\leq C' \left(\prod_{i=1}^{d} H_K(P) \right)^{\frac{1}{[K:\mathbb{Q}]}}$$

$$\leq C' H_K(P)^{\frac{d}{[K:\mathbb{Q}]}}$$

$$\leq C' H_{\mathbb{Q}(P)}(P)$$

We can now conclude the proof

$$\#\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) \mid \deg(P) = d \text{ and } H_n(P) \leq B\}$$

$$\leq d \, \#\{Q \in \mathbb{P}^N(\mathbb{Q}) \mid H_N(Q) \leq C'B\} < +\infty \quad \square$$

I Mordell - Weil theorem

Let us now apply this to elliptic curves

1) Naïve height on elliptic curve

Naïve height

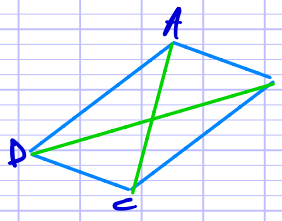
Let K be a number field
and let
$$E : Y^2 = X^3 + aX + b$$
be an elliptic curve over K
We define a morphism
$$\phi_x : E(K) \longrightarrow \mathbb{P}^1_K$$
$$[t : x : y] \mapsto [t : x] \text{ if } P \neq [0:0:1]$$
$$[t : x : y] \mapsto [x^2 + at^2 : y^2 - bt^2] \text{ where this is defined}$$
well-defined since $t(y^2 - bt^2) = x(x^2 + at^2)$
we define H_x as the height defined by ϕ_x
and $\|(x,t)\|_v = \max(|x|_v, |t|_v)$ for $v \in Val(K)$.
$h_x = \log \circ H_x$

Theorem

The map
$$C(K) \times C(K) \longrightarrow \mathbb{R}$$
$$(P, Q) \mapsto h_x(P+Q) + h_x(P-Q) - 2h_x(P) - 2h_x(Q)$$
is bounded.

Remark

This should remind you of the parallelogram equality
In a euclidean space
$$\|\vec{u} + \vec{v}\|^2 + \|\vec{u} - \vec{v}\|^2 - 2\|\vec{u}\|^2 - 2\|\vec{v}\|^2 = 0$$



$AC^2 + BD^2 = 2(AB^2 + BC^2)$

Proof

$$C \times C \xrightarrow{\phi} \mathbb{P}^1_K \times \mathbb{P}^1_K \xrightarrow{\text{Segre}} \mathbb{P}^2_K$$

$$([u_1 : v_1], [u_2 : v_2]) \mapsto [u_1 u_2 : u_1 v_2 + v_1 u_2 : v_1 v_2]$$

claim

$H(\phi(P,Q)) / H_x(P) H_x(Q)$ is bounded and thus $|h(\phi(P,Q)) - h_x(P) + h_x(Q)|$ is bounded

Proof

- $H(\phi(P,Q)) \leq C H(P) H(Q)$ by definition
- Let us prove the converse

  write $y_0 = u_1 u_2$, $y_1 = u_1 v_2 + v_1 u_2$, $y_2 = v_1 v_2$

  then

$$u_1^2 u_2^2 = u_1 u_2 y_0$$
$$u_1^2 v_2^2 = u_1 v_2 y_1 - v_1 v_2 y_0$$
$$v_1^2 u_2^2 = v_1 u_2 y_1 - u_1 u_2 y_3$$
$$v_1^2 v_2^2 = v_1 v_2 y_3$$

so

$$\max(|u_1|_v, |v_1|_v)^2 \max(|u_2|_v, |v_2|_v)^2$$
$$= \max(|u_1^2 u_2^2|_v, |u_1^2 v_2^2|_v, |v_1^2 u_2^2|_v, |v_1^2 v_2^2|_v)$$
$$\leq C_v \max(|y_0|_v, |y_1|_v, |y_2|_v) \max(|u_1|_v, |v_1|_v) \max(|u_2|_v, |v_2|_v)$$

($C_v = 1$ if v finite)

which implies

$$C' H(P) H(Q) \leq H(\phi(P,Q)).$$

On the other hand we have a morphism

$$\Psi : C \times C \longrightarrow C \times C$$
$$(P, Q) \longmapsto (P+Q, P-Q)$$

Let us now consider the diagram

$$\begin{array}{ccc} C \times C & \xrightarrow{\Psi} & C \times C \\ \downarrow \phi_x \times \phi_x & & \downarrow \phi_x \times \phi_x \\ ([t_1 : x_1], [t_2 : x_2]) \mathbb{P}^1 \times \mathbb{P}^1 & & \mathbb{P}^1 \times \mathbb{P}^1 \\ \downarrow \quad \downarrow \pi & & \downarrow \pi \\ [t_1 t_2 : t_1 x_2 + x_1 t_2 : x_1 x_2] \; \mathbb{P}^2 & \overset{\overline{\Psi}?}{- - - - \to} & \mathbb{P}^2 \end{array}$$

Let us construct $\overline{\Psi}$

- If $P = [1 : x_1 : y_1]$, $Q = [1 : x_2 : y_2]$
  $P+Q = [1 : x_3 : y_3]$, $Q = [1 : x_4 : y_4]$
  and assume $P \neq Q$ and $P \neq -Q$ (PQ): $Y = pX + q$

$$p_3 = \frac{y_2 - y_1}{x_2 - x_1} \qquad x_3 = p_3^2 - x_1 - x_2$$

Similarly

$$p_4 = \frac{y_2 + y_1}{x_2 - x_1} \qquad x_4 = p_4^2 - x_1 - x_2$$

$$x_3 + x_4 = p_3^2 + p_4^2 - 2(x_1 + x_2)$$
$$= 2\,\frac{y_1^2 + y_2^2 - (x_2 - x_1)^2 (x_1 + x_2)}{(x_2 - x_1)^2}$$

$$= 2\,\frac{x_1^3 + x_2^3 + a(x_1 + x_2) + 2b - (x_2 - x_1)^2 (x_1 + x_2)}{(x_2 - x_1)^2}$$

$$= 2\,\frac{(x_1 + x_2)(a + x_1 x_2) + 2b}{(x_1 + x_2)^2 - 4 x_1 x_2}$$

This is given by symmetric polynomials

Similarly

$$x_3 x_4 = (P_3^2 - x_1 - x_2)(P_4^2 - x_1 - x_2)$$

$$= \frac{(y_1^2 + y_2^2 - (x_1+x_2)(x_1-x_2)^2)^2 - 4 y_1^2 y_2^2}{(x_1-x_2)^4}$$

$$= \frac{(x_1^3 + x_2^3 + a(x_1+x_2) + 2b - (x_1+x_2)(x_1-x_2)^2)^2 - 4(x_1^3+ax_1+b)(x_2^3+ax_2+b)}{(x_1-x_2)^4}$$

$$= \frac{(x_1-x_2)^2 \left((x_1-x_2)^2 (x_1+x_2)^2 - 2(x_1+x_2)(x_1^3+x_2^3+a(x_1+x_2)+2b) + (x_1^2+x_1x_2+x_2^2+a)^2\right)}{(x_1-x_2)^4}$$

$$= \frac{x_1^2 x_2^2 - 2a x_1 x_2 - 4b(x_1+x_2) + a^2}{(x_1-x_2)^2}$$

$$= \frac{(x_1x_2 - a)^2 - 4b(x_1+x_2)}{(x_1+x_2)^2 - 4x_1x_2}$$

On définit donc

$$\Psi : \mathbb{P}^2_K \longrightarrow \mathbb{P}^2_K$$

$$[S^0 : S^1 : S^2] \longmapsto [S_1^2 - 4S_2S_0 : 2S_1(aS_0+S_2) + 4bS_0^2 : (S_2 - aS_0)^2 - 4bS_0S_1]$$

homogeneous of degree 2.

Well defined

If $S_1^2 - 4S_2S_0 = S_1(aS_0+S_2) + 2bS_0^2 = (S_2 - aS_0)^2 - 4bS_0S_1 = 0$

If $S_0 = 0$ then $S_1^2 = S_2^2 = 0$

Therefore $S_0 = S_1 = S_2 = 0$

otherwise put $x = \frac{S_1}{2S_0}$

then

$$x^2 = \frac{S_2}{S_0}$$ by the first equation

and

$$(x^2 - a)^2 - 8bx = 0 \quad \text{and} \quad 4(x^3 + ax + b) = 0$$

so $\gcd(X^4 - 2aX^2 - 8bX + a^2,\ X^3 + aX + b) \neq 1$

$\gcd(-3aX^2 - 9bX + a^2,\ X^3 + aX + b) \neq 1$

$R(-3aX^2 - 9bX + a^2,\ X^3 + aX + b) = 0$

$$\begin{vmatrix} 1 & 0 & -3a & 0 & 0 \\ 0 & 1 & -9b & -3a & 0 \\ a & 0 & a^2 & -9b & -3a \\ b & a & 0 & a^2 & -9b \\ 0 & b & 0 & 0 & a^2 \end{vmatrix} = \begin{vmatrix} 1 & -9b & -3a & 0 \\ 0 & 4a^2 & -9b & -3a \\ a & 3ab & a^2 & -9b \\ b & 0 & 0 & a^2 \end{vmatrix}$$

$$= \begin{vmatrix} 4a^2 & -9b & -3a \\ 12ab & 4a^2 & -9b \\ 9b^2 & 3ab & a^2 \end{vmatrix} = 16a^6 + 729b^4 - 108a^3b^2 + 108a^3b^2 + 108a^3b^2 + 108a^3b^2$$

$$= (4a^3 + 27b^2)^2 \neq 0 !$$

By the previous computation we have a commutative diagram

$$\begin{array}{ccc} \mathbb{C}\times\mathbb{C} & \xrightarrow{\Psi} & \mathbb{C}\times\mathbb{C} \\ \downarrow \phi_x \times \phi_x & (P,Q) \mapsto (P+Q, P-Q) & \downarrow \phi_x \times \phi_x \\ \mathbb{P}^1 \times \mathbb{P}^1 & & \mathbb{P}^1 \times \mathbb{P}^1 \\ \downarrow S & & \downarrow S \\ \mathbb{P}^2 & \xrightarrow{\overline{\Psi}} & \mathbb{P}^2 \end{array}$$

(still true if $0 \in \{P, Q, P+Q, P-Q\}$
also follows from the fact that
$\mathbb{C}\times\mathbb{C}$ is irreducible)

and, by the proposition, seen last time
$|h(\overline{\Psi}(P)) - 2h(P)|$ is bounded

But $\forall (P,Q) \in \mathbb{P}^1(\bar{K})^2 \quad |h(S(P,Q)) - h(P) - h(Q)|$
is bounded as well (cf. proof of Northcott theorem)

So

$$|h_x(P+Q) + h_x(P-Q) - 2h_x(P) - 2h_x(Q)|$$

is bounded □

Remark

In particular

$$|h_x(2P) - 4h_x(P)|$$

is bounded

2) NÉRON-TATE height

Definition

Let E be an elliptic curve over a number field K. For any $P \in E(K)$, the sequence $\frac{h_x(2^n P)}{4^n}$ converges and the NÉRON-TATE height of P is defined as

$$h_{NT}(P) = \lim_{n \to +\infty} \frac{h_x(2^n P)}{4^n}$$

Proof

if $p, q \in \mathbb{N}$ and $p \leq q$

$$\left| \frac{h_x(2^p P)}{4^p} - \frac{h_x(2^q P)}{4^q} \right| \leq \sum_{k=p}^{q-1} \left| \frac{h_x(2^{k+1} P) - 4h_x(2^k P)}{4^{k+1}} \right|$$

$$\leq \sum_{k=p}^{q-1} \frac{C}{4^{k+1}}$$

previous remark

$$\leq \frac{C}{3}\left(\frac{1}{4^p} - \frac{1}{4^q}\right)$$

Thus $\frac{h_x(2^k P)}{4^k}$ is a CAUCHY sequence and converges. □

Proposition 1

$$\forall P, Q \in E(K) \quad h_{NT}(P+Q) + h_{NT}(P-Q) = 2(h_{NT}(P) + h_{NT}(Q))$$

(really equals!)

Proof

By the previous proposition, there exists a constant C

$$|h_x(P+Q) + h_x(P-Q) - 2(h_x(P) + h_x(Q))| < C$$

we apply to $2^n P$ and $2^n Q$ we get

$$|h_x(2^n(P+Q)) + h_x(2^n(P-Q)) - 2(h_x(2^n P) + h_x(2^n Q))| < C$$

and so

$$\left| \frac{h_x(2^n(P+Q))}{4^n} + \frac{h_x(2^n(P-Q))}{4^n} - 2\left(\frac{h^x(2^n P)}{4^n} + \frac{h^x(2^n Q)}{4^n}\right)\right| < \frac{C}{4^n}$$

Taking the limit as $n \to +\infty$ gives the wanted formula. ☒

Proposition 2

The map

$$C(K) \times C(K) \longrightarrow \mathbb{R}_{\geq 0}$$

$$(P, Q) \longmapsto \langle P, Q\rangle_{NT} = \frac{h_{NT}(P+Q) - h_{NT}(P) - h_{NT}(Q)}{2}$$

is symmetric & $\mathbb{Z}$-bilinear.

Proof

- It is symmetric.
- Have to compute, for $P, Q, R \in E(K)$

$$2(\langle P, Q+R\rangle - \langle P, Q\rangle - \langle P, R\rangle)$$

$$= h_{NT}(P+Q+R) - \cancel{h_{NT}(P)} - h_{NT}(Q+R)$$
$$- h_{NT}(P+Q) + \cancel{h_{NT}(P)} + h_{NT}(Q)$$
$$- h_{NT}(P+R) + h_{NT}(P) - h_{TT}(Q)$$
$$= \frac{1}{2}(h_{NT}(P+Q+R) + h_{NT}(P+Q-R) - 2h_{NT}(P+Q) - 2h_{NT}(R)$$
$$- h_{NT}(P+Q-R) - h_{NT}(P-Q-R) + 2h_{NT}(P-R) + 2h_{NT}(Q)$$
$$+ h_{NT}(P-Q-R) + h_{NT}(P+Q+R) - 2h_{NT}(Q+R) - 2h_{NT}(P)$$
$$- 2h_{NT}(P+R) - 2h_{NT}(P-R) + 4h_{NT}(P) + 4h_{NT}(R))$$
$$= 0. \quad \square$$

Remarks

a) Let E be a normed vector space. The norm $\|\cdot\|$ on E is euclidean if and only if it satisfies the parallelogram equality:

$$\|\vec{u}+\vec{v}\|^2 + \|\vec{u}-\vec{v}\|^2 - 2\|\vec{u}\|^2 - 2\|\vec{v}\|^2 = 0$$

for any $\vec{u}, \vec{v} \in E$.

b) This implies that h_{NT} defines a bilinear symmetric form on the real vector space

$$E(K)_{\mathbb{R}} = E(K) \otimes_{\mathbb{Z}} \mathbb{R}$$

Prop 3

For any real number $B \in \mathbb{R}$

$$E(K)_{h_{NT} \leq B} = \{P \in E(K) \mid h_{NT}(P) \leq B\}$$

is finite.

Lemma

$|h_x - h_{NT}|$ is bounded

Proof of the lemma

Recall that there exists C such that

$$|h_x(2P) - 4h_x(P)| < C$$

So

$$\left|h_x(P) - \frac{h_x(2^n P)}{4^n}\right| \leq \sum_{k=0}^{n-1} \left|\frac{h_x(2^k P)}{4^k} - \frac{h_x(2^{k+1}P)}{4^{k+1}}\right|$$

$$\leq C \sum_{k=0}^{n-1} \frac{1}{4^k} < +\infty. \quad \square$$

Proof of the proposition

Let C be such that

$$\forall P \in E(K) \quad |h_x(P) - h_{NT}(P)| \leq C$$

then for any $B \in \mathbb{R}$

$$\{P \in E(K) \mid h_{NT}(P) \leq B\} \subset \{P \in E(K) \mid h_x(P) \leq B + C\}$$

But if $P, Q \in E(K)$ satisfy $\phi_x(P) = \phi_x(Q)$

then $Q \in \{-P, P\}$.

$$\{P \in E(K) \mid h_N(P) \leq B\} \leq 2 \#\{P \in \mathbb{P}^1(K) \mid h(P) \leq B + C\} < +\infty$$ By Northcott theorem □

Prop 4

$$P \in E(K)_{tors} \Leftrightarrow h_{NT}(P) = 0$$

Proof

By proposition 2,

$$h_{NT}(NP) = N^2 h_{NT}(P)$$

$\Rightarrow$) If $P \in E(K)_{tors}$

then $\{NP, N \in \mathbb{N}\}$ is finite

$\Rightarrow \{N^2 h_{NT}(P), N \in \mathbb{N}\}$ is finite

$\Rightarrow h_{NT}(P) = 0$.

