北京大学

北京 lecture

2016

DIOPHANTINE STATISTICS

Emmanuel Peyre

Consider a simple polynomial equation like

$$X_1^4 + X_2^4 + X_3^4 = X_4^4.$$

Finding a solution with modern computers ought to be easy: it is enough to check for all triple of integers whether the sum of their fourth powers is itself a fourth power. However, one of the first solution found by N. Elkies with $X_1X_2X_3 \neq 0$ was

$$95800^4 + 217519^4 + 414560^4 = 422481^4,$$

which can not be effectively found with a naive approach. The central question is to be able to locate the solutions either for real topology, or by looking at the reduction modulo N of the coordinates. In other words, one would want to understand the distribution of the solutions of diophantine equations.

As an example, one can cansider the real surface given by the equation

$$X^2 + Y^2 = T(T-1)(T+1)$$

and the rational solutions on this surface with bounded size; we get figure 1. When the bound

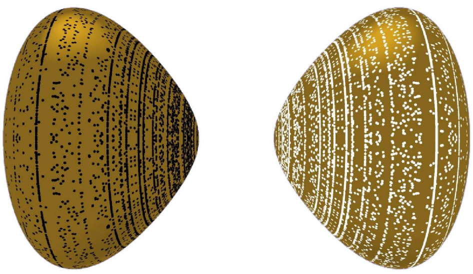


FIGURE 1. Châtelet surface

goes to infinity, is the distribution given by a measure with a continuous density on the surface? If this is the case why do we see circles on the picture?

Outline

1. First examples.
2. Counting measures, convergence.
3. Accumulating phenomena.
4. Adeles, and adelic measures.
5. Back to examples.
6. Obstructions to density.
7. Equidistribution.
8. Slopes and accumulation.

Prerequisite

This lecture requires no previous knowledge of advanced mathematics and is open to third-year and fourth-year students who are majoring in mathematics. The necessary notions in algebraic number theory and algebraic geometry will be introduced as needed during the lecture.

References

[1] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Vieweg & Sohn, 1997.

[2] T. Browning, *Quantitative Arithmetic of Projective Varieties*, Progress in Mathematics, Vol. 277, 2010.

Emmanuel Peyre, Institut Fourier, UFR IM^{2}AG, UMR 5582, Université de Grenoble-Alpes, BP 74, 38402 Saint-Martin d'Hères CEDEX, France

Diophantine statistics

Speaker： Emmanuel Peyre, Université Grenoble Alpes

Sponsored by：

Time： From 2016-04-11 09:00 To 2016-07-01 11:00

Venue： Quan 29, Quanzhai, BICMR

Time： Every Monday &Wednesday (9:00-11:00), From 2016-04-11 to 2016-07-01

Considering a diophantine equation with integral coefficients, there are algorithms to get solutions over the real numbers or modulo an integer. The question is how the rational solutions are distributed relatively to these real or modulo N solutions. More precisely, by putting a bound on the size of the solution we get a finite set of solutions. The reduction modulo an integer gives a map from this finite set to the finite set of solutions modulo that integer. Do all the fibres of this map have approximately the same cardinal ? If not, can we find an invariant explaining the differences?

北京
2016

Diophantine statistics

11/4/2016

I Introduction, Some history

1) Oldest example

The theme I want to speak about has a very long history. In modern terms, I am interested in the solutions of polynomial equations with integral coefficients:

$$\sum_{i_1,\dots,i_n} a_{i_1,\dots,i_n} X_1^{i_1} \cdots X_n^{i_n} = 0$$

with $a_{i_1,\dots,i_n} \in \mathbb{Z}$.

The oldest reference I know to this kind of problem is a babylonian tablet PLIMPTON 322 by the script used it was probably written 3 800 years ago.

If you are not fluent in babylonian, let me explain the content of this tablet. First of all, the structure should look familiar to you since it is organized like an EXCELL file with a table of cells, except that the line numbers are on the right. Each cell contains a number, except on the top where you can find the titles of the columns. I am going to concentrate on the 2nd and 3rd columns. Here is a translation of these columns of the tablet

Table

short side	diagonal
119	169
3367	4825*
4601	6649
12709	18541
65	97

You can easily check that they satisfy the following relations

$$169^2 - 119^2 = 120^2$$
$$4825^2 - 3367^2 = 3456^2$$
$$6649^2 - 4601^2 = 4800^2$$
$$18541^2 - 12709^2 = 13500^2$$
$$97^2 - 65^2 = 72^2$$

In other words you get Pythagorean triples that is solutions of the equation

$$(*) \qquad X^2 + Y^2 = Z^2$$

My motivation in showing you this tablet goes beyond stressing the antiquity of Diophantine equations (By the way, I would be interested to know what is the oldest Chinese study of a Diophantine equation) well before DIOPHANTUS (2^{nd} – 3^{rd} century AD). As you can see, some of these numbers are quite large. So A natural question is: how were babylonians able to produce these rather large solutions? There are at least two possible answers

1) There are a "lot" of solutions, Later, I will come back to this statement and make it precise;

The second answer which is related to the first one is that

2) there is a method to produce all solutions.

You probably know it already but let me remind you how it is done

- If $(x,y,z) \neq 0$ is solution, $d = \gcd(x,y,z)$
$(x/d, y/d, z/d)$ is also a solution
We may assume (x,y,z) primitive (ie $\gcd(x,y,z)=1$)
All babylonian solutions are primitive
- If we look modulo 4 (in $\mathbb{Z}/4\mathbb{Z}$)
a square is 0 or 1 so looking at the solutions in $\mathbb{Z}/4\mathbb{Z}$ since one of the numbers is odd we get that
z is odd and either x or y is odd
(not both of them) By exchanging x and y we may assume x odd, y even. $y = 2y'$,
Write $x, y, z \geq 0$

$$\left(\frac{z-x}{2}\right)\left(\frac{z+x}{2}\right) = y'^2$$

But if p prime divides x and z it divides z
so $\gcd(x,z) = 1 \Rightarrow \gcd\left(\frac{z-x}{2}, \frac{z+x}{2}\right) = 1$
Using the unicity of the decomposition of

北京大学

integers in a product of prime numbers, we get that $\frac{z-x}{2}$ and $\frac{z+x}{2}$ are squares

$\exists\, u, v \in \mathbb{Z}^2$, $\gcd(u,v)=1$ and $\frac{x+z}{2}=u^2$, $\frac{z-x}{2}=v^2$

we get

$$x=u^2-v^2 \qquad y=2uv \qquad z=u^2+v^2$$

3rd table

$(12,5) \to (119, 169)$
$(27,64) \to (3367, 4825)$
$(32,75) \to (4601, 6649)$
$(54,125) \to (12709, 18541)$
$(4,9) \to (65, 97)$

So it is quite fair to suppose that babylonian knew this method of solving the problem or a similar one. One can say that Diophantus was the first to write a book about solving various kind of polynomial equations in several variable with integral equations including equations of higher degree. One of his problem was

Problem II. 8 rational solutions of

$$X^2+Y^2=a^2.$$

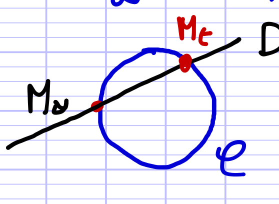
This solution can be interpreted geometrically and gives a more geometric interpretation of the previous parametrization.

circle $\mathcal{C}$

- $\{(x,y,z)\in\mathbb{Z}^3 \text{ primitive } \& \ X^2+Y^2=z^2\} \to \{(x,y)\in\mathbb{Q}^2,\ x^2+y^2=1\}$

$$(x,y,z) \longmapsto \left(\frac{x}{z}, \frac{y}{z}\right)$$

- $M_\infty=(-1,0)$ is an obvious point on the circle



An affine line through M_∞ has an equation of the form

- $D_t : y = t(x+1)$

$D_t \cap \mathcal{C}$: $\begin{cases} x^2+t^2(x+1)^2=1 \\ y=t(x+1)\end{cases} \Leftrightarrow \begin{cases}(x+1)((1+t^2)x+1-t^2)=0 \\ y=t(x+1)\end{cases}$

which gives two points $M_\infty=(-1,0)$ & $M_t=\left(\frac{1-t^2}{1+t^2},\frac{2t}{1+t^2}\right)$

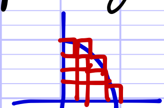
taking $t=\frac{u}{v}$ we get $\frac{u^2-v^2}{u^2+v^2}, \frac{2uv}{u^2+v^2}$

which is the previous parametrization. This parametrization give a precise estimate of the number of primitive solutions with bounded coordinates

$$N(B)=\#\{(x,y,z)\in\mathbb{Z}^3 \mid (x,y,z) \text{ primitive}, x^2+y^2=z^2, |z|\le B\}$$

$$= 16\, \overbrace{\#\{(u,v)\in\mathbb{N}^2 \mid (u,v) \text{ primitive}, u^2+v^2\le B\}}^{N'(B)}$$

↑ may exchange x, y, signs; the only difficulty is to deal with the primitive condition



$$M(B)=\#\{(u,v)\in\mathbb{N}^2-\{0\} \mid u^2+v^2\le B\}$$

$$= \text{Area}(\{(u,v)\in\mathbb{R}^2_{\ge 0} \mid u^2+v^2\le B\})+O(B^{1/2}) = \frac{\pi}{4}B+O(B^{1/2})$$

$$N'(B)=M(B)-\sum_{p \text{ prime}} \#\{(u,v)\in\mathbb{N}^2 \mid p|u, p|v, u^2+v^2\le B\}$$

if u,v are divisible by the product of 2 primes, removed them twice!

$$+\sum_{p_1,p_2 \text{ primes},\ p_1\ne p_2} \#\{(u,v)\in\mathbb{N}^2 \mid p_1p_2|u, p_1p_2|v, u^2+v^2\le B\}$$

$$=\sum_{d\ge 1}\mu(d)\, M\left(\frac{B}{d^2}\right)$$ where μ is the Moebius function

(i) $\mu(ab)=\mu(a)\mu(b)$ if $\gcd(a,b)=1$

(ii) $\mu(p^k)=\begin{cases} 1 & \text{if } k=0 \\ -1 & \text{if } k=1 \\ 0 & \text{otherwise}\end{cases}$

Moreover $M(B)=0$ if $B<1$

$$\left|N'(B)-\sum_{d\le B^{1/2}}\mu(d)\frac{B}{d^2}\right| \le C\sum_{d\le B^{1/2}}\frac{B^{1/2}}{d} \quad \& \quad \sum_{d> B^{1/2}}\mu(d)\frac{B}{d^2}<C'B^{1/2}$$

we get $N(B) = 16 \times \left(\sum_{d\geq 1} \frac{\mu(d)}{d^2}\right) \frac{\pi}{4} B + O(B^{1/2} \log(B))$

But

$$\sum_{d\geq 1} \frac{\mu(d)}{d^2} = \prod_p \left(\sum_k \frac{\mu(p^k)}{p^{2k}}\right) = \prod_p \left(1 - \frac{1}{p^2}\right) = \left(\sum_{n\geq 1} \frac{1}{n^2}\right)^{-1}$$

$$= \zeta(2)^{-1} = \frac{6}{\pi^2}$$

So $N(B) \sim \frac{24}{\pi} B$.

2) Higher degree

You may think I spent too much time on the case of the circle; but it is a good sandbox example to start with. It was in the margin of a translation of the work of DIOPHANTUS, next to this problem that Pierre de FERMAT made his famous statement

Last Theorem of FERMAT (FERMAT 1762, WILES 1995)

Let $n \geq 3$, for any $x, y, z \in \mathbb{Z}$

$$x^n + y^n = z^n \Rightarrow xyz = 0$$

In other words the only solutions are the obvious ones. The situation is radically different in degree two and for higher degrees. Can we explain that? I am not going to prove Fermat last theorem in 5 minutes; But there is a very simple argument to explain the number of solutions for homogeneous polynomials

$$F = \sum_{i_1 + \dots + i_n = d} a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n}$$

Put $C = \sum_{i_1, \dots, i_n} |a_{i_1, \dots, i_n}|$;

If $|x_i| \leq B$ for $i \in \{1, \dots, n\}$ $F(x_1, \dots, x_n) \leq C B^d$

we get a map

$$\mathbb{Z}^n \cap [-B, B]^n \longrightarrow [-CB^d, CB^d]$$

cardinal $\sim (2B+1)^n$ cardinal $2CB^d$

So if one believes that a polynomial function behaves randomly enough on integers, you may naively hope that

Naive hope

- If $n > d$ $\approx C B^{n-d}$ solutions
- If $n = d$ "few" solutions
- If $n < d$ a finite number of solutions (or none)

It is of course too naive and almost everything can go wrong. First there might be

3) Too few points

a) If there is a primitive solutions in $\mathbb{Z}^n$ there is a non-zero one in $\mathbb{R}^n$

Example

$$\sum_{i=1}^{n} a_i X_i^2 = 0$$ has no non zero solution if $a_i > 0$ for $i \in \{1, \dots, n\}$

b) Given a ring A, let us say that $(x_1, \dots, x_n) \in A^n$ is primitive if $\exists (u_1, \dots, u_n) \in A^n$ st

$$\sum_{i=1}^{n} u_i x_i = 1$$

if $F(X_1, \dots, X_n) = 0$ has a primitive solution $/\mathbb{Z}$ it has one in $\mathbb{Z}/M\mathbb{Z}$ for any M

Example

$X^2 + 3Y^2 + 4Z^2 = 0$ has no non zero solution $/\mathbb{Z}$, because it has none $/ \mathbb{Z}/9\mathbb{Z}$

The only squares in $\mathbb{Z}/3\mathbb{Z}$ are 0 and 1

Thus

$(x, y, z) \in (\mathbb{Z}/9\mathbb{Z})^3$ primitive solution

$3 \mid x$ and $3 \mid z \Rightarrow x^2 + 4z^2 \equiv 0 \ (9)$

Thus $3 \mid y$ absurd $\lightning$.

Why is the point of these remarks

Fact

a) and b) can be tested with an algorithm

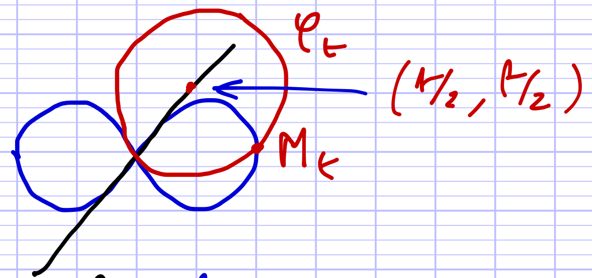
I am not claiming that there is an efficient algorithm only that, theoritically, there exists one.

4) Too many points

Let us consider Bernouilli's lemniscate

$$\mathcal{L} : \quad (X^2+Y^2)^2 - X^2 + Y^2 = 0$$

Drawing



As for the circle the rational solutions of this equation correspond to the primitive integral solutions of

$$(*) \quad (X^2+Y^2)^2 - X^2T^2 + Y^2T^2 = 0$$

of degree four. The degree is strictly bigger than the number of variables so we should have very few solutions right? wrong!

For any $t \in \mathbb{Q}$ let $\mathcal{C}_t$ be the circle centered at (t,t) and passing through $(0,0)$. It intersects $\mathcal{L}$ in exactly one more point. $\{M_t, (0,0)\} = \mathcal{C}_t \cap \mathcal{L}$.

This give the following parametrization of the rational solutions:

$$M_t = \left(\frac{t(1+t^2)}{1+t^4} , \frac{t(1-t^2)}{1+t^4} \right)$$

From this we can deduce that

# of primitive solutions of $(*)$ with $\max(|x|, |y|, |t|) \leq B$

is $\sim c_{te} B^{1/2}$. So there are a lot of solutions. The main point for this particular case is that the curve is not smooth. If we put

$$F(X,Y) = (X^2+Y^2)^2 - X^2 + Y^2$$

$\frac{\partial F}{\partial X}(0,0) = \frac{\partial F}{\partial Y}(0,0) = 0$ that's the way we produce the parametrization. So now we are a little bit less naive and our hopes are more reasonable and I can state a few

5 Some positive results

Chronologically the first general positive result is due to MINKOWSKI over $\mathbb{Q}$

Theorem (MINKOWSKI, 1890)

Let q be a non degenerate quadratic form with integral coefficients then it has a primitive solutions in $\mathbb{Z}^n$ if and only if it has a non zero real solution and a primitive solutions in $\mathbb{Z}/N\mathbb{Z}$ for any $N \geq 1$.

Theorem (BIRCH, 1962)

F homogeneous of degree d in n variable such that

(i) $F=0$ has a non zero real solution

(ii) $\forall M \geq 2$ F has a primitive solution in $(\mathbb{Z}/M\mathbb{Z})^n$

(iii) $d_x F = 0 \Rightarrow x = 0$ in $\mathbb{C}^n$

(iv) $n > (d-1)2^d$ a lot of variable

Then

$$\#\{(x_1,..,x_n)\in\mathbb{Z}^n \mid \text{primitive}, F(x_1,-,x_n)=0 \ \& \max(|x_i|) \leq B\} \sim C_F B^{n-d}$$

Theorem (FALTINGS, 1983)

If $F(X,Y,Z)$ homogeneous of degree $d > 3$

satisfies

$\forall x \in \mathbb{C}^3, \ d_x F = 0 \Rightarrow x = 0$

then $F(x,y,z) = 0$ has a finite number of solutions.

So we could believe everything is settled but

A little less naive hope

F homogeneous

Assume conditions (i) – (iii) of BIRCH's theorem

– If $d \geq n$ "few" solutions

– If $d < n$ $\sim C_F \, B^{n-d}$ solutions

it is far from true

6 More problems

a) no solutions

?

(1) $5X^3 + 9Y^3 + 10Z^3 + 12T^3 = 0$ (SWINNERTON-DYER)

satisfies (i) – (iii) but has no primitive solution

This one corresponds to a homogeneous equation but is rather more complicated to explain so instead I am going to explain:

(2) $Y^2 + Z^2 = (3U^2 - V^2)(V^2 - 2U^2)T^2$

In that case a "primitive" solution ought to be defined differently:

On can reduce a non trivial solution to one with

$$\gcd(U,V) = \gcd(X,Y,Z) = 1$$

(i') F has a solution $/\mathbb{R}$ with $(U,V) \neq 0$ and $(X,Y,Z) \neq 0$

(ii') F ——— $/\mathbb{Z}/M\mathbb{Z}$ with (u,v) and (x,y,z) primitive (I may explain that much later in the lecture)

(iii') $P = (x,y,z,u,v)$

$d_P F = 0 \Rightarrow (u,v) = 0$ and $(x,y,z) = 0$.

But F has no "primitive" solution $/\mathbb{Z}$.

__Sketch of the proof__

we use the following quite classical

__Fact__ which I am not going to prove today.

$n \in \mathbb{Z}$ is the sum of two squares if and only if

(i) $n \geq 0$

(ii) for any prime p, $p \equiv -1 \ (4)$, $v_p(n)$ is even where

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

Those conditions which are relative to $\mathbb{R}$ and odd prime numbers imply

$$(\ast\ast) \quad n / 2^{v_2(n)} = \prod_{p \equiv 1 (4)} p^{v_p(n)} \prod_{p \equiv 3 (4)} (p^2)^{\frac{v_p(n)}{2}} \equiv 1 \ (4)$$

So If (2) has a "primitive" solution,

then $(3u^2 - v^2)(v^2 - 2u^2) > 0$

$\Rightarrow \frac{v}{u} \in]-\sqrt{3}, -\sqrt{2}[\cup]\sqrt{2}, \sqrt{3}[$

← french notation for open interval.

$\Rightarrow$ In fact, $3u^2 - v^2 \geq 0$ and $v^2 - 2u^2 \geq 0$

Similarly,

$$\gcd(3u^2 - v^2, v^2 - 2u^2) = \gcd(u^2, v^2) = 1 \quad \leftarrow \det\begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix} = 1$$

So for any prime $p \equiv -1 \ (4)$

$$v_p(3u^2 - v^2, v^2 - 2u^2) \equiv 0 \ (2)$$

$$\Rightarrow v_p(3u^2 - v^2) \equiv 0 \ (2) \text{ and } v_p(v^2 - 2u^2) \equiv 0 \ (2)$$

Thus $3u^2 - v^2$ and $v^2 - 2u^2$ have to be sums of two squares. let's look at the condition $(\ast\ast)$

- If u & v are odd $u^2 \equiv v^2 \equiv 1 \ (4) \Rightarrow v^2 - 2u^2 \equiv 3 (4)$ which is absurd ↯ But they are coprime, thus
- If u even, v odd then $3u^2 - v^2 \equiv 3 \ (4)$ ↯

In 1970, Manin explained in his ICM address that the known examples can be explained through a new obstruction, now called the BRAUER–MANIN obstruction. This lead to a new question

Question

Is the BRAUER–MANIN obstruction the only one?
Well in some sense the answer is given by the following

Theorem (DAVIS, PUTNAM, ROBINSON, MATIJACEVIC, 1970)
$\exists$ $F(X_1, \ldots, X_n, T)$ (not homogeneous) in 12 variables with coefficients in $\mathbb{Z}$ such that there is no algorithm to compute the map

$$t \longmapsto \begin{cases} 1 \text{ if } f(X_1, \ldots X_n, t) = 0 \text{ has a solution} \\ 0 \text{ otherwise} \end{cases}$$

Remarks

This proves that
Hilbert 10th problem : Given a diophantine equation with any number of unknown quantities and integral coefficients. Find an algorithm to determine if there exists a solution with integral coordinates. You can see this theorem in two ways
1) In a negative way as the final blow to the hope of solving diophantine equations
2) In a positive manner, it means that whatever methods you have found to prove that a given equation has no solutions there is somewhere an equation to which it does not apply and for which you have to find a new method and our job will never be done.

b) Too many solutions

Already with quadrics consider

(1) $XY - ZT = 0$

There is a map from the set

$$\{((u_1, u_2), (v_1, v_2)) \in \mathbb{Z}^4 \mid (u_1, u_2), (v_1, v_2) \text{ primitive}\}$$

to the quadric given by

$$((u_1, u_2), (v_1, v_2)) \underset{(2:1)}{\longmapsto} (u_1 v_1, u_2 v_2, u_1 v_2, u_2 v_1)$$

$$\max_{i,j} (|u_i v_j|) = \max(|u_1|, |u_2|) \max(|v_1|, |v_2|)$$

we get that the cardinal of the set of primitive solutions with bounded coordinates is

$$\frac{1}{2} \sum_{\substack{(u_1, u_2) \text{ primitive} \\ \max(|u_1|, |u_2|) \leq B}} \#\left\{(v_1, v_2) \text{ primitive}, \max(|v_1|, |v_2|) \leq \frac{B}{\max(|u_1|, |u_2|)}\right\}$$

With a similar argument to the one given for points in a disk

$$\sim \frac{1}{2} \sum_{d \leq B} \underbrace{\sum_{\substack{(u,v) \text{ primitive} \\ \max(|u|, |v|) = d}}}_{\sim \frac{6}{\pi^2} d} \frac{4 \times 6}{\pi^2} \frac{B^2}{d^2} \sim 4 \left(\frac{6}{\pi^2}\right)^2 B^2 \log(B)$$

<u>Next guess</u> $B^{n-d} \log(B)^{t-1}$

for some geometrical invariant t of the quadric

(2) $\sum_{i=0}^{3} X_i^3 = 0$ cubic surface

expected $B (\log B)^{t-1}$

Over $\mathbb{C}$, projective cubic surfaces contain 27 lines.

This particular surface contains the projective line

$$X_1 = -X_2\,,\; X_3 = -X_4$$

and the one obtained by permutations

$$(u,v) \text{ primitive } \longmapsto (u,-u,v,-v)$$

gives $\sim$ cste B^2 solutions

But it turns out

Conjecture (BATYREV – MANIN) still open

On a cubic surface the number of solutions with bounded coordinate outside the 27 line is the expected one.

This is the first example of accumulating subset

And there are more complicated examples of accumulating subset

Problem

How to characterize accumulating subsets?

Diophantine statistics

Emmanuel Peyre

Université Grenoble Alpes

北京大学

History (18th century bc.)