$\Leftarrow$) if $h_{NT}(P) = 0$

then $\forall N \in \mathbb{N} \; h_{NT}(NP) = 0$

so $\{NP, N \in \mathbb{N}\} \subset \{P \in E(K) \mid h_{NT}(P) = 0\}$ which is finite by proposition 4

so $P \in E(K)_{tors}$

Corollary

$E(K)_{tors}$ is finite

Proof

As we have first seen

$$E(K)_{tors} = \{P \in E(K) \mid h_{NT}(P) = 0\} \text{ is finite. } \square$$

Remark (Reminder)

Choosing a morphism $\sigma : K \to \mathbb{C}$

$$E(K)_{tors} \subset E(\mathbb{C})_{tors}$$

and therefore there exist $(d_1, d_2) \in \mathbb{N}$, $d_1 \mid d_2$ such that

$$E(K) \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} . \square$$

3) Proof of MORDELL-WEIL theorem for elliptic curves

Theorem (Reminder)

If E is an elliptic curve over a number field K then $E(K)$ is finitely generated

Proof

Already seen:

$E(K)/2$ is finite

Let $P_1, \dots, P_m \in E(K)$ be such that their classes $\{[P_1], \dots, [P_m]\} = E(K)/2$

and let $B = \max_{1 \leq i \leq m} h_{NT}(P_i)$

We put

$$S = \{P \in E(K) \mid h_{NT}(P) \leq B\}$$

it is a finite set

It is enough to prove that S generates $E(K)$.

Let us assume that it is not the case

and let P be an element of $E(K) - \langle S \rangle$ of minimal height

(it exists since $\forall B \in \mathbb{R}$ $\{P \in E(K) \mid h_{NT}(P) \leq B\}$ is finite).

By definition of the P_i, there exists $i \in \{1, \dots, m\}$ such that

$$[P] = [P_i] \text{ in } E(K)/2$$

Then $P - P_i \in 2E(K)$ and $P + P_i \in 2E(K)$

write $(P - P_i) = 2Q$ and $(P + P_i) = 2R$

we have $h_{NT}(P - P_i) + h_{NT}(P + P_i) = 2h(P) + 2h(P_i)$

$< 4h(P)$

(Since $P \notin \langle S \rangle$ $P \notin S$)

But $2h(Q) + 2h(R) < 4h(P)$

So $h(Q) < h(P)$ or $h(R) < h(P)$

So $Q \in \langle S \rangle$ or $R \in \langle S \rangle$

But $P = P_i + 2Q = -P_i + 2R$

So $P \in \langle S \rangle$ contradiction ↯. □

4) NÉRON's theorem

Notations

Let E be an elliptic curve over a number field K in WEIERSTRAß form

Let h_{NT} be the NÉRON-TATE height on $E(K)$

$H_{NT} = \exp \circ h_{NT}$

$r = rk(E(K)) = \dim_{\mathbb{R}} (E(K)_{\mathbb{R}})$

$n = \# E(K)_{tors}$

$\Delta = \det(\langle \gamma_i, \gamma_j \rangle_{NT})$ where the $(\gamma_i)_{1 \leq i \leq r}$ is a basis of the $\mathbb{Z}$-module $E(K)/E(K)_{tors}$

Remark

We have seen that, by MORDELL-WEIL's theorem

$$E(K) \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \mathbb{Z}^r$$

with $d_1 | d_2$ and $w = d_1 d_2$;

Theorem (NÉRON)

$$\#\{E(K) \mid H_{NT} \leq B\} \underset{B \to +\infty}{\sim} \frac{\pi^{r/2}}{\Gamma(\frac{r}{2}+1)} \times \frac{w}{\sqrt{\Delta}} \log(B)^{r/2}$$

Remark

Remember that for the projective space

$$\#\{\mathbb{P}^n(\mathbb{Q}) \mid H \leq B\} \underset{B \to +\infty}{\sim} \frac{\mathrm{Vol}(B_{\|\cdot\|_\infty}(0,1))}{2\,\zeta_{\mathbb{Q}}(n+1)} B^{n+1}$$

So there are much less points on a elliptic curve. This can be explained by the exponential growth of the heights of points

$$H_{NT}(nP) = H_{NT}(P)^{n^2}$$

Let me now prove the theorem. Note that we have to prove that $\Delta \neq 0$ (the form is non-degenerate)

Lemma

There exists a unique bilinear form $\langle , \rangle$ on $E(K)_{\mathbb{R}}$ such that

$$\langle P \otimes 1, Q \otimes 1 \rangle = \langle P, Q \rangle_{NT}$$

for any $P, Q \in E(K)$ and this form is a scalar product (definite positive)

Proof

We have already seen that

$\langle , \rangle_{NT}$ is symmetric and $\mathbb{Z}$-bilinear on $E(K)$

Existence

If $P \in E(K)$ and $Q \in E(K)_{tors}$
then let $N \geq 1$ be such that $NQ = 0$
we get

$$\langle P, Q \rangle = \frac{1}{N} \langle P, NQ \rangle = 0$$

so the torsion points are in the kernel of the bilinear form which means it factors through the quotient

gives $\langle , \rangle : \left(E(K)/E(K)_{tors}\right)^2 \to \mathbb{R}$

$\downarrow \wr$

$\mathbb{Z}^r$

This extends to $E(K) \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{R}^r$ with

$$\langle P \otimes \lambda, Q \otimes \mu \rangle = \lambda\mu \langle P, Q \rangle$$

Unicity

The $P \otimes 1$ for $P \in E(K)$ generates the vector space $E(K)_{\mathbb{R}}$.

---

positivity

We now that

$$\forall B \in \mathbb{R}, \quad E(K)_{h_{NT} \leq B} \text{ is finite}$$

and

$$h_{NT}(NP) = N^2 h_{NT}(P)$$

So $\forall P \in E(K) \quad h_{NT}(P) \geq 0$

any element in $E(K) \otimes_{\mathbb{Z}} \mathbb{Q}$ might be written as $\frac{1}{b}(P \otimes 1)$ with $P \in E(K)$ and $b \in \mathbb{Z}\setminus\{0\}$

so $\forall x \in E(K)_{\mathbb{Q}}, \quad \langle x, x \rangle \geq 0$

Since $E(K)_{\mathbb{Q}}$ is dense in $E(K)_{\mathbb{R}}$ we get that the bilinear form is positive.

definite (which is the tricky point)

Let $x = \sum_{i=1}^{r} \gamma_i \otimes \lambda_i$ be such that $\langle x, x\rangle = 0$

then

$$\langle x+tg, x+tg\rangle = 2t\langle x,y\rangle + t^2\langle y,y\rangle$$

if $\langle x,y\rangle \neq 0$ this takes negative value values for small values of t.

So x is in the kernel of the bilinear form.

Let $\pi\ E(K)_{\mathbb{R}} \longrightarrow E(K)_{\mathbb{R}}/\mathbb{R}x$ be the projection

Then $\langle\ ,\ \rangle$ factors through π

$$\langle x,y\rangle = \langle \pi(x), \pi(y)\rangle$$

But $\{P \in E(K) \mid P\otimes 1 \in \mathbb{R}x\} \subset \{P \in E(K) \mid h_{NT}(P) = 0\}$ is finite

so $E(K)/E(K)_{tors} \longrightarrow E(K)_{\mathbb{R}}/\mathbb{R}x$

$P \longmapsto \pi(P\otimes 1)$

is injective, its image is a $\mathbb{Z}$ module of rank r

$> \dim\left(E(K)_{\mathbb{R}}/\mathbb{R}x\right) = r-1$; it is dense!

But

$$h_{NT}(P) = \langle \pi(P\otimes 1)\ \pi(P\otimes 1)\rangle$$

We get $\{P \in E(K) \mid h_{NT}(P) \leq 1\}$ is infinite $\lightning$. □

Remark

In particular $\Delta \neq 0$.

End of the proof

So put $\Lambda = \{P\otimes 1,\ P \in E(K)\}$ lattice in $E(K)_{\mathbb{R}}$

$$E(K)_{H_{NT} \leq B} = w\ \#\{P \in \Lambda \mid \langle P, P\rangle \leq \log(B)\}$$

$$\sim \frac{\mathrm{Vol}(B^r(0,1))}{\mathrm{Covol}(\Lambda)}\, w \left(\log(B)^{1/2}\right)^r. \quad \square$$

5| Upper bound for the rank in a particular case

Let us assume that

$E: Y^2T = (X-\alpha T)(X-\beta T)(X-\delta T)$ with $\alpha, \beta, \delta \in \mathbb{Z}$

$\Delta = (\alpha-\beta)^2(\beta-\delta)^2(\delta-\alpha)^2$

By the proof of the weak MORDELL-WEIL theorem

$$2^{r+2} \leq \#E(\mathbb{Q})/2 \leq \#\ker\left(\mathbb{Q}^*/\mathbb{Q}^{*2} \xrightarrow[P \nmid \Delta]{} \bigoplus \mathbb{Z}/2\mathbb{Z}\right)^2$$

$\downarrow S$

$$\{\pm 1\} \times \bigoplus_{p \in P} \mathbb{Z}/2\mathbb{Z}$$

Conclusion (naïve upper bound)

$$r \leq 2\,\#\{p \in P \mid p \mid (\alpha-\beta)(\beta-\delta)(\delta-\alpha)\}$$

Notation

Let a_1 be the number of $p \in P$ dividing exactly one of $(\alpha-\beta), (\beta-\delta), (\delta-\alpha)$

a_2 be the number of $p \in P$ dividing all three of them

Theorem

$$r \leq a_1 + 2a_2 - 1$$

Proof

We may assume $\alpha < \beta < \delta$

$$E(\mathbb{Q})/2 \longrightarrow \{\pm 1\}^2 \times \prod_{p \mid \Delta} (\mathbb{Z}/2\mathbb{Z})^2$$

$\varphi_\alpha, \varphi_\beta$ → $\mathbb{Q}^*/\mathbb{Q}^{*2}$ → sgn, v_p

If $[1:x:y] \in E(\mathbb{Q})$

$$x-\alpha > x-\beta > x-\delta$$

$(x-\alpha)(x-\beta)(x-\delta)$ is a square;

So $x-\alpha \geq 0$ so $\operatorname{sgn} \circ \varphi_\alpha = 1$

If p divides only one of $\alpha-\beta$, $\beta-\gamma$, $\gamma-\alpha$, say $\alpha-\beta$; then if $x \notin \{\alpha, \beta\}$

$v_p(x-\alpha) + v_p(x-\beta) + v_p(x-\gamma)$ is even

If $v_p(x-\alpha) < 0$ $\exists\, v_p(x-\alpha)$ is even $\Rightarrow v_p(x-\alpha)$ is

If $v_p(x-\alpha) > 0$ then $v_p(x-\beta) > 0$

and $v_p(x-\gamma) = 0$

and $v_p(x-\alpha) + v_p(x-\beta)$ is even

If $v_p(x-\alpha) = 0$ then $v_p(x-\beta) = 0$

and $v_p(x-\alpha) + v_p(x-\beta)$ is even

If $x = \alpha$,

$$v_p(\varphi_\alpha(P)) = v_p((\alpha-\beta)(\alpha-\gamma)) = v_p(\alpha-\beta) = v_p(\varphi_\beta(P))$$

in all cases

$(v_p(\varphi_\alpha(P)), v_p(\varphi_\alpha(P)) \in \mathbb{Z}/2\mathbb{Z}(1,1)$ □

Example

$$Y^2 T = X(X-T)(X+T)$$

$\Delta = 2^2$ $a_1 = 1$, $a_2 = 0$

So $r \leq 1-1 = 0$

Thus

$E(\mathbb{Q})$ is finite.

Remark

This upper bound is far from optimal!

VI Picard group and Jacobians

1) Function field of curves

Definition

Let K be a field and let C be an algebraic curve in $\mathbb{P}^2_K$ defined by an irreducible homogeneous polynomial $F \in K[T,X,Y]$ with $T \nmid F$. Then the function field of C is the field

$$K(C) = Fr(K[X,Y]/(F(1,X,Y)))$$

For this definition to make sense, we have to check that $F(1,X,Y)$ is irreducible; If $F=T$ we may permute the variables

Reminder

If $P \in K[X,Y]$ $\deg(P)=d$

$\tilde{P} = T^d P(\frac{X}{T}, \frac{Y}{T})$ homogeneous of degree d

Note that $\widetilde{PQ} = \tilde{P}\tilde{Q}$

Remarks

a) If $\deg(F(1,X,Y)) < \deg(F)$ then $T \mid F$ and this contradicts the fact that $\deg(F) \geq 2$ and F is irreducible

b) $F(1,X,Y)$ is irreducible as well

otherwise we may write

$F(1,X,Y) = Q(X,Y)R(X,Y)$ with

$\deg(F(1,X,Y)) = \deg(Q) + \deg(R)$, $q = \deg(Q) \geq 1$, $r = \deg(R) \geq 1$

Thus $\tilde{Q}\tilde{R} = \widetilde{F(1,X,Y)} \mid F(T,X,Y)$

contradicts the fact that P is irreducible

Therefore $K[X,Y]/F(1,X,Y)$ is integral

c] If $\deg_Y (F(1,X,Y)) > 0$
Then $F(1,X,Y)$ is irreducible in $K(X)[Y]$
and
$K(C)$ is isomorphic to $K(X)[Y]/(F(1,X,Y))$

d] We could do the same with the variables X or Y (if $X \nmid F$ and $Y \nmid F$)

$$\mathrm{Fr}\left(K[T,X]/(F(T,X,1))\right) \Rightarrow \mathrm{Fr}\left(K[X,Y]/(F(1,X,Y))\right)$$

$$T \longmapsto \frac{1}{Y}$$

$$X \longmapsto \frac{X}{Y}$$

$$P(T,X,1) \longmapsto P\left(\frac{1}{Y},\frac{X}{Y},1\right) = \frac{1}{Y^d} P(1,X,Y) = 0$$

e] The transcendance degree of $K(C)$ over K is one by the remark c) (we may have to exchange X and Y if necessary to apply it).

f] We keep the notations of the definition
Let $\varphi \in \mathrm{Mor}(C, \mathbb{P}^1_K)$ be such that φ is not the constant morphism with value $\infty = [0:1]$
Then φ is defined by pairs $(D_i, N_i)_{1 \le i \le n}$ of homogeneous polynomials of deg d in $K[T,X,Y]$ and $D_i \neq 0$ for all $i \in \{1, \dots, n\}$. Moreover for any $i,j \in \{1, \dots, n\}$

$$F \mid D_i N_j - N_i D_j$$

Therefore

$$\frac{\overline{N_i(1,X,Y)}}{\overline{D_i(1,X,Y)}} = \frac{\overline{N_j(1,X,Y)}}{\overline{D_j(1,X,Y)}} \quad \text{in } K(C) = \mathrm{Fr}\left(K[X,Y]/F(1,X,Y)\right)$$

If 2 morphisms φ and φ' have the same image we get

$$F(1,X,Y) \mid N_i'(1,X,Y) D_j(1,X,Y) - D_i'(1,X,Y) N_j(1,X,Y)$$

and therefore, as before

$$F \mid N_i' D_j - D_i' N_j,$$

So $[D_i'(t,x,y) : N_i(t,x,y)] = [D_j(t,x,y) : N_j(t,x,y)]$
whenever these points are defined. In other words $\varphi = \varphi'$

Conversely if $f = \frac{N(X,Y)}{D(X,Y)} \in k(C)$
then let $d = \max(\deg(N), \deg(D))$
We may consider $\hat{N}(T,X,Y) = T^d N(\frac{X}{T}, \frac{Y}{T})$ $\hat{D}(T,X,Y) = T^d D(\frac{X}{T}, \frac{Y}{T})$
and the map

$$[t:x:y] \to [D(t,x,y) : N(t,x,y)]$$

defined where $(D(t,x,y), N(t,x,y)) \neq (0,0)$
One can show that this extends to C
and defines a morphism

$$\varphi : C \to \mathbb{P}^1_k$$

Conclusion

One can see $k(C)$ as the set $\mathrm{Mor}(C, \mathbb{P}^1_k) - \{\infty\}$
where ∞ denotes the constant morphism $C \to \mathbb{P}^1_k$.

$$[t:x:y] \longmapsto [0:1]$$

There are very strong analogies between
number fields and function fields of curves.

Remark

If $N, D \in k[T,X,Y]$ are homogeneous
of some degree d, with $D \neq 0$; then
the quotient

$$\frac{N(T,X,Y)}{D(T,X,Y)}$$

defines an element in $k(C)$ (namely $\frac{N(1,X,Y)}{D(1,X,Y)}$)

Examples

a) For $\mathbb{P}^1_k \simeq$ projective line in $\mathbb{P}^2_a$

$$C : aT + bX + cY = 0 \text{ with } (b,c) \neq (0,0)$$

If $c \neq 0$

gives $F_2(K[X,Y]/(a+bX+cY)) \simeq F_2(K[X]) \simeq K(Y)$

b) For a conic C with a rational point seen as exercise

$$K(T) \simeq K(C)$$

c) For an elliptic curve E

$$K(C) \simeq F_2(K(X)[Y]/(Y^2 - X^3 - aX - b))$$

quadratic extension of $K(X)$.

Remark

Thinking of $f \in K(C)$ as a morphism $f : C \to \mathbb{P}^1_K$ means that for any field extension L of K f defines a map

$$f : C(L) \longrightarrow L \cup \{\infty\}$$

2) Analogy with number fields

Convention

In the rest of this chapter, we assume that K is algebraically closed in $K(C)$ (that is any element in $K(C)$ which is algebraic over K comes from K)

N.B.

We can always reduce to that case by replacing K by its algebraic closure in $K(C)$.

Definition

$Val(K(C)/K)$ is the set of non-trivial places in $K(C)$ with a trivial restriction to K

Example

Take $C = \mathbb{P}^1$ (given by $Y = 0$ in $\mathbb{P}^2_K$)

Then $K(C) \simeq K(X)$ field of rational functions in one variable. We have seen that

Any monic irreducible polynomial P in $K[X]$ defines a place by

$$\left|\frac{N}{D}\right|_P = \begin{cases} \exp(v_P(D) - v_P(N)) & \text{if } N \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

and there is a place at ∞ given by

$$\left|\frac{N}{D}\right|_\infty = \begin{cases} \exp(\deg(N) - \deg(D)) & \text{if } N \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

all places in $Val(K(X)/K)$ is the class of exactly one of theses.

Indeed $|\cdot| \in Val(K(X)/K)$ is ultra-metric:

$$|x+y|^m = \left|\sum_{k=0}^{n} \binom{m}{k} x^k y^{m-k}\right| \leq m \max(|x|, |y|)^m$$

So $|x+y| \leq m^{1/m} \max(|x|, |y|)$ and $m^{1/m} = \exp\left(\frac{\log(m)}{m}\right) \xrightarrow[m \to +\infty]{} 1$

If $|X| > 1$ then if $P = \sum_{i=0}^{d} a_i X^i$ with $a_d \neq 0$

$$\left|\sum_{i=0}^{d} a_i X^i\right| = |X|^d$$

and we get $\left|\frac{N}{D}\right| = \begin{cases} |X|^{\deg(N) - \deg(D)} & \text{if } N = 0 \\ 0 & \text{otherwise} \end{cases}$ $\quad |\cdot| \sim |\cdot|_\infty$

otherwise $|x| \leq 1$

and $K[x] \subset \{Q \in K(x) \mid |Q| \leq 1\}$

let $\mathfrak{p} = \{P \in K[x] \mid |P| < 1\}$

$\mathfrak{p} \neq (0)$ otherwise $|\cdot|$ is the trivial absolute value

Indeed if $|Q| = 1$ for $Q \in K[x] - \{0\}$, $|F| = 1$ for $F \in K(x)^*$.

and $\mathfrak{p}$ is a prime ideal so there exists a unique

$P \in \mathcal{I}_K$ such that $\mathfrak{p} = (P)$, and $|\cdot| \sim |\cdot|_P$.

Since any $F \in K(x)^*$ may be written as

$$F = u \prod_{P \in \mathcal{I}_K} P^{v_P(F)}$$

where $\mathcal{I}_K$ is the set of monic irreducible polynomials in $K[T]$

Reference about basic properties of absolute values

LANG Algebra, SPRINGER Verlag.

Prop

If $K = \bar{K}$ is algebraically closed and C is smooth over $\bar{K}$

then there is a unique bijection

$$\mathrm{Val}(\bar{K}(C)/\bar{K}) \overset{1:1}{\leftrightarrow} C(\bar{K})$$

such that if $|\cdot|$ corresponds to the point $P \in C(\bar{K})$

$\{f \in \bar{K}(C) \mid |f| < 1\}$ corresponds to the morphism

$\varphi : C \to \mathbb{P}^1_{\bar{K}}$ such that $\varphi(P) = [1:0]$.

Sketch of proof

- Since $\bar{K}(C)$ is a finite extension of $\bar{K}(T)$ any absolute value is ultra metric

- At least one of the following is true
  (i) $\left|\frac{X}{T}\right| \leq 1$ and $\left|\frac{Y}{T}\right| \leq 1$ where these quotients are seen in $K(C)$
  (ii) $\left|\frac{T}{X}\right| \leq 1$ and $\left|\frac{Y}{X}\right| \leq 1$
  (iii) $\left|\frac{T}{Y}\right| \leq 1$ and $\left|\frac{X}{Y}\right| \leq 1$

(Indeed if $\left|\frac{X}{T}\right| > 1$ and $\left|\frac{Y}{X}\right| > 1$ then $\left|\frac{T}{Y}\right| < 1$ and $\left|\frac{X}{Y}\right| < 1$)

By permuting the coordinates, we may assume that

$$K[X,Y]/(P(1,X,Y)) \subset \mathcal{O} = \{f \in K(C), |f| \leq 1\}$$

$$\mathfrak{p} = \{f \in K[X,Y]/(F(1,X,Y)) \mid |f| < 1\} \text{ prime ideal} \neq (0)$$

- HILBERT's Nullstellensatz (or rather one of the statements I used in its proof)

there exists $x, y \in K$ with $P(1,x,y) = 0$ such that

$$\mathfrak{p} \subset (\overline{X-x}, \overline{Y-y}) = \mathfrak{m} \text{ maximal ideal}$$

$P = [1:x:y] \in C(K)$. By a theorem of commutative algebra about dimensions any non zero prime ideal is maximal

$\mathfrak{m} = \mathfrak{p}$ and $\{f \in \bar{K}(C) \mid |f| < 1\} = \{f \in \bar{K}(C) \mid f(P) = [1:0]\}$

- Conversely if $P \in C(K)$

$\mathcal{O} = \{f \in K(C) \mid f(P) \neq \infty\}$ is a subring with maximal ideal $\mathfrak{m} = \{f \in K(C) \mid f(P) = 0\}$

Up to a permutation of the coordinate we may assume

$$P = [1:x:y] \; ; \; \mathfrak{m} = (\overline{X-x}, \overline{Y-y})$$

Since C is smooth at P, $\overline{X-x}$ or $\overline{Y-y}$ generate the K vector space $\mathfrak{m}/\mathfrak{m}^2$

(the equation of the tangent belongs to $\mathfrak{m}^2$)

We get that $\mathfrak{m} = \mathcal{O}\pi$

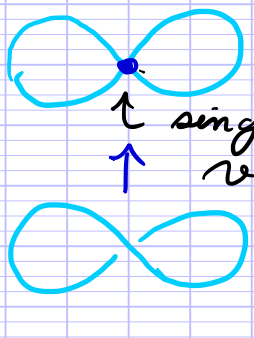
By a result of commutative algebra this implies that the map $v : A - \{0\} \to \mathbb{N}$ given by

$$v(f) = \max\{n \in \mathbb{N} \mid f \in \mathfrak{m}^n\}$$

extends in a valuation of K which defines

an absolute value $|.|$ on K.

Drawing

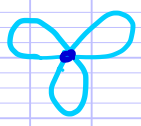


BERNOULLI's lemniscate

↑ singular corresponds to 2 absolute values

↑

$\mathbb{P}^1_K$



3 absolute values

Definition

If C is a smooth plane curve in $\mathbb{P}^2_K$
then the set of closed points of C is

$$C_{(0)} = \mathrm{Val}(K(C)/K)$$

For any $P \in C_{(0)}$ there exists a unique surjective valuation

$$v_P : K(C)^* \longrightarrow \mathbb{Z}$$

such that P is the class of the absolute value defined by v_P
Let $\mathcal{O}_P = \{ f \in K(C) \mid v_P(f) \geq 0 \}$
and $m_P = \{ f \in K(C) \mid v_P(f) > 0 \}$
then the residue field at P is

$$K(P) = \mathcal{O}_P / m_P$$

It is a finite extension of K and $\deg(P) = [K(P) : K]$

Remark

From the point of view of schemes
A closed points of a scheme X is a point such that $\{P\}$ is closed.

Examples

* For $C = \mathbb{P}^1_K$, if
  P is the class of $|\cdot|_\infty$ then $K(P) = K$ $\deg(P) = 1$
  if P is defined by $\mathfrak{p} \in \mathcal{P}_K$ then $K(P) = K[x]/(\mathfrak{p})$
  and $\deg(P) = \deg(\mathfrak{p})$.
* If $K = \overline{K}$
  $K(P) = K$ and $\deg(P) = 1$ for any P
* In general
  $\{ P \in C_{(0)} \mid \deg(P) = 1 \} \leftrightarrow C(K)$
* Exercise : If K is perfect
  $C_{(0)}$ corresponds to the orbits of $\mathrm{Gal}(\overline{K}/K)$
  in $C(\overline{K})$ and the degree is the cardinal of the orbit.

Normalization of the absolute value

If $P \in C_{(0)}$, $|f|_P = \begin{cases} \exp(-\deg(P)\, v_P(f)) & \text{if } f \neq 0 \\ 0 & \text{otherwise} \end{cases}$

Product Formula

$$\forall f \in K(C)^*, \quad \prod_{P \in C_0} |f|_P = 1$$

The proof is quite similar to the number field case

Idea of the proof (without the details)

* If $C = \mathbb{P}^1_K$, $K(C) = K(T)$
  write $f \in K(C)^*$ as $u \prod_{\mathfrak{p} \in \mathcal{P}_K} \mathfrak{p}^{v_\mathfrak{p}(f)}$

  then $\deg(f) = \sum_{\mathfrak{p} \in \mathcal{P}_K} v_\mathfrak{p}(f) \deg(\mathfrak{p})$

  so

  $$|f|_\infty = \exp\left(\sum_{\mathfrak{p} \in \mathcal{P}_K} v_\mathfrak{p}(f) \deg(\mathfrak{p}) \right)$$

  and

$$\prod_{P \in \mathcal{S}_K} |P| = \exp\left(-\sum_{P \in \mathcal{S}_K} v_P(f) \deg(P)\right)$$

(see the proof for $\mathbb{Q}$)

* In general $K(C)$ is a finite extension of $K(T)$ and using the norm $N_{K(C)/K}$ we reduce to the previous case.

Other expression

Taking the logarithm this formula might be written as

$$\forall f \in K(C)^*, \sum_{P \in C_{(0)}} v_P(f) \deg(P) = 0.$$

* Remark

BERKOVICH's space : the points are absolute values on a ring A. *

3) Divisors, Picard group

Remember

If $K = \bar{K}$ and $C = \mathbb{P}^1_{\bar{K}}$, I introduced the group

$$\mathrm{Div}(\mathbb{P}^1_{\bar{K}}) = \mathbb{Z}^{(\mathbb{P}^1(\bar{K}))}$$

with a degree map $\deg : \mathrm{Div}(\mathbb{P}^1_{\bar{K}}) \to \mathbb{Z}$

We are going to generalize this

Definition

For a smooth irreducible plane curve C in $\mathbb{P}^2_K$ (with K algebraically closed in $K(C)$), the divisor group of C is defined as

$$\mathrm{Div}(C) = \mathbb{Z}^{(C_{(0)})}$$

($C_{(0)}$ closed points of C)

An element of $\mathrm{Div}(C)$ is denoted by $\sum_{P \in C_{(0)}} n_P P$

The degree morphism

$$\deg : \mathrm{Div}(C) \to \mathbb{Z}$$
$$\sum_{P \in C_{(0)}} n_P P \longmapsto \sum_{P \in C_{(0)}} n_P \deg(P)$$

and the division map

$$\mathrm{div} : K(C)^* \to \mathbb{Z}$$
$$f \longmapsto \sum_{P \in C_{(0)}} v_P(f) P$$

The Picard group of C is the quotient

$$\mathrm{Pic}(C) = \mathrm{Div}(C) / \mathrm{im}(\mathrm{div})$$

By the product formula, the degree map induces a morphism of groups

$$\deg : \mathrm{Pic}(C) \to \mathbb{Z}$$

We define

$$\mathrm{Pic}^0(C) = \ker(\deg)$$

Examples

a) $\mathbb{P}^1_k$, conics

Since we have that any $R \in K(T)^*$ may uniquely be written as

$$R = a \prod_{P \in \mathbb{S}_k} P^{v_P(F)}$$

we get an exact sequence

$$0 \to k^* \to K(T)^* \to \mathrm{Div}(\mathbb{P}^1_k) \xrightarrow{\deg} \mathbb{Z} \to 0$$

$$\mathrm{Div}(\mathbb{P}^1_k) \cong \mathbb{Z} \oplus \bigoplus_{P \in \mathbb{S}_k} \mathbb{Z}$$

Therefore

$$\deg : \mathrm{Pic}(\mathbb{P}^1_k) \to \mathbb{Z}$$

is an isomorphism, and $\mathrm{Pic}^0(\mathbb{P}^1_k) = \{0\}$.

b] Elliptic curves in WEIRSTRASS's form / $K = \overline{K}$

We define a map

$$\varphi : E(\overline{K}) \longrightarrow Pic^0(E)$$
$$P \longmapsto [P] - [O]$$

Reminder : O is the unique point of intersection of E with the line $T = 0$

- Let P, Q, R be three aligned points on $E(\overline{K})$ and let $aX + bY + cT$ be the equation of the corresponding line. Then

$$\frac{aX+bY+cT}{T} \in K(C)$$

and

$$\operatorname{div}\left(\frac{aX+bY+cT}{T}\right) = P+Q+R-3O$$
$$= P+O+Q-O+R-O$$

So $\varphi(P) + \varphi(Q) + \varphi(R) = 0$

Moreover $\varphi(O) = 0$

So φ is a morphism of groups.

- Let $D \in Pic^0(E)$

We may write $D = \sum_{P \in E(\overline{K})} n_P [P]$ with $\sum_{P \in E(\overline{K})} n_P = 0$

Thus

$$D = \sum_{D \in E(\overline{K})} n_P \left([P] - [O]\right) \in Im(\varphi)$$

So φ is surjective.