The old babylonian clay tablet called "Plimpton 322"

Translation

Short Side	Diagonal
119	169
3367	4825*
4601	6649
12709	18541
65	97
319	481
2291	3541
799	1249

* Corrected value

Translation

Short Side	Diagonal
119	169
3367	4825*
4601	6649
12709	18541
65	97
319	481
2291	3541
799	1249

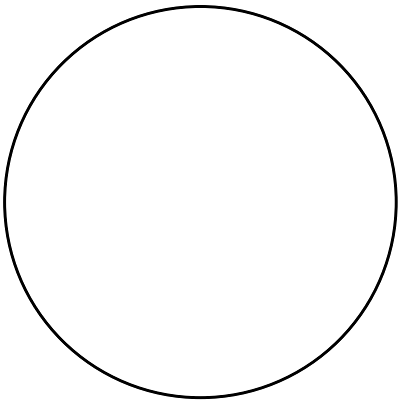
* Corrected value

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

Integral solutions of $X^2 + Y^2 = Z^2$

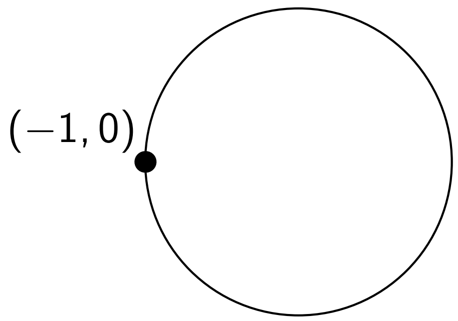
u	v	$2uv$	$u^2 - v^2$	$u^2 + v^2$
12	5	120	119	169
64	27	3456	3367	4825*
75	32	4800	4601	6649
125	54	13500	12709	18541
9	4	72	65	97
20	9	360	319	481
54	25	2700	2291	3541
32	15	960	799	1249

Diophantus (2nd-3rd century ad)



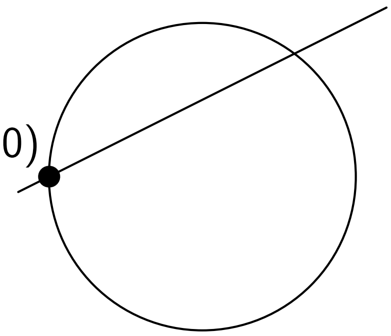
- $X^2 + Y^2 = 1$ defines a circle of radius 1 ;

Diophantus (2nd-3rd century ad)



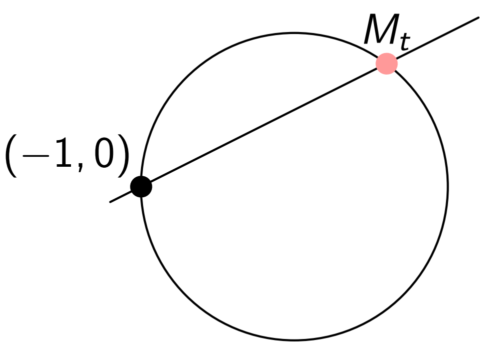
- $X^2 + Y^2 = 1$ defines a circle of radius 1 ;
- $M_0 = (-1, 0)$ is a point on this circle ;

Diophantus (2nd-3rd century ad)



- $X^2 + Y^2 = 1$ defines a circle of radius 1 ;
- $M_0 = (-1, 0)$ is a point on this circle ;
- The equation $Y = t(X + 1)$ defines a line D_t through this point ;

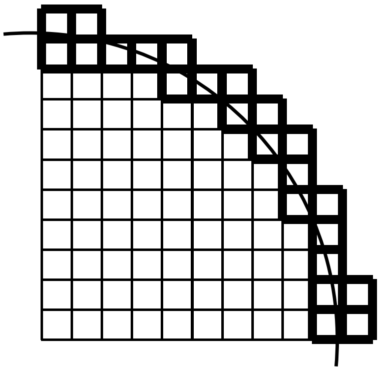
Diophantus (2nd-3rd century ad)



- $X^2 + Y^2 = 1$ defines a circle of radius 1 ;
- $M_0 = (-1, 0)$ is a point on this circle ;
- The equation $Y = t(X + 1)$ defines a line D_t through this point ;
- Let M_t be the second point of intersection of D_t with the circle ;

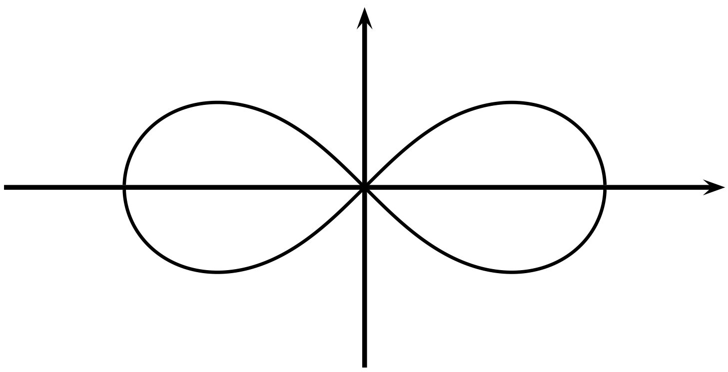
Points in a disk

$$\left|\sharp\{\,(u,v)\in\mathbf{N}^2 \mid 0<u^2+v^2\leqslant B\,\}-\pi(\sqrt{B})^2\right|\leqslant C\sqrt{B}.$$

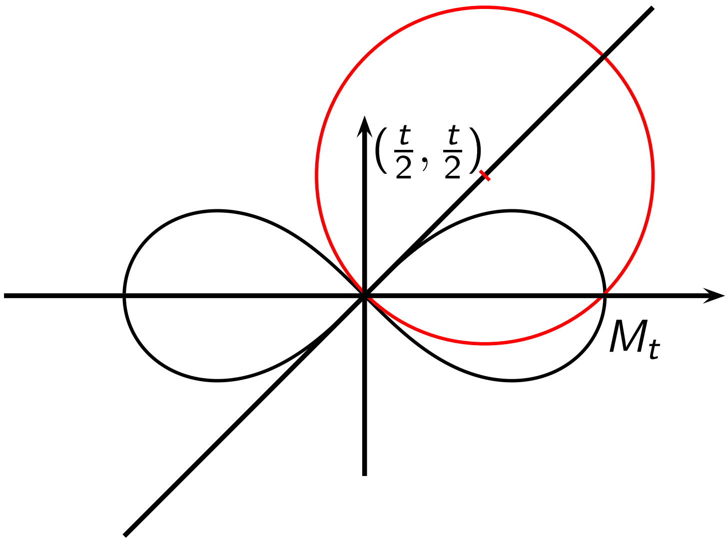


Bernoulli's Lemniscate

$$(X^2 + Y^2)^2 - X^2 + Y^2 = 0$$



Bernoulli's lemniscate (parametrisation)



$$\begin{cases} x = \frac{t(1+t^2)}{1+t^4}, \\ y = \frac{t(1-t^2)}{1+t^4}. \end{cases}$$

Matijacevič's theorem

Theorem (Davis, Putnam, Robinson, Matijacevič, et al. (1970))

There exists a polynomial $P(X_1, \dots, X_{11}, T)$ in 12 variables with integral coefficients such that the application mapping a integer n to

$$\begin{cases} 1 \text{ if } P(X_1, \dots, X_{11}, n) = 0 \text{ has a solution} \\ 0 \text{ otherwise} \end{cases}$$

can not be computed with an algorithm.

In particular, Hilbert's tenth problem can not be solved.

Hilbert's tenth problem

Hilbert gave during the 1900 International Congress of Mathematicians a list of the problems he thought the most important for the 20th century.

10. Entscheidung der Lösbarkeit einer diophantischen Gleichung. Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoefficienten sei vorgelegt : man soll ein Verfahren angeben, nach welchen sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

10. Determination of the solvability of a Diophantine equation. Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients : To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.

14/4/12016 Today, I am going to explain more precisely very elementary examples. My aim is to have a more precise idea about what can be expected when counting solutions of equations with bounded coordinates

II Elementary examples

1) The projective space

a) points on $\mathbb{P}^n$

Def / Notation

- Let A be a commutative ring not necessarily integral such that any ideal of A is generated by one element (eg $\mathbb{Z}/n\mathbb{Z}$)
Such a ring is called a principal ideal ring
- For such a ring,

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

where A^* is the group of invertible elements in A. I denote by

$$\pi : \{\text{primitive elements in } A^{n+1}\} \longrightarrow \mathbb{P}^n(A)$$

the projection and put

$$[x_0 : \ldots : x_n] = \pi(x_0, \ldots, x_n)$$

for $(x_0, \ldots, x_n) \in A^{n+1}$

$(x_0, \ldots, x_n)$ are called homogeneous coordinates of the point $[x_0 : \ldots : x_n]$.

- Let A be a commutative ring and let $F_1, \ldots, F_r \in A[T_0, \ldots, T_n]$ be homogeneous polynomials
We put $I = (F_1, \ldots, F_r)$ the ideal generated by $\{F_1, \ldots, F_r\}$
For any A-algebra B which is a principal ideal ring, we can define

$$V_I(B) = \{[x_0 : \dots : x_n] \in \mathbb{P}^n(B) \mid \underbrace{\forall i \in \{1, \dots, r\}, F_i(x_0, \dots, x_n) = 0}_{\text{this condition does not depend on the choice of homogeneous coordinate}}\}$$

Remarks

- For a field primitive = non zero.
- If $\varphi : B \to C$ is a morphism of A-algebras which are principal ideal rings then we have a map

$$\varphi : \mathbb{P}^n(B) \to \mathbb{P}^n(C)$$
$$[b_0 : b_1 : \dots : b_n] \longmapsto [\varphi(b_0) : \varphi(b_1) : \dots : \varphi(b_n)]$$

Indeed

If $\sum_{i=0}^{n} u_i b_i = 1$ then $\sum_{i=0}^{n} \varphi(u_i)\varphi(b_i) = 0$

So φ maps primitive elements to primitive elements and invertible elements to invertible elements

$$\varphi(V_I(B)) \subset V_I(C)$$

we get a map $\varphi : V_I(B) \to V_I(C)$

Example

The map $\mathbb{P}^n(\mathbb{Z}) \to \mathbb{P}^n(\mathbb{Q})$ is bijective

Indeed, take $(x_0, \dots, x_n) \in \mathbb{Q}^{n+1} - \{0\}$ let u be least common multiple of the denominators

$d = \gcd(u x_0, \dots, u x_n) \in \mathbb{Z}^{n+1}$

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

$\left(\frac{u x_0}{d}, \dots, \frac{u x_n}{d}\right)$ is primitive in $\mathbb{Z}^{n+1}$.

b) Elementary height

Definition

Let $\|\cdot\|_v$ be a norm on $\mathbb{R}^{n+1}$

I remind you that any two norms are equivalent on $\mathbb{R}^{n+1}$.

We define the <u>exponential height associated to $\|\cdot\|_\infty$</u> as a function $H : \mathbb{P}^n(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0}$ defined by

$$H([x_0 : \ldots : x_n]) = \|(x_0, \ldots, x_n)\|_\infty$$

if $(x_0, \ldots, x_n) \in \mathbb{Z}^{n+1}$ is primitive

<u>Examples</u>

As norms, we may take

$$\|(x_0, \ldots, x_n)\|_\infty = \max_{0 \leq i \leq n} |x_i|.$$

or

$$\|(x_0, \ldots, x_n)\|_\infty = \sqrt{\sum_{i \geq 0}^{n} x_i^2}.$$

<u>Notation</u>

$F_1, \ldots, F_r \in \mathbb{Z}[X_0, \ldots, X_n]$ homogeneous which defines V

H defined by $\|\cdot\|_\infty$ on $\mathbb{P}^n(\mathbb{Q})$

$W \subset V(\mathbb{Q}) \subset \mathbb{P}^N(\mathbb{Q})$ any subset but what follows will be interesting only for infinite W

$$W_{H \leq B} = \{P \in W \mid H(P) \leq B\}$$

<u>NB</u>

This set is finite. It is enough to prove it for $\mathbb{P}^n(\mathbb{Q})$ and we are going to prove a more precise statement

<u>b) Result</u>

<u>Notation</u>

$$\# X = \text{cardinal of } X.$$

Proposition

$$\# \mathbb{P}^n(\mathbb{Q})_{H \leq B} \sim \frac{\mathrm{Vol}(\mathbb{B}(0,1))}{2 \times \zeta(n+1)} B^{n+1} + \begin{cases} O(B^n) & \text{if } n \geq 2 \\ O(B \log(B)) & \text{if } n = 1. \end{cases}$$

where $\mathbb{B}(x, r) = \{ y \in \mathbb{R}^{n+1} \mid \|y - x\|_\infty \leq r \}$.

Proof

$$\# \mathbb{P}^n(\mathbb{Q})_{H \leq B} = \frac{1}{2} \# \left\{ (x_0, \dots, x_n) \in \mathbb{Z}^{n+1} \;\middle|\; \begin{array}{l} \gcd(x_0, \dots, x_n) = 1 \\ \|(x_0, \dots, x_n)\|_\infty \leq B \end{array} \right\}$$

$$= \frac{1}{2} \sum_{d \geq 1} \mu(d) \# \left\{ (x_0, \dots, x_n) \in (d\mathbb{Z})^{n+1} - \{0\} \;\middle|\; \|(x_0, \dots, x_n)\|_\infty \leq B \right\}$$

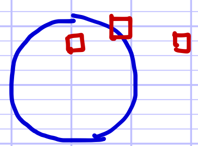
$$= \frac{1}{2} \sum_{d \geq 1} \mu(d) \, M\left(\frac{B}{d}\right)$$

where $M(B) = \# \underbrace{\{ x \in \mathbb{Z}^{n+1} - \{0\} \mid \|x\|_\infty \leq B \}}_{\mathcal{N}(B)}$

for $x \in \mathbb{R}^{n+1}$ write $C_x = x + [0, 1]^{n+1}$

small cube of size 1 at x. We have implication

$$C_x \subset \mathbb{B}_{\|\cdot\|_\infty}(0, B) \Rightarrow \|x\|_\infty \leq B \Rightarrow C_x \cap \mathbb{B}_{\|\cdot\|_\infty}(0, B) \neq \emptyset$$



Let $\alpha, \beta > 0$ be such that, for any $(x_0, \dots, x_n) \in \mathbb{R}^{n+1}$,

$$\alpha \max_{0 \leq i \leq n} (|x_i|) \leq \|(x_0, \dots, x_n)\|_\infty \leq \beta \max_{0 \leq i \leq n} (|x_i|)$$

$\forall y \in C_x \quad \max_{0 \leq i \leq n} (|y_i - x_i|) \leq 1$ and thus $\|y - x\| \leq \beta$

$$M(B) = \mathrm{Vol}\left(\bigcup_{x \in \mathcal{N}(B)} C_x \right) - 1$$

$$\mathrm{Vol}\left(\bigcup_{C_x \subset B(0,B)} C_x \right) \leq M(B) + 1 \leq \mathrm{Vol}\left(\bigcup_{C_x \cap B(0,B) \neq \emptyset} C_x \right)$$

$$/\!/ \qquad \leq \mathrm{Vol}(\mathbb{B}(0, B)) \leq \qquad /\!/$$

$$|M(B) - Vol(B(0,B))| \le 1 + Vol\Big(\bigcup_{C_x \cap \partial B(0,B) \neq \emptyset} C_x\Big)$$

$$\le 1 + Vol\{y \in \mathbb{R}^{n+1} \mid d(y, \partial B(0,B)) \le \beta\}$$

$$\le 1 + Vol(B(0, B+\beta)) - Vol(B(0, B-\beta))$$

$$= 1 + Vol(B(0,1))\left[(B+\beta)^{n+1} - (B-\beta)^{n+1}\right]$$

$$\le C\, B^n \quad \text{for} \quad B \ge \alpha.$$

Moreover $M(B) = 0$ if $B < \alpha$.

Since $\|x\|_\infty < \alpha \Rightarrow \max_{0 \le i \le n} |x_i| < 1 \Rightarrow x = 0$.

$$\left| \#\mathbb{P}^n(\mathbb{Q})_{H \le B} - \frac{1}{2}\left(\sum_{d \le \frac{B}{\alpha}} \mu(d) \frac{Vol(B(0,1))}{d^{n+1}}\right) B^{n+1} \right|$$

$$\le C \sum_{d \le \frac{B}{\alpha}} \underbrace{|\mu(d)|}_{\le 1} \left(\frac{B}{d}\right)^n \le C B^n \underbrace{\sum_{d \le \frac{B}{\alpha}} \frac{1}{d^n}}_{\le 2 \begin{cases} \text{cste} & \text{if } n > 1 \\ 1 + \log\left(\frac{B}{\alpha}\right) & \text{if } n = 1 \end{cases}}$$

and
$$\left|\sum_{d > \frac{B}{\alpha}} \mu(d) \frac{1}{d^{n+1}}\right| < \sum_{d > \frac{B}{\alpha}} \frac{1}{d^{n+1}} \le 2 \left(\frac{\alpha}{B}\right)^n$$

and
$$\left(\sum_{d \ge 1} \mu(d) \frac{1}{d^{n+1}}\right)^{-1} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^{n+1}}\right)^{-1} = \prod_{p \text{ prime}} \Big(\sum_{k \ge 0} p^{-k(n+1)}\Big)$$

$$= \sum_{d \ge 1} \frac{1}{d^{n+1}} = \zeta(n+1).$$

Which concludes the proof □

The nice point of this statement is that we see precisely how the main term in asymptotic behaviour depends on the choice of the norm on $\mathbb{R}^{n+1}$.

The second example I want to speak about is the product of 2 projective spaces

2) The product of two projective spaces

a) Heights

First of all I have to realize it as V_I for some ideal I generated by homogeneous polynomials. Choose $a_1, a_2 \geq 1$

$$\phi_{a,b} : \mathbb{P}^m_{\mathbb{Q}} \times \mathbb{P}^n_{\mathbb{Q}} \longrightarrow \mathbb{P}^N_{\mathbb{Q}}$$

$$([x_0 : \cdots : x_m], [y_0 : \cdots : y_n]) \longmapsto [(M(x_0, \ldots, x_m, y_0, \ldots, y_n))_{M \in \mathcal{M}}]$$

$$\mathcal{M} = \left\{ \prod_{i=0}^{m} X_i^{\alpha_i} \prod_{j=0}^{n} Y_j^{\beta_j},\ \sum_{i=0}^{m} \alpha_i = a \ \& \ \sum_{j=0}^{m} \beta_j = b \right\}$$

$$N = \# \mathcal{M} - 1$$

$$I = \{ P \in \mathbb{Z}[X_M, M \in \mathcal{M}] \mid P((M)_{M \in \mathcal{M}}) = 0 \}$$

(for example $T_{X_0^a Y_0^b} T_{X_1^a Y_1^b} - T_{X_0^a Y_1^b} T_{X_1^a Y_0^b} \in I$)

$M \in \mathcal{M}$

I is an ideal generated by a finite number of homogeneous polynomials

$$\phi_{a,b} : \mathbb{P}^m(\mathbb{Q}) \times \mathbb{P}^n(\mathbb{Q}) \longrightarrow V_I(\mathbb{Q}) \subset \mathbb{P}^N(\mathbb{Q})$$

is a bijective map.

I take for $(t_m)_{m \in \mathcal{M}} \in \mathbb{R}^{\mathcal{M}}$

$$\|(t_m)_{m \in \mathcal{M}}\|_\infty = \max_{m \in \mathcal{M}} |t_m|$$

Then

$$\|(M(x_0, \ldots, x_m, y_0, \ldots, y_n))_{M \in \mathcal{M}}\|_\infty = \|(x_0, \ldots, x_m)\|_\infty^a \, \|(y_0, \ldots, y_n)\|_\infty^b$$

if

$$\|(x_0, \ldots, x_m)\|_\infty = \max_{0 \leq i \leq n} |x_i|$$

$$\|(y_0, \ldots, y_m)\|_\infty = \max_{0 \leq j \leq n} |y_j| .$$

we get

$$H_{a,b}(P,Q) = H(\phi_{a,b}(P,Q)) = H(P)^a\, H(Q)^b .$$

↖ definition

Proposition

The cardinal $\#(\mathbb{P}^m(\mathbb{Q}) \times \mathbb{P}^n(\mathbb{Q}))_{H_{a,b} \leq B}$ is equivalent to

(i) $\left(\sum_{P \in \mathbb{P}^m(\mathbb{Q})} \frac{1}{H(P)^{\frac{a}{b}(n+1)}} \right) C(\mathbb{P}^n(\mathbb{Q}))\, B^{\frac{n+1}{b}}$ if $\frac{a}{b} > \frac{m+1}{n+1}$

(ii) $\left(\sum_{P \in \mathbb{P}^m(\mathbb{Q})} \frac{1}{H(P)^{\frac{b}{a}(m+1)}} \right) C(\mathbb{P}^m(\mathbb{Q}))\, B^{\frac{m+1}{a}}$ if $\frac{b}{a} > \frac{n+1}{m+1}$

(iii) $C\, C(\mathbb{P}^m(\mathbb{Q}))\, C(\mathbb{P}^n(\mathbb{Q}))\, B^{\frac{m+1}{a}} \log\left(B^{\frac{m+1}{a}}\right)$ if $\frac{b}{a} = \frac{n+1}{m+1}$

Remarks

(i) First example with a power of log

One has to explain this phenomena

(ii) if $\frac{a}{b} > \frac{m+1}{n+1}$ Take $P \in \mathbb{P}^m(\mathbb{Q})$

$pr_1 : \mathbb{P}^m(\mathbb{Q}) \times \mathbb{P}^n(\mathbb{Q}) \longrightarrow \mathbb{P}^m(\mathbb{Q})$ 1^{st} projection

$$\#(pr_1^{-1}(P))_{H_{a,b} \leq B} = \#\left\{ Q \in \mathbb{P}^n(\mathbb{Q}) \mid H(Q)^b \leq \frac{B}{H(P)^a} \right\}$$
$$\sim C(\mathbb{P}^n(\mathbb{Q})) \left(\frac{B}{H(P)^a} \right)^{\frac{n+1}{b}}$$

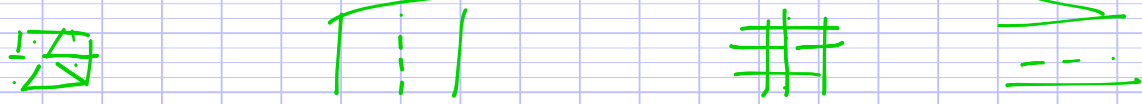
So the main term is in fact the sum of the main terms on each fibre and

$$\underline{\lim}_{B \to +\infty} \left(\frac{\#(pr_1^{-1}(B))_{H_{a,b} \leq B}}{\#(\mathbb{P}^m(\mathbb{Q}) \times \mathbb{P}^n(\mathbb{Q}))_{H_{a,b} \leq B}} \right) > 0$$

The contribution of each fibre is not negligeable whereas if $\frac{a}{m+1} = \frac{b}{n+1}$ the contribution of each fibre is negligeable. Let me show you 4 pictures.

Picture

$\mathbb{P}^1 \times \mathbb{P}^1(\mathbb{Q})$



$\mathbb{P}^2(\mathbb{Q})$ case $\frac{a}{b} > \frac{m+1}{n+1}$ $\frac{a}{b} = \frac{m+1}{n+1}$ $\frac{a}{b} < \frac{m+1}{n+1}$

Proof

$$\# \, \mathbb{P}^m(\mathbb{Q}) \times \mathbb{P}^n(\mathbb{Q})_{H_{a,b} \leq B}$$

$$= \sum_{P \in \mathbb{P}^m(\mathbb{Q})} \# \left(pr_1^{-1}(P)\right)_{H_{a,b} \leq B}$$

$$= \sum_{P \in \mathbb{P}^m(\mathbb{Q})} \underbrace{\# \left\{ Q \in \mathbb{P}^n(\mathbb{Q}) \mid H(Q) \leq \left(\frac{B}{H(P)^a}\right)^{\frac{1}{b}} \right\}}_{||}$$

$$c(\mathbb{P}^n(\mathbb{Q})) \left(\frac{B}{H(P)^a}\right)^{\frac{n+1}{b}} + O\left(\left(\frac{B}{H(P)^a}\right)^{\frac{n}{b}+\varepsilon}\right)$$

Lemma

$f : X \longrightarrow \mathbb{R}_{>0}$ $\quad X_{f \leq B} = \{x \in X \mid f(x) \leq B\}$

Assume that

$$\underbrace{\# X_{f \leq B}}_{\text{is finite}} \sim c B^a \log(B)^{b-1}$$

Then $s \in \mathbb{C}$

$$\sum_{x \in X} \frac{1}{f(x)^s} \begin{cases} \text{converges if } \operatorname{Re}(s) > a \\ \text{diverges if } s \in \mathbb{R},\ s < a \end{cases}$$

Proof

I am going to use STIELTJES notations (See TENENBAUM, Introduction to analytic and probabilistic number theory I.0.1)

Let $g : \mathbb{R}_{\geq 0} \longrightarrow \mathbb{R}_{\geq 0}$ $\quad s = \sigma + i\tau$

$t \longmapsto \# X_{\leq t}$ $\quad \sigma, \tau \in \mathbb{R}$

then $\sum_{x \in X} \frac{1}{|f(x)^s|} = \int_0^{+\infty} \frac{1}{t^\sigma} \, dg(t)$

$\left(\int_a^b h \, dg(t) = \sum_{\{x \in X,\, a < f(x) \leq b\}} h(f(x)) \right)$

Abel summation gives if h is of class $\mathcal{C}^1_b$

$$\int_a^b h \, dg(t) = \left[h(t) g(t) \right]_a^b - \int_a^b h'(t) g(t) \, dt$$

So

$$\sum_{x \in X} \frac{1}{|f(x)^s|} = 0 + \int_0^{+\infty} \frac{\sigma}{t^{\sigma+1}} \underbrace{g(t)}_{0 \text{ for } t \text{ small}} dt$$

But $g(t) < C_\varepsilon t^{a+\varepsilon}$ for any $\varepsilon > 0$.