- If P is in the kernel of φ, then

$$[P] - [O] = \operatorname{div}(f)$$

for some $f \in \overline{K}(E) = K(X)[Y]/(Y^2 - X^3 - aX - b)$

$$= K(X) + K(X)\,\overline{Y}$$

If $f = \frac{N(X)}{D(X)}$ then $\operatorname{div}(f) = \sum_P \left(n_P [P] + [-P]\right)$ with $\sum_P n_P = 0$

If $f = R_1(x) + R_2(x)\,\overline{Y}$ with $F_2 \neq 0$

$= R(x)\,(N_1(x) + N_2(x)\,Y)$ with $\gcd(N_1, N_2) = 1$

we may assume $F = 1$

then $\begin{cases} Y = -N_1(x)/N_2(x) \\ Y^2 = X^3 + aX + b \end{cases}$

we find $N_1(x)^2 - (X^3 + aX + b)\,N_2(x)^2 = \prod_{i=1}^{d} (X - \alpha_i)$

so $\operatorname{div}(f) = \sum_{i=1}^{d} [P_i] - d[0]$ with $d \geq 3$

where $P_i = \left[1 : \alpha_i : \frac{N_2(\alpha_i)}{N_1(\alpha_i)}\right]$

In particular the set $\{P_i,\ 1 \leq i \leq d\}$ contains no pairs $\{P, -P\}$ unless α_i is a root of $X^3 + aX + b$. But in that case, we would have $(X - \alpha_i)^2 \mid N_2^2$, $(X - \alpha_i) \mid N_1$ and $(X - \alpha_i) \mid N_2$ which contradicts $\gcd(N_1, N_2) = 1$. □

Conclusion

For an elliptic curve $E/K = \overline{K}$ we get an isomorphism $E(\overline{K}) \xrightarrow{\sim} \operatorname{Pic}^0(E)$

So we have a description of the $\operatorname{Pic}^0(E)$ as a an algebraic space. We wish to generalize that to arbitrary curves. In order to do that we have to study more precisely de divisor map

Prop

In general we have exact sequences

$$1 \to K^* \to K(C)^* \to \operatorname{Div}(C) \longrightarrow \operatorname{Pic}(C) \to 0$$

and

$$0 \to \operatorname{Pic}^0(C) \to \operatorname{Pic}(C) \xrightarrow{\deg} \mathbb{Z} \to 0$$

Proof

The only thing to check is that

$$K^* = \ker(\mathrm{div})$$

But if $f \in K(C)^* - K^*$ then f is transcendant / K (by hypothesis, it is not algebraic)

So $K(f) \supsetneq K(T)$ and we may take $|\cdot|_\infty$ on $K(T)$

$K(C)/K(T)$ is a finite extension

we may extend $|\cdot|$ to $K(C)$ and $|f| > 1$. □

4) Space of sections

We keep the notations for the curve C.

Definitions

A divisor $D = \sum_{P \in C_{(0)}} n_P P$ is said to be effective if $n_P \geq 0$ for any $P \in C_{(0)}$. We write $D \geq 0$.

If $D \in \mathrm{Div}(C)$ we define the space of section of D as

$$H^0(C, \mathcal{O}_C(D)) = \{ f \in K(C)^* \mid \mathrm{div}(f) + D \geq 0 \}$$

Remark

a) If $D = \sum_{P \in C_{(0)}} n_P P$ let us write $D_+ = \sum_{P \in C_{(0)}} \max(0, n_P) P$ and $D_- = \sum_{P \in C_{(0)}} \max(0, -n_P) P$ then D_+ and D_- are effective and $D = D_+ - D_-$

b) $H^0(C, \mathcal{O}(D))$ is a K-vector space of finite dimension.

Indeed we may see $K(C)$ as a finite extension of $K(T)$ (by choosing any $f \in K(C) - K$)

Let $\mathcal{O}$ be the integral closure of $K[T]$ in $K(C)$

it is a free $K[T]$ module of finite rank and a Dedekind ring.

Write $D = \sum_P n_P P$, and $D^+ = \sum_P n_P^+ P$

If $\{P \in C_{(0)} \mid P \neq \infty\}$ coincides with $\mathrm{Spec}(G) - \{(0)\}$

Let $B_0 \in \prod_{P \neq \infty} P^{n_P^+}$ (ideal of G)

let $f \in H^0(C, \mathcal{O}_C(D))$ then $A = B_0 f \in G$

we then consider the condition for $P \neq \infty$

$$\sum_{P \neq \infty} -v_P(B_0 f) = \sum_{P \neq \infty} -v_P(B_0 f)\deg(P) \leq \sum_{P \neq \infty} \left(-v_P(B_0) + n_P^+\right)\deg(P)$$

so $B_0 f$ belongs to a K subspace of G of finite dimension. □

Prop

If $[D] = [D']$ then

$H^0(C, \mathcal{O}_C(D))$ and $H^0(C, \mathcal{O}_C(D'))$

are isomorphic

Proof

Let $f \in K(C)$ be such that

$$D - D' = \mathrm{div}(f)$$

Then

$$H^0(C, \mathcal{O}_C(D)) \longrightarrow H^0(C, \mathcal{O}_C(D'))$$

$$g \longmapsto gf$$

$\mathrm{div}(g) + D \geq 0$ $\qquad$ $\mathrm{div}(gf) + D' = \mathrm{div}(g) + D \geq 0$ □

Notation

$h^0(C, \mathcal{O}_C(D)) = \dim\left(H^0(C, \mathcal{O}_C(D))\right)$

depends only on $[D] \in \mathrm{Pic}(C)$.

we also write

$$h^0([D]) = h^0(C, \mathcal{O}_C(D))$$

To explain the terminology "space of section", I need to introduce another point of view

5] The line bundles

Notation

We denote by $\mathbb{L}$ the affine line $\mathbb{A}^1_k$ equipped with

$$+ : \mathbb{L} \times \mathbb{L} \longrightarrow \mathbb{L}$$
$$(a, b) \longmapsto a + b$$

and the product

$$\times : \mathbb{L} \times \mathbb{L} \longrightarrow \mathbb{L}$$
$$(a, b) \longmapsto ab$$

The points $0, 1 \in \mathbb{L}(k)$

and the opposite

$$- : \mathbb{L} \longrightarrow \mathbb{L}$$
$$a \longmapsto -a$$

All those maps are morphisms of (affine) algebraic sets and define a "ring scheme" all the properties of rings corresponding to commutative diagrams

Definition which I should have given earlier

- A quasi-projective algebraic space is a functor of the form

$$V(A) = \left\{ [x_0 : \cdots : x_n] \in \mathbb{P}^n(A) \;\middle|\; \begin{cases} P_i(x_0, \ldots, x_n) = 0 \text{ for } 1 \le i \le k \\ Q_j(x_0, \ldots, x_n) \neq 0 \text{ for } 1 \le j \le l \end{cases} \right\}$$

for any PIR A

Example

Since $\mathbb{A}^n_k \to \mathbb{P}^n_k$ with image $X_0 \neq 0$ any affine space is quasi-projective

Definition

- A <u>vector bundle</u> E over a quasi-projective space X is a quasi projective space E with a morphism

$$\pi : E \to X$$

and morphisms above X

$$\begin{aligned} + &\quad E \times_X E \to E \\ \times &\quad \mathbb{L} \times E \to E \\ 0 &\quad X \to E \\ - &\quad E \to E \end{aligned}$$

such that all diagrams defining a $\mathbb{L}$ module commute and there is a covering of X by open sets U_i, $r \in \mathbb{N}$, and isomorphisms

$$E_{|U_i} \xrightarrow{\sim} \mathbb{L}^r \times U_i$$

compatible with $+, \times, 0, -$

- r is called the <u>rank of E</u>
- a <u>line bundle</u> is a vector bundle of rank 1

Explanations

a] $E \times_X E(A) = \{(y, y') \in E(A)^2 \mid \pi(y) = \pi(y')\}$

b] morphism above X means that the maps commutes with the natural morphisms to X

eg $+ : E \times_X E \to E$ commutes

$$\begin{array}{ccc} E \times_X E & \xrightarrow{+} & E \\ & \searrow^{(\pi/\pi)} \quad \swarrow_{\pi} & \\ & X & \end{array}$$

Examples

a) For any X: $\mathbb{L} \times X$, with $\pi = pr_2 : \mathbb{L} \times X \to X$ trivial line bundle (also denoted by $\mathcal{O}_X$)

b) Over $\mathbb{P}^n_K$:

$\mathcal{O}_{\mathbb{P}^n_K}(-1) \subset \mathbb{P}^n_K \times \mathbb{A}^{n+1}_K$ given by $X_i Y_j - X_j Y_i = 0$

$([X_0 : \dots : X_n], (Y_0, \dots, Y_n))$

this corresponds to the pairs $(D, y) \in \mathbb{P}^n_K \times \mathbb{A}^{n+1}_K$ such that $y \in D$ (Remember that an element in $\mathbb{P}^n(K)$ is a subspace of K^{n+1} of dimension 1).

c) More generally over $\mathbb{P}^n_K$: Let $k \in \mathbb{Z}$ $\mathcal{O}_{\mathbb{P}^n_K}(k)$ given by

$$\mathcal{O}_{\mathbb{P}^n}(k) \subset \mathbb{P}^n_K \times \mathbb{A}^{n+1}_K \quad X_i^{-k} Y_j - X_j^{-k} Y_i = 0 \text{ if } k < 0$$

$$\mathcal{O}_{\mathbb{P}^n}(k) \subset \mathbb{P}^n_K \times \mathbb{P}^{n+1}_K \begin{cases} X_i^k Y_j - X_j^k Y_i = 0 & \text{if } k \geq 0 \\ (Y_0, \dots, Y_n) \neq (0, \dots, 0) \end{cases}$$

Let us check that is locally trivial

$U_i : X_i \neq 0 \subset \mathbb{P}^n_K$

$k < 0$ $\quad U_i \times \mathbb{A}^1_K \xrightarrow{\sim} \mathcal{O}_{\mathbb{P}^n}(k)_{|U_i}$

$([X_0 : \dots : X_n], T) \longmapsto ([X_0 : \dots : X_n], T\left(\frac{X_0}{X_i}\right)^{-k}, \dots, T\left(\frac{Y_n}{X_i}\right)^{-k})$

$k \geq 0$ $\quad U_i \times \mathbb{A}^1_K \xrightarrow{\sim} \mathcal{O}_{\mathbb{P}^n}(k)$

$([X_0 : \dots : X_n], T) \longmapsto ([X_0 : \dots : X_n], [T X_i^k : X_0^k : \dots : X_n^k]$

Note that the change of charts are given by

$$U_i \cap U_j \times \mathbb{A}^1_K \longrightarrow U_j \cap U_i \times \mathbb{A}^1_K \quad \text{for any } k!$$

$$([X_0 : \dots : X_{i-1} : 1 : X_{i+1} : \dots : X_n], T) \longmapsto \left(\left[\frac{X_0}{X_j} : \dots : \frac{1}{X_i} : \dots : \frac{X_n}{X_j}\right], T X_j^{-k}\right)$$

d) If $E \to X$ and $F \to X$ are vector bundles then $E \oplus F = E \times_X F$ is a vector bundle of rank $rk(E) + rk(F)$

Remark

It is possible to define a vector bundle $E \otimes F$ as well.

c) if $E \to Y$ is a vector bundle and $f : X \to Y$ is a morphism then $E \times_Y X$ with $\pi = pr_2 : E \times_Y X \to X$ is a vector bundle called the pull-back of E to X and denoted by $f^*(E)$.

Definition

* If E is a vector-bundle over X, L an extension of k and $x \in X(L)$ then $x^*(E)$ is a L vector space, called the fibre of E at x and denoted by E_x.
* If E is a vector bundle then the space of section of π (that is the set of morphisms $s : X \to E$ such that $\pi \circ s = Id_X$) is a k-vector space denoted $\Gamma(X, E)$.

Example

a) The sections $s \in \Gamma(X, \mathcal{O}_X)$ are the morphisms $f : X \to \mathbb{A}^1_k$ (that is the functions from X to k which are locally given by polynomials).

b) Let us consider $X = \mathbb{P}^n_k$. Recall that

$$\mathcal{O}_{\mathbb{P}^n_k}(1)_x = x$$

Let us look for the sections of $\mathcal{O}(1)$. On the charts they are given by

$$\begin{array}{ccc} U_i & \longrightarrow & \mathbb{A}^n_k \\ \uparrow s & \nearrow_{s_i \text{ polynomial}} & \\ \mathbb{A}^n_k & & \end{array} \qquad s_i \in k[x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n]$$

The description for the change of charts gives
$S_i\left(\frac{X_0}{X_i}, \dots, \frac{X_{i-1}}{X_i}, \frac{1}{X_i}, \frac{X_{i+1}}{X_i}, \dots, \frac{X_{j-1}}{X_j}, \frac{X_{j+1}}{X_j}, \dots, \frac{X_n}{X_j}\right) = X_j^{-k} S_i(X_0, \dots, X_{i-1}, X_{i+1}, \dots, X_n)$
In $k[X_0, \dots, X_n]$ let us write
$$\tilde{S}_i = X_i^k \, S\left(\frac{X_0}{X_i}, \dots, \frac{X_{j-1}}{X_i}, \frac{X_{j+1}}{X_i}, \dots, \frac{X_n}{X_i}\right)$$
Then $\tilde{S}_i = \tilde{S}_j$.
So we get an element $S \in k[X_0, \dots, X_n]$ homogeneous of degree k
But $S(X_1, \dots, X_{i-1}, 1, X_{i+1}, \dots, X_n) \in k[X_0, \dots, X_{i-1}, X_{i+1}, \dots, X_n]$ for all $i \in \{1, \dots, n\}$, therefore $S \in k[X_0, \dots, X_n]$
Therefore
$$k \geq 0 \quad \text{or} \quad S = 0$$

Conclusion
$$\Gamma\left(\mathbb{P}^n_k, \mathcal{O}_{\mathbb{P}^n_k}(k)\right) = \begin{cases} \text{Vector space of homogeneous} \\ \text{polynomials of degree } k \text{ if } k \geq 0 \\ \{0\} \quad \text{otherwise} \end{cases}$$

So what is the connection with the Picard group?

Definition
Let L be a line bundle over a smooth projective curve C such that k is algebraically closed in $k(C)$
Since C is covered by open subsets on which L is trivial there exists $S \subset C$ finite and sections $s : U \to L$ distinct from $0_{|U}$.
at each point $P \in C_{(0)}$ we may choose a trivialization of L defined on an open set containing P so s induces $s_P \in k(C)$ and $v_P(s_P)$ does not depend on the trivialization
$$\operatorname{div}(s) = \sum_{P \in C_{(0)}} v_P(s_P) P$$

Proof

If we have 2 trivializations

$$L_{|U_1} \simeq U_1 \times \mathbb{L} \quad \text{and} \quad L_{|U_2} \simeq U_2 \times \mathbb{L}$$

at P then $P \in U_1 \cap U_2$

$$\begin{array}{ccc} L_{|U_1 \cap U_2} & = & L_{U_2 \cap U_1} \\ \downarrow s & & \downarrow s \end{array}$$

and $\varphi : U_1 \cap U_2 \times \mathbb{L} \xrightarrow{\sim} U_2 \cap U_1 \times \mathbb{L}$

defines an application

$$f : U_1 \cap U_2 \longrightarrow \mathbb{L}$$
$$Q \longmapsto p_2(\varphi(Q,1))$$

which has no zeroes (otherwise it is not an isomorphism)

and $s_P^2 = f s_P^1$ in $U \cap U_1 \cap U_2$

f extends in $f \in \mathcal{O}_P^* \subset K(C)$

gives $v_P(s_P^2) = 0 + v_P(s_P^1)$. □

Prop

$[\operatorname{div}(s)] \in \operatorname{Pic}(C)$ does not depend on the choice of s. This is called the <u>Chern class of L</u> and denoted by $c_1(L)$.

Proof

If s_1 and s_2 are 2 sections on $U_1 \cap U_2$

then $s_1/s_2 : U_1 \cap U_2 \longrightarrow \mathbb{P}^1_K$

$$P \longmapsto [u:v] \text{ such that } v s_2(P) = u s_1(P)$$

extends to $f : C \to \mathbb{P}^1_K$

and $\operatorname{div}(s_1) = \operatorname{div}(f) + \operatorname{div}(s_2)$. □

Remark

In fact, for smooth curves, c_1 gives a bijection

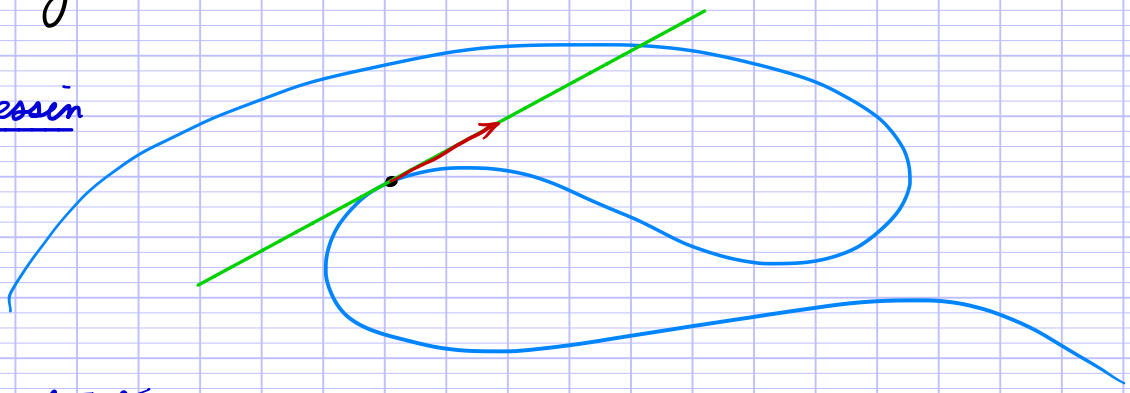
$$\text{Isom classes of line bundles} \xrightarrow{1:1} \text{Pic}(C)$$

(see HARTSHORNE chapter II.6)

6) The tangent line bundle

We have to be quite careful to define the tangent line bundle

Dessin



Construction

In the affine setting

$$TC_{|C\cap\mathbb{A}^2_K} \subset C\cap\mathbb{A}^2_K \times \mathbb{A}^2_K$$

$$F_0(x,y) = F_0(1,x,y)$$

$$\{(x,y,u,v) \mid \begin{cases} F_0(x,y)=0 \\ dF_0(x,y)(u,v)=0 \end{cases}\}$$

$$= \left\{(x,y,u,v) \,\middle|\, \begin{cases} F(1,x,y)=0 \\ \frac{\partial F}{\partial x}(1,x,y)\,u + \frac{\partial F}{\partial y}(1,x,y)\,v = 0 \end{cases}\right\}$$

We have to understand the change of variables

$U_0 \subset \mathbb{P}^2_K$ given by $T\neq 0$

$U_1 \subset \mathbb{P}^2_K$ ——— $X\neq 0$

$$\varphi\ U_0\cap U_1 \longrightarrow U_1\cap U_0$$

$$[1:X:Y] \longmapsto \left[\frac{1}{X} : 1 : \frac{Y}{X}\right]$$

The differential is given by

$$\text{Mat}\left(d\varphi_{(x,y)}\right) = \begin{pmatrix} -\frac{1}{x^2} & 0 \\ -\frac{y}{x^2} & \frac{1}{x} \end{pmatrix}$$

$$T U_0 \subset \mathbb{P}^2_k \times \mathbb{P}^{2\vee}_k$$

given by

$$\begin{cases} F(1,X,Y) = 0 \\ \frac{\partial F}{\partial X}(1,X,Y)\,U + \frac{\partial F}{\partial Y}(1,X,Y)\,V = 0 \end{cases}$$

as is $T U_1 \subset \mathbb{P}^3$

$$\begin{cases} F(T,1,Y) \\ \frac{\partial F}{\partial T}(T,1,Y)\,U + \frac{\partial F}{\partial Y}(T,1,Y)\,V = 0 \end{cases}$$

The change of charts is given by

$$T\varphi\,([1:X:Y],(U,V)) = \left[\tfrac{1}{X} : 1 : \tfrac{Y}{X}\right], \left(-\tfrac{1}{X^2}U,\ -\tfrac{Y}{X^2}U + \tfrac{1}{X}V\right)$$

and indeed using $T\frac{\partial F}{\partial T} + X\frac{\partial F}{\partial X} + Y\frac{\partial F}{\partial Y} = F$ and $F(1,X,Y) = 0$

$$\frac{\partial F}{\partial T}\left(\tfrac{1}{X},1,\tfrac{Y}{X}\right)\left(-\tfrac{1}{X^2}U\right) + \frac{\partial F}{\partial Y}\left(\tfrac{1}{X},1,\tfrac{Y}{X}\right)\left(-\tfrac{Y}{X^2}U + \tfrac{1}{X}V\right)$$

$$= \frac{\partial F}{\partial X}(1,X,Y)\left(\frac{U}{X^{d+2}}\right) + \frac{\partial F}{\partial Y}(1,X,Y)\left(\frac{UY}{X^{d+1}} - \frac{UY}{X^{d+1}}\right) + \frac{\partial F}{\partial Y}(1,X,Y)\left(\frac{V}{X^{d+1}}\right) = 0$$

N.B.

For TU_0 we take

$$(U,V) = \left(\frac{\partial F}{\partial Y}(1,X,Y), -\frac{\partial F}{\partial X}(1,X,Y)\right)$$

as section. (as the curve is smooth it has neither zero nor pole)

Changing charts this gives

$$(U',V') = \left(-\frac{1}{X^2}\left(\frac{\partial F}{\partial Y}(1,X,Y)\right), -\frac{Y}{X^2}\frac{\partial F}{\partial Y}(1,X,Y) - \frac{1}{X}\frac{\partial F}{\partial X}(1,X,Y)\right)$$

$$= \left(-X^{d-3}\left(\frac{\partial F}{\partial Y}\left(\tfrac{1}{X},1,\tfrac{Y}{X}\right)\right), X^{d-3}\frac{\partial F}{\partial T}\left(\tfrac{1}{X},1,\tfrac{Y}{X}\right)\right)$$

$$= T'^{3-d}\left(-\frac{\partial F}{\partial Y}(T',1,Y'), \frac{\partial F}{\partial T}(T',1,Y')\right)$$

Remember that the intersection of C with the projective line $T = 0$ contains d points counted with multiplicities

Conclusion

The tangent line bundle TC on a curve C is isomorphic to $\mathcal{O}_{\mathbb{P}^2_K}(3-d)|_C$ and

$$\deg(TC) = d(3-d)$$

Definition

The genus of the curve is

$$g(C) = \frac{2 - \deg(TC)}{2}$$

Remark

This gives, for plane curves,

$$g(C) = \frac{2 - d(3-d)}{2} = \frac{d^2 - 3d + 2}{2} = \frac{(d-1)(d-2)}{2}$$

Note that this means that for a smooth algebraic curve in $\mathbb{P}^2_K$ the value of the genus is constrained. This does not mean that all genii are not possible.

This means that not all algebraic curve are isomorphic to a smooth curve $C \subset \mathbb{P}^2_K$.

Example

For an elliptic curve E we get $\deg(TC) = 0$ (and $g(C) = 1$)

In that case we have an isomorphism

$$t_p : E \to E$$
$$Q \mapsto P + Q$$

for any point P.

$$Tt_p : TE \to TE$$

induces an isomorphism from T_0E to T_pE

So we get an isomorphism

$$T_0E \times E \longrightarrow TE$$
$$(a, p) \mapsto (Tt_p(a))$$

So $TE \simeq \mathcal{O}_E$. which explains for which reason the degree has to be 0.

Définition

$K = -c_1(TC) \in \mathrm{Pic}(C)$. is called the the canonical class

7) Riemann-Roch theorem

which I am going to state without proof.

Theorem

Let C be a smooth curve of genus g then

$h^0(D) - h^0(K-D) = \deg(D) + 1 - g$ for any $D \in \mathrm{Pic}(C)$

See Hartshorne chapter IV.1 for the proof

Prop

If $\deg(D) < 0$ then $h^0(D) = 0$

Proof

If $f \in H^0(C, \mathcal{O}(D)) - \{0\}$

$\mathrm{div}(f) + D \geq 0$

Taking the degree we get

$\deg(D) \geq 0$. □

Corollary

If $\deg(D) > 2g-2$ then

$$h^0(C, \mathcal{O}(D)) = \deg(D) + 1 - g.$$

Proof

$\deg(K) = 2g-2$

so $\deg(K-D) = 2g-2-\deg(D) < 0$ if $\deg(D) > 2g-2$. □

8] Construction of the Jacobian

I am going to skip some technical points.

Reminder

If we define $S^k \mathbb{P}^n_K$ as the quotient $(\mathbb{P}^n_K)^k / \mathfrak{S}_k$

then we have a natural map of functors

$$S^k \mathbb{P}^n_K \longrightarrow \mathbb{P}^N_K$$

$$([x_0 : \dots : x_n]) \longmapsto \text{coefficients of } \prod_{i=0}^{k} \left(\sum_{j=0}^{n} x_i y_i \right)$$

which is injective. The image is defined by polynomials (property of proper morphism in algebraic geometry) and thus we may see $S^k \mathbb{P}^n_K$ as an algebraic space

If C is a curve $C \subset \mathbb{P}^n_K$

then we get $S^k C \subset S^k \mathbb{P}^n_K \subset \mathbb{P}^N_K$

Example

If $C = \mathbb{P}^1_K$

$$S^k \mathbb{P}^1_K \xrightarrow{\sim} \mathbb{P}\left(K[U,V]_{=d} \right)$$

($K[U,V]_{=d}$: vector space of homogeneous polynomials of degree d)

$$([u_i : v_i]) \longmapsto \prod_{i=1}^{k} (v_i U + u_i V)$$

Indeed over $\bar{K}$ any polynomial in $K[U,V]_{=d}$ decomposes into a product of linear forms which is unique up to permutation

So $S^k \mathbb{P}^1_K \simeq \mathbb{P}^k_K$

Notation

$$\mathrm{Pic}^k(C) = \{ \alpha \in \mathrm{Pic}(C) \mid \deg(\alpha) = k \}$$

N.B.

- If $\mathrm{Pic}^k(C) \neq \emptyset$ then for any $\alpha \in \mathrm{Pic}^k(C)$
$\mathrm{Pic}^0(C) \longrightarrow \mathrm{Pic}^k(C)$ is bijective
$\beta \longmapsto \alpha + \beta$

Example

If C is a conic such that $C(k) = \emptyset$
One can show that
$\mathrm{Pic}^k(C) \neq \emptyset \iff k$ is even

Construction

There is a natural map
$$S_r : S^r C \longrightarrow \mathrm{Pic}^r(C)$$
$$[(P_1, \dots, P_r)] \longmapsto \sum_{i=1}^{r} [P_i]$$
Let $D \in \mathrm{Div}(C)$, $\deg(D) = r$

- Let $(P_1, \dots, P_r) \in S^r C$
If $\sum_{i=1}^{r} [P_i] = [D]$
then there exists $f \in k(C)^*$ such that
$$\mathrm{div}(f) = \sum_{i=1}^{r} P_i - D$$
In particular
$$\mathrm{div}(f) + D \geq 0$$
and $f \in H^0(C, \mathcal{O}_X(D))$.
- Conversely if $f \in H^0(C, \mathcal{O}_C(D))$
then $\mathrm{div}(f) + D \geq 0$
and $\deg(\mathrm{div}(f) + D) = \deg(D) = r$
so $\mathrm{div}(f) + D \in \mathrm{Im}(S_r)$
- Note that if $\mathrm{div}(f) + D = \mathrm{div}(g) + D$

Then $\operatorname{div}(f/g) = 0$
which implies that $f/g \in k^*$
Therefore
$$s_n^{-1}([D]) = \mathbb{P}(H^0(C, \mathcal{O}_C(D)))$$
which is empty if $H^0(C, \mathcal{O}_C(D)) = \{0\}$.

- If $n > 2g-2$, by the corollary to RIEMANN-ROCH theorem
$$h^0(C, \mathcal{O}_C(D)) = n + 1 - g > 0$$

Conclusion

If $n > 2g-2$
$$s_n : S^n C \longrightarrow \operatorname{Pic}^n(C)$$
is a fibration in projective spaces, where the fiber over $[D]$ is given by $\mathbb{P}(H^0(C, \mathcal{O}_C(D)))$ which is a projective space of dimension $n - g$.

And $S^n C$ has an algebraic structure. We want to get an algebraic structure on $\operatorname{Pic}^n(C)$ from that description

Remarks We know $h^0(D)$ if $\deg(D) \notin [0, 2g-2]$

a) If $\deg(D) = 0$
If $f \in H^0(C, \mathcal{O}_C(D)) - \{0\}$
$$\operatorname{div}(f) + D \geq 0$$
But $\deg(\operatorname{div}(f) + D) = 0$
Therefore $\operatorname{div}(f) + D = 0$
and $[D] = 0$

So if $\deg(D) = 0$, $h^0([D]) > 0 \iff [D] = 0$.

b] If $D \in \mathrm{Div}(C)$ and $P \in C(K)$
$H^0(C, \mathcal{O}_C(D)) \subset H^0(C, \mathcal{O}_C(D+P))$ by definition
then there exists an exact sequence
$0 \to H^0(C, \mathcal{O}_C(D)) \to H^0(C, \mathcal{O}_C(D+P)) \to \{f \in K(C)^* \mid v_P(f) \geq -k-1\} / \{f \in K(C)^* \mid v_P(f) \geq -k\}$
where k is the multiplicity of P in D (and the quotient is $\cong K$)
so
$h^0(C, \mathcal{O}_C(D)) \leq h^0(C, \mathcal{O}_C(D+P)) \leq h^0(C, \mathcal{O}_C(D)) + 1$

c] if $D = P_1 + \dots + P_s$ and $P \notin \{P_1, \dots, P_s\}$,
then $f \in H^0(C, \mathcal{O}_C(D))$ belongs to $H^0(C, \mathcal{O}_C(D-P))$
if and only if $f(P) = 0$
So $h^0(C, \mathcal{O}_C(D)) = h^0(C, \mathcal{O}_C(D-P))$
$\Leftrightarrow P \in \bigcap_{i=1}^{h^0(C, \mathcal{O}_C(D))} Z(f_i)$ where $f_1, \dots, f_{h^0(C, \mathcal{O}_C(D))}$ is a basis of $H^0(C, \mathcal{O}_C(D))$
If $h^0(C, \mathcal{O}_C(D)) > 0$ it is a finite subset of C.

Proposition

a] There is a non empty open subset U in $S^g C$ such that
$U(K) = \{D \in S^g(C) \mid h^0([D]) = 1\}$

b] Let $D_0 \in S^{n-g} C(K)$
Then the map
$\iota_{D_0} : U \longrightarrow \mathrm{Pic}^n(C)$
$D \longmapsto [D] + [D_0]$
is injective

c] Over $\overline{K}$
$\mathrm{Pic}^n(C) = \bigcup_{D_0 \in S^{n-g} C(\overline{K})} \iota_{D_0}(U(\overline{K}))$

Sketch of the proof

a) if $D \in S^g C$

$h^0([D]) - h^0(K-[D]) = 1$

so $h^0([D]) = 1 + h^0(K-[D]) \geq 1$

with equality iff $h^0(K-[D]) = 0$

Using the last remark

On an open set of $S^g C$

$$h^0(K-[D]) = h^0(K) - g$$
$$= (2g-2) + 1 - g + h_0(G_K) - g$$
$$= 0$$

So $h^0([D]) = 1$ on that open set.

b) $[D] + [D_0] = [D'] + [D_0]$

$\Leftrightarrow [D'] - [D] = \mathrm{div}(f)$

$\Rightarrow f \in H^0(C, \mathcal{O}_C(D))$ of dim 1

$\Rightarrow [D'] = [D]$.

c) By the above discussion

$$S^n C \longrightarrow \mathrm{Pic}^n(C)$$

is surjective

End of the construction

- For fixed $D_0 \in S^{n-g} C$

$S^{n-1}(\iota_{D_0}(U))(K)$ is an open set in $S^n C$

(those $D \in S^n C$ such that

$[D] = [D_0] + [D']$ $\quad D' \in S^g C$

with $h^0([D']) = 1$

$\Leftrightarrow h^0([D] - [D_0]) = 1$)

- Choose $D_1, \dots, D_n \in S^{n-g}$ such that

$S^n C = \bigcup_{i=1}^{n} S^{n-1}(\iota_{D_i}(U))$

then $\mathrm{Pic}^n(C) = \bigcup_{i=1}^{n} \iota_{D_i}(U)$ and use the ι_{D_i}

as charts on $\mathrm{Pic}^n(C)$ to define a scheme structure on $\mathrm{Pic}^n(C)$.
The statement may be summarized as follows:

Theorem
There exists an abelian variety J/K and a morphism of functor
$$\mathrm{Pic}^0(C) \longrightarrow J$$
such that for any L/K such that $C(L) \neq \emptyset$
$$\mathrm{Pic}^0(C)(L) \to J(L)$$
is an isomorphism of groups.
J is called the Jacobian of C and denoted by $\mathrm{Jac}(C)$.