So the integral converges if $\sigma > a$.

also $g(t) > C'_\varepsilon t^{a-\varepsilon}$

So the integral diverges if $\sigma < a$.

The first two statements follow from the lemma

It remains to consider the equality case

<u>End of the proof</u>

Assume $\frac{a}{m+1} = \frac{b}{n+1}$

we have to compute

$$\sum_{\substack{P \in \mathbb{P}^m(\mathbb{Q}) \\ H^a \leq B}} \left(C(\mathbb{P}^n(\mathbb{Q})) \left(\frac{B}{H(P)^a} \right)^{\frac{n+1}{b}} + O\left(\left(\frac{B}{H(P)^a} \right)^{\frac{n}{b}+\varepsilon} \right) \right)$$

Write $g(t) = \# \mathbb{P}^m(\mathbb{Q})_{H \leq t^{1/a}}$

we have to compute

$$\int_1^{B^{1/a}} \frac{1}{t^{\frac{a}{b}(m+1)}} \, dg(t) = \left[\frac{g(t)}{t^{\frac{a}{b}(m+1)}} \right]_1^B + \int_1^B \frac{\frac{a}{b}(m+1)}{t^{\frac{a}{b}(m+1)+1}} g(t) \, dt$$

But $g(t) = C(\mathbb{P}^m(\mathbb{Q})) t^{m+1} + O(t^{m+\varepsilon})$

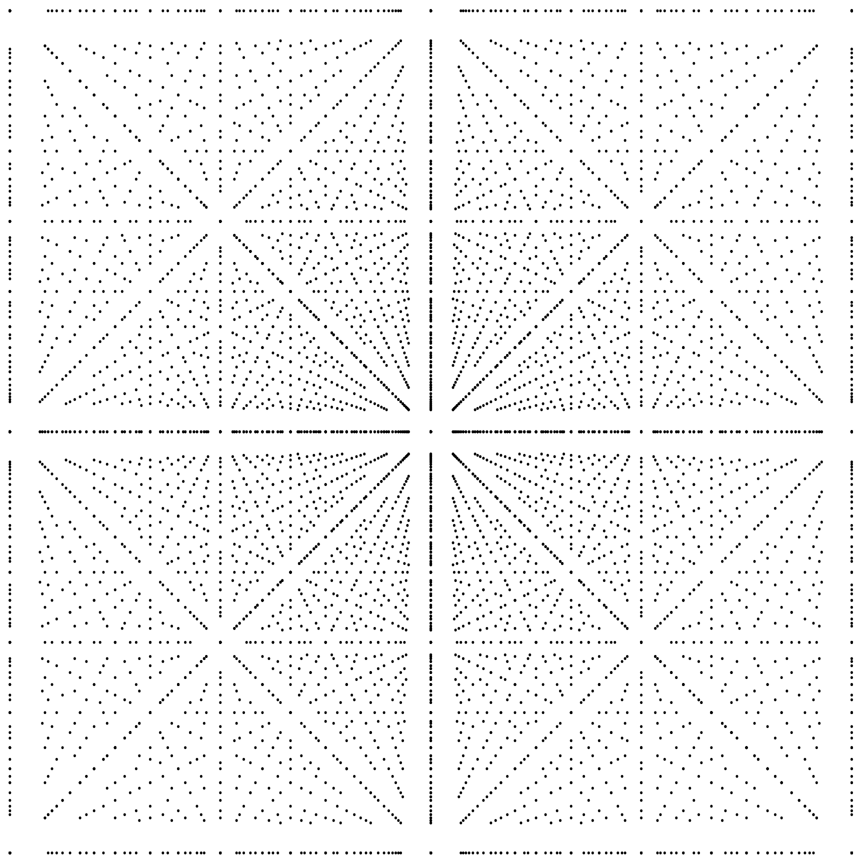
Diophantine statistics

Emmanuel Peyre

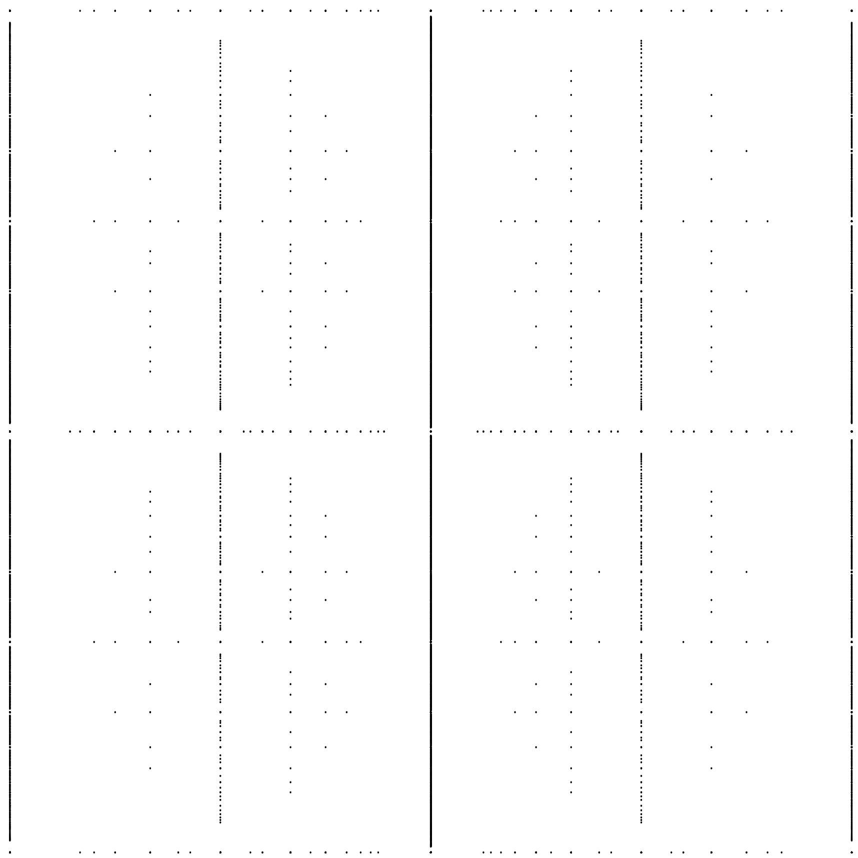
Université Grenoble Alpes

北京大学

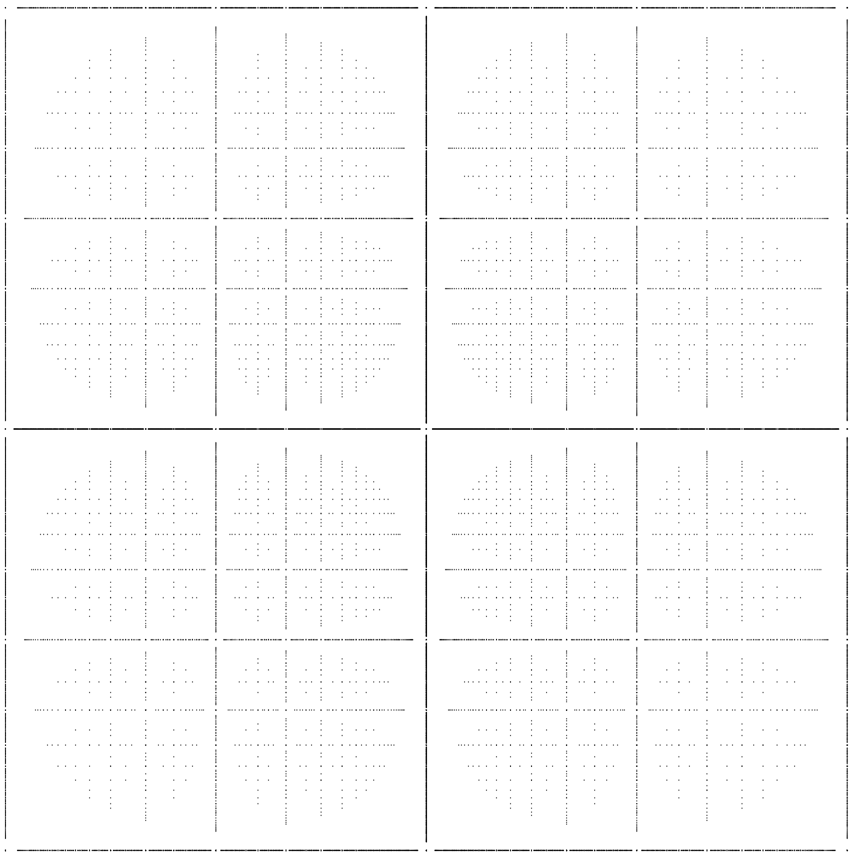
$\mathbf{P}^2(\mathbf{Q})$



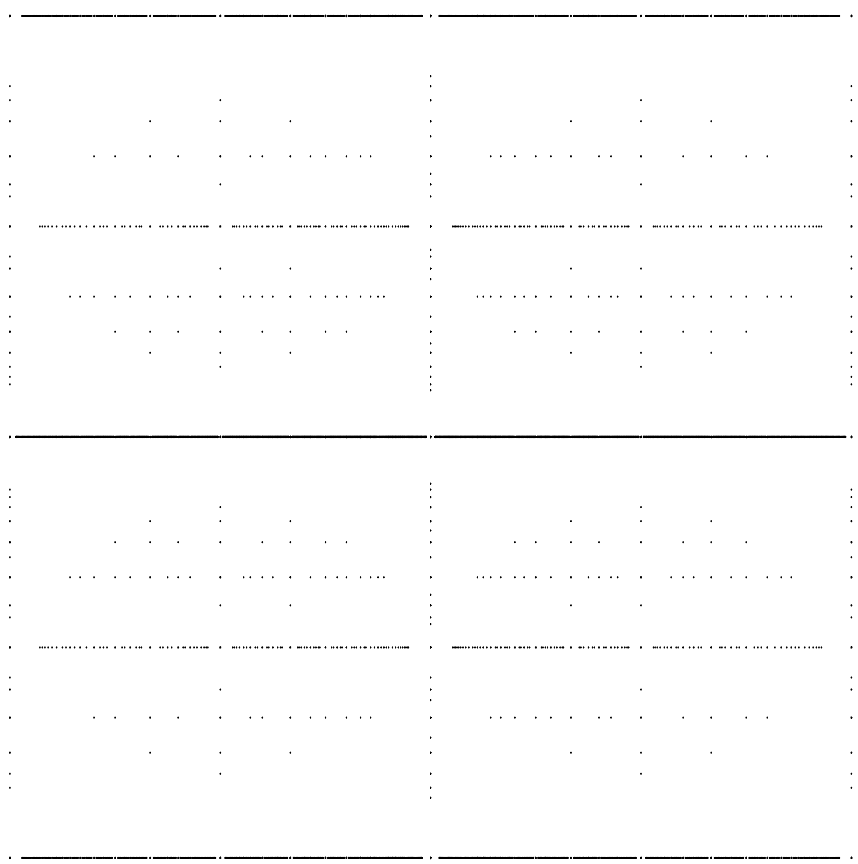
$\mathbf{P}^1(\mathbf{Q}) \times \mathbf{P}^1(\mathbf{Q})$



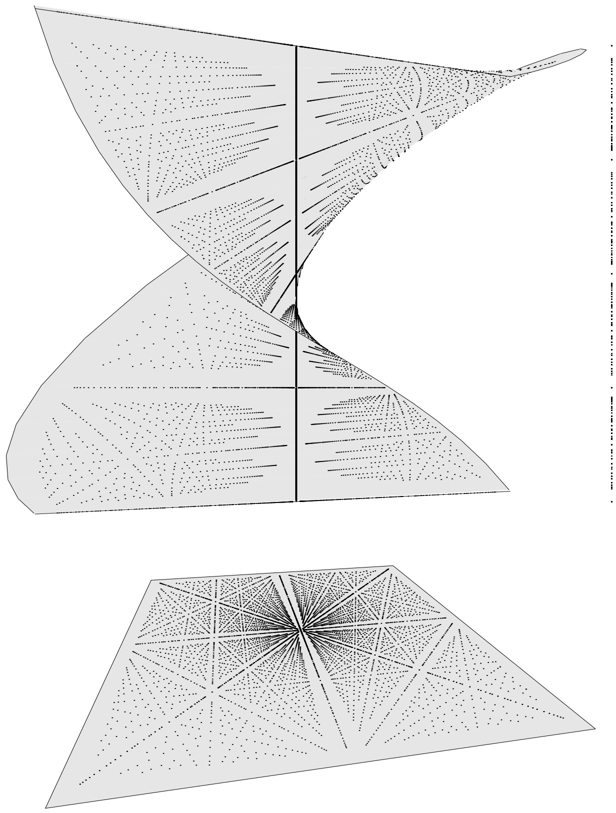
$\mathbf{P}^1(\mathbf{Q}) \times \mathbf{P}^1(\mathbf{Q})$



$\mathbf{P}^1(\mathbf{Q}) \times \mathbf{P}^1(\mathbf{Q})$



Plane blown in a point



北京大学

Since $\frac{m+1}{a} = \frac{n+1}{b}$, We get

$$\#\left(\mathbb{P}^m(\mathbb{Q}) \times \mathbb{P}^n(\mathbb{Q})\right)_{H_{a,b} \leq B}$$

$$= C(\mathbb{P}^m(\mathbb{Q}))\, C(\mathbb{P}^n(\mathbb{Q}))\, B^{\frac{n+1}{b}} \underbrace{\frac{a}{b}(n+1)\int_1^{B^{1/a}} \frac{1}{t}\, dt}_{\log\left(B^{\frac{n+1}{b}}\right)} + \overbrace{E(B)}^{\text{error term}}$$

For the error term

$$E(B) < \text{Cste } B^{\frac{n+1}{b}} \qquad \square$$

Let us turn to our last example today

18/4/2016 3) <u>The plane blown up in a point</u>

a) <u>The result</u>

$V \subset \mathbb{P}^2 \times \mathbb{P}^1$ equation $yu = xv$
$[x:y:z]\ [u:v]$ $\qquad P_0 = [0:0:1] \in \mathbb{P}^2(\mathbb{Q})$

$\pi = pr_1 : V \longrightarrow \mathbb{P}^2$

$$\pi^{-1}(P) = \begin{cases} \{([x:y:z],[y:x])\} & \text{if } P \neq P_0 \\ \{([0:0:1],[u:v]),\ [u,v] \in \mathbb{P}^1(\mathbb{Q})\} & \text{if } P = P_0 \end{cases}$$

<u>Drawing</u>

$\pi \downarrow$

$E = \pi^{-1}(P_0) \subset V(\mathbb{Q})$
$U = V(\mathbb{Q}) - \pi^{-1}(P_0)$
$A - B = \{x \in A \,/\, x \notin B\}$.

Again there is a two parameters family of heights

$$H_{a,b}((P,Q)) = H(P)^a H(Q)^b$$

$$\|(x,y,z)\|_\infty = \sqrt{x^2+y^2+z^2} \qquad \|(u,v)\|_\infty = \sqrt{u^2+v^2}$$

served as benchmark of the theory

<u>Theorem</u> (SERRE, MANIN, BATYREV & TSCHINKEL)

- Assume $b > 0$

$$\# E_{H \leq B} = C(\mathbb{P}^1) B^{\frac{2}{b}}$$

Assume $a+b>0$ and $a>0$

$$\# U_{H_{a,b} \leq B} \sim \begin{cases} \left(\sum_{Q \in \mathbb{P}^1(\mathbb{Q})} C(pr_2^{-1}(Q))\right) B^{\frac{2}{a}} & \text{if } \frac{3}{a+b} < \frac{2}{a} \\ \frac{1}{6}\pi^2 \prod_{p \text{ prime}} \left(1-\frac{1}{p}\right)^2\left(1+\frac{2}{p}+\frac{1}{p^2}\right) B^{\frac{2}{a}} \log\left(B^{\frac{2}{a}}\right) & \text{if } \frac{3}{a+b} = \frac{2}{a} \\ C\left(\frac{a}{a+b}\right) B^{\frac{3}{a+b}} & \text{if } \frac{3}{a+b} > \frac{2}{a} \end{cases}$$

Remarks

- $\# U_{H_{a,b} \leq B} = o\left(\# E_{H_{a,b} \leq B}\right)$ if $b<a$
- $\lim_{B \to +\infty} \dfrac{\# pr_2^{-1}(Q)_{H_{a,b} \leq B}}{\# U(\mathbb{Q})_{H_{a,b} \leq B}} > 0$ if and only if $\frac{3}{a+b} < \frac{2}{a}$

So we have various behaviours about the contribution of strict subvarieties that we have to explain.

b) Beginning of the proof, main term

- Let us start with E

$$H_{a,b}([0:0:1], Q) = H(Q)^b$$

Thus we can deduce this part of the result from the case of $\mathbb{P}^n$

- From now on we restrict ourselves to U
  ie $(x,y) \neq (0,0)$
  consider $(x,y,z,u,v) \in \mathbb{Z}^5$
  $\gcd(x,y,z)=1$, $\gcd(u,v)=1$, $uy=vx$
  We put $d = \gcd(x,y)$ then

$$u = \varepsilon \frac{y}{d}, \quad v = \varepsilon \frac{x}{d} \quad \text{with } \varepsilon \in \{-1,1\}$$

We can parametrize the points of V by

$$\{(u,v,d,z)\in\mathbb{Z}^4 \mid \gcd(u,v)=\gcd(d,z)=1\} \xrightarrow{\rho} V(\mathbb{Q})$$
$$(u,v,d,z) \longmapsto ([dv:du:z],[u:v])$$

Given a point P in U

$$\#\rho^{-1}(P) = 2\times 2$$

sign of (u,v) ↗ ↖ sign of (d,z).

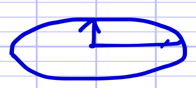
$$\#U_{H_{a,b}\le B} = \frac{1}{4}\#\left\{(u,v,d,z)\in\mathbb{Z}^4 \;\middle|\; \begin{array}{l}\gcd(u,v)=\gcd(d,z)=1\\ d\neq 0\\ \sqrt{u^2+v^2}^{\,b}\sqrt{x^2+d^2(u^2+v^2)}^{\,a}\le B\end{array}\right\}$$

$$= \sum_{\substack{(u,v)\in\mathbb{Z}^2\\ \gcd(u,v)=1\\ H(u,v)^{a+b}\le B}} \frac{1}{4}\,\underbrace{\#\left\{(d,z)\in\mathbb{Z}^2 \;\middle|\; \begin{array}{l}\gcd(d,z)=1,\ d\neq 0\\ \sqrt{x^2+h^2d^2}^{\,a}\le \frac{B}{h^b}\end{array}\right\}}_{N_{(u,v)}(B)}$$

where $h = H(u,v)$

To estimate this we may again apply the case of $\mathbb{P}^1$ we get

$$N_{(u,v)}(B) = \frac{1}{\zeta(2)}\mathrm{Vol}\left((d,z)\in\mathbb{R}^2 \;\middle|\; \sqrt{x^2+h^2d^2}^{\,a}\le\frac{B}{h^b}\right) + E_{u,v}(B)$$



$\updownarrow$ $\dfrac{B^{1/a}}{h^{\frac{a+b}{a}}}$

$\leftrightarrow$ $\dfrac{B^{1/a}}{h^{b/a}}$

we get $\pi\dfrac{B^{2/a}}{h^{\frac{a+2b}{a}}}$ for the main term.

Let us consider only the main term

We have found

$$MT(B) = \frac{1}{2}\sum_{\substack{Q\in\mathbb{P}^1(\mathbb{Q})\\ H\le B^{\frac{1}{a+b}}}} \frac{\pi}{\zeta(2)}\,\frac{B^{2/a}}{H(Q)^{\frac{a+2b}{a}}}$$

Let us put

$$f(t) = \frac{1}{t^{\frac{a+2b}{a}}} \quad\text{and}\quad g(t) = \#\mathbb{P}^1(\mathbb{Q})_{H\le t}$$

So we can write

$$MT(B) = \frac{\pi}{2\zeta(2)} B^{2/a} \overbrace{\int_1^{B^{\frac{1}{a+b}}} f(t)\, dg(t)}^{I(B)}$$

Using Abel inversion formula again, we get

$$I(B) = \underbrace{\left[f(t) g(t) \right]_1^{B^{\frac{1}{a+b}}}}_{I_1(B)} + \underbrace{\int_1^{B^{\frac{1}{a+b}}} f'(t) g(t)\, dt}_{I_2(B)}$$

Remember that

$$g(t) = \frac{\pi}{2\zeta(2)} t^2 + O(t \log(t))$$

So

$$I_1(B) = O\left(B^{\frac{2}{a+b}} B^{-\frac{a+2b}{a} \times \frac{1}{a+b}} \right)$$

$$= O\left(B^{-\frac{1}{a+b}} \right) \xrightarrow[B \to +\infty]{} 0$$

Now for $I_2(B)$

$$I_2(B) = \frac{\pi^2}{\zeta(2)^2} B^{2/a} \frac{a+2b}{a} \underbrace{\int_1^{B^{\frac{1}{a+b}}} \frac{1}{t^{\frac{2a+2b}{a}}} t^2\, dt}_{} + E'(B)$$

converges as $B \to +\infty$ iff $\frac{2a+2b}{a} - 2 > 1$

ie $\frac{2}{a} > \frac{3}{a+b}$

So if $\frac{2}{a} > \frac{3}{a+b}$ (that is $2b > a > 0$) the sum converges and we get

$$MT(B) = \frac{\pi}{2\zeta(2)} \left(\sum_{Q \in \mathbb{P}^1(\mathbb{Q})} \frac{1}{H(Q)^{\frac{a+2b}{a}}} \right) B^{\frac{2}{a}}$$

which corresponds to the 1^{st} case in the theorem.

Assuming $\sum E_{u,v}(B)$ is negligible we get formula for $\frac{2}{a} > \frac{3}{a+b}$

If $\frac{2}{a} = \frac{3}{a+b}$ (that is $a=2b$) we get

$$I_2(B) \sim \frac{\pi^2}{\zeta(2)^2} B^{2/a} \frac{a+2b}{a} \underbrace{\int_1^{B^{\frac{1}{a+b}}} \frac{1}{t}\, dt}_{\frac{2}{3}\log\left(B^{\frac{2}{a}}\right)}$$

which is the expected main term.

If $\frac{2}{a} < \frac{3}{a+b}$ get $\mathrm{Cst}\, B^{2/a} B^{-\frac{-a+2b}{(a+b)a}} = \mathrm{cste}\ B^{\frac{3}{a+b}}$.

Let me speak precisely about the error term because it shows one of the main problem you get into in these counting situations.

c) Error term, points of a lattice in bounded domain

The point is that when we compare the number of points of a lattice in a bounded open Domain of $\mathbb{R}^n$, the argument I gave last time can be easily be generalized as follow

Definition

Λ lattice of $\mathbb{R}^n$, that is Λ is generated by a basis of $\mathbb{R}^n$:

- $\Lambda = \sum_{i=1}^{n} \mathbb{Z} f_i$ where $(f_1, \dots, f_n)$ is a basis of $\mathbb{R}^n$

A fundamental domain for Λ is a set of the form

$$F = \left\{ \sum_{i=1}^{n} t_i f_i,\ 0 \leq t_i < 1 \text{ for } i \in \{1, \dots, n\} \right\}$$

where $\{f_1, \dots, f_n\}$ is a set of generators of Λ

- We can define

$$\mathrm{covol}(\Lambda) = \mathrm{Vol}(\mathbb{R}^n/\Lambda) = \mathrm{Vol}(\underset{\text{any fundamental domain}}{F}) = \left|\det_{(e_1,\dots,e_n)}(f_1, \dots, f_n)\right|$$

[for the euclidean norm

where $(e_1, \dots, e_n)$ is the usual basis of $\mathbb{R}^n$

Then the proof I explained last times give us the following Choose a fundamental domain for Λ

Lemma

Let $\mathcal{D}$ be any bounded subset of $\mathbb{R}^n$

closure for real topology

$$\left| \#(\Lambda \cap \mathcal{B}) - \frac{Vol(\overline{\mathcal{D}})}{covol(\Lambda)} \right| \leq \#\{\lambda \in \Lambda / (\lambda + \mathcal{F}) \cap \partial \mathcal{D} \neq \emptyset\}$$

where $\partial \mathcal{D} = \overline{\mathcal{D}} - \mathring{\mathcal{D}}$ boundary of $\mathcal{D}$

It remains to give an upper bound of this term

In general, it could be big; but we are in a particular case, Indeed we want to apply it to a domain of the form $\mathcal{D}_B = B\,\mathcal{D}_1$. I do not want to assume that the set $\mathcal{D}_1$ is convex. Instead I assume that

Assumption

There exists N functions

$$\psi_i : W_i \longrightarrow \mathbb{R}^n \quad \text{avec } W_i \subset [0,1]^{n-1}$$

which are K-Lipschitz:

$$\forall x, y \in [0,1]^{n-1} \quad \|\psi_i(x) - \psi_i(y)\| \leq K \|x-y\|$$

so that $\partial \mathcal{D}_1 \subset \bigcup_{i=1}^{N} \psi_i([0,1]^{n-1})$

Now we need to introduce an important invariant for Λ. Let me describe it:

Definition

The i-th minimum of Λ is defined by

$$\lambda_i(\Lambda) = \min\{\lambda \in \mathbb{R}_{>0} \mid \lambda B(0,1) \cap \Lambda \text{ contains } i \text{ linearly independent vectors}\}$$

euclidean ball

In particular $\lambda_1(\Lambda)$ is the length of the smallest non zero vector in Λ.