N.B.
$\dim_{\mathbb{C}}(\mathrm{Jac}(C)) = g(C)$.

Remark
If $K = \mathbb{C}$ there is an exact sequence
$$0 \to 2i\pi\mathbb{Z} \to \mathbb{C} \xrightarrow{\exp} \mathbb{C}^* \to 1$$
Which gives a long exact sequence
$$0 \to 2i\pi\mathbb{Z} \to \mathbb{C} \xrightarrow{\exp} \mathbb{C}^* \quad \text{may prove that}$$
$$\to H^1(X, 2i\pi\mathbb{Z}) \to H^1(X, \mathbb{C}) \to H^1(X, \mathbb{C}^*) \to H^2(X, 2i\pi\mathbb{Z})$$
$$\downarrow \wr \qquad\qquad \| \qquad (*)$$
$$\mathrm{Pic}(X) \xrightarrow{2i\pi \deg} 2i\pi\mathbb{Z}$$
So $\mathrm{Pic}^0(X) \simeq H^1(X, \mathbb{C}) / \underbrace{H^1(X, 2i\pi\mathbb{Z})}_{\text{lattice in } H^1(X, \mathbb{C})}$
gives a structure of torus on $\mathrm{Pic}^0(X)$.

9) Functoriality

Notation

Let $\varphi : C' \to C$ be a non-constant morphism between smooth projective curves over K.

It induces a morphism of fields

$$\varphi^* : K(C) \longrightarrow K(C')$$

given by $f \longmapsto f \circ \varphi$

$$\begin{array}{ccc} C & \xrightarrow{f} & \mathbb{P}^1 \\ \uparrow & \nearrow_{\varphi^*(f)} & \\ C' & & \end{array}$$

As any morphism of fields this morphism is injective and

We may see $K(C')$ as a finite extension of $K(C)$. The <u>degree of φ</u> is

$$\deg(\varphi) = [K(C') : K(C)]$$

The restriction of absolute values induces a map which I also denote by $\varphi : C'_{(0)} \longrightarrow C_{(0)}$

$$Q \longmapsto Q_{|K(C)}$$

Definition

If $Q \in C'_{(0)}$ the <u>ramification index</u> of φ at Q is the unique integer $e_Q \geq 1$ such that

$$\begin{array}{ccc} K(C') & \xrightarrow{v_Q} & \mathbb{Z} \\ \uparrow & & \uparrow e_Q \\ K(C) & \xrightarrow{v_{\varphi(Q)}} & \mathbb{Z} \end{array}$$

commutes. (Remember that v_P and $v_{\varphi(P)}$ are surjective).
One says that φ is ramified at Q and $\varphi(Q)$ a branch point if $e_Q > 1$ and that Q is unramified otherwise.

Formula

For any $P \in C(\bar{k})$

$$\deg(\varphi) = \sum_{Q \in \varphi^{-1}(P)} e_Q \overbrace{[k(Q) : k(P)]}^{\text{residual degree}}$$

Proof

Let $K(C)_P$ be the completion of $k(C)$ at P
then $K(C)_P \simeq k(P)((T))$ (SERRE's corps locaux)
with $v_P(T) = 1$

$$K(C')_Q \simeq k(Q)((T^{1/e_Q}))$$

$$[K(C')_Q : K(C)_P] = e_Q [k(Q) : k(P)]$$

and

$$K(C') \otimes_{K(C)} K(C)_P \simeq \prod_{Q \in \varphi^{-1}(P)} K(C')_Q \quad . \square$$

Def

$$\varphi^* : \mathrm{Div}(C) \longrightarrow \mathrm{Div}(C')$$
$$P \longmapsto \sum_{Q \in \varphi^{-1}(P)} e_Q Q$$

NB

The diagrams

$$\begin{array}{ccc} K(C') & \xrightarrow{\mathrm{div}} & \mathrm{Div}(C') \\ \uparrow \varphi^* & & \uparrow \varphi^* \\ K(C) & \xrightarrow{\mathrm{div}} & \mathrm{Div}(C) \end{array}$$

and

$$\begin{array}{ccc} \mathrm{Div}(C') & \xrightarrow{\deg} & \mathbb{Z} \\ \uparrow \varphi^* & & \uparrow \deg(\varphi) \\ \mathrm{Div}(C) & \xrightarrow{\deg} & \mathbb{Z} \end{array}$$

commute

Déf From these diagrams we get morphisms

$$\varphi^* : \mathrm{Pic}(C) \longrightarrow \mathrm{Pic}(C')$$

and

$$\varphi^* : \mathrm{Pic}^0(C) \longrightarrow \mathrm{Pic}^0(C')$$

and therefore a morphism of algebraic groups

$$\mathrm{Jac}(C) \longrightarrow \mathrm{Jac}(C').$$

Déf

We say that φ is separable if the extension

$$K(C')/K(C)$$

is separable

Exemple

If $\mathrm{char}(k) = p$ $\varphi : \mathbb{P}^1_k \longrightarrow \mathbb{P}^1_k$

$$[x:y] \longmapsto [x^p : y^p]$$

is purely inseparable since the correspondinc extension is

$$K(T^{1/p})/K(T)$$

Remark

In the inseparable case the tangent map is 0!

Déf

If φ is separable

$$T\varphi : TC' \longrightarrow TC$$

induces a map $TC' \longrightarrow \varphi^*(TC)$

and therefore a section s_φ of $\varphi^*(TC) \otimes TC'^{\vee}$

The ramification divisor is

$$R_\varphi = \mathrm{div}(s_\varphi).$$

Prop

If $\mathrm{char}(K) \nmid e_Q$ then the order of R_φ at Q is $e_Q - 1$.

Proof

Let $P = \varphi(Q)$

Pick $\pi \in K(C)$ with $v_P(\pi) = 1$

and $\pi' \in K(C')$ with $v_Q(\pi') = 1$

then $\pi \circ \varphi = u(\pi')^{e_Q}$ with $v_Q(u) = 0$

Differentiating formally we get

$$d\pi_P \circ d\varphi_Q = e_Q \underbrace{(\pi')^{e_Q - 1} u \, d\pi' + \pi'^{e_Q} du}_{\text{zero of order } e_Q - 1} \quad \square$$

$e_Q \neq 0$

Corollary

If $\mathrm{char}(K) = 0$

$$R_\varphi = \sum_{Q \in C'} (e_Q - 1) Q$$

HURWITZ formula

$$K_{C'} = f^*(K_C) + [R] \text{ in } \mathrm{Pic}(C')$$

This follows from the construction

Corollary

$$2g(C') - 2 = \deg(\varphi)(2g(C) - 2) + \deg(R)$$

N.B.

In particular $\deg(R)$ is even.

Remark

If $K(C')/K(C)$ is purely inseparable, one can show that φ is a composition of Frobenius isomorphisms corresponding to elevating coordinates to the p^{th} power. and $g(C) = g(C')$ (in fact C and C' are isomorphic as schemes)

VII Main steps of the proof of FALTINGS theorem

Reference G. CORNELL & J. H. SILVERMAN, Arithmetic Geometry (Springer Verlag).

1) Generalization to higher dimensions

Several of the constructions I explained for curves might be extended to higher dimensions

"Definitions" (See [HARTSHORNE's II.6])

Let V be a smooth, projective, irreducible and geometrically irreducible algebraic variety (geometrically irreducible means that V is irreducible $/\overline{K}$)

The function field is

$$K(V) = \varinjlim_{U \subset V \text{ open}} \Gamma(U, \mathcal{O}_V) = \varinjlim_{U \subset V \text{ open}} \mathrm{Mor}_K(U, \mathbb{P}^1_K)$$

The set $V^{(1)}$ is the set of strict irreducible algebraic subsets of V which are maximal for these properties (in otherwords of codim (1))

$$\mathrm{Div}(V) = \mathbb{Z}^{(V^{(1)})}$$

and there is a division map

$$\mathrm{div} : K(V)^* \to \mathrm{Div}(V)$$

The Picard group of V is

$$\mathrm{Pic}(V) = \mathrm{Div}(V) / \mathrm{im}(\mathrm{div})$$

The Picard group might be equipped with an algebraic structure and

$\mathrm{Pic}^0(V)$ is the connected component of 0

and the NÉRON-SEVERI group is the quotient

$$NS(V) = \mathrm{Pic}(V) / \mathrm{Pic}^0(V)$$

For any line bundle L/V one may define $c_1(L) \in \mathrm{Pic}(V)$

Examples

a) For a curve C

$$\deg : NS(C) \xrightarrow{\sim} \mathbb{Z}$$

isomorphism

b) For A an abelian variety, the dual abelian variety is given by

$$A^\vee(L) = \mathrm{Pic}^0(A)(L)$$

It comes with the Poincaré line bundle

$$\mathcal{P} \downarrow A \times A^\vee$$

such that $\forall\, a \in \mathrm{Pic}^0(A)(L)$, $c_1(\mathcal{P}_{|A \times \{a\}}) = a$.

c) If

$$V \xrightarrow{f} \mathbb{P}^N_k$$

is a morphism $L = f^*(\mathcal{O}_{\mathbb{P}^N}(1))$ is a line bundle on V, and for $i \in 0, \dots, N$ we have a section s_i of L given by

$$V \xrightarrow{f} \mathbb{P}^N_k \xrightarrow{X_i} L$$

- Conversely if L is a line bundle on V and $(s_0, \dots, s_N)$ is a basis of $\Gamma(X, L)$ such that

$$\bigcap_{i \in \{0,\dots,N\}} \{x \in V \mid s_i(x) = 0(x)\} \text{ is empty}$$

$$V \longrightarrow \mathbb{P}^N_k$$

$$x \longmapsto [\lambda_0 : \dots : \lambda_N] \text{ such that } \lambda_i \cdot s_j(x) = \lambda_j \cdot s_i(x)$$

defines a morphism $V \to \mathbb{P}^N_k$

If this map induces an isomorphism from V to its image, one says that L (or $c_1(L) \in \mathrm{Pic}(V)$) is very ample. So morphisms to projective spaces are classified by line bundles

$\alpha \in \mathrm{Pic}(V)$ is said to be ample if there is $m \geq 1$ such that $m\alpha$ is very ample

2| Polarization

Definition

Let A and B be abelian varieties
an isogeny from A to B is a morphism $\varphi : A \to B$ which is surjective over $\overline{K}$ and has finite kernel

Example

A non-constant morphism between elliptic curves is an isogeny.

Theorem of the square

For any $\alpha \in \mathrm{Pic}(A)$ and any $a, b \in A(K)$

$$t_{a+b}^{*}(\alpha) + \alpha = t_a^{*}(\alpha) + t_b^{*}(\alpha)$$

Corollary

If $\alpha \in \mathrm{Pic}(A)$ the map

$$\varphi_\alpha : A \to A^{\vee}$$
$$a \mapsto t_a^{*}(\alpha) - \alpha$$

is a morphism.

Definition

A polarization of an abelian variety A is an isogeny $\lambda : A \to A^{\vee}$ of the form φ_α for some ample $\alpha \in \mathrm{Pic}(A)$.

Notation

Let C be a smooth projective geometrically irreducible curve / K such that $C(K) \neq \emptyset$ and let $J = \mathrm{Jac}(C) = \mathrm{Pic}^0(C)$

Then for $P \in C(K)$, we may consider

$$\begin{aligned} S^{g-1}C &\longrightarrow J \\ D &\longmapsto [D] - (g-1)P \end{aligned}$$

The image defines a hypersurface Θ in J

(Indeed its dimension is $g-1$ and it is irreducible since $S^{g-1}C$ is irreducible)

Theorem

The map $\varphi_\Theta : J \longrightarrow J^\vee$ where $t_a : J \to J$, $x \mapsto a+x$

$$a \longmapsto t_a^*(\Theta) - \Theta$$

is an isomorphism of abelian varieties called the canonical polarization of $\mathrm{Jac}(C)$

Remark

By the theorem of the square it does not depend on the choice of P.

3] Torelli's theorem

Theorem [TORELLI]

Let C and C' be curves of genus $g \geq 2$ over a perfect field K if their polarized abelian varieties $(\mathrm{Jac}(C), \varphi_\Theta)$ and $(\mathrm{Jac}(C'), \varphi'_{\Theta'})$ are isomorphic then C is isomorphic to C'.

Idea of the proof

For $r \leq g-1$

$$D \longmapsto [D] - r[P]$$

$$\begin{array}{ccc} S^r C & \xrightarrow{s_r} & J \\ & & \downarrow \alpha \\ S^r C' & \xrightarrow{s'_r} & J' \end{array} \qquad \text{put } W^r = \mathrm{im}(s_r), \quad W'^r = \mathrm{im}(s'_r)$$

$$D \longmapsto [O] - r[P']$$

- if $r = g-1$ $\exists\, a \in J'$ such that $\alpha(\Theta_C) = a + \Theta_{C'}$ (uses that α is compatible with polarizations)
- Compute intersections

If $x, x' \in W^1$, $x \neq x'$:

$$(W^{g-1} - x) \cap (W^{g-1} - x') = W^{g-2} \cup (x + x' - W^{g-2})$$

and $W^1 = \bigcap \{ W^{g-1} - a,\ a \in W^{g-2} \}$

So may reconstruct W^1 from W^{g-1} and $s_1 : C \xrightarrow{\sim} W^1$. □

3| Siegel module space, modular heights

Example

An elliptic curve

$$E : Y^2 = X^3 + AX + B$$

is classified, up to isomorphism, by its j invariant

$$j(E) = \frac{1728\,(4A)^3}{-16\,(4A^3 + 27B^2)} \in \mathbb{P}^1(K) - \infty$$

Notation

$A_{g,d,n}(K)$ set of isomorphism classes of abelian varieties of dimension g equipped with a polarization

of degree d^2 and an isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^{2g} \xrightarrow{\sim} A[n]$$

Theorem

The functor $A_{g,d,n}$ is representable by a scheme $\mathcal{X}_{g,d,n}$ over $\mathbb{Z}[1/n]$

$\mathcal{X}_g = \mathcal{X}_{g,1,1}$ classifies abelian varieties

Over $\mathbb{C}$

For $g = 1$

$\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$

$\Gamma = SL_2(\mathbb{Z})$ acts on $\mathbb{H}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$$

Λ lattice in $\mathbb{C}$

$\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ with $\mathrm{Im}(\tau) > 0$

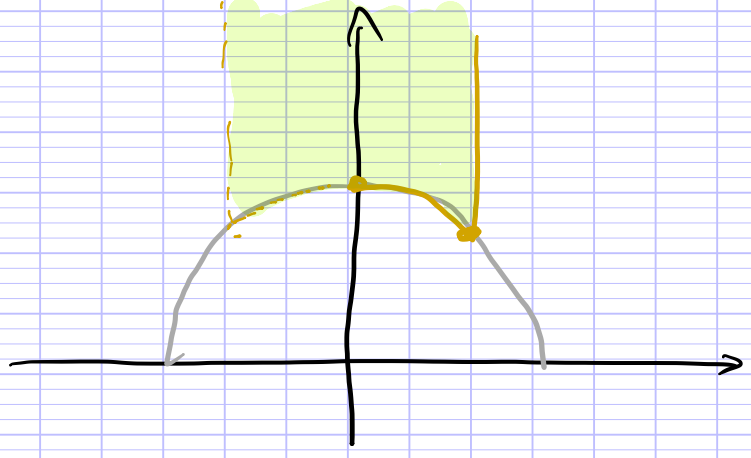
$\mathbb{Z} + \mathbb{Z}\tau = \mathbb{Z} + \mathbb{Z}\tau'$

$\Leftrightarrow \exists\, \gamma \in SL_2(\mathbb{Z}) \mid \gamma.\tau = \tau'$.

We want to consider $\mathbb{H}/\Gamma$

Fundamental domain:

$D = \{z \in \mathbb{C},\ \mathrm{Re}(z) \in]-\frac{1}{2}, \frac{1}{2}],\ |z| \geq 1$ and $\mathrm{Re}(z) \geq 0$ if $|z| = 1\}$



For a lattice $\Lambda \subset \mathbb{C}$ there exists a unique $\tau \in \mathcal{D}$ such that $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$.
(see SERRE's cours d'arithmétique)

For higher g

Symplectic group

$$Sp_{2g}(\mathbb{R}) = \left\{ \gamma \in M_{2g}(\mathbb{R}) \;\middle|\; {}^t\gamma \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} \gamma = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} \right\}$$

$\cup$

$$\Gamma_g(n) = \{ \gamma \in Sp_{2g}(\mathbb{Z}) \mid \gamma \equiv I_{2g} \pmod{n} \}$$

$$\mathcal{H}_g = \{ \Omega \in M_g(\mathbb{C}) \mid \Omega = {}^t\Omega \text{ and } \operatorname{Im}(\Omega) \text{ is positive-definite} \}$$

$$Sp_{2g}(\mathbb{R}) \curvearrowright \mathcal{H}_g \quad \text{via} \quad \begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot \Omega = (A\Omega + B)(C\Omega + D)^{-1}$$

$\mathcal{A}_{g,1,n}(\mathbb{C})$ is a disjoint union of copies of $\Gamma_g(n) \backslash \mathcal{H}_g$

In particular

$$\mathcal{A}_g \simeq \Gamma_g(1) \backslash \mathcal{H}_g$$

Problem

$\mathcal{A}_g$ is not projective

Faltings's heights

It is possible to construct a compactification $\overline{\mathcal{A}}_g$ and to define heights $\mathcal{A}_g(K) \to \mathbb{R}_{\geq 0}$

4) Sketch of the proof

Let C/K be a smooth curve of genus $g \geq 2$
We want to prove that $C(K)$ is finite

a) Enough to show that for some K'/K finite $C(K')$ is finite
Construct K'/K and $\varphi : C' \to C$ of degree $m > 2$ over K' such that $C' \to C$ is unramified
(Idea $\pi^{-1}(C)$ is not trivial)
use

Theorem [HERMITE-MINKOWSKI]
For a number field K, $S \subset \mathrm{Val}(K)$ finite there are only a finite number of field extensions K'/K of fixed degree unramified outside S.

So there exists K_1/K' such that for any $x \in X(K')$ $\phi^{-1}(x)$ contains m points defined over K_1
Let $D = \phi^{-1}(x) - \{y\}$ for some $y \in \phi^{-1}(x)$ and construct a morphism

$$C'_x \longrightarrow C'$$

ramified exactly over D with bad reduction (ie the curve defined over $\mathbb{F}_v = G_v/\mathfrak{m}_v$ is not smooth) in an explicit set S (depending only on φ).

Using the fact that if $g(C) \geq 2$ the set
$$\mathrm{Mor}(C', C)$$
is finite we are reduced to prove

Theorem

There are only finitely many isomorphism classes of smooth curves of genus $g \geq 2$ with good reduction outside S

b) Using TORELLI's theorem, this reduces to

Theorem (SHAFAREVICH Conjecture FACTINGS)

Let S be a finite set of places of K, $d > 0$
then there are only finitely many isomorphism classes of abelian varieties $/K$ of dimension g and polarization of degree d with good reduction outside S.

2 steps!

a) There is a finite number of isogeny classes of abelian varieties which satisfy the condition
(uses techniques coming from representation of $\mathrm{Gal}(\bar{K}/K)$: if ℓ is a prime number
$$T_\ell(A) = \varprojlim A[\ell^n](\bar{K}) \quad \mathbb{Z}_\ell \text{ module}$$
$V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ $\mathbb{Q}_\ell$ vector space of dimension $2g$
$\cup$
$\mathrm{Gal}(\bar{K}/K)$ gives a representation of $\mathrm{Gal}(\bar{K}/K)$ of dimension $2g$ over $\mathbb{Q}_\ell$)

b) In each isogeny class, the FALTINGS's height is bounded

$\Rightarrow$ finite set. $\square$

Exercises, September 19, 2022

Arithmetics under the influence of geometry

Exercise 1

In this exercise, we consider the plane curve $\mathscr{C}$ defined by the equation

$$Y^2 = X^3 + X^2. \tag{1}$$

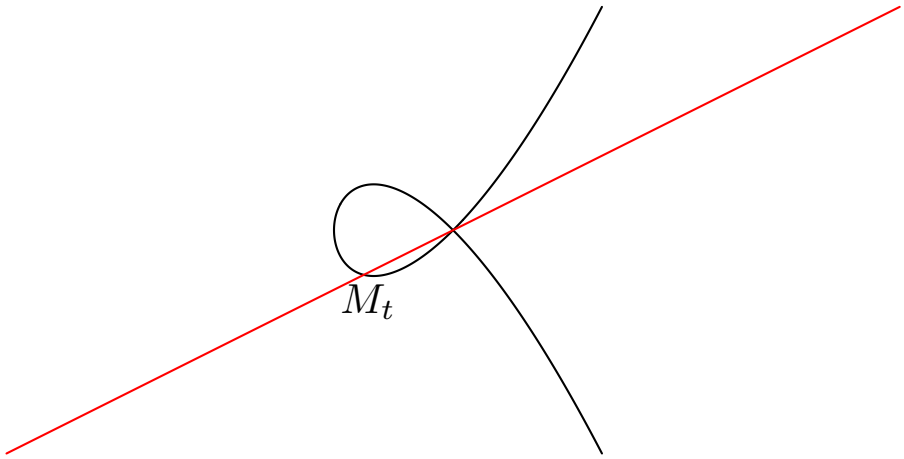


FIGURE 1. Singular cubic

1. Let D_t be the line going through the origin $(0,0)$ of slope t. Proves that, if $t \notin \{-1,1\}$, D_t meets the curve $\mathscr{C}$ in one other point M_t. Compute the coordinates of M_t.
2. Prove that there is a bijection from $\mathbf{Q} - \{-1,1\}$ to $\mathscr{C}(\mathbf{Q}) - \{(0,0)\}$.
3. Prove that $Y^2 - X^3 - X^2$ is irreducible in $\mathbf{Q}(X)[Y]$.
4. Prove that the quotient $\mathbf{Q}(X)[Y]/(Y^2 - X^3 - X^2)$ is a field isomorphic to the field of rational functions in one variable $\mathbf{Q}(T)$.

Exercise 2

In this exercise, we consider the plane curve $\mathscr{L}$ defined by the equation

$$(X^2 + Y^2)^2 - X^2 + Y^2 = 0. \tag{2}$$

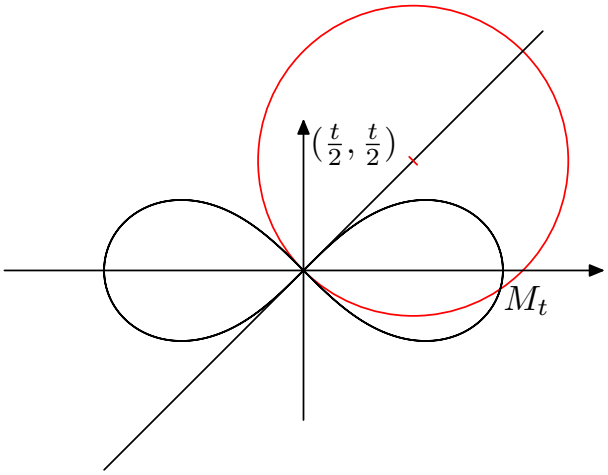


FIGURE 2. Bernoulli's lemniscate

1. Let $\mathscr{C}_t$ be the circle with center $(\frac{t}{2}, \frac{t}{2})$ going through $(0,0)$.
   (a) Write the equation of the circle $\mathscr{C}_t$.
   (b) If $t \neq 0$, proves that the intersection of $\mathscr{L}$ and $\mathscr{C}_t$ contains exactly two points: $(0,0)$ and another point M_t and compute the coordinates of M_t.
2. Proves that there is a bijection from $\mathbf{Q}^*$ to the set $\mathscr{L}(\mathbf{Q})-\{(0,0)\}$ of rational solutions of the equation (2).
3. Prove that $(X^2+Y^2)^2 - X^2 + Y^2 = 0$ is irreducible in $\mathbf{Q}(X)[Y]$
4. Prove that the field $\mathbf{Q}(X)[Y]/((X^2+Y^2)^2 - X^2 + Y^2)$ is isomorphic to the field of rational functions in one variable $\mathbf{Q}(T)$.

Exercise 3

In this exercise[(1)] we consider an elliptic curve given by the affine equations

$$Y^2 = X(X-\alpha)(X-\beta)$$

where $\sharp\{1, \alpha, \beta\} = 3$. We assume that there exist rational functions $f = \frac{P}{Q}$ and $g = \frac{R}{S}$ in $\mathbf{Q}(T)$, with $\gcd(P,Q) = \gcd(R,S) = 1$ such that

$$f^2 = g(g-\alpha)(g-\beta).$$

1. Show that $S^3 | Q^2 | S^3$.
2. Show that four non-collinear linear combinations of R and S in $\mathbf{C}[T]$ (that is polynomials of the form $\lambda R + \mu S$, for four pairwise non-collinear vectors $(\lambda, \mu) \in \mathbf{C}^2$) are squares.

(1) Inspired by M. Reid

3. (a) Prove that if R and S in $\mathbf{C}[T]$ are coprime polynomials, not both constant, and if R, S, $R-S$ and $R-\lambda S$ with $\lambda \notin \{0,1\}$ are all squares, then there exist coprime polynomials U and V with $0 < \max(\deg(U), \deg(V)) < \max(\deg(R), \deg(S))$ and four non-collinear linear combinations of U and V are squares.
   (b) Show that we may assume that these linear combinations are U, V, $U-V$ and $U-\gamma V$ for some $\gamma \neq 1$.
4. Show that f and g are constant polynomials.
5. Show that there is no morphism from the field

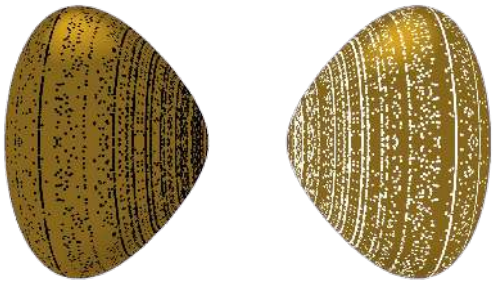
$$\mathbf{Q}(X)[Y]/(Y^2 - X(X-\alpha)(X-\beta))$$

to the field $\mathbf{Q}(T)$.

Exercise 4

In this exercise, we consider the surface $\mathscr{S}$ defined by the equation

$$Y^2 + Z^2 = 2X(X^2-3) \tag{3}$$



1. Check that the point $P_0 = (-1, 0, 2)$ belongs to the surface. Find the equation of the tangent plane of the surface at the point P_0.
2. Let D be a line through P_0 not contained in the plane $X = -1$. Prove that the intersection of D with $\mathscr{S}$ contains two points: P_0 and another point and compute the coordinates of that point.
3. Using a rational parametrization of the circle, construct a map φ from $\mathbf{Q}^2$ to $\mathscr{S}(\mathbf{Q})$.
4. Is this map injective ? Prove that for a well-chosen φ, $\sharp\varphi^{-1}(P) \leqslant 2$ for any $P \in \mathscr{S}(\mathbf{Q})$.
5. Prove that there is a number $a \in \mathbf{Q}$ such that for any $(x, y) \in \mathbf{Q}^2$, the first coordinate of $\varphi(x, y)$ is bigger or equal to a.

6. Prove that there are infinitely many points of $\mathscr{S}(\mathbf{Q})$ which are not in the image of φ.
7. (a) Prove that $Y^2 + Z^2 - 2X(X^2 - 3)$ is irreducible in $\mathbf{R}(X, Y)[Z]$.
   (b) Prove that the field $\mathbf{Q}(X, Y)[Z]/(Y^2 + Z^2 - 2X(X^2 - 3))$ is isomorphic to a subfield of the field $\mathbf{Q}(U, V)$ of rational functions in two variables.
8. (a) Prove that $\mathscr{S}(\mathbf{R})$ has at least two connected compenents.
   (b*) Deduce from the previous question that the $\mathbf{R}$-algebra

$$\mathbf{R}(X, Y)[Z]/(Y^2 + Z^2 - 2X(X^2 - 3))$$

   is *not* isomorphic to the $\mathbf{R}$-algebra $\mathbf{R}(U, V)$.
   (c*) Deduce from the previous question that the field

$$\mathbf{Q}(X, Y)[Z]/(Y^2 + Z^2 - 2X(X^2 - 3))$$

   is *not* isomorphic to the field $\mathbf{Q}(U, V)$.
   (d) Prove that the field $\mathbf{Q}(i)(X, Y)[Z]/(Y^2 + Z^2 - 2X(X^2 - 3))$ is isomorphic to the field $\mathbf{Q}(i)(U, V)$.

Problem

The aim of this problem is a proof of Lüroth's theorem.
In this problem $\mathbf{K}$ is a commutative field and T, X, Y are indeterminates.

Part I

Automorphisms of $\mathbf{K}(T)$

Let $F \in \mathbf{K}(T) - \mathbf{K}$. Let us write $F(T) = N(T)/D(T)$ with $N, D \in \mathbf{K}[T]$ coprime. We then consider $h(F) = \sup(\deg N, \deg D)$ and $\mathbf{L} = \mathbf{K}(F) \subset \mathbf{K}(T)$.

1. (a) Prove that the polynomial $N(X) - FD(X) \in \mathbf{L}[X]$ is not zero. What is its degree?
   (b) Prove that the element T of $\mathbf{K}(T)$ is algebraic over $\mathbf{L}$.
   (c) Prove that F is transcendental over $\mathbf{K}$.
2. (a) Prove that the polynomial $N(X) - FD(X) \in \mathbf{L}[X]$ is irreducible. (One may first prove that $N(X) - YD(X)$ is irreducible in $\mathbf{K}[X, Y]$ and therefore in $\mathbf{K}(Y)[X]$.)
   (b) Prove that $[\mathbf{K}(T) : \mathbf{L}] = h(F)$.
3. (a) Find all F in $\mathbf{K}(T)$ such that $\mathbf{K}(T) = \mathbf{K}(F)$.
   (b) Let $\mathrm{Aut}(\mathbf{K}(T)/\mathbf{K})$ be the group of automorphisms of the $\mathbf{K}$-algebra $\mathbf{K}(T)$. Let $\mathrm{PGL}_2(\mathbf{K})$ be the quotient group $\mathrm{GL}_2(\mathbf{K})/(\mathbf{K}^* I_2)$ where I_2 denotes the unit matrix. Prove that there is a group isomorphism

$$\psi : \mathrm{PGL}_2(\mathbf{K}) \to \mathrm{Aut}(\mathbf{K}(T)/\mathbf{K})$$

given by

$$\psi\left(\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right]\right)(T) = \frac{aT+c}{bT+d}$$

where $[\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)]$ is the class of the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{K})$.

Part II

Subfields of $\mathbf{K}(T)$

Let $\mathbf{L}$ be a subfield of $\mathbf{K}(T)$ containing $\mathbf{K}$ and not equal to $\mathbf{K}$.

1. Prove that $\mathbf{K}(T)$ is algebraic over $\mathbf{L}$.
2. Let $P(X) = \mathrm{Irr}_{\mathbf{L}}^{T}(X)$ be the unitary minimal polynomial of T over $\mathbf{L}$ and write $P = \sum_{i=0}^{d} a_i X^i$ with $a_i \in \mathbf{L}$ and $a_d \neq 0$.
   (a) Prove that there exist an integer $i \in \{0, \ldots, d\}$ such that $a_i \notin \mathbf{K}$.