Minkowski's 2^{nd} theorem

$$\frac{2^n}{n!}\operatorname{covol}(\Lambda) \leq \prod_{i=1}^{n} \lambda_i(\Lambda) \leq \frac{2^n}{\operatorname{Vol}(B(0,1))}\operatorname{covol}(\Lambda)$$

Moreover one can prove that

Fact

We can find a basis $(f_1, \ldots, f_n)$ generating Λ such that $\|f_i\| < n\,\lambda_i(\Lambda)$.

Reference

J.W.S Cassels, An introduction to the Geometry of numbers.

Using this, I am now going to prove the

Proposition (MASSER–VAALER)

$$\left| \#(\Lambda \cap B\mathcal{D}_1) - B^n \frac{\operatorname{Vol}(\mathcal{D}_1)}{\operatorname{covol}(\Lambda)} \right| \leq C_n N \left(\frac{K}{\lambda_1(\Lambda)} B + 1 \right)^{n-1}$$

Proof

Up to now we had taken any fundamental domain which meant that it could a terrible error term

We now take a basis corresponding to the last fact

Let M be the matrice of the coordinate of $f_1, \ldots, f_n$ in the standard basis $(e_1, \ldots, e_n)$

then

$$M^{-1} = \frac{1}{\det(M)} \begin{pmatrix} L_1 \\ \vdots \\ L_n \end{pmatrix}$$

where L_i is given by the determinant of $(n-1)\times(n-1)$ submatrices of M without the coefficients of f_i

Notation

$A \ll_n B$ means $\exists C_n \in \mathbb{R}_{>0}$ $A \leq C_n B$

$$\|L_i\| \leq \sqrt{(n-1)!} \prod_{j\neq i} \|y_j\| \ll_n \prod_{j \neq i} \lambda_j(\Lambda)$$

So $\|L_i\| \ll_n \dfrac{\mathrm{covol}(\Lambda)}{\lambda_i(\Lambda)} \ll_n \dfrac{|\det(M)|}{\lambda_1(\Lambda)}$

Now consider the norm on $\mathbb{R}^n$ defined by

$$\Big\|\sum_{i=1}^n t_i f_i\Big\|' = \max_{1\leq i\leq n} |t_i|$$

Then for $x = \sum_{i=1}^n x_i e_i$ $\quad \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} = \begin{pmatrix} L_1 \\ \vdots \\ L_n \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

ie $t_i = L_i \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

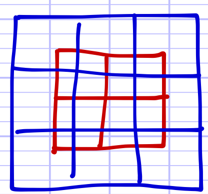
So $\|x\| \leq Cste_n \dfrac{1}{\lambda_1(\Lambda)} \|x\|$ can take the norm of the max

So $\forall x, y \in W_i$ $\quad \|\psi_i(x) - \psi_i(y)\|' \leq C_n \dfrac{K}{\lambda_1(\Lambda)} \|x-y\|$

But for any $x \in \mathbb{R}^n$

$\overline{B}'(x, 1) = \{ y \in \mathbb{R}^n \mid \|y-x\|' \leq 1 \}$ cube is contained in 3^n cells of Λ.

(where a cell is $\lambda + F$ for some $\lambda \in \Lambda$)



Now we break $[0,1]^{n-1}$ into small cubes

$$[0,1]^{n-1} \subset \bigcup_{i=1}^{\left(\frac{BK}{\lambda_1(\Lambda)}C_n+1\right)^{n-1}} x_i + \left[0, \frac{\lambda_1(\Lambda)}{BKC_n}\right]^{n-1}$$

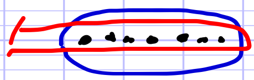
$\psi_i\left(\left(x_i + \left[0, \frac{\lambda_1(\Lambda)}{BKC_n}\right]^{n-1}\right) \cap W_i\right)$ meets at most 3^n cells of Λ

So the error term is bounded by

$$C'_n \left(\frac{K}{\lambda_1(\Lambda)} B + 1\right)^{n-2}$$

as wanted $\square$

Let us go back to our very particular case to see what kind of error term it gives:



The product MK corresponds to the length of the ellipse

In fact in this case you may get that point using

$$\#\{x \in \Lambda \mid (x + [0,1]^2) \cap \partial \mathcal{D}_B \neq \emptyset\}$$
$$\leq \operatorname{Vol}\left(\{y \in \mathbb{R}^2 \mid d(y, \partial \mathcal{D}_B) \leq \sqrt{2}\}\right)$$
$$\leq 2\sqrt{2}\, B \operatorname{length}(\partial B_1) + \pi \sqrt{2}^2$$

But if the ellipse is very flat this is bad

More precisely

$$\operatorname{Vol}(\mathcal{D}_B) = \pi \frac{B^{\frac{2}{a}}}{h^{\frac{2a+b}{a}}}$$

$$\operatorname{length}(\partial \mathcal{D}_B) \Big/ \frac{B^{\frac{1}{a}}}{h^{b/a}} \text{ is bounded}$$

We get an error term bigger than the main term if $h^{\frac{a+b}{a}} > B^{\frac{1}{a}}$ that is $h > B^{\frac{1}{a+b}}$

which can perfectly happen. But that is precisely the place where we are going to use that we are counting on the open subset U. We are counting

$$\left\{(d, z) \in \mathbb{Z}^2 \;\middle|\; \gcd(d, z) = 1 \quad d \neq 0 \quad \sqrt{z^2 + h^2 d^2} \leq \frac{B^{1/a}}{h^{b/a}}\right\}$$

which is 0 if

$$h > B^{1/a} / h^{b/a} \quad \text{ie } h > B^{1/a+b}$$

So it is by restricting to U that we are counting where the error term is less than the main term.

These points on the picture are removed by the conditions

$d \neq 0$ and $\gcd(d, 2) = 1$

In fact from the point of view of the fibration $pr_2 : V(\mathbb{Q}) \longrightarrow \mathbb{P}^1(\mathbb{Q})$ the fibres of which are isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$ the accumulating subset gives that most fibers contain only one point

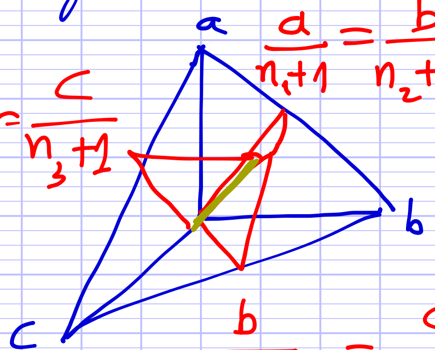
The end of the proof use Abel's summation formula once more and I leave it to you $\square$

Remark (left as an exercise)

For $V = \mathbb{P}^{n_1} \times \mathbb{P}^{n_2} \times \mathbb{P}^{n_3}$
the heights are parametrized
by 3 numbers (a, b, c) we may see in $\mathbb{R}^3_{>0}$

$\frac{a}{n_1+1} = \frac{b}{n_2+1}$

$\frac{a}{n_1+1} = \frac{c}{n_3+1}$



$$H_{a,b,c}(P, Q, R) = H(P)^a H(Q)^b H(R)^c$$

We write $\mathbb{R}^3_{\geq 0} = C_1 \cup C_2 \cup C_3$

$\frac{b}{n_2+1} = \frac{c}{n_3+1}$

line $\frac{a}{n_1+1} = \frac{b}{n_2+1} = \frac{c}{n_3+1}$

On the interiors of the sub-cones $\overset{\circ}{C}_1, \overset{\circ}{C}_2, \overset{\circ}{C}_3$
the asymptotic behaviour is given by
$C B^a$

on $C_i \cap C_j - C_1 \cap C_2 \cap C_3$ $\quad C B^a \log(B)$ red planes

on $C_1 \cap C_2 \cap C_3$ $\quad C B^a \log(B)^2$ yellow line.

20/4/2016 4) Remark about the constant

Now that we have three examples, let us look at the constants we got

a) $\mathbb{P}^n(\mathbb{Q})$

$$C(\mathbb{P}^n) = \frac{1}{2}\operatorname{Vol}(B(0,1)) \times \frac{1}{\zeta(n+1)}$$

$$= \frac{1}{2}\operatorname{Vol}(B(0,1)) \times \prod_{p \text{ prime}} \left(1 - \frac{1}{p^{n+1}}\right)$$

$$= \frac{1}{2}\operatorname{Vol}(B(0,1)) \times \prod_{p \text{ prime}} \left(1-\frac{1}{p}\right) \underbrace{\left(1+\frac{1}{p}+\dots+\frac{1}{p^n}\right)}_{= \frac{\# \mathbb{P}^n(\mathbb{F}_p)}{\# \mathbb{F}_p^n}}$$

where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for p prime

b) $\mathbb{P}^m(\mathbb{Q}) \times \mathbb{P}^n(\mathbb{Q})$

In the case $\frac{a}{m+1} = \frac{b}{n+1}$

$$= \frac{1}{4}\operatorname{Vol}(B^{m+1}(0,1))\operatorname{Vol}(B^{n+1}(0,1))$$

$$\times \prod_{p \text{ prime}} \left(1-\frac{1}{p}\right)^2 \frac{\# \mathbb{P}^m(\mathbb{F}_p) \times \# \mathbb{P}^n(\mathbb{F}_p)}{\# \mathbb{F}_p^{m+n}}$$

c) for the plane blown up

In the case $\frac{3}{a+b} = \frac{2}{a}$

$$C(V) = \frac{1}{6}\pi^2 \prod_{p \text{ prime}} \left(1-\frac{1}{p^2}\right)^2$$

$$\left(1-\frac{1}{p}\right)^{2} {}'' \left(1+\frac{2}{p}+\frac{1}{p^2}\right)$$

What is the number of points of V on $\mathbb{F}_p$?

$$\# V(\mathbb{P}) = \# \mathbb{P}^2(\mathbb{F}_p) - 1 + \# \mathbb{P}^1(\mathbb{F}_p)$$
$$= 1 + 2p + p^2.$$

It turns out that this phenomena is very general

d) For Birch theorem (circle method)

Remember that in that case we are considering

$$V(\mathbb{Q}) = \{[x_0 : \dots : x_n] \in \mathbb{P}^n(\mathbb{Q}) \mid F(x_0, \dots, x_n) = 0\}$$

$$C(V) = \underbrace{\sigma_\infty}_{\text{some volume integral}} \times \prod_{p \text{ prime}} \sigma_p$$

$$\sigma_p = \left(1 - \frac{1}{p}\right) \times \frac{\overbrace{\# \{[x_0 : \dots : x_n] \in \mathbb{P}^n(\mathbb{F}_p) \mid F(x_0, \dots, x_n) = 0\}}^{\text{in } \mathbb{F}_p}}{\# \mathbb{F}_p^n}$$

for almost all p all primes outside a finite set.

But it is the right place to remind you that

Reminder

For any $N > 0$ there is a reduction modulo N map

$$\text{red}_N : V(\mathbb{Q}) \to V(\mathbb{Z}/N\mathbb{Z})$$

So it is quite natural to ask: What happens if we only count points for which the reduction modulo p is a given point in $V(\mathbb{F}_p)$? This leads to

5) First point of view on equidistribution

I am going to do it for the projective space

a) reduction modulo M

Write $[P]_M$ for $\text{red}_M(P)$

Fix $P_0 \in \mathbb{P}^n(\mathbb{Z}/M\mathbb{Z})$ $M > 1$.

Proposition

$$\frac{\#\{P\in\mathbb{P}^n(\mathbb{Q}) \mid H(P)\le B \text{ and } [P]_M = P_0\}}{\#(\mathbb{P}^n(\mathbb{Q})_{H\le B})} \xrightarrow[B\to+\infty]{} \frac{1}{\#\mathbb{P}^n(\mathbb{Z}/M\mathbb{Z})}$$

One can say that the points of the projective space are evenly distributed with respect to their reduction modulo M. This side does not depend on the choice of P_0

Proof

Write $P_0 = [x_0 : \dots : x_n]$ with $(x_0, \dots, x_n)$ primitive

Let $\tilde{x}_0, \dots, \tilde{x}_n$ be representants of $x_0, \dots, x_n$ in $\mathbb{Z}$; then since $(x_0, \dots, x_n)$ is primitive we can choose

$$u_1, \dots, u_n \in \mathbb{Z}^n, \quad M \mid \sum_{i=0}^{n} u_i x_i - 1$$

we get $v\in\mathbb{Z}$ such that

$$\sum_{i=0}^{n} u_i x_i + vM = 1$$

Let $d = \gcd(x_i)$ $\quad \gcd(d, M) = 1$

So $d \in (\mathbb{Z}/M\mathbb{Z})^*$ and

$$[x_0 : \dots : x_n] = [d^{-1}x_0 : \dots d^{-1}x_n]$$

So by dividing $\tilde{x}_0, \dots, \tilde{x}_n$ by d

we may assume $f_0 = (\tilde{x}_0, \dots, \tilde{x}_n)$ is primitive

We complete it in a basis $(f_1, \dots, f_n)$ of $\mathbb{Z}^n$ and take $(f_0^\vee, \dots, f_n^\vee)$ be the dual basis

($f_i^\vee(x)$ is the i-th coordinate of x in the basis $(f_0, \dots, f_n)$)

It is formed of linear forms with integral coefficients

$$\mathrm{red}_M([y_0 : \dots y_n]) = \mathrm{red}_M([\tilde{x}_0 : \dots : \tilde{x}_n])$$

$$\Leftrightarrow \mathbb{Z}/M\mathbb{Z}(y_0, \dots, y_m) = \mathbb{Z}/M\mathbb{Z}(x_0, \dots, x_n) \subset (\mathbb{Z}/M\mathbb{Z})^{n+1}$$

$$\Leftrightarrow (\overline{y}_0, \dots, \overline{y}_m) \in \mathbb{Z}/M\mathbb{Z}(x_0, \dots, x_n)$$

$(y_0, \dots, y_n)$ primitif

reduction modulo M

$\Leftrightarrow M \mid f_i^\vee(y)$ for $i \geq 1$

Let $\Lambda = \{ y \in \mathbb{Z}^{n+1} \mid M \mid f_i^\vee(y) \text{ for } i \geq 1 \}$

Then Λ is a sublattice of $\mathbb{Z}^{n+1}$

and $[\Lambda : \mathbb{Z}^{n+1}] = M^n$

(Indeed $(f_1, \dots, f_n)$ induces an isomorphism from $\mathbb{Z}^{n+1}/\Lambda$ to $(\mathbb{Z}/M\mathbb{Z})^n$)

Now

$$N_{P_0}(B) = \#\{ P \in \mathbb{P}^n(\mathbb{Q}) \mid H(P) \leq B \ \& \ [P]_M = P_0 \}$$

$$= \frac{1}{2} \#\left\{ (x_0, \dots, x_n) \in \Lambda \;\middle|\; \begin{array}{l} \gcd(x_0, \dots, x_n) = 1 \\ \|(x_0, \dots, x_n)\| \leq B \end{array} \right\}$$

$\mathbb{Z}$ We count elements in Λ but the gcd condition is in $\mathbb{Z}^{n+1}$

$$N_{P_0}(B) = \frac{1}{2} \sum_{d \geq 1} \mu(d) \underbrace{\#\{ x \in \Lambda \cap (d\mathbb{Z})^{n+1} \mid \|x\| \leq B \}}_{\displaystyle \| \atop \displaystyle \frac{\mathrm{Vol}(\mathbb{B}(0,1))}{\mathrm{covol}(\Lambda \cap (d\mathbb{Z})^{n+1})} B^{n+1} + O\left(\frac{1}{d^n} B^n\right)}$$

the error term depends on the lattice, I have to explain that

$\mu(d) \neq 0 \Rightarrow d = p_1 \cdots p_r$; $p_1, \dots, p_r$ distinct prime

Using the basis $(f_0, \dots, f_n)$ $\qquad \prod_{p \mid d, p \nmid M} p \times M$

$$\Lambda = \mathbb{Z} f_0 \oplus \bigoplus_{i=1}^n M\mathbb{Z} f_i .$$

$$\Lambda \cap (d\mathbb{Z})^{n+1} = d\mathbb{Z} f_0 \oplus \bigoplus_{i=1}^n \mathrm{lcm}(d, M) \mathbb{Z} f_i$$

Since $(Md\mathbb{Z})^{n+1} \subset \Lambda \cap (d\mathbb{Z})^{n+1} \subset (d\mathbb{Z})^{n+1}$

By dividing each coordinate by d

$$\#\{ x \in (d\mathbb{Z})^{n+1} \cap \Lambda \mid \|x\| \leq B \}$$

$$= \#\left\{ x \in \left(\frac{1}{d}\Lambda\right) \cap \mathbb{Z}^{n+1} \;\middle|\; \|x\| \leq \frac{B}{d} \right\}$$

But $\left(\frac{1}{d}\Lambda\right) \cap \mathbb{Z}^{n+1} = \mathbb{Z} f_0 \oplus \bigoplus_{i=1}^n \frac{M}{\gcd(d, M)} \mathbb{Z} f_i = \Lambda_{\gcd(d,M)}$

$\Lambda_{\gcd(d,M)} = \left(\frac{1}{d}\Lambda\right) \cap \mathbb{Z}^{n+1}$ is a lattice

in a finite set of lattices indexed by the divisors of M.

Using the same methods as for $\mathbb{P}^n(\mathbb{Q})$ we get the estimate

$$N_{P_0}(B) \sim \frac{1}{2}\operatorname{Vol}(\mathbb{B}(0,1))\underbrace{\left(\sum_{d\geq 1}\mu(d)\frac{1}{\operatorname{Covol}(\Lambda\cap(d\mathbb{Z})^{n+1})}\right)}B^{n+1}$$

It remains to compute the value of this sum

$$\sum_{d\geq 1}\frac{\mu(d)}{d^{n+1}\left(\frac{M}{\gcd(M,d)}\right)^n} = \frac{1}{M^n}\sum_{d\geq 1}\underbrace{\frac{\mu(d)\gcd(M,d)^n}{d^{n+1}}}_{\varphi(d)}$$

φ is multiplicative:

$$\varphi(ab)=\varphi(a)\varphi(b) \text{ if } \gcd(a,b)=1$$

we get

$$\frac{1}{M^n}\prod_{\substack{p \text{ premier}\\ p\nmid M}}\left(1-\frac{1}{p^{n+1}}\right)\times\prod_{\substack{p \text{ premier}\\ p\mid M}}\left(1-\frac{1}{p}\right)$$

Then we have to devide by the product $\prod_{p \text{ prime}}\left(1-\frac{1}{p^{n+1}}\right)$

We get

$$\frac{1}{M^n\prod_{p \text{ prime}}\left(1+\frac{1}{p}+\cdots+\frac{1}{p^n}\right)}$$

Claim

$$\#\mathbb{P}^n(\mathbb{Z}/M\mathbb{Z}) = \left(\frac{M}{\prod_{p\mid M}p}\right)^n\times\prod_{p\mid M}\#\mathbb{P}^n(\mathbb{F}_p)$$

Indeed both sides of this equality are multiplicative so it is enough to prove it when M is the power of a prime number $M=p^k$

But in that case,

$$\# \mathbb{P}(\mathbb{Z}/p^k\mathbb{Z}) = \frac{1}{\#(\mathbb{Z}/p^k\mathbb{Z})^*} \times \#\{y \text{ primitive in } (\mathbb{Z}/p^k\mathbb{Z})^{n+1}\}$$

But y primitive $\iff$ y is not 0 modulo p

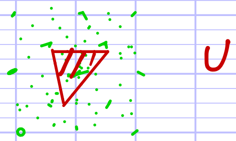
We get

$$\# \mathbb{P}(\mathbb{Z}/p^k\mathbb{Z}) = \frac{1}{p^{k-1}(p-1)} \times p^{(k-1)n+1} \times (p^{n+1}-1)$$
$$= p^{(k-1)n} \times \# \mathbb{P}^n(\mathbb{F}_p). \quad \square$$

b) Distribution for real topology

For real topology a natural question is to consider a "simple" open set U in $\mathbb{P}^n(\mathbb{R})$

Picture



The question what is the proportion of points in U?

Question

Let U be a "suitable" open set in $\mathbb{P}^n(\mathbb{R})$

Does the quotient

$$\frac{\#(\mathbb{P}^n(\mathbb{Q}) \cap U)_{H \leq B}}{\#\mathbb{P}^n(\mathbb{Q})_{H \leq B}}$$

converges to something meaningful

Now I have to explain what I mean by suitable.

Definition

A strictly convex polyhedral cone in $\mathbb{R}^{n+1}$ is a subset $\sigma \subset \mathbb{R}^{n+1}$ such that

(i) $\exists\, v_1, \dots, v_k \in \mathbb{R}^{n+1}$

$$\sigma = \left\{ \sum_{i=1}^{k} t_i v_i,\ (t_1, \dots, t_k) \in \mathbb{R}^k_{\geq 0} \right\}$$

(I denote it by $\sum_{i=1}^{k} \mathbb{R}_{\geq 0} v_i$)

(ii) $\sigma \cap -\sigma = \{0\}$.

I shall say that an open subset U of $\mathbb{P}^n(\mathbb{R})$ is elementary if it is of the form $\pi(\mathring{\sigma})$ for a strictly convex polyhedral cone of $\mathbb{R}^{n+1}$.

<u>Reminder</u>

The topology on $\mathbb{P}^n(\mathbb{R})$ is the quotient topology of $\mathbb{R}^{n+1} - \{0\} / \mathbb{R}^*$

A set $U \subset \mathbb{P}^n(\mathbb{R})$ is open if and only if $\pi^{-1}(U)$ is open in $\mathbb{R}^{n+1} - \{0\}$

<u>Proposition</u>

Let U be an elementary open subset of $\mathbb{P}^n(\mathbb{R})$ then

$$\frac{\#(U \cap \mathbb{P}^n(\mathbb{Q}))_{H \leq B}}{\# \mathbb{P}^n(\mathbb{Q})_{H \leq B}} \longrightarrow \frac{Vol(\pi^{-1}(U) \cap \mathbb{B}(0,1))}{Vol(\mathbb{B}(0,1))}$$

<u>Proof</u>

Let $\mathcal{D}_B = B\left(\mathbb{B}(0,1) \cap \pi^{-1}(U)\right)$

then we can apply MASSER & VAALER to get that for $B \geq 1$

$$\left|\#(\mathcal{D}_B \cap \mathbb{Z}^{n+1}) - B^{n+1} Vol(\mathbb{B}(0,1) \cap \pi^{-1}(U))\right| \leq C B^n$$

But

$$\#(\mathbb{P}^n(\mathbb{Q}) \cap U)_{H \leq B} = \frac{1}{2} \sum_{d \geq 1} \mu(d) \, \#\left(\mathbb{B}(0,\tfrac{B}{d}) \cap \pi^{-1}(U) \cap \mathbb{Z}^{n+1}\right)$$

We conclude as for $\mathbb{P}^n(\mathbb{Q})$. $\square$

What about an open set which is not elementary

<u>Remark</u>

1) Let $F = \pi(\sigma)$ σ as above, F is closed in $\mathbb{P}^n(\mathbb{R})$

The same proof shows that

$$\frac{\#(F\cap \mathbb{P}^n(\mathbb{Q}))_{H\leq B}}{\#(\mathbb{P}^n(\mathbb{Q}))_{H\leq B}} \xrightarrow[B\to\infty]{} \frac{\mathrm{Vol}(\mathbb{B}(0,1)\cap \pi^{-1}(F))}{\mathrm{Vol}(\mathbb{B}(0,1))}$$

and the contribution of ∂F is negligible.

2) Consider the set $\mathcal{M}$ of measurable subsets W of $\mathbb{P}^n(\mathbb{R})$ such that

$$\frac{\#(W\cap \mathbb{P}^n(\mathbb{Q}))_{H\leq B}}{\#\,\mathbb{P}^n(\mathbb{Q})_{H\leq B}} \xrightarrow[B\to+\infty]{} \omega(W) = \frac{\mathrm{Vol}(\mathbb{B}(0,1)\cap\pi^{-1}(W))}{\mathrm{Vol}(\mathbb{B}(0,1))}$$

definition

What can we say about it?

(i) elementary open sets belong to $\mathcal{M}$

(ii) $\mathcal{M}$ contains $\pi(\sigma)$ for σ strictly convex polyhedral cone

(iii) $\mathcal{M}$ is stable by complement

$$W \longmapsto \mathbb{P}^n(\mathbb{R}) - W$$

(iv) It is stable by disjoint union

(v) Since the intersection of two elementary open subsets is an elementary subset and

$$\#(A\cup B) = \#A + \#B - \#(A\cap B)$$

$\mathcal{M}$ contains the union of a finite number of elementary open subsets

(vi) (Squeeze property)

If we have sequences $(U_n)_{n\in\mathbb{N}}$ and $(V_n)_{n\in\mathbb{N}}$ of elements of $\mathcal{M}$ such that

- $(U_n)_{n\in\mathbb{N}}$ is increasing for inclusion: $\forall n\in\mathbb{N},\ U_n\subset U_{n+1}$
- $(V_n)_{n\in\mathbb{N}}$ is decreasing
- $U_n \subset V_n$ for any $n\in\mathbb{N}$ and
- $\omega(V_n) - \omega(U_n) \xrightarrow[n\to+\infty]{} 0$

then for any W such that

$$\bigcup_{n\in\mathbb{N}} U_n \subset W \subset \bigcap_{n\in\mathbb{N}} V_n$$

belongs to $\mathcal{U}$.

Proof

Take $\varepsilon > 0$

N such that $\quad \omega(V_N) - \omega(U_N) < \frac{\varepsilon}{2}$

and B_0 such that

for any $B \geq B_0$

$$\left| \frac{\#(\mathbb{P}(\mathbb{Q}) \cap V_N)_{H\leq B}}{\#(\mathbb{P}(\mathbb{Q}))_{H\leq B}} - \omega(V_N) \right| < \frac{\varepsilon}{4}$$

and similarly for U_N

From

$$\omega(U_N) \leq \overbrace{\omega(W) \leq \omega(V_N)}^{\leq \varepsilon/2}$$

and

$$\#(\mathbb{P}(\mathbb{Q}) \cap U_N)_{H\leq B} \underset{\leq \varepsilon/4}{\leq} \#(\mathbb{P}(\mathbb{Q}) \cap W)_{H\leq B} \leq \#(\mathbb{P}(\mathbb{Q}) \cap V_N)_{H\leq B} \quad \leq \varepsilon/4$$

(after dividing by $\#(\mathbb{P}(\mathbb{Q}))_{H\leq B}$)

we get

$$\left| \omega(W) - \#(\mathbb{P}(\mathbb{Q}) \cap W)_{H\leq B} \right| < \varepsilon$$

for $B \geq B_0$

Remark

On the other hand the elementary open sets form a basis of the real topology: for any open set U in $\mathbb{P}^n(\mathbb{R})$ and any $x \in U$ there exists an elementary open set W such that

$$x \in W \subset U$$

In fact we have an even more precise statement:

Any open set in $\mathbb{P}^n(\mathbb{R})$ is of the form $\bigcup_{i\in I} W_i$ where $(W_i)_{i\in I}$ is a countable family of elementary open sets

From this you might be led to believe that any open set U is in $\mathcal{M}$ it is FALSE!

2 Not all open sets are in $\mathcal{M}$.

Indeed $\mathbb{P}^n(\mathbb{Q})$ is a countable set

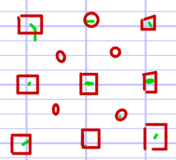
Choose a sequence $(P_n)_{n\in\mathbb{N}}$ such that

$$\mathbb{P}^n(\mathbb{Q}) = \{P_n, n\in\mathbb{N}\}$$

Then for any $n\in\mathbb{N}$, choose an elementary open subset U_n such that $P_n \in U_n$ and

$\omega(U_n) \leq \frac{\varepsilon}{2^{n+1}}$ It is possible

Drawing



Take $U = \bigcup_{n\in\mathbb{N}} U_n$ Then $\omega(U) \leq \sum_n \omega(U_n) \leq \varepsilon$

But $\mathbb{P}^n(\mathbb{Q}) \subset U$ so $\frac{\#(\mathbb{P}^n(\mathbb{Q})\cap U)_{H\leq B}}{\#(\mathbb{P}^n(\mathbb{Q}))_{H\leq B}} = 1 \underset{B\to+\infty}{\not\to} \varepsilon$

Explanation

Since $\mathbb{P}^n(\mathbb{Q}) \subset U$ and $\mathbb{P}^n(\mathbb{Q})$ is dense in $\mathbb{P}^n(\mathbb{R})$, U is dense in $\mathbb{P}^n(\mathbb{R})$; $\overline{U} = \mathbb{P}^n(\mathbb{R})$

and $\partial U = \mathbb{P}^n(\mathbb{R}) - U$ has volume $\omega(\partial U) \geq 1-\varepsilon$

The only finite union of elementary open sets which contains U is $\mathbb{P}^n(\mathbb{R})$ itself!

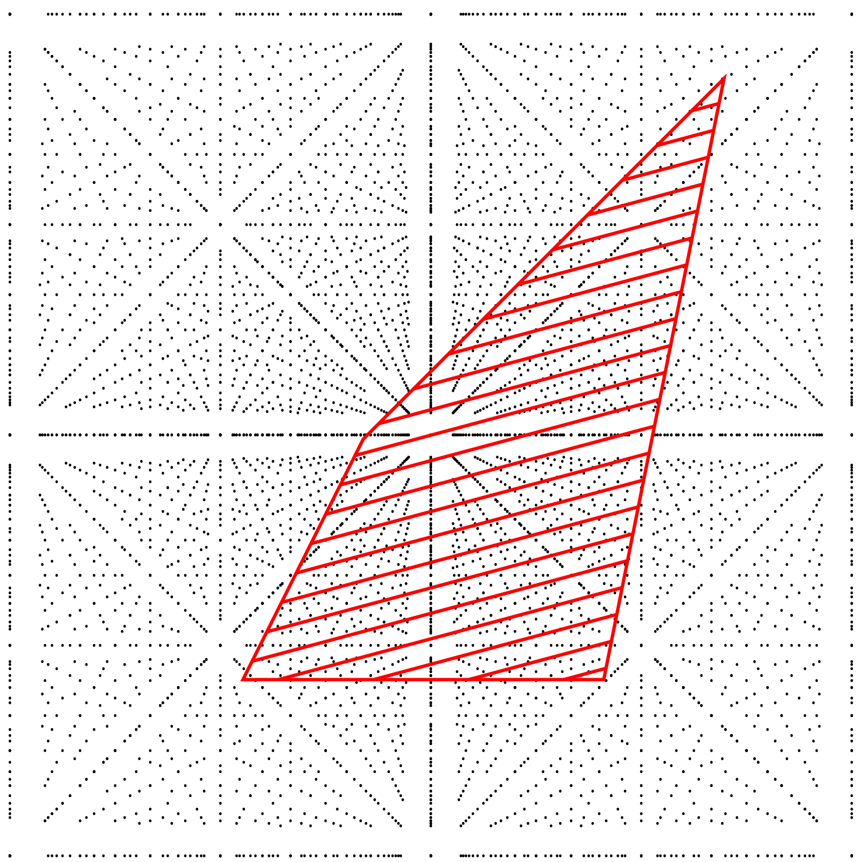
Diophantine statistics

Emmanuel Peyre

Université Grenoble Alpes

北京大学

$\mathbf{P}^2(\mathbf{Q}) \cap U$



25/4/2016 It is high time to use some tools of probability theory

c) Tools of probability theory

Definition

Let X be a topological space. We equip it with the σ-algebra $\mathcal{B}$ of Borel subsets which is generated from open subsets and stable under difference of sets and countable union.

For any non-empty finite subset W of X we define the counting probability measure associated to W as the measure

$$\delta_W = \frac{1}{\# W} \sum_{P \in W} \delta_P \quad \text{Dirac measure in } P$$

In other words

$$\forall B \in \mathcal{B} \qquad \delta_W(B) = \frac{\#(W \cap B)}{\# W}$$

and if $f \in \mathcal{C}(X, \mathbb{R})$

$$\int_X f \, \delta_W = \frac{1}{\# W} \sum_{P \in W} f(P).$$

So now the problem we are dealing with may be rephrased as:

Question

Given a family of probability measures $(\sigma_B)_{B \in \mathbb{R}}$ (or $(\sigma_n)_{n \in \mathbb{N}}$) What does it mean for it to converge? This is extremely classical in the theory of probability.

Definition proposition

A family $(\varpi_B)_{B\in\mathbb{R}}$ of probabilities on X converges weakly to a probability measure ϖ as $B \to +\infty$ if it satisfies the following equivalent conditions

(i) for any $f \in \mathcal{C}_b(X, \mathbb{R})$
bounded

$$\int_X f\,\varpi_B \xrightarrow[B\to+\infty]{} \int_X f\,\varpi$$

(ii) for any subset $W \in \mathcal{B}$ such that $\varpi(\partial W)=0$

$$\varpi_B(W) \xrightarrow[B\to+\infty]{} \varpi(W)$$

(iii) for any closed subset F of X

$$\overline{\lim_{B\to+\infty}}\ \varpi_B(F) \leq \varpi(F)$$

(iv) for any open subset U of X

$$\underline{\lim_{B\to+\infty}}\ \varpi_B(U) \geq \varpi(U).$$

we denote it $\varpi_B \xrightarrow[B\to+\infty]{w} \varpi$.

Reference

SHIRYAEV, probability, Graduate Texts in Mathematics, chapter III.

Definition

A set $\mathcal{H} \subset \mathcal{B}$ is called a convergence determining class if for any family $(\varpi_B)_{B\in\mathbb{R}}$ of probabilities and any probability ϖ the following two assertions are equivalent

(i) $\forall A \in \mathcal{K}$, $\varpi(\partial A) = 0 \Rightarrow \varpi_B(A) \xrightarrow[B \to +\infty]{} \varpi(A)$

(ii) $\varpi_B \xrightarrow[B \to +\infty]{w} \varpi$

Proposition

Elementary open subsets form a convergence determining class on $\mathbb{P}^n(\mathbb{R})$

This follows from the fact that

(i) the intersection of two elementary subsets is still elementary

Thus if the convergence is true on elementary subsets, it is true on the Boole algebra generated by these sets.

(ii) Any open set is the countable union of elementary subsets.

Conclusion

$$\mathcal{E}_{\mathbb{P}^n(\mathbb{Q})_{H \leq B}} \xrightarrow[B \to +\infty]{w} \omega$$

where $\omega(W) = \dfrac{\mathrm{Vol}\left(\mathbb{B}(0,1) \cap \pi^{-1}(W)\right)}{\mathrm{Vol}\left(\mathbb{B}(0,1)\right)}$

where $\pi : \mathbb{R}^{n+1} - \{0\} \to \mathbb{P}^n(\mathbb{R})$ is the projection map

and $\mathbb{B}(0,1) = \{ x \in \mathbb{R}^{n+1}, \|x\|_\infty \leq 1 \}$

norm chosen to define the height.

Now we have seen various example and phenomena which occur when counting rational points of bounded height on varieties it is time to try to interpret all that. In some sense, we are doing experimental mathematics: we consider various examples on which we constat various results and then we try to construct a theory which can explain all the results obtained for the various examples. Here the hope is to have a geometric interpretation of the arithmetic phenomena. In order to do this, we need

III Schemes and beyond (the HARTSHORNE and SGA4 in two hours)

Reference

HARTSHORNE, algebraic geometry.

I am not going to repeat the HARTSHORNE but go beyond

1) Starting point of algebraic geometry

- One of the motivation of algebraic geometry comes from the realization that "Morphisms between commutative algebras $/\mathbb{C}$ are the points of a geometric object defined by polynomial equations" More generally and precisely

Let A be a noetherian commutative ring, let B and C be finitely generated commutative A algebras. We can find integers n, r,

$$f_1, \dots, f_r \in A[T_1, \dots, T_n]$$

and an isomorphism

$$A[T_1, \dots, T_n]/(f_1, \dots, f_r) \xrightarrow{\sim} B$$

Then there is a canonical bijection

$$\mathrm{Mor}_{A\text{-alg}}(B, C) \longrightarrow \{(c_1, \dots, c_n) \in C^n \mid \forall_i \ f_i(c_1, \dots, c_n) = 0\}$$

- On the hand differential geometry tought people that
  A geometric object is obtained by glueing together pieces of a more elementary type (open sets of $\mathbb{R}^n$ for differential geometry)
  It was Grothendieck who was able to produce the first good category, namely the category of schemes

Aim

Define a category Sch (category of schemes) with a functor
Spec : Category of commutative ring $\to$ Schm
which contravariant and fully faithful: that is for any commutative rings A and B the functor gives a bijective map

$$\mathrm{Mor}_{\text{ring}}(A, B) \longrightarrow \mathrm{Mor}_{\mathrm{Sch}}(\mathrm{Spec}(B), \mathrm{Spec}(A))$$

In fact you get back the ring A from its corresponding scheme as the ring of functions on Spec(A).
Moreover to each object in Sch corresponds a topological space and is obtained by glueing together Spectrum of rings.
As often in mathematics the important thing is the properties of the object (here the category of schemes) you want to get not the explicit

construction you use to get it. What one should remember about schemes is the description I just gave.

2) Grothendieck topologies, presheaves, sheaves

For later use, I wish to introduce the very nice idea of Grothendieck to see a topology as a category

References

- ARTIN (1962) Grothendieck Topologie
- GROTHENDIECK et al. SGA 4
- MILNE Étale cohomology

a) Classical topology (Reminder)

A topology on set X is a set $\mathcal{U} \subset \overbrace{\mathcal{P}(X)}^{\text{set of subsets of } X}$ of subsets of X such that

(i) $\emptyset \in \mathcal{U}$

(ii) for any finite family $(U_i)_{i \in I}$ of elements of $\mathcal{U}$ with $I \neq \emptyset$ $\bigcap_{i \in I} U_i \in \mathcal{U}$

(iii) for any family $(U_i)_{i \in I}$ of elements of $\mathcal{U}$ $\bigcup_{i \in I} U_i \in \mathcal{U}$

NB. (iii) $\Rightarrow$ (i) for $I = \emptyset$

The corresponding category is defined $\mathcal{T}_X$:

- objects are the open subsets of X
- morphisms are $j : U \longrightarrow V$ if $U \subset V$
  $x \longmapsto x$

The conditions (ii) and (iii) may be translated as the existence of some products or coproducts

b) Direct and inverse limits

Let I be a category. It is said to be <u>filtered</u> iff it has an object,

(i) for any diagram

$$\begin{tikzcd} & j \\ i \arrow[ur] \arrow[dr] & \\ & j' \end{tikzcd}$$ can be completed as $$\begin{tikzcd} & j \arrow[dr] & \\ i \arrow[ur] \arrow[rr] \arrow[dr] & & k \\ & j' \arrow[ur] & \end{tikzcd}$$

(ii) for any pairs j, j' of objects there exist

$$\begin{tikzcd} j \arrow[dr] & \\ & k \\ j' \arrow[ur] & \end{tikzcd}$$

It is said to be cofiltered if the opposite category I^0 obtained by reversing arrows is filtered

<u>Example</u>

Let I be a set with a partial order $\leqslant$ such that for any $j, j' \in I$ there exists $k \in I$, $j \leq k$ & $j' \leq k$ (filtered set)

Then take as a category:

- Objects $i \in I$
- morphisms pairs $(i,j) \in I^2$, $i \leq j$

$(j,k) \circ (i,j) = (i,k)$.

(In particular we may take $\mathbb{N}, \leq, \geq$ or $\mathbb{N} - \{0\}$, $|$ or its opposite
divisibility

the collection of objects is a set

. Let I be a small filtered category
Let C be a category and $F : I \to C$ be a functor. We write $C_i = F(i)$
then a inverse limit of F denoted by $\varprojlim_I F$ or $\varprojlim_{i \in I} C_i$ is an object L of C with a family of morphisms $f_i : L \to C_i$ for $i \in Obj(I)$
so that $\forall \alpha : i \to j$

$$\begin{tikzcd} & C_i \arrow[d, "F(\alpha)"] \\ L \arrow[ur, "f_i"] \arrow[r, "f_j"'] & C_j \end{tikzcd}$$ commute

and such that for any objects X of C and any family $g_i : X \to C_i$ which satisfies
$\forall \alpha : i \to j$

$$\begin{tikzcd} & C_i \arrow[d, "F(\alpha)"] \\ X \arrow[ur, "g_i"] \arrow[r, "g_j"'] & C_j \end{tikzcd}$$ commute

there exists a unique $\varphi : X \to L$ so that $\forall i$

$$\begin{tikzcd} X \arrow[d, "\varphi"'] \arrow[dr, "g_i"] & \\ L \arrow[r, "f_i"'] & C_i \end{tikzcd}$$ commute

Such L is unique up to a unique isomorphism

Examples

In the category Sets of sets we may take

this functor is now contravariant

$$\left\{ (x_i)_{i \in I} \in \prod_{i \in I} X_i \;\middle|\; \forall \alpha : j \to j',\ F(\alpha)(x_{j'}) = x_j \right\}$$

Same construction in the category Ab of abelian

abelian groups or the category of commutative rings

Particular cases

- If I is a category with 3 objects and morphisms

$$\begin{tikzcd} & j' \arrow[loop right, "\mathrm{Id}_{j'}"] \arrow[d] \\ j \arrow[r] \arrow[loop below, "\mathrm{Id}_j"] & i \arrow[loop below, "\mathrm{Id}_i"] \end{tikzcd}$$

a functor F from this category to C is a diagram

$$\begin{tikzcd} & X_1 \arrow[d, "f_1"] \\ X_2 \arrow[r, "f_2"'] & Y \end{tikzcd} \quad \text{in } C$$

If the inverse limits exists we denote it $X_1 \times_Y X_2$ (remember unique up to isomorphism) and we say that the square

$$\begin{tikzcd} X_1 \times_Y X_2 \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & X_2 \arrow[d] \\ X_1 \arrow[r] & Y \end{tikzcd}$$

is cartesian (denoted by the square in the square)

In the category of Sets

$$X_1 \times_Y X_2 = \{(x_1, x_2) \in X_1 \times X_2 \mid f_1(x_1) = f_2(x_2)\}$$

- If X_1 and X_2 are subsets of Y and $f_1 : X_1 \to Y$, $f_2 : X_2 \to Y$ are the inclusion maps $X_1 \times_Y X_2 = X_1 \cap X_2$.

finite inverse limits generalize intersections

- If the only morphisms in I are the identities id_X for X object of I (<u>discrete category</u>) then a functor from I to C is a family $(X_i)_{i\in I}$ of objects C and if it exists, the inverse limit is the <u>product</u> $\prod\limits_{i\in I} X_i$

- One way to define the p-adic integers is to take the category associated to $\mathbb{N}_{\geq}$ and define the functor in the category of rings defined by
$$R_n = \mathbb{Z}/p^n\mathbb{Z} \quad \text{where } p \text{ is a prime number}$$
and for $m \to n$ (ie $m \geq n$)
$$\mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z} \text{ is the only morphism}$$
of rings
$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \subset \prod_n \mathbb{Z}/p^n\mathbb{Z}$$

It is equipped with the topology induced by the product topology (each $\mathbb{Z}/p^n\mathbb{Z}$ being equipped with the discrete topology)

<u>direct limits</u> in C are inverse limits in C^o

they are denoted by $\varinjlim_I F$ or $\varinjlim_{i\in I} F_i$

<u>Examples</u>

- In the category of sets $(X_i)_{i\in \mathrm{Obj}\, I}$
$$L = \coprod_{i\in I} X_i \Big/ R$$
where $x_i \underset{R}{\sim} x_j$ if $\exists$ diagram $i \xrightarrow{\alpha} k \xleftarrow{\beta} j$ in I

and $x_k \in X_k$ such that $\alpha_i = F(\alpha)(x_k)$ and $\alpha_j = F(\beta)(x_k)$

- In the category Ab of abelian groups

$\bigoplus_{i\in I} A_i / C$ where C is generated by the elements of the form, for $\alpha : j \to j'$

$$(a_i)_{i\in I} \text{ where } \begin{cases} a_i = 0 & \text{for } i \notin \{j, j'\} \\ a_j = -F(\alpha)(a_{j'}) \end{cases}$$

Particular case

- For a discrete category I and a functor $F : I \to C$ corresponding to a family $(X_i)_{i\in I}$ we get the sum (or coproduct) denoted by

$\coprod_{i\in I} X_i$ or, when it is meaningful, $\bigoplus_{i\in I} X_i$

c) An example: the glueing of spaces

Data

$(X_\lambda)_{\lambda\in L}$ family of topological spaces

For $(\lambda, \kappa) \in L^2$, $U_{\lambda\kappa}$ open subset of X_λ

and a continuous map

$$\varphi_{\kappa\lambda} : U_{\lambda,\kappa} \xrightarrow{\sim} U_{\kappa,\lambda}$$

Such that

(i) $\forall \lambda \in L$, $U_{\lambda,\lambda} = X_\lambda$ and $\varphi_{\lambda\lambda} = Id_{X_\lambda}$

(ii) $\forall \lambda, \mu, \kappa \in L$ $\forall x \in U_{\lambda\kappa} \cap U_{\lambda\mu}$ $h_{\kappa\lambda}(x) \in U_{\kappa,\mu}$ and $h_{\mu\kappa}(h_{\kappa\lambda}(x)) = h_{\mu\lambda}(x)$

From a more categorical point of view, using a a total order on L, this data may be given as follows

Let I be the category
- objects : finite subsets of L,
- morphism (A,B) if $B \subset A$
$A \to B$

Then we consider a functor $F : I \to Top_{op}$.
where Top_{op} is the category of topological spaces with the open immersions as morphisms such that $\forall A, B \subset L$

$$\begin{tikzcd} F(A \cup B) \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & F(B) \arrow[d] \\ F(A) \arrow[r] & F(A \cap B) \end{tikzcd}$$

is cartesian if $A \cap B \neq \emptyset$

(take $F(A) = \bigcap_{K \in A} U_{\min(A), K}$)

Then $X = \varprojlim_I F$ is the space obtained by glueing together the $(X_\lambda)_{\lambda \in L}$ along $U_{\lambda\mu}$ using the homeomorphisms $\varphi_{\mu\lambda}$

<u>Prop</u>

Let $f_\lambda : X_\lambda \to X$ be the canonical map.
Then
(i) $f_\lambda(X_\lambda)$ is open in X
and f_λ is an homeomorphism from X_λ to $f_\lambda(X_\lambda)$
In particular
(ii) $U \subset X$ is open (resp. closed) iff $\forall \lambda \in L$, $U \cap f_\lambda(X_\lambda)$ is open (resp. closed).
(iii) $g : X \to Y$ is continuous iff $\forall \lambda \in L$, $g \circ f_\lambda$ is continuous.

北京大学

Remark

This does not say anything about the morphisms to X!

$$\mathbb{P}^n(A) = \mathrm{Mor}(\mathrm{Spec}(A), \mathbb{P}^n)$$

are not that easy to describe.

25/4/2016

d) Grothendieck Topology

Definition

A Grothendieck topology is a category T equipped with a collection $\mathrm{Cov}(T)$ of families $(U_i \xrightarrow{\phi} U)_{i \in I}$ of morphisms in T called coverings, such that

(i) For any isomorphism φ in T, (φ) belongs to $\mathrm{Cov}(T)$.

(ii) If $(U_i \xrightarrow{\phi_i} U)_{i\in I}$ is a covering of U, and for any $i \in I$, $(V_{ij} \xrightarrow{\phi_{ij}} U_i)_{j \in J_i}$ a covering of U_i, then

$$\left(V_{i,j} \xrightarrow{\phi_i \circ \phi_{ij}} U\right)_{(j,i) \in \coprod_{i\in I} J_i}$$

(iii) If $(U_i \xrightarrow{\phi_i} U)_{i \in I}$ is a covering of U and $V \longrightarrow U$ a morphism then $U_i \times_U V$ exists for any $i \in I$ and $(U_i \times_U V \to V)$ is a covering of V

Reminder

In the category of sets, $\coprod_{i \in I} J_i$ is formally constructed as

$$\left\{ (j,i) \in \left(\bigcup_{i\in I} J_i\right) \times I \;\middle|\; j \in J_i \right\}$$

Remark

In the following we consider topologies on categories T which admits finite inverse limits an finite coproducts.

e) Presheaves

Definition

- Let T and A be categories a presheave on T with values in A is a contravariant functor F from T to A. If T admits an initial object ϕ and A a terminal object 0 we impose that

$$F(\phi) = 0$$

- A morphism of presheaves from F to G is a natural transformation from F to G

So the presheaves on C with values in A form a category.

Fundamental example

Let X be an object of C

We define a presheaf h_X on C with values in Set by

$$h_X(Y) = \mathrm{Hom}_C(Y, X)$$

and $h_X(f : Y \to Y') : \mathrm{Hom}_C(Y', X) \to \mathrm{Hom}_C(Y, X)$

$$g \longmapsto g \circ f$$

Theorem (YONEDA)

The functor which maps X to h_X is fully faithful

Definition

A presheaf F from C to Sets is said to be <u>representable</u> if there exists an object X of C such that F is isomorphic to h_X.
An object X of C with an isomorphism from h_X to F is called a <u>realization</u> of F.

Exercise

Let I be a filtered category and C be a category.
Let F be a functor from I to C.
For any X in C let $k_X : I \to C$ be the functor mapping any object to X and any morphism to Id_X. Check that the presheaf which maps an object X of C to $\mathrm{Hom}_{\mathrm{Fonct}(I,C)}(k_X, F)$ is $\varprojlim_I h_X \circ F$ and that, if it exists, $\varprojlim_I F$ gives a realization of $\varprojlim_I h_X \circ F$.

f) Sheaves

Definition

Let C be a category with a Grothendieck topology.
Let A be a category admitting products.
A sheave on C with values in A is a presheave F on C with values in A such that for any covering $(U_i \xrightarrow{\varphi_i} U)_{i \in I}$

the sequence

$$F(U) \xrightarrow{\varphi} \prod_{i \in I} F(U_i) \underset{\psi_2}{\overset{\psi_1}{\rightrightarrows}} \prod_{(i,j)\in I^2} F(U_i \times_U U_j)$$

exact, where

φ is characterized by $pr_i \circ \varphi = \varphi_i$ for any $i \in I$ and ψ_1, ψ_2 by the commutativity of the diagrams

$$\begin{array}{ccc} \prod_{i \in I} F(U_i) & \xrightarrow{\psi_1} & \prod_{(i,j)\in I^2} F(U_i \times_U U_j) \\ \downarrow & & \downarrow \\ F(U_i) & \xrightarrow{F(pr_1)} & F(U_i \times_U U_j) \end{array}$$

$$\begin{array}{ccc} \prod_{i \in I} F(U_i) & \xrightarrow{\psi_2} & \prod_{(i,j)\in I^2} F(U_i \times_U U_j) \\ \downarrow & & \downarrow \\ F(U_j) & \xrightarrow{F(pr_2)} & F(U_i \times_U U_j) \end{array}$$

and a diagram

$$X \xrightarrow{f} Y \underset{g_2}{\overset{g_1}{\rightrightarrows}} Z$$

is said to be exact if for any object U of C

$$Hom(U, X) \longrightarrow Hom(U, Y) \rightrightarrows Hom(U, Z)$$

is exact: that is for any $h : U \longrightarrow Y$ such that $g_1 \circ h = g_2 \circ h$ there exists a unique $u : U \to X$ such that $h = f \circ u$

Remarks

- If A is a subcategory of the category of sets, this means that f is a bijection from X to $\{ y \in Y \mid g_1(y) = g_2(y)\}$
- If A is an abelian category this means that

$$0 \to F(U) \xrightarrow{\varphi} \prod_{i \in I} F(U_i) \xrightarrow{\psi_1 - \psi_2} \prod_{(i,j)\in I^2} F(U_i \times_U U_j) \quad \text{is exact}$$

Example

If X is a (classical) topological space and $\mathcal{U}$ the corresponding category of its open subsets with the open coverings
For any topological space Y, the functor $h_Y : U \mapsto \mathcal{C}(U, Y)$ is a sheaf.

Definition

A morphism of sheaves is a morphism of presheaves, let $\sigma : \mathcal{S} \longrightarrow \mathcal{P}$ be the inclusion functor from the category of sheaves to the category of presheaves

Theorem

The inclusion functor $\iota : \mathcal{S} \to \mathcal{P}$ admits a left adjoint. In other words, for any presheaf $\mathcal{F}$ there exist a sheaf $\mathcal{F}^{\#}$ and a morphism of presheaves $\varphi : \mathcal{F} \to \mathcal{F}^{\#}$ so that for any sheaf $\mathcal{G}$

$$\mathrm{Hom}_{\mathcal{S}}(\mathcal{F}^{\#}, \mathcal{G}) \longleftrightarrow \mathrm{Hom}_{\mathcal{P}}(\mathcal{F}, i(\mathcal{G}))$$

equivalence of functors (in $\mathcal{G}$)]

3) Schemes

[cf. HARTSHORNE, skipped]

4) Group scheme

Definition

Let X be a scheme.

- The category Sch_X of schemes above X is the following category

  Objects: Schemes Y with a morphism $\pi_Y : Y \to X$ called structural morphism:

  Morphisms: a morphism from Y to Y' is a morphism of schemes $\varphi : Y \to Y'$ such that

$$\begin{tikzcd} Y \arrow[rr, "\varphi"] \arrow[dr, "\pi_Y"'] & & Y' \arrow[dl, "\pi_{Y'}"] \\ & X & \end{tikzcd}$$

  commute (Denoted by $Hom_X(Y, Y')$)

Many algebraic structures, like groups or rings may be interpreted as commutative diagrams in the category of sets. Therefore, they have analogs in the theory of schemes.

- A group scheme over X is a scheme G over X (that is with a morphism $\pi_G : G \to X$) equipped with morphisms in Sch_X

$$m : G \times_X G \longrightarrow G$$
$$e : X \longrightarrow G$$
$$i : G \longrightarrow G$$

  so that the following diagrams commute:

(associativity)

$$\begin{tikzcd} G \times_X G \times_X G \arrow[r, "m \times Id_G"] \arrow[d, "Id_G \times m"'] & G \times_X G \arrow[d, "m"] \\ G \times_X G \arrow[r, "m"] & G \end{tikzcd}$$

(identity element)

$$\begin{tikzcd}
G \arrow[rr, "\sim"] \arrow[d, "s"'] \arrow[ddrr, "Id_G"] & & X \times_X G \arrow[d, "e \times Id_G"] \\
G \times_X X \arrow[dr, "Id_G \times e"] & & G \times_X G \arrow[d, "m"] \\
& G \times_X G \arrow[r, "m"'] & G
\end{tikzcd}$$

(Inverse)

$$\begin{tikzcd}
G \arrow[rr, "(Id_G, \iota)"] \arrow[d, "(\iota, Id_G)"'] \arrow[dr, "\pi_G"] & & G \times_X G \arrow[d, "m"] \\
& X \arrow[dr, "e"] & \\
G \times_X G \arrow[rr, "m"'] & & G
\end{tikzcd}$$

Reference

A. BOREL. Linear algebraic groups (Graduate Texts in Mathematics, Springer)

Remark

Let A be a commutative ring and G be group scheme over $Spec(A)$ then G defines a covariant functor from the category of commutative A-algebras to the category of groups

$$B \longmapsto G(B) = Hom_{Spec(A)}(Spec(B), G)$$

The multiplication is given by:

$$(\varphi, \psi) \in G(B) \times G(B)$$

$$\begin{tikzcd}
Spec(B) \arrow[r, "\varphi"] \arrow[d, "\psi"'] & G \arrow[d, "\pi_G"] \\
G \arrow[r, "\pi_G"'] \arrow[ur, phantom, "\circlearrowright"] & Spec(A)
\end{tikzcd}$$

gives
$$\begin{tikzcd}
Spec(B) \arrow[r, "(\varphi, \psi)"] \arrow[rr, bend right, "\varphi \cdot \psi"'] & G \times_{Spec(A)} G \arrow[r, "m"] & G
\end{tikzcd}$$

Notation

X a scheme over a commutative ring A

B a commutative A-algebra

$$X_B = \mathrm{Spec}(B) \times_{\mathrm{Spec}(A)} X \quad \text{(extension of scalars)}$$

$$X(B) = \mathrm{Hom}_{\mathrm{Spec}(A)}(\mathrm{Spec}(B), X) \quad B\text{-points of } X.$$

Examples

- $\mathbb{G}_a$ (additive group)

$$\mathbb{G}_a = \mathrm{Spec}(\mathbb{Z}[T]),$$

$$m : \mathbb{G}_a \times \mathbb{G}_a \to \mathbb{G}_a$$
$$1\otimes T + T \otimes 1 \leftarrow\!\shortmid T$$

$$e : \mathrm{Spec}\,\mathbb{Z} \to \mathbb{G}_a$$
$$0 \leftarrow\!\shortmid T$$

$$\iota : \mathbb{G}_a \longrightarrow \mathbb{G}_a$$
$$-T \leftarrow\!\shortmid T$$

B-points

There is a canonical isomorphism from $\mathbb{G}_a(B)$ to the additive group B for $+$

- $\mathbb{G}_m$ (multiplicative group)

$$\mathbb{G}_m = \mathrm{Spec}(\mathbb{Z}[T, T^{-1}])$$

$$m \quad \mathbb{G}_m \times \mathbb{G}_m \longrightarrow \mathbb{G}_m$$
$$T \times T \leftarrow\!\shortmid T$$

$$e : \mathrm{Spec}(\mathbb{Z}) \longrightarrow \mathbb{G}_m$$
$$1 \leftarrow\!\shortmid T$$

$$\iota : \mathbb{G}_m \longrightarrow \mathbb{G}_m$$
$$T^{-1} \leftarrow\!\shortmid T$$

B-points

$\mathbb{G}_m(B)$ is the multiplicative group B^* of invertible elements in B

IV Vector bundles, Picard group, K_0

1) Vector bundles

a) Matrices

Definition

$M_{m,n} = \mathrm{Spec}\left(\mathbb{Z}[T_{i,j},\ 1 \le i \le m,\ 1 \le j \le n]\right)$

With

$+ : M_{m,n} \times M_{m,n} \longrightarrow M_{m,n}$ morphism of schemes

defined by $T_{i,j} \mapsto T_{i,j} \otimes 1 + 1 \otimes T_{i,j}$

and

$\times : M_{m,n} \times M_{n,p} \longrightarrow M_{m,p}$

defined by $T_{i,j} \longmapsto \sum_{k=1}^{n} T_{ik} \otimes T_{kj}$

Similarly on $\mathbb{A}^n = \mathrm{Spec}\left(\mathbb{Z}[T_1, \dots, T_n]\right)$

we may define

$+ : \mathbb{A}^n \times \mathbb{A}^n \longrightarrow \mathbb{A}^n$ addition

by $T_i \longmapsto T_i \otimes 1 + 1 \otimes T_i$

$\times : \mathbb{A}^1 \times \mathbb{A}^n \longrightarrow \mathbb{A}^n$ multiplication by a scalar

by $T_i \longmapsto T \otimes T_i$

and an action of M_n

$\times : M_{m,n} \times \mathbb{A}^n \longrightarrow \mathbb{A}^m$

defined by $T_i \longmapsto \sum_{k=1}^{n} T_{i,k} \otimes T_k$

Write $M_n = M_{n,n}$

Remark 1

All this laws are compatible which means that we have a lot of commutative diagrams

$$\begin{array}{ccc} M_n \times M_n \times \mathbb{A}_n & \xrightarrow{\mathrm{Id} \times \times} & M_n \times \mathbb{A}_n \\ {\scriptstyle \times \times \mathrm{Id}} \downarrow & & \downarrow {\scriptstyle \times} \\ M_n \times \mathbb{A}_n & \xrightarrow{\times} & \mathbb{A}_n \end{array}$$

or

$$\begin{tikzcd}
M_n \times M_n \times \mathbb{A}_n \arrow[r, "+\times \mathrm{Id}"] \arrow[d, "\text{2 multiplications}"'] & M_n \times \mathbb{A}_n \arrow[d, "\times"] \\
\mathbb{A}_n \times \mathbb{A}_n \arrow[r, "+"] & \mathbb{A}_n
\end{tikzcd} \quad \dots$$

Remark 2

We may use Yoneda lemma and consider a scheme S as a functor which I also denote by $S : \underbrace{\mathrm{CRings}}_{\text{category of commutative rings}} \longrightarrow \mathrm{Sets}$

$$A \longmapsto \underbrace{S(A)}_{A\text{-points}} = \mathrm{Hom}(\mathrm{Spec}(A), S)$$

Then $M_n(A)$ is the A-algebra of $n \times n$ matrices and $\mathbb{A}^n(A)$ is A^n seen as a $M_n(A)$-module

- The linear group

$$GL_n = \mathrm{Spec}\left(\mathbb{Z}[T_{ij},\ 1 \le i,j \le n]\left[\frac{1}{\mathrm{Det}(T_{ij})_{\substack{1\le i\le n\\ 1\le j\le n}}}\right]\right)$$

wich is an open subscheme of M_n with the induced Multiplication

$\times\ GL_n \times GL_n \longrightarrow GL_n$

$e : \mathrm{Spec}(\mathbb{Z}) \longrightarrow GL_n$

$\begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases} \longleftarrow\!\shortmid\ T_{ij}$

$\iota : GL_n \longrightarrow GL_n$

$$\frac{(-1)^{i+j}}{\mathrm{Det}(T_{ij})}\, \mathrm{Det}\underbrace{\left(\underbrace{T_{k,l}}_{j \text{ removed}} \right)}_{i \text{ removed}} \longleftarrow\!\shortmid\ T_{ij}$$

defines an algebraic group

<u>B points</u>

$$GL_n(B) = M_n(B)^* = \text{"} GL_n(B) \text{"}$$

b) <u>Vector bundles</u>

I want to consider vector bundles as schemes and not as coherent sheaves.

Let $n \in \mathbb{N}$ we consider the category

V_n : objects are products $X \times \mathbb{A}^n$

a morphism $U \times \mathbb{A}^n \longrightarrow X \times \mathbb{A}^n$

is a morphism of schemes $\psi : U \times \mathbb{A}^n \to X \times \mathbb{A}^n$

such that there exists

- an open immersion $\iota : U \to X$
- a morphism $f : U \longrightarrow M_n$

such that

$$\begin{tikzcd}
U \times \mathbb{A}^n \arrow[r, "Id \times f \times Id"] \arrow[d, "\psi"'] & U \times M_n \times \mathbb{A}^n \arrow[d, "Id \times \times"] \\
X \times \mathbb{A}^n & U \times \mathbb{A}^n \arrow[l, "\iota \times Id"']
\end{tikzcd}$$

commutes

(In terms of A-points, this means

$$U(A) \times \mathbb{A}^n \longrightarrow X(A) \times \mathbb{A}^n$$
$$(u, t) \longmapsto (\iota(u), f(u) \times t) \;)$$

There are two functors from V_n to the category of schemes

(i) i the inclusion functor

(ii) pr the projection functor which map $X \times \mathbb{A}^n$ to X

for any object $X \times \mathbb{A}^n$ of V_n, $\pi_X : X \times \mathbb{A}^n \to X$ defines a natural transformation from i to pr.
for any E of V_n we also have the addition morphism $+ : i(E) \times_{pr(E)} i(E) \to i(E)$ which may also be seen as a natural transformation between functors
and the multiplication
$$\times : \mathbb{A}_1 \times i(E) \to i(E)$$

2 for $n \geq 2$ the matrices do not commute so
$$\begin{array}{ccc} M_n \times E & \xrightarrow{\times} & E \\ \downarrow \mathrm{Id} \times \phi & & \downarrow \phi \\ M_n \times E & \xrightarrow{\times} & E \end{array}$$
is not commutative

Thus the multiplication by M_n does not define a natural transformation

Definition

- Let X be a scheme. A vector bundle of rank n E over X is a scheme E with
  (i) a projection map $\pi : E \to X$
  (ii) an addition map $+ : E \times_X E \to E$
  (iii) a scalar multiplication $\times$ $\mathbb{A}_1 \times_X E \to E$

such that E is obtained by glueing together objects from V_n that is there is a set L and a functor F from the category $I = \mathcal{P}_f(L)$ of finite non empty sets of L to V_n such that
i. $F(A \supseteq B)$ (morphism in I) is an open immersion of schemes and
$$\begin{array}{ccc} F(A \cup B) & \longrightarrow & F(A) \\ \downarrow & \square & \downarrow \\ F(B) & \longrightarrow & F(A \cap B) \end{array}$$
when $A \cap B \neq \emptyset$

such that $E = \varprojlim_{I} i \circ F$, $X = \varprojlim_{I} pr \circ F$,

π is induced by $\pi : i \to pr$

$+$ ———————— $+ : i \times_{pr} i \to i$

and $\times$ ———————— $\times \quad \mathbb{A}_1 \times i \to i$

π is called the structural morphism of E

A vector bundle of rank 1 is called a line bundle.

- Let E be a vector bundle of rank m over X and F ———————— n over X

a morphism $\varphi : E \to F$ is a morphism of schemes such that

$$\begin{tikzcd} E \arrow[rr, "\varphi"] \arrow[dr, "\pi_E"'] & & F \arrow[dl, "\pi_F"] \\ & X & \end{tikzcd} \qquad \begin{tikzcd} + \; E \times E \arrow[r] \arrow[d, "\varphi\times\varphi"] & E \arrow[d, "\varphi"] \\ + \; F \times F \arrow[r] & F \end{tikzcd} \text{ and } \begin{tikzcd} \mathbb{A}^1 \times E \arrow[r] \arrow[d, "Id\times\varphi"] & E \arrow[d, "\varphi"] \\ \mathbb{A}^1 \times F \arrow[r] & F \end{tikzcd}$$

commute.

The vector bundles with these morphisms form a category.

<u>Remark</u>

From the point of view of A-points we get maps

$$\pi : \quad E(A) \to X(A)$$

$$+ : \quad E(A) \times_{X(A)} E(A) \to E(A)$$

$$\text{and } \times : \quad A \times E(A) \longrightarrow E(A)$$

so that for any $x \in X(A)$ $\pi^{-1}(x)$ has a structure of A-module.

We denote $E(x) = \pi^{-1}(x)$ and call it the fibre of E at x.

if $\varphi : A \to B$ is a morphism of commutative rings

let $x_B = x \circ \mathrm{Spec}(\varphi) : \mathrm{Spec}(B) \to X$, $x_B \in X(B)$

We get an isomorphism

$$E(X)\otimes_A B \xrightarrow{\sim} E(X_B)$$

This follows from the fact that $E(X)$ is, by definition, locally free of constant rank n and we can check locally wether a morphism is an isomorphism.

c) Sections

Definition

Let E be a vector bundle on X of rank n and U an open set of X
a section s of E over U is a morphism $s: U \to E$ such that $\pi\circ s$ is the injection map from U to X.
The set $\Gamma(U,E)$ of these sections has a structure of $\mathcal{O}_X(U)$ module:
for $f\in\mathcal{O}_X(U)$, $s\in\Gamma(U,E)$

$$\begin{tikzcd} U \arrow[r, "f\times s"] \arrow[dr, "fs"'] & \mathbb{A}^1\times E \arrow[d, "\times"] \\ & E \end{tikzcd}$$

Facts

(i) $U\longmapsto\Gamma(U,E)$ defines a coherent sheaf of $\mathcal{O}_X$-module which is locally free of constant rank n

(ii) This defines an equivalence of categorie between the category of vector bundle on X and the category of coherent $\mathcal{O}_X$-modules which are locally free of constant rank

and in the litterature the vector bundles are sometimes defined as coherent sheaves but I prefer to see them as schemes.

d) Examples and construction

① Trivial vector bundle:

$$\pi : \mathbb{A}^n \times X \longrightarrow X.$$

its sheaf of sections is $\mathcal{O}_X^n$

② The projective space $\mathbb{P}^n$ may be defined over $\mathbb{Z}$ as the glueing of $n+1$ affine spaces

$$U_i = \operatorname{Spec}\left(\mathbb{Z}[T_0, \dots, \hat{T_i}, \dots, T_n]\right)$$

$$U_{i,j} = \operatorname{Spec}\left(\mathbb{Z}[T_0, \dots, \hat{T_i}, \dots, T_n]\left[\tfrac{1}{T_j}\right]\right)$$

$$U_{i,j} \longrightarrow U_{j,i}$$

$$T_k/T_j \longleftarrow T_k \qquad k \neq i, j$$

$$1/T_j \longleftarrow T_i$$

We glue the $\mathbb{A}^1 \times U_i$ using the morphisms (in V_1): $\mathbb{A}^1 \times U_{i,j} \longrightarrow \mathbb{A}^1 \times U_{j,i}$

$$T \otimes 1/T_j \longleftarrow T \otimes 1$$

For $k \in 0, \dots, n$, we have commutative diagrams

$$\begin{tikzcd}
T_k/T_j \ (1/T_j \text{ if } k=i) & U_{i,j} \arrow[r] \arrow[d] & U_{j,i} \arrow[d] & T_k \ (\text{resp } 1 \text{ if } k=j) \arrow[lll, mapsto] \\
T \otimes \frac{1}{T_j} \arrow[u, mapsto] & \mathbb{A}^1 \times U_{i,j} \arrow[r] & \mathbb{A}^1 \times U_{j,i} & T \otimes 1 \arrow[u, mapsto] \arrow[lll, mapsto]
\end{tikzcd}$$

which define a section T_k of this line bundle. This line bundle is denoted as $\mathcal{O}(1)$.

北京大学

(3) Let E be a vector bundle over X and $f: Y \to X$ be a morphism of schemes then $E \times_X Y$ is a vector bundle over Y with pr_2 as the structural map

Indeed if $E = \varinjlim_{i \in I} U_i \times \mathbb{A}^n$

then $E \times_X Y = \varinjlim_{i \in I} f^{-1}(U_i) \times \mathbb{A}^n$

$f^*(E) = E \times_X Y$ is called the <u>pull-back</u> of E by f

In particular if U is an open subset of X $E_{|U} = E \times_X U$ is called the <u>restriction</u> of E to U

<u>Terminology</u>

By definition for any vector bundle E of rank n over X there exists an open covering $(U_i)_{i \in I}$ of X and a family of isomorphisms of vector bundles

$(\phi_i : U_i \times \mathbb{A}^n \to E_{|U_i})$.

Such a covering is said to trivialize E and the family $(\phi_i)_{i \in I}$ is called a local trivialization of E.

(4) <u>Definition</u>

A linear representation of an algebraic group G is a morphism of algebraic groups

$$G \longrightarrow GL_m$$

Construction

Let $\rho : GL_n \to GL_m$ be a representation of GL_m and let E be a vector bundle given as

$$E \xrightarrow{\sim} \varinjlim_I i \circ F$$

where $F : I \to V_n$ is a glueing data. In fact all morphisms $F(\varphi)$ are given by pairs (ι, f) where $\iota : U \to V$ is an open immersion and $f : U \to GL_n$ a morphism.

We denote by V_n^* the category with the same objects as V_n but with this type of morphisms.

Then define a functor

$$\rho : V_n^* \to V_m^*$$

by $\rho(U \times \mathbb{A}^n) = U \times \mathbb{A}^m$

and if $\varphi : U \times \mathbb{A}^n \to V \times \mathbb{A}^n$ corresponds to $\iota : U \to V$ and $f : U \to GL_n$ and $\rho(\varphi)$ is defined by

$$\begin{tikzcd} U \times \mathbb{A}^m \arrow[rr] \arrow[dr, "Id \times \rho\circ f \times Id"'] & & V \times \mathbb{A}^m \\ & U \times GL_n \times \mathbb{A}^m \arrow[ur, "i \times X"'] & \end{tikzcd}$$

We define

$$\rho_*(E) \text{ as } \varinjlim_I \iota \circ \rho \circ G$$

Since it is defined using a functor on V_n^*, $\rho_*(E)$, up to isomorphism, depends only on ρ and the class of isomorphism of E.

and ρ_* is functorial on the category of vector bundles of rank n.

This works also for representations of products of GL_n: If we have a morphism of algebraic groups $\prod_{i=1}^{r} GL_{n_i} \to GL_m$, we get a functor

$$\prod_{i=1}^{r} \mathcal{P}_{n_i}(X) \to \mathcal{P}_m(X)$$

where $\mathcal{P}_{n_i}(X)$ denotes the category of vector bundles of rank n_i over X.

5 Applications

We can apply this construction to the functorial construction in linear algebra

- direct sums

$$GL_{n_1} \times GL_{n_2} \longrightarrow GL_{n_1+n_2}$$

$$(M_1, M_2) \longmapsto \begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix} \quad \text{(in terms of } A \text{ points)}$$

Taking vector bundles E_1, E_2 on X we get a vector bundle $E_1 \oplus E_2$ called the direct seem of E_1 and E_2.
For any commutative ring A and any $x \in X(A)$, we have a canonical isomorphism

$$E_1 \oplus E_2(x) \xrightarrow{\sim} E_1(x) \oplus E_2(x)$$

— tensor product

Let $(e_1, \dots, e_m)$ (resp. $(f_1, \dots, f_n)$) be the usual basis of $\mathbb{Z}^m$ (resp. $\mathbb{Z}^n$)

Then $(e_i \otimes f_j)_{(i,j) \in \{1,\dots,m\} \times \{1,\dots,n\}}$ is a basis of $\mathbb{Z}^m \otimes \mathbb{Z}^n$

and we get a representation

$$GL_m \times GL_n \longrightarrow GL_{mn}$$

$$\left((a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le m}}, (b_{k,l})_{\substack{1 \le k \le n \\ 1 \le l \le n}} \right) \longmapsto (a_{ij} b_{k,l})$$

Taking vector bundles E_1, E_2 on X we get a vector bundle

$$E_1 \otimes E_2$$

called the tensor product of the vector bundles

$$E_1 \otimes E_2 (x) \cong E_1(x) \otimes E_2(x)$$

4/5/2016 In particular

— the functor $E \mapsto E^{\otimes k}$

Taking the usual basis $(e_1, \dots, e_n)$ of $\mathbb{Z}^n$

$(e_{i_1} \otimes \cdots \otimes e_{i_k})_{(i_1, \dots, i_k) \in \{1,\dots,n\}^k}$

is a basis of $(\mathbb{Z}^n)^{\otimes k}$ giving a representation

$$GL_n \longrightarrow GL_{n^k}$$

and $E^{\otimes k}$ is the vector bundle obtained from E

Reminder (tensor algebra)

Given a commutative ring A and a A-module M

$$T^* M = \bigoplus_{n\in\mathbb{N}} T^n(M) \quad \text{where } T^n(M) = M^{\otimes n}$$

is a graded algebra over A, the product being defined by

$$(x_1\otimes\cdots\otimes x_m)\otimes(y_1\otimes\cdots\otimes y_n) = x_1\otimes - \otimes x_m\otimes y_1\otimes - \otimes y_n$$

and

$$T^m(M)\otimes T^n(M) = T^{m+n}(M)$$

we define

$$\Lambda^* M = T^* M \,/\, (x\otimes x,\ x\in M)$$

bilateral ideal generated by $x\otimes x$

This ideal is graded:

$I = (x\otimes x,\ x\in M)$ $\qquad I = \bigoplus_{n\in\mathbb{N}} I_n$ where $I_n = I\cap T^n(M)$

and we define

$$\Lambda^*(M) = T^*(M)/I = \bigoplus_{n\in\mathbb{N}} \Lambda^n(M)$$

where

$$\Lambda^n(M) = T^n(M)/I_n$$

The product in $\Lambda^* M$ is denoted by $\wedge$

$$x\wedge y = (-1)^{m+n}\, y\wedge x \text{ for } x\in\Lambda^m M,\ y\in\Lambda^n M$$

Prop

- if M is a free A-module with a basis $(e_1, -, e_n)$ then $\Lambda^k M$ is free with a basis given by $(e_{i_1}\wedge - \wedge e_{i_k})_{1\le i_1<-<i_k\le n}$

- By defining $\Lambda^k \varphi(x_1 \wedge \dots \wedge x_k) = \varphi(x_1) \wedge \dots \wedge \varphi(x_k)$ we get functor from A-Mod to A-Mod

Exterior product

Thus we have a representation $GL_n \to GL_{\binom{n}{k}}$ and we can define
$\Lambda^k E$ which is a vector bundle of rank $\binom{n}{k}$ for a vector bundle of rank n

In particular
$\det(E) = \Lambda^n E$ is a line bundle.

Symmetric product

Similarly $S^*(M) = T^*(M) / (x \otimes y - y \otimes x,\ x, y \in M)$ is a graded commutative algebra over A and we can define
$S^n E$ which is a vector bundle of rank $n^k - \binom{n}{k}$

- dual

We consider the contragredient representation
$$GL_n \longrightarrow GL_n$$
$$M \longmapsto {}^tM^{-1}$$
We get a functor $\mathcal{P}_n(X) \to \mathcal{P}_n(X)$
we denote by $E^\vee$ the image of the vector bundle of E and call it the dual of E.
$E \longrightarrow E^\vee$ defines a contravariant functor which is an equivalence of category from $\mathcal{P}$ to $\mathcal{P}^o$
$$E^\vee(x) \cong \mathrm{Hom}_{A\text{-mod}}(E, A)$$

- Internal Hom

$$\underline{\mathrm{Hom}}(E, F) = E^\vee \otimes F$$

Exercise

There is an natural equivalence

between

$$\Gamma(X, \underline{Hom}(E,F)) \xrightarrow{\sim} Hom_{v.b.}(E,F)$$

e) Vector bundles and projective modules

Let me state a result from commutative algebra

Theorem / Definition

Let A be a commutative noetherian ring and let P be a finitely generated A-module. Then P is projective if and only if it satisfies the following equivalent conditions:

(i) The functor $M \longmapsto Hom_{A\text{-Mod}}(P, M)$ is exact

(ii) There exists a A-module Q such that $P \oplus Q$ is a free A-module

(iii) For any A-algebra B which is a local ring, $P \otimes_A B$ is a free B-module

(iv) for any prime ideal $\mathfrak{p}$ of A, $P \otimes_A A_{\mathfrak{p}}$ is free

(v) for any maximal ideal $\mathfrak{m}$ of A, $P \otimes_A A_{\mathfrak{m}}$ is free

(v) There exist a primitive element $(f_1, \ldots, f_r) \in A^r$ such that for $i \in \{1, \ldots, r\}$ $P \otimes A[f_i^{-1}]$ is free

(vi) The functor $M \longrightarrow M \otimes_A P$ is exact.

For any prime ideal $\mathfrak{p}$ of A, the rank of the free $A_{\mathfrak{p}}$ module $P \otimes A_{\mathfrak{p}}$ is called the rank of M at $\mathfrak{p}$. This defines a map $Spec(A) \longrightarrow \mathbb{N}$

北京大学

which is locally constant (The inverse image of an integer is an open subset of Spec (A)). If it is constant of value r then one says that M has <u>constant rank</u> r

Remark

If A is integral then Spec(A) is connected and therefore any finitely generated projective module has a constant rank.

Prop

Let A be a commutative noetherian ring

Let $\eta = Id_{Spec(A)} \in [Spec(A)](A)$

The functor $E \to E(\eta)$ defines an equivalence of categories from the category of vector bundles of rank r over Spec (A) to the category of Projective A-modules of constant rank r.

Example

If A is a principal domain, any sub-module of a free module is free and therefore any projective module is free. Thus any vector bundle over Spec(A) is isomorphic to Spec(A) $\times \mathbb{A}^r$ where r is the rank of the vector bundle and the category of vector bundles over Spec(A) is equivalent to the category of free modules of finite rank over A.

北京大学

e) Subbundles, quotient, exact sequences

Definition

A subbundle of bundle E is a subscheme F equipped with a structure of vector bundle over X so that the inclusion map
$$i: F \longrightarrow E$$
is a morphism of vector bundles

Remark

We have commutative diagrams

$$\begin{tikzcd} F \arrow[r, "i"] \arrow[dr, "\pi_F"'] & E \arrow[d, "\pi_E"] \\ & X \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} F\times_X F \arrow[r, "+"] \arrow[d, "i\times i"] & F \arrow[d, "i"] \\ E\times_X E \arrow[r, "+"] & E \end{tikzcd}$$

So there is a unique structure of vector bundle on F which makes it a subbundle of E.

Example

Let E be a vector bundle on a scheme then the zero section $0: X \to E$ defines an isomorphism from X to a subbundle 0_X of E (the rank of this subbundle is 0)

We want to define the kernel of morphisms but there is a problem with that.

Reminder

In a additive category the kernel of a morphism $\varphi: E \to F$ is a morphism $k: K \to A$

such that, for any object H

$$0 \to Hom(H,K) \longrightarrow Hom(H,E) \longrightarrow Hom(H,F)$$
$$\psi \longmapsto k\circ\psi$$

is exact.

The cokernel is defined as the kernel in the opposite category:

The cokernel is a morphism $\gamma : F \to C$ such that, for any object H:

$$0 \to Hom(C,H) \to Hom(F,H) \to Hom(E,H)$$

is exact

Example

Take $X = Spec(\mathbb{Z})$. Take E as the trivial vector bundle of rank 1. As I explained the category of vector bundles over $\mathbb{Z}$ is isomorphic to the category of free $\mathbb{Z}$-modules.

Take the morphism f of vector bundles corresponding to

$$\varphi : \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}$$

For any n

$$Hom(\mathbb{Z}^n, \mathbb{Z}) \xrightarrow{\times 2} Hom(\mathbb{Z}^n, \mathbb{Z})$$
$$\psi \longmapsto \varphi\circ\psi$$

is injective and

$$Hom(\mathbb{Z}, \mathbb{Z}^n) \xrightarrow{\times 2} Hom(\mathbb{Z}, \mathbb{Z}^n)$$
$$\psi \longmapsto \psi\circ\varphi$$

is injective. Thus in the category of vector bundles

$$Ker(f) = 0 \quad \text{and} \quad coker(f)$$

But

2

i) f is not an isomorphism
(and f is not the kernel of its cokernel
since $0 \to \mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z}) \longrightarrow \mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z}) \to 0$
$\psi \longmapsto \varphi \circ \psi$
is not exact)

ii) If we consider the $\mathbb{F}_2$ point of $\mathrm{Spec}(\mathbb{Z})$
$x : \mathrm{Spec}(\mathbb{F}_2) \to \mathrm{Spec}(\mathbb{Z})$
$f : E(x) \longrightarrow E(x)$
is the zero map and has a non trivial kernel and cokernel.
So the kernel does not commute with fibers!

(iii) The cokernel of $\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}$ is not 0 in the category of $\mathbb{Z}$-module
so the functor from the category vector bundles to the category of coherent sheaves does not preserve cokernels

The point is that the category of vector bundle is not an abelian category but it has a nice notion of short exact sequences:

Notation

Let X be a scheme. We denote by $X_{(k)}$ the set of points of dimension k of X. In particular $X_{(0)}$ is the set of closed points of X. For the spectrum of a ring, it corresponds to the set of maximal ideals of the ring.

If $x \in X$, $\mathcal{O}_{X,x}$ is the local ring at x
$m_{X,x}$ its maximal ideal and $k(x) = \mathcal{O}_{X,x}/m_{X,x}$ its residue field

Definition

A sequence

$$0 \to D \xrightarrow{\varphi} E \xrightarrow{\psi} F \to 0$$

of vector bundles over a scheme X is exact if it satisfies the following equivalent conditions

(i) For any point x of X the sequence of $\mathcal{O}_{X,x}$ modules

$$0 \to D(\eta_x) \to E(\eta_x) \to F(\eta_x) \to 0$$

is exact, where $\eta_x : \mathrm{Spec}(\mathcal{O}_{X,x}) \to X$

This condition says exactly that

(ii) Let $\mathcal{D}, \mathcal{E}, \mathcal{F}$ be the sheaf of section of D, E and F respectively. The sequence

$$0 \to \mathcal{D} \to \mathcal{E} \to \mathcal{F} \to 0$$

is exact

(iii) For any closed point x of X the sequence of $K(x)$ vector spaces

$$0 \to D(x) \to E(x) \to F(x) \to 0$$

is exact (here x denotes also the morphism $\mathrm{Spec}(K(x)) \to X$)

(iv) For any commutative ring A and any $x \in X(A)$, the sequence of A-modules

$$0 \to D(x) \to E(x) \to F(x) \to 0$$

is exact

Note that in conditions (i) and (iii) we are considering free module of constant rank. This works only for short exact sequence

Definition of the kernel for vector bundles

- Let $\varphi : E \to F$ be a morphism of vector bundles over the scheme X. Then $\varphi^{-1}(O_X) = E \times_F O_X$

is a closed subscheme of E

Assume that the rank of φ is constant, that is

$$X \longrightarrow \mathbb{N}$$
$$x \longmapsto rk(\varphi_x : E(x) \longrightarrow F(x))$$

is constant, then $\varphi^{-1}(O_X)$ is a subbundle K of E so that the inclusion map is a kernel of φ in the sense of additive categories.

We denote it by $\mathrm{Ker}(\varphi)$

Now the duality is an equivalence of category

So we may define

- If φ is of constant rank, so is $\varphi^\vee : F^\vee \longrightarrow E^\vee$ and $\mathrm{Coker}(\varphi) = \mathrm{ker}(\varphi^\vee)^\vee$.

Example

If S is a subbundle of E then the inclusion map i has constant rank and the quotient E/F is defined as $\mathrm{coker}(i)$

For any commutative ring A and any $x \in X(A)$ $E/F(x)$ is canonically isomorphic to $E(x)/F(x)$ and we shall identify these A modules.

The sequence $0 \to F \to E \to E/F \to 0$ is exact

Up to isomorphism, all exact sequences are of this form

2 Even if φ and ψ have constant rank, the rank of $\psi \circ \varphi$ may not be constant

Example

L trivial line bundle of rank $1 / \mathbb{A}^1$ $\quad L = \mathbb{A}^1 \times \mathbb{A}^1$ (x, t)

$$L \longrightarrow L \oplus L \longrightarrow L$$
$$(x,t) \longmapsto (x, tx, t) \overset{pr_2}{\longmapsto} (x, tx)$$

e) Tangent bundle, cotangent bundle, canonical bundle

Definition

Let A be a noetherian commutative ring.
Let X be smooth connected scheme over $\mathrm{Spec}(A)$.
The tangent bundle over X is defined as the unique scheme TX such that
the functor of points associated to TX
which maps a commutative A-algebra
$$B \to \mathrm{Hom}_{\mathrm{Spec}(A)}(\mathrm{Spec}(B), TX)$$
is isomorphic to the functor
$$B \to \mathrm{Hom}_{\mathrm{Spec}(A)}(\mathrm{Spec}(B[T]/(T^2)), X)$$
with the morphism $\pi : TX \to X$ corresponding to the natural transformation
$$\mathrm{Hom}(\mathrm{Spec}(B[T]/(T^2)), X) \to X(B)$$
induced by $B[T]/(T^2) \longrightarrow B$
$$T \longmapsto 0$$
The scalar multiplication is induced by morphisms
$$B[T]/(T^2) \longrightarrow B[T]/(T^2)$$
$$T \longmapsto bT$$
for $b \in B$
and the addition map might be constructed as follows:
$$TX(B) \times_{X(B)} TX(B) = \mathrm{Hom}\Big(\mathrm{Spec}(B[T]/(T^2)) \underset{\mathrm{Spec}(B)}{\overset{\text{coproduct}}{\amalg}} \mathrm{Spec}(B[T]/(T^2)), X\Big)$$
But the commutative diagram

$$\begin{tikzcd}
B[T_1,T_2]/(T_1^2,T_1T_2,T_2^2) \arrow[r, "\substack{T_1 \mapsto T \\ T_2 \mapsto 0}"] \arrow[d, "\substack{T_1 \mapsto 0 \\ T_2 \mapsto T}"'] \arrow[dr, phantom, "\square"] & B[T]/(T^2) \arrow[d] \\
B[T]/(T^2) \arrow[r] & B
\end{tikzcd}$$

in the category of rings.

which gives an isomorphism

$$\begin{tikzcd}
\operatorname{Spec}(B[T_1,T_2]/(T_1^2,T_1T_2,T_2^2)) & \operatorname{Spec}(B[T]/(T^2)) \coprod_{\operatorname{Spec}(B)} \operatorname{Spec}(B[T]/(T^2)) \arrow[l, "\sim"'] \\
\operatorname{Spec}(B[T]/(T^2)) \arrow[u, "\substack{T_1 \mapsto T \\ T_2 \mapsto T}"] \arrow[ur] &
\end{tikzcd}$$

(See below for a simpler proof)

Remember: the direct limits does not exist in general in the category of rings so it is only in that particular case that the glueing of these spectra is an affine scheme

9/5/2015 **Remark**

a) It is only to check that TX is locally of the form $X \times \mathbb{A}^n$ that we need to assume X to be smooth over $\operatorname{Spec}(A)$. In general, the above construction yields an abelian group scheme TX on X

b) Fibers: Let B be a commutative A-algebra and assume X is affine $X = \operatorname{Spec}(C)$

Let $x \in X(B)$ corresponds to a morphism of C-algebras $\varphi: C \to B$

Now $B[T]/(T^2)$ as a B module is free of rank 2 with a basis given by $(1, \varepsilon)$, where $\varepsilon = \overline{T}$. Write $T_x X \overset{\text{def}}{=} TX(x)$

If $y \in T_x X$, then y corresponds to a morphism
$$\varphi : C \longrightarrow B[T]/(T^2)$$
given by
$$\varphi(c) = \varphi_0(c) + T\,\delta(c)$$
δ is A linear and satisfies
$$\delta(c_1 c_2) = \varphi_0(c_1)\,\delta(c_2) + \delta(c_1)\,\varphi(c_2)$$
So it is a derivation from the A-algebra C into the A-module $B\varepsilon$. We get in that way an isomorphism of B modules
$$T_x X \xrightarrow{\sim} \mathrm{Der}_A(C, B\varepsilon)$$

Example

If $C = A[X_1, \ldots, X_n]/(f_1, \ldots, f_r)$

Then
$$T\,\mathrm{Spec}(C) = \mathrm{Mor}_{A\,alg}\left(A[X_1, \ldots, X_n]/(f_1, \ldots, f_r),\ B[T]/(T^2)\right)$$
can be identified with
$$= \left\{(x_1 + \varepsilon u_1, \ldots, x_n + \varepsilon u_n) \in B[T]/(T^2)^n \;\middle|\; f_i(x_1+\varepsilon u_1, \ldots, x_n + \varepsilon u_n) = 0 \text{ for } i \in \{1, \ldots, r\}\right\}$$
$$= \left\{((x_1, \ldots, x_n), (u_1, \ldots, u_n)) \in (B^n)^2 \;\middle|\; \begin{array}{l} f_i(x_1, \ldots, x_n) = 0 \text{ for } i = 1, \ldots, r \\ \sum \frac{\partial f_i}{\partial x_j}(x_1, \ldots, x_n)\, u_j = 0 \text{ for } i \in [1, r] \end{array}\right.$$
$$\boxed{= \left\{(x, u) \in X(B) \times B^n \;\middle|\; u \in \bigcap_{i=1}^{r} \mathrm{Ker}(d_x f_i)\right\}}$$

Proof of the statement

I have to proof that TX is unique (up to isomorphism) and exists as a vector bundle.

北京大学

Unicity

Since all schemes are obtained by glueing together spectra and the fact that

$$h_X : Y \longmapsto \mathrm{Hom}(Y, X)$$

is a sheaf, h_X is determined by its restriction to spectra of rings. We then apply Yoneda's lemma to get that X is determined by its functor of points

$$B \longmapsto X(B).$$

Existence

We only have to check that X admits a covering $(U_i)_{i \in I}$ by open subscheme so that

$$TX_{|U_i} = TU_i \text{ is a vector bundle } / U_i.$$

We may therefore assume that

$$X = \mathrm{Spec}\ C$$

where $C = A[T_1, \ldots, T_n]/(f_1, \ldots, f_r)$ and $df : \mathbb{A}^n_A \longrightarrow M_{r,n}$ has constant rank.

But then by the example I gave,

$$TX(B) = \{(x, u),\ x \in X(B),\ u \in \ker(d_x f)\}$$

That is, if we see as a morphism between trivial vector bundles,

$$df : \mathbb{A}^n_A \times \mathbb{A}^n_A \to \mathbb{A}^r$$

and $TX = \ker(df)$. $\square$

From now on, I denote G_V for the trivial bundle on V (although it is rather its sheaf of sections)

Definition

- Let X, Y be smooth connected schemes over $\mathrm{Spec}(A)$ and $f : X \to Y$ be a morphism

北京大学

of schemes. Then the natural transformation

$$\mathrm{Hom}_{\mathrm{Spec}(A)}(\mathrm{Spec}(B[T]/(T^2)), X) \xrightarrow{-\circ f} \mathrm{Hom}_{\mathrm{Spec}(A)}(\mathrm{Spec}(B[T]/(T^2)), Y)$$

induces a map

$$\begin{array}{ccc} TX & \longrightarrow & TY \\ \downarrow \pi & & \downarrow \pi \\ X & \xrightarrow{f} & Y \end{array}$$

such that

and a morphism of vector bundles over X:

$$df : TX \to f^*(TY)$$

- If f is a closed immersion, which means that df is of constant rank $\dim(X)$, then

$$\mathcal{N}_{X/Y} = f^*(TY)/df(TX)$$

as a vector bundle on X.

- The cotangent bundle is the dual of the tangent budle, it is denoted by $\Omega^1 X$. Its sections are the 1-forms. We put $\Omega^k X = \Lambda^k(\Omega^1 X)$ its section are the k-forms.

There is a product

$$\Gamma(U, \Omega^p X) \times \Gamma(U, \Omega^q X) \to \Gamma(U, \Omega^{p+q} X)$$

- The canonical line bundle is

$$\omega_X = \Omega^n X$$

the anticanonical line bundle is its dual

$$\omega_X^{-1} = \omega_X^\vee \cong \det(TX).$$

This line bundle is going to play a central role in our game.

Examples

1) The projective space

First, remember that we defined a line bundle $\mathcal{O}_{\mathbb{P}^n}(1)$ on the projective space

$$\mathcal{O}_{\mathbb{P}^n}(k) = \begin{cases} \mathcal{O}_{\mathbb{P}^n}(1)^{\otimes k} & \text{if } k \geq 1 \\ \text{trivial line bundle} & \text{if } n=0 \\ (\mathcal{O}_{\mathbb{P}^n}(1)^\vee)^{\otimes -k} & \text{if } k<0 \end{cases}$$

It is a line bundle on $\mathbb{P}^n$. The sections of $\mathcal{O}_{\mathbb{P}^n}(1)$ give by duality $n+1$ morphisms of vector bundle

$$X_i : \mathcal{O}_{\mathbb{P}^n}(-1) \longrightarrow \mathcal{O}_{\mathbb{P}^n}$$

and

$f : (X_0, \dots, X_n) : \mathcal{O}_{\mathbb{P}^n}(-1) \longrightarrow \mathcal{O}_{\mathbb{P}^n}^{n+1}$

By construction X_i does not vanish on

$$U_i = \operatorname{Spec}(k[X_0, \dots, \hat{X}_i, \dots, X_n])$$

Thus f is of constant rank 1, it give en embedding of $\mathcal{O}_{\mathbb{P}^n}(-1)$ in $\mathbb{P}^n \times \mathbb{A}^{n+1}_{\mathbb{P}^n}$

Looking at fibres, we get for any commutative ring A and any $x \in \mathbb{P}^n(A)$

$$\mathcal{O}_{\mathbb{P}^n}(-1)(x) \subset A^{n+1}$$

is a projective submodule of constant rank 1. Moreover everywhere locally it is a direct factor so the quotient $Q = A^{n+1}/\mathcal{O}_{\mathbb{P}^n}(-1)(A)$ is everywhere locally free and hence projective By definition of projective modules

$$\mathrm{Mor}(Q, A^{n+1}) \to \mathrm{Hom}(Q,Q) \to 0 \quad \text{is exact}$$
$$s \longleftarrow\!\shortmid \mathrm{Id}_Q$$

and this gives a splitting

$$0 \to G_{\mathbb{P}^n}(-1)(A) \to A^{n+1} \underset{s}{\to} Q \to 0$$

and thus

$$A^{n+1} = Q \oplus \, g\left(G_{\mathbb{P}^n}(-1)(A)\right)$$

In fact, we get in that way

Proposition

The map

$$\mathbb{P}^n(A) \longrightarrow g(G_{\mathbb{P}^n}(-1)(A))$$

is a bijection from the A-points of $\mathbb{P}^n$ to the set of submodules L of A^{n+1} such that

(i) L is a direct summand:
$\exists Q \subset A^{n+1}$ such that $L \oplus Q = A^{n+1}$

In particular L is projective

(ii) L is of rank 1

Note that it is always worthwhile to describe a space as a moduli space, that is to have a nice interpretation of the functor of points.

Remark

If A is a principal ideal ring and $(x_0, -, x_n) \in A^{n+1}$ is primitive that is $\exists (u_0, -, u_n) / \sum_{i=0}^{n} u_i x_i = 1$

Then let

$$L = A(x_1, \text{—}, x_n)$$
$$Q = \ker \left(A^{n+1} \longrightarrow A \right)$$
$$(\, _0, -, \, _n) \longmapsto \sum u_i x_i$$

We have $A^{n+1} = L \oplus Q$

2 Remember that in general a projective module of rank 1 is not generated by one of its elements

Now let us turn back to the tangent space

Let $x \in \mathbb{P}^n(A)$ corresponding to $L \subset A^{n+1}$

We want to describe the tangent space at x

As a A-module $(A[T]/(T^2))^{n+1} = A^{n+1} \oplus \varepsilon A^{n+1}$

We apply our description of points to the ring $B = A[T]/(T^2)$. A point $y \in T_x X$ corresponds to a B-submodule $M \subset A^{n+1} \oplus \varepsilon A^{n+1}$ such that $pr_1(M) = L$ and it is a direct factor of rank 1

From $\varepsilon(x + \varepsilon y) = \varepsilon x$

We get $\varepsilon M = \varepsilon L \subset \varepsilon A^{n+1}$

If A is a principal domain, L is free of rank 1 generated by a primitive element u

Let $w \in M$ be of the form $w = u + \varepsilon v$

Then $(u + \varepsilon v, \varepsilon u)$ is a basis of the A-module M

(You can complete $(u + \varepsilon v, \varepsilon u)$ in a basis of $A^{n+1} + \varepsilon A^{n+1}$

$A(u+\varepsilon v) + \varepsilon u A \subset M$ which is free of rank 2, we get equality)

We get $\varepsilon A_{n+1} \cap M / \varepsilon M$ is 0 locally

and therefore $\varepsilon A_{n+1} \cap M = \varepsilon M$

and $L \simeq M/\varepsilon M \subset A^{n+1} \oplus \varepsilon(A^{n+1}/L)$

Thus $M/\varepsilon M$ is the graph Γ_u of a morphism $u : L \to \varepsilon(A^{n+1}/L)$

Conversely, one can check that given $u : L \to A^{n+1}/L$

$\{x + \varepsilon y \in A^{n+1} + \varepsilon A^{n+1} \mid x \in L,\ \bar{y} = u(x) \text{ in } A^{n+1}/L\}$

is a B-submodule of $A^{n+1} + \varepsilon A^{n+1}$ which satisfies the conditions.

So we may summarize as follows

Conclusion

Let $x \in \mathbb{P}^n(A)$ corresponds to the A-submodule $L \subset A^{n+1}$, then there is a canonical isomorphism

$$T_x \mathbb{P}^n \xrightarrow{\sim} Hom(L, A^{n+1}/L)$$

Remark

Using the fact that L is projective,

$$Hom(L, A^{n+1}/L) \xrightarrow{\sim} A^{n+1}/L \otimes L^\vee$$
$$\xrightarrow{\sim} A^{n+1} \otimes L^\vee / L \otimes L^\vee$$

Thus we get an exact sequence

$$0 \to \mathcal{O}_{\mathbb{P}^n} \xrightarrow{(X_0, \dots, X_n)} \mathcal{O}_{\mathbb{P}^n}(1)^{n+1} \to T\mathbb{P}^n \to 0$$ -1

In particular

$$\omega_{\mathbb{P}^n}^{-1} \xrightarrow{\sim} \mathcal{O}_{\mathbb{P}^n}(n+1)$$

2) Let A be an integral domain $K = Fr(A)$

Let $V \subset \mathbb{P}^n_A$ be defined by

$$f_i(x_0, \dots, x_n) = 0 \quad \text{for } i \in \{1, \dots, r\}$$

where f_i is homogeneous of degree d_i

that is $f_i(TX_0, \dots, TX_n) = T^{d_i} f(X_0, \dots, X_n)$

for any $x \in \mathbb{P}^n(A)$ corresponding to $L \subset A^{n+1}$

$K \otimes L \subset K^{n+1}$ is a vector space of dim 1

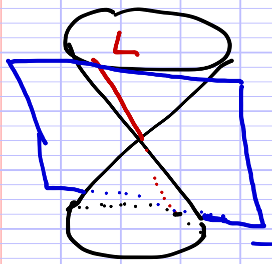
So for $(x_0, \dots, x_n) \in L - \{0\}$, $(y_0, \dots, y_n) \in L - \{0\}$

$$f_i(x_0, \dots, x_n) = 0 \Leftrightarrow f_i(y_0, \dots, y_n) = 0$$

$V(A)$ corresponds to the set L

such that $f_i|_L = 0$ for $i \in \{1, \dots, r\}$.

Assume V smooth over $\operatorname{Spec} A$



Over a field k

$W = \pi^{-1}(V) \cup \{0\} \subset \mathbb{A}^{n+1}_k$

defined by $f_i = 0$

$x \in X(k)$ corresponds to a line $L \subset W$

$T_L W$ $\quad T_L W = \bigcap_{i=1}^{r} \operatorname{Ker} d_y f_i \subset k^{n+1}$

for $y \in L - \{0\}$

$$T_x V \xrightarrow{\sim} \operatorname{Hom}(L, T_L W/L) \subset T_x \mathbb{P}^n.$$

In a more intrinsic manner

Prop

The space $\Gamma(\mathbb{P}^n_A, \mathcal{O}_{\mathbb{P}^n}(d))$ is isomorphic to the space of homogeneous polynomials of degree d over A

See, for example HARTSHORNE's book (prop. 5.13)

Let $\mathcal{O}_V(n) = i^{-1}(\mathcal{O}_{\mathbb{P}^n}(n)) \qquad i: V \to \mathbb{P}^n$

$\frac{\partial f}{\partial x_i}$ defines a morphism of vector bundle

$$\mathcal{O}_V(1) \longrightarrow \mathcal{O}_V(d_i)$$

and therefore

$d f_i$ may be seen as morphism of vector bundles : $\mathcal{O}_V(1)^{n+1} \longrightarrow \mathcal{O}_V(d_i)$

The formula

$$\sum_{i=0}^{n} x_i \frac{\partial f}{\partial x_i} = d_i f$$

implies it vanishes on the image of

$$\mathcal{O}_V \xrightarrow{(x_0 \dots x_n)} \mathcal{O}_V(1)^{n+1}$$

We get a morphism

$$df : i^*(T\mathbb{P}^n) \longrightarrow \bigoplus_{i=1}^{r} \mathcal{O}_V(d_i)$$

Since V is smooth this morphism has constant rank and

$$T V \simeq \ker(df)$$

In particular if V is a complete intersection $r = n - \dim(V)$ we have an exact sequence

$$0 \to TV \to i^*(T\mathbb{P}^n) \to \bigoplus_{i=1}^{r} \mathcal{O}(d_i) \to 0$$

and $\omega_V^{-1} \simeq \det(i^*(T\mathbb{P}^n)) \otimes \det(\bigoplus_{i=1}^{r} \mathcal{O}(d_i))^{-1} = \mathcal{O}_V(n+1-\sum_{i=1}^{r} d_i)$

2) The Picard group

Definition

On smooth varieties there are several equivalent definitions:
The Picard group of a scheme V is the set of isomorphism classes of line bundles over V equipped with $\otimes$
The neutral element is $\mathcal{O}_V$,
The opposite of L is the dual $L^\vee$.
It is denoted by $\mathrm{Pic}(V)$.

Examples

- If A is a principal ring $\mathrm{Pic}(\mathrm{Spec}(A)) = \{0\}$
- The map
$$\mathbb{Z} \to \mathrm{Pic}(\mathbb{P}^n), \quad k \mapsto \mathcal{O}_{\mathbb{P}^n}(k)$$
is an isomorphism of groups (See HARTSHORNE, corollary 6.17)

Definition

Let k be a field, $\bar{k}$ an algebraic closure of k

- A nice variety over k is a smooth, projective variety over k which is geometrically integral (that is $V_{\bar{k}}$ is integral)

Theorem

Let V be a nice variety / field k, $n = \dim(V)$

The map $\quad \mathrm{Div}(V) \longrightarrow \mathrm{Pic}(V)$

$$D \longmapsto \mathcal{O}(D)$$

induces an exact sequence of abelian group

$$0 \to k^* \to k(V)^* \xrightarrow{\mathrm{div}} \mathrm{Div}(V) \longrightarrow \mathrm{Pic}(V) \to 0$$

(HARTSHORNE, §1.6)

$$\mathrm{Div}(V) = \bigoplus_{P \in V_{(n-1)}} \mathbb{Z}P$$

The reason for which the Picard group plays a central role in our game is the following one:

Remark

Let $\phi : V \to \mathbb{P}^n_k$ be a morphism of k-varieties

Then

$L = \phi^*(\mathcal{O}_{\mathbb{P}^n}(1))$ defines an element in $\mathrm{Pic}(V)$

and
$$\begin{array}{ccc} V & \longrightarrow & \mathbb{P}^n_k \\ & \searrow^{s_i} & \downarrow X_i \\ & & \mathcal{O}_{\mathbb{P}^n}(1) \end{array}$$
defines $n+1$ sections s_i of L such that

$$(*) \qquad \bigcap_{i=0}^{n} \{ x \mid s_i(x) = 0 \text{ in } L(x) \} = \emptyset$$

Conversely given a line bundle L and $s_0, \dots, s_n \in \Gamma(V, L)$ such that $(*)$, this defines a morphism

$$\phi : V \longrightarrow \mathbb{P}^n_k$$

by $(u_0, \dots, u_n) \in \phi(x) \iff u_i s_j(x) = u_j s_i(x)$ for $i, j \in \{0, \dots, n\}$

(In fact $\phi(x) = \mathrm{Ker}(s \mapsto s(x))^\perp \subset \Gamma(V, L)^\vee$ dual)

Remember that heights were defined by such morphisms

Up to linear transformation the morphism is determined

北京大学

by the class of L in the Picard group

Definition

$L \in Pic(V)$ is said to be effective if $\Gamma(V, L) \neq \{0\}$

11/4/2016

3) Grothendieck ring $K_0(X)$

Definition

Let X be a connected noetherian scheme

Let $K_0(X)$ be the group

- generated by $[E]$ where E is a vector bundle $/X$
- relations: for any short exact sequences

$$0 \to F \to E \to Q \to 0,$$

$$[E] = [F] + [Q]$$

There is a unique structure of ring on $K_0(X)$ which satisfies

$$[E].[F] = [E \otimes F]$$

Remarks

1) It follows from the fact that the tensor by a projective module is exact that

If $0 \to F \to E \to Q \to 0$ is exact

then $0 \to F \otimes G \to E \otimes G \to Q \otimes G \to 0$ is exact

and therefore the product is well defined

2) There is another operation on $K_0(X)$

$$\lambda_i : K_0(X) \longrightarrow K_0(X)$$

which satisfies

$$\lambda_i([E]) = [\Lambda^i E]$$

and

$$\lambda_i(x+y) = \sum_{a+b=i} \lambda_a(x)\lambda_b(y).$$

$K_0(X)$ is what is called a λ-anneau (SGA 6).

Prop

- $rk : K_0(X) \to \mathbb{Z}$ is a morphism of rings. Its kernel I is called the augmentation ideal
- The determinant defines a group homomorphism

$$K_0(X) \longrightarrow Pic(X)$$
$$[E] \longrightarrow [\det(E)]$$

Indeed if $0 \to F \to E \to Q \to 0$ is exact $\det(E) \simeq \det(F) \otimes \det(Q)$.
Later, I shall explain an arithmetic analog of this ring. Now let us turn back to points of bounded height

Examples

* If A is a principal domain, any projective A module of finite rank is free. So they are classified by their rank

$$K_0(\mathrm{Spec}(A)) \longrightarrow \mathbb{Z}$$
$$[E] \longmapsto rk(E)$$

is an isomorphism

* For $\mathbb{P}^n$, we have a morphism of rings

$$ev : \mathbb{Z}[T] \to K_0(\mathbb{P}^n)$$
$$T \longmapsto [\mathcal{O}_{\mathbb{P}^n}(1)]$$

Theorem

ev induces an isomorphism of rings

$$\mathbb{Z}[T] / (T-1)^{n+1} \xrightarrow{\sim} K_0(\mathbb{P}^n)$$

This is rather difficult to prove.

Idea (See QUILLEN Higher K-theory)

The category of coherent sheaves on X is an abelian category, so we can define

$K_0'(X)$ = group generated by isomorphism classes of coherent sheave and relations given by the short exact sequences

We have a morphism $K_0(X) \longrightarrow K_0'(X)$ which is an isomorphism if X is smooth and from the exact sequence of sheaves

$$0 \to \mathcal{O}_{\mathbb{P}^n}(-1) \xrightarrow{X_i} \mathcal{O}_{\mathbb{P}^n}(1) \to \mathcal{O}_{H_i} \to 0$$

and the fact that

$$\mathcal{O}_{H_i} \otimes_{\mathcal{O}_{\mathbb{P}^n}} \mathcal{O}_{H_j} \xrightarrow{\sim} \mathcal{O}_{H_i \cap H_j}$$

hyperplane

we get a morphism $\mathbb{Z}[T]/_{(T-1)^{n+1}} \longrightarrow K_0(X)$

Then the result is a consequence of the existence of explicit resolutions:

For any vector bundle on $\mathbb{P}^n$, there exists a surjective morphism

$$\mathcal{O}_{\mathbb{P}^n}(-m)^k \twoheadrightarrow F$$

by taking the kernel of this morphism and iterating we get a resolution

$$\mathcal{O}_{\mathbb{P}^n}(-m_r)^{k_r} \to \cdots \to \mathcal{O}_{\mathbb{P}^n}(-m_1)^{k_1} \to F \to 0$$

The problem is to shows that it stops. Using cohomology,

Theorem There exists a finite resolution of this type

2) In general $K_0(X)$ is extremely big (eg not finitely generated).

4) Back to heights

a) Absolute values

Definition

An absolute value on a field $\mathbb{K}$
is a map $|\cdot| : \mathbb{K} \longrightarrow \mathbb{R}_{\geq 0}$ such that

(i) $|x| = 0 \Leftrightarrow x = 0$

(ii) $\forall x, y \in \mathbb{K} \quad |xy| = |x|\,|y|$

(iii) $\forall x, y \in \mathbb{K} \quad |x+y| \leq |x| + |y|$

$|\cdot|$ is said to be ultrametric if

(iii') $\forall x, y \in \mathbb{K}, \quad |x+y| \leq \sup(|x|, |y|)$

archimedean otherwise

Examples

- On any field

$$\begin{aligned} \mathbb{K} &\longrightarrow \mathbb{R}_{\geq 0} \\ x &\longmapsto |x| = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{otherwise} \end{cases} \end{aligned}$$

is an absolute which is called trivial

- On $\mathbb{Q}$: $\begin{cases} |\cdot|_\infty \text{ usual absolute value} \\ p \text{ prime} \\ \left|\dfrac{a}{b}\right|_p = p^{v_p(b) - v_p(a)} \text{ if } a, b \neq 0 \end{cases}$

Put $\mathcal{V}\!\ell(\mathbb{Q}) = \{\text{prime numbers}\} \cup \{\infty\}$
one has

$$\forall x \in \mathbb{Q}^*, \quad \prod_{v \in \mathcal{V}\!al(\mathbb{Q})} |x|_v = 1 \quad \text{(product formula)}$$

Remark

If $|\cdot|$ is ultrametric
$\{x \in K \mid |x| \leq 1\}$ is a subring $\mathcal{O}_K$ of K
and $\{x \in K \mid |x| < 1\}$ is an ideal of $\mathcal{O}_K$.

Definition

- For an absolute value $|\cdot|$ on $\mathbb{K}$

$d(x,y) = |x-y|$ defines a distance on $\mathbb{K}$
The corresponding topology on $\mathbb{K}$ is called the topology defined by $|.|$
It gives the structure of topological field on $\mathbb{K}$:
$+, \times, -, (\cdot)^{-1}$ are continuous

- $|\cdot|$ and $|\cdot|'$ are said to be <u>equivalent</u> if they define the same topology

<u>Proposition</u>

Let $|\cdot|$ and $|\cdot|'$ be absolute values on $\mathbb{K}$
The following assertions are equivalent

(i) $|\cdot|$ and $|\cdot|'$ are equivalent,
(ii) $\{x \in \mathbb{K} \mid |x| < 1\} = \{x \in \mathbb{K} \mid |x|' < 1\}$
(iii) $\exists \lambda > 0$ such that $\forall x \in \mathbb{K}$, $|x|' = |x|^\lambda$

<u>Reference</u>

JACOBSON Basic algebra II §9
NEUKIRCH Algebraic number theory § II. 3

<u>Definition</u>

A place of field $\mathbb{K}$ is a topology defined by a non trivial absolute value on $\mathbb{K}$
I denote by $Pl(\mathbb{K})$ the set of places of $\mathbb{K}$

<u>Theorem</u> [OSTROWSKI]

Let $\mathcal{P}$ be the set of prime integers

$$\begin{aligned} \mathcal{P} \cup \{\infty\} &\longrightarrow Pl(\mathbb{K}) \\ v &\longmapsto |\cdot|_v \end{aligned}$$

is a bijective map.

b) Completions

Let $\mathbb{K}$ be a field and let v be a place of $\mathbb{K}$ defined by an absolute value $|\cdot|$.
The completion of $\mathbb{K}$ for v is denoted $\mathbb{K}_v$; it is a $\mathbb{K}$-algebra which is a field with an absolute value which extends $|\cdot|$ so that

(i) $\mathbb{K}_v$ is complete for the corresponding topology

(ii) $\mathbb{K}$ is dense in $\mathbb{K}_v$

Up to isomorphism, this characterize $\mathbb{K}_v$

Example

- $\mathbb{R} = \mathbb{Q}_\infty$
- $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ for $|\cdot|_p$

Construction in a particular case

Définition

A discrete valuation on a field $\mathbb{K}$ is a map

$$v : \mathbb{K} \longrightarrow \mathbb{Z} \cup \{+\infty\}$$

such that

(i) $v^{-1}(\{+\infty\}) = \{0\}$

(ii) $\forall x, y \in \mathbb{K} \quad v(xy) = v(x) + v(y)$

(iii) $\forall x, y \in \mathbb{K} \quad v(x+y) \geq \min(v(x), v(y))$

with the usual convention:

$$x + (+\infty) = +\infty \qquad \min(x, +\infty) = x.$$

Remark

a discrete valuation define a place of $\mathbb{K}$ via

$$|x|_v = \lambda^{-v(x)} \text{ for some } \lambda > 1$$

北京大学

Note that the place does not depend on the choice of λ. This place is ultrametric with a ring and ideal given by

$$\mathcal{O}_v = \{ x \in \mathbb{K} \mid v(\mathcal{O}_v) \geq 0 \}$$
$$\mathfrak{m}_v = \{ x \in \mathbb{K} \mid v(\mathcal{O}_v) \geq 1 \}$$

<u>Example</u>

If p is a prime number $a, b \in \mathbb{Z}$, $b \neq 0$

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$$

is a discrete valuation which defines the place corresponding to p.

<u>Lemma</u>

If v is a discrete valuation, then $\mathcal{O}_v$ is a euclidean ring (with euclidean division) and any ideal of $\mathcal{O}_v$ is of the form $\mathfrak{m}_v^k$ for some $k \in \mathbb{N}$. In particular $\mathfrak{m}_v$ is the only maximal ideal in $\mathcal{O}_v$

$$\mathbb{K}_v = \mathcal{O}_v / \mathfrak{m}_v \text{ is a field.}$$

<u>Proof</u>

- Since $\mathcal{O}_v = \{ x \in \mathbb{K} / v(x) \geq 0 \}$

$$a \mid b \text{ in } \mathcal{O}_v \iff v(b) \leq v(a).$$

So if $a, b \in \mathcal{O}_v$ with $b \neq 0$

either

$$a = b \times \frac{b}{a} + 0 \quad \text{if } v(b) \leq v(a)$$

or

$$a = b \times 0 + a \quad \text{if } v(a) \leq v(b)$$

$v : \mathcal{O}_v - \{0\} \longrightarrow \mathbb{N}$ gives the euclidean division.

- $\mathrm{Im}(v_{|\mathbb{K}^*})$ is a subgroup of $\mathbb{Z}$
let $d \in \mathbb{N}$ be its nonnegative generator
If $d = 0$ then $\mathbb{K} = \mathcal{O}_v$ and it has two ideals m_v^0 and $m_v = \{0\}$
Otherwise let $\pi \in m_v$ be such $v(\pi) = d$
We have
$$m_v = (\pi)$$
(π is called a uniformizer)
Let I be a non zero-ideal of $\mathcal{O}_v$
and let $k = \min\{v(x),\ x \in I - \{0\}\}$
and let $x \in I$ be such that $v(x) = k$
By the proof of the fact that euclidean rings are principal
$$I = (x) = (\pi^k) = m_v^k. \quad \square \quad]$$

<u>Notation</u>

Let $\hat{\mathcal{O}}_v = \varprojlim_{k \geq 1} \mathcal{O}_v / m_v^k$, $\hat{\mathbb{K}}_v = \mathrm{Frac}(\hat{\mathcal{O}}_v)$

$\hat{\mathcal{O}}_v$ is an $\mathcal{O}_v$-algebra, we put $\hat{m}_v = m_v \hat{\mathcal{O}}_v = \pi \hat{\mathcal{O}}_v$
and define
$$\hat{v}(x) = \max\{k \in \mathbb{Z} \mid \pi^{-k} x \in \hat{\mathcal{O}}_v\}$$
for $x \in \hat{\mathbb{K}}_v$

<u>Proposition</u>

(i) The morphism $\mathcal{O}_v \to \hat{\mathbb{K}}_v$ extends to a morphism $\mathbb{K} \to \hat{\mathbb{K}}_v$

(ii) $\hat{v}$ defines a discrete valuation on $\hat{\mathbb{K}}_v$ which extends v.

(iii) As a $\mathbb{K}$ algebra with the place defined by $\hat{v}$,

$\widehat{\mathbb{K}}_v$ is the completion of $\mathbb{K}$ for v
and $\widehat{\mathcal{O}}_v$ is the closure of the image of $\mathcal{O}_v$ in $\widehat{\mathbb{K}}_v$

(iv) The morphism of rings
$$\mathcal{O}_v/\mathfrak{m}_v^k \longrightarrow \widehat{\mathcal{O}}_v/\widehat{\mathfrak{m}}_v^k$$
is an isomorphism

Proof

(i) The kernel of the morphism
$$\mathcal{O}_v \longrightarrow \varprojlim_k \mathcal{O}_v/\mathfrak{m}_v^k$$
is $\bigcap_{k\in\mathbb{N}} \mathfrak{m}_v^k = \{x \in \mathcal{O}_v \mid v(x) \geq k,\ \forall k \in \mathbb{N}\}$
$= \{x \in \mathcal{O}_v \mid v(x) = +\infty\} = \{0\}$

So $\mathcal{O}_v \hookrightarrow \widehat{\mathcal{O}}_v$
and we get a morphism $\mathbb{K} \longrightarrow \widehat{\mathbb{K}}_v$
which means that we may see $\widehat{\mathbb{K}}_v$ as a $\mathbb{K}$-algebra

(ii) Let $x \in \widehat{\mathcal{O}}_v$, $\hat{v}$ is well defined on $\widehat{\mathcal{O}}_v$
$$x = \left(\overline{x_k}^k\right)_{k\geq 1} \quad \text{where } x_k \in \mathcal{O}_v$$
and $\overline{x_k}^k$ is its reduction modulo $\mathfrak{m}_v^k$
so that $\overline{x_k}^l = \overline{x_l}^l$ for $l < k$.

This means that
$$x_l - x_k \in \mathfrak{m}_v^l \text{ for } l < k$$
$$\iff v(x_l - x_k) \geq \min(l,k) \quad \text{for any } l, k$$

- If $\overline{x_1} \neq 0$, we have $v(x_k) = 0$ for any $k \geq 1$ and $x_k \in \mathcal{O}_v^*$, so $\overline{x_k}^k \in \left(\mathcal{O}_v/\mathfrak{m}_v^k\right)^*$

Moreover
$$\overline{\left(x_k^{-1}\right)}^l = \left(\overline{x_l}^l\right)^{-1} = \overline{x_l^{-1}}^l$$
and
$$\left(\overline{x_k^{-1}}\right)_{k\geq 1} \text{ is an inverse of } x \text{ in } \widehat{\mathcal{O}}_v.$$

- Let $\ell = \sup\{k \mid \overline{x_k}^{\,k} = 0\} \in \mathbb{N}\cup\{+\infty\}$
we can take $x_k = 