   In the sequel i_0 denotes an integer such that $a_{i_0} \notin \mathbf{K}$ and we put $F = a_{i_0}$. As in the first part, we write $F = N/D$ with $N, D \in \mathbf{K}[T]$ coprime. Let $m = h(F)$ and $n = [\mathbf{K}(T) : \mathbf{L}]$.

   (b) Compare n and the degree of P. Prove that $n \mid m$ and that $n = m$ if and only if $\mathbf{L} = \mathbf{K}(F)$
   (c) Prove that $P(X) \mid D(X) - FN(X)$ in $\mathbf{L}[X]$.
3. (a) Prove that the element P of $\mathbf{K}(T)[X]$ may be written as $P(X) = A(T, X)/B(T)$ with $A(T, X)$ primitive in $\mathbf{K}[T][X]$ (that is the gcd of its coefficients is one) and B an element of $\mathbf{K}[T]$.
   (b) Prove that there exists a polynomial $Q(T, X)$ of $\mathbf{K}[T, X]$ such that

   $$N(T)D(X) - D(T)N(X) = A(T, X)Q(T, X).$$

   (c) Prove that $\deg_T A(T, X) \geqslant m$ and that $Q(T, X) \in \mathbf{K}[X]$.
   (d) Prove that $Q \in \mathbf{K}$. (One may first prove that $N(T)D(X) - D(T)N(X)$ is primitive in $\mathbf{K}[T][X]$.)
   (e) Prove that $\mathbf{L} = \mathbf{K}(F)$.
4. (a) Let $F \in \mathbf{L} - \mathbf{K}$. Prove that $\mathbf{L} = \mathbf{K}(F)$ if and only if $h(F)$ is minimal.
   (b) Prove that there exists an isomorphism

   $$\mathbf{K}(Y) \xrightarrow{\sim} \mathbf{L}.$$

Sheet 1

Exercise 1

1°] $D_t : Y = tX$

$D_t \cap C$ is given by

$$t^2 X^2 = X^2(X+1)$$

the solution $X = 0$ corresponds to the origin

the othe solution is

$$M_t = (t^2 - 1, t^3 - t)$$

which is different from $(0,0)$ if and only if

$$t \notin \{-1, 1\}$$

2°] the map

$$\mathbb{Q} - \{-1, 1\} \longrightarrow C(\mathbb{Q}) - \{(0,0)\}$$
$$t \longmapsto (t^2 - 1, t^3 - t)$$

is bijective with on inverse given by

$$C(\mathbb{Q}) - \{(0,0)\} \longrightarrow \mathbb{Q} - \{-1, 1\}$$
$$(x, y) \longmapsto y/x$$

3°] $Y^2 - X(X-1)(X+1) \in \mathbb{Q}[X][Y]$

we may apply Eisenstein's irreducibility criterion with $A = \mathbb{Q}[X]$ and $p = X$

Prop [EISENSTEIN]

Let A be a principal domain

Let $p \in A$ be an irreducible element

Let $P = \sum_{i=0}^{n} a_i X^i \in A[X]$

Let $K = Fr(A)$ fraction field of A

Assume that

(i) $p \mid a_i$ for $i \in \{1, \dots, n\}$

(ii) $p \nmid a_n$

(iii) $p \mid a_0$ but $p^2 \nmid a_0$
then P is irreducible in $\mathbb{K}[X]$.

So P is irreducible.
4°] $\mathbb{Q}(X)[Y]/(Y^2 - X^3 - X^2)$
is a a field by 3°]
Let us consider the morphism of $\mathbb{Q}$-algebras

$$\Psi_0 : \mathbb{Q}[X,Y] \longrightarrow \mathbb{Q}(T)$$
$$X \longmapsto T^2 - 1$$
$$Y \longmapsto T^3 - T$$

Then since if $P \in \mathbb{Q}[X]$,
$\deg(P(T^2 - T)) = 2 \deg(P)$
Ψ_0 is injective
Thus Ψ_0 extends to

$$\Psi_1 : \mathbb{Q}(X)[Y] \longrightarrow \mathbb{Q}(T)$$

with $\Psi_1(Y^2 - X^3 - X^2) = (T^3 - T)^2 - (T^2 - 1)^3 - (T^2 - 1)^2$
$= T^6 - 2T^4 + T^2 - T^6 + 3T^4 - 3T^2 + 1$
$- T^4 + 2T^2 - 1 = 0$

(which also follows from the fact that any $\alpha \in \mathbb{Q}$ is a 0 of the polynomial which thus has only many 0s!)
We get a morphism of fields

$$\Psi : \mathbb{Q}(X)[Y]/(Y^2 - X^3 - X^2) \to \mathbb{Q}(T)$$

which has to be injective (as any morphism of fields)
Since $\Psi(Y/X) = T$ the morphism is surjective.

Exercise 2

1° a) $(x-\frac{t}{2})^2+(y-\frac{t}{2})^2=\frac{t^2}{2}$

which is equivalent to

$$x^2+y^2-t(x+y)=0$$

b) $\mathcal{C}_t \cap \mathcal{L}$ is given by

$$\begin{cases} (x^2+y^2)^2 - x^2+y^2 \\ x^2+y^2 = t(x+y) \quad (**) \end{cases}$$

$$\begin{cases} t^2(x+y)^2 - x^2+y^2 \\ x^2+y^2 = t(x+y) \end{cases}$$

$$\begin{cases} t^2(x+y)^2 - (x+y)(x-y) = 0 \\ x^2+y^2 = t(x+y) \end{cases}$$

$$\begin{cases} (x+y)\left((t^2-1)x+(t^2+1)y\right)=0 \\ x^2+y^2 = t(x+y) \end{cases}$$

The solution $x+y=0$ gives $x^2+y^2=0$ and therefore the origin.

So we are reduced to

$$\begin{cases} y=\frac{1-t^2}{1+t^2}x \\ x^2\left(1+\left(\frac{1-t^2}{1+t^2}\right)^2\right)=t\left(1+\frac{1-t^2}{1+t^2}\right)x \end{cases}$$

Again $x=0$ corresponds to the origin, so we get a unique point

$$M_t=\left(\frac{t(1+t^2)}{1+t^4}, \frac{t(1-t^2)}{1+t^4}\right)$$

2° Let us consider the map

$$\varphi : \mathbb{Q}^* \longrightarrow \mathcal{L}\setminus\{(0,0)\}$$
$$t \longmapsto M_t$$

and (**) gives the inverse map

$$\mathcal{L}(a) - \mathcal{L}(g_0) \longrightarrow \mathbb{Q}^*$$
$$(x, y) \longmapsto \frac{x^2+y^2}{x+y}$$

3°]

$$(X^2+Y^2)^2 - X^2 + Y^2 = Y^4 + Y^2(2X^2+1) + X^2(X^2-1)$$

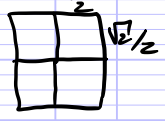
The polynomial $2X^2+1$ is irreducible in $\mathbb{Q}[X]$

by reducing modulo $2X^2+1$, we get the polynomial

$$Y^4 + \frac{3}{4} = Y^4 + \frac{(1+i\sqrt{2})(1-i\sqrt{2})}{4} \in \mathbb{Q}[i\sqrt{2}][Y]$$

$\mathbb{Z}[i\sqrt{2}]$ is a euclidean domain for $|\ |$

$|a+ib\sqrt{2}| = a^2 - 2b^2$ since $\left(\frac{\sqrt{2}}{2}\right)^2 + \frac{1}{4} = \frac{3}{4} < 1$



and $1+i\sqrt{2}$ is irreducible in $\mathbb{Z}[i\sqrt{2}]$

by applying Eisenstein criterium to $A = \mathbb{Z}[i\sqrt{2}]$

and $p = 1+i\sqrt{2}$

we get that $Y^4 + \frac{3}{4}$ is irreducible in $\mathbb{Q}[i\sqrt{2}][Y]$

and therefore $(X^2+Y^2)^2 - X^2 + Y^2$ is irreducibe in $\mathbb{Q}(X)[Y]$.

$$\left[(X^2+Y^2)^2 - X^2 + Y^2 = \left(Y^2 + X^2 + \frac{1}{2}\right)^2 - 2X^2 - \frac{1}{4} \right]$$

Réduction modulo $X-2$ gives

$$\overline{P} = Y^4 + Y^2 9 + 4 \times 3$$

We then apply EISENSTEIN's criterion with $p=3$

Thus $\overline{P}$ is irreducible

Thus P is irreducible

4°) We consider the map

$$\mathbb{Q}[X][Y] \longrightarrow \mathbb{Q}(T)$$
$$X \longmapsto \frac{T(1+T^2)}{1+T^4}$$
$$Y \longmapsto \frac{T(1-T^2)}{1+T^4}$$

since any $f \in \mathbb{Q}(T)$ is transcendant over $\mathbb{Q}$, (see question 1 of problem).
as before it induces a morphism of fields

$$\mathbb{Q}(X)[Y]/(X^2+Y^2)-X^2+Y^2 \longrightarrow \mathbb{Q}(T)$$

which is injective and surjective.

Question

What is the connection between the parametrization of a curve and field isomorphisms?

Let C be a curve given by an affine equation

$$P(X,Y)=0$$

with $P \in \mathbb{Q}[X,Y]$ irreducible and $\deg_Y(P) > 0$
and assume there exists an isomorphism

$$\varphi : \mathbb{Q}(X)[Y]/(P) \xrightarrow{\sim} \mathbb{Q}(T)$$

Then the map

$$\mathbb{Q} \longrightarrow C(\mathbb{Q})$$
$$t \longmapsto (\varphi(X)(t), \varphi(Y)(t))$$

is defined outside a finite set of points (namely the roots of the denominators of $\varphi(X)$ and $\varphi(Y)$).
and its image is the complement of a finite set of points in $C(\mathbb{Q})$ with an inverse given by

$$(x,y) \longmapsto \varphi^{-1}(T)(x,y)$$

Exercise 3

1°] As $f = \frac{P}{Q}$ and $g = \frac{R}{S}$, the equation might be rewritten as

$$S^3 P^2 = Q^2 R(R-\alpha S)(R-\beta S)$$

as $\gcd(Q,P) = 1$, $Q^2 \mid S^3$

as $\gcd(R,S) = 1$ we get $\gcd(R-\alpha S, S) = \gcd(R-\beta S, S) = 1$

and $\gcd(S^3, R(R-\alpha S)(R-\beta S)) = 1$

Therefore

$$S^3 \mid Q^2$$

2°] Let $a = \frac{Q^2}{S^3} \in \mathbb{Q}$

we get the relation

$$P^2 = a\, R(R-\alpha S)(R-\beta S)$$

Since $\gcd(R, S) = 1$, the polynomial $R, (R-\alpha S), (R-\beta S)$ are pairwise coprime

If we denote $\mathcal{P}_{\mathbb{K}[T]}$ the set of unitary irreducible polynomials in $\mathbb{K}[T]$ we may write the prime decomposition of $Q \in \mathbb{K}[T]$ as

$$Q = u \prod_{P \in \mathcal{P}_{\mathbb{K}[T]}} P^{v_P(Q)}$$

then for any $P \in \mathcal{P}_{\mathbb{K}[T]}$

$v_P(R) + v_P(R-\alpha S) + v_P(R+\alpha S)$ is even

and 2 of them are 0

So R, $R-\alpha S$ and $R-\beta S$ are squares in $\mathbb{K}[T]$

On the other hand S^3 is a square

So S has also to be a square

So R, S, $R-\alpha S$ and $R-\beta S$ are all squares.

3° a) Write $R = U^2$, $S = V^2$ we have $\gcd(U, V) = 1$

then $R - S = U^2 - V^2$ and $R - \lambda S = U^2 - \lambda^2 V^2$

Let γ be a square root of λ.

we get

$$U^2 - V^2 = (U-V)(U+V)$$

But $U-V$ and $U+V$ are coprime so, again both are squares

Similarly $U^2 - \lambda V^2 = (U-\gamma V)(U+\gamma V)$

and both $(U-\gamma V)$ and $(U+\gamma V)$ are squares

b] Write the four linear combinations as

$$a_i U + b_i V$$

with $[a_i : b_i] \in \mathbb{P}^1(\mathbb{C})$.

The group $PGL_2(\mathbb{C})$ acts 3 transitively on $\mathbb{P}^1(\mathbb{C})$:

Since $[a_i : b_i] \in \mathbb{P}^1(\mathbb{C})$ are 4 different points we may find $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{C})$ such that

$g \cdot [a_1 : b_1] = [1 : 0]$

$g \cdot [a_2 : b_2] = [0 : 1]$

$g \cdot [a_3 : b_3] = [1 : -1]$

and $g \cdot [a_4 : b_4] = [1 : -\lambda]$

Take $U' = (dU - cV)/ad - bc$

$V' = (-bU + aV)/ad - bc$

then $U = aU' + cV'$

and $V = bU' + dV'$

and $a_i U + b_i V = (a a_i + b b_i) U' + (c a_i + d b_i) V'$

we get that

U', V', $U' - V'$ and $U' - \lambda V'$ are all squares

3°] If R and S are not constant, by taking in question 2° polynomial R and S of minimal degree we get a contradiction

So R and S are constant, so is Q and therefore P.

we get that f and g are constant in $\mathbb{C}[T]$ and therefore in $\mathbb{Q}[T]$.

5) Otherwise we would have

$$\varphi : \mathbb{Q}[X,Y] \to \mathbb{Q}(T)$$

such that $g = \varphi(X)$ and $f = \varphi(Y)$ satisfy

$$f^2 = g(g-\alpha)(g-\beta)$$

and g not constant.

Exercice 4

1°) $2^2 = 4 = 2 \times (-1)((-1)^2 - 3)$

donc $(-1, 0, 2) \in S(\mathbb{Q})$

le plan tangent à $(x, y, z) \in S(\mathbb{Q})$ est donné par l'équation

$$2y(Y-y) + 2z(Z-z) = (3x^2-3)(X-x)$$

ce qui donne pour P_0 :

$$4(Z-2) = 0$$

donc $Z = 2$.

2°) L'intersection du plan avec S est donnée par

$$\begin{cases} Z = 2 \\ Y^2 + 4 = 2X(X^2-3) \end{cases}$$

soit

$$\begin{cases} Z = 2 \\ Y^2 = 2(X^3 - 3X - 2) \end{cases}$$

soit

$$\begin{cases} Z = 2 \\ Y^2 = 2(X+1)^2(X-2) \end{cases}$$

L'équation d'une droite passant par P_0 dans le plan est donnée par $Y = t(X+1)$

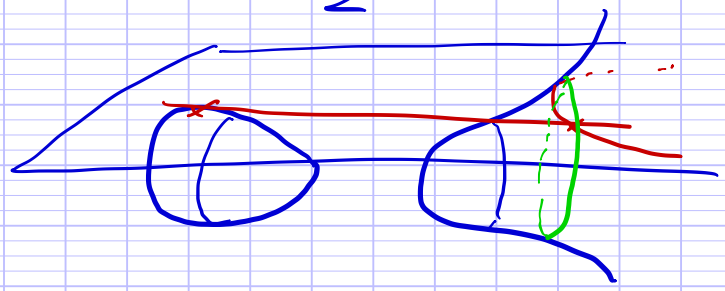
Si on intersecte avec S on obtient

$$\begin{cases} z = 2 \\ y = t(x+1) \\ t^2(x+1)^2 = 2(x+1)^2(x-2) \end{cases}$$

Donc en dehors de P_0, cela donne

$$\begin{cases} z = 2 \\ x = 2 + \frac{t^2}{2} \\ y = 3t + \frac{t^3}{2} \end{cases}$$

3°)



On fait tourner la paramétrisation trouvée autour de l'axe de révolution, l'axe des x en utilisant

$$t \longmapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{2t}{1+t^2} & -\frac{1+t^2}{1+t^2} \\ 0 & \frac{1-t^2}{1+t^2} & \frac{2t}{1+t^2} \end{pmatrix} \begin{pmatrix} \frac{s^2+4}{2} \\ \frac{s^3+6s}{2} \\ 2 \end{pmatrix}$$

cela donne une application

$$\mathbb{Q}^2 \longrightarrow S(\mathbb{Q})$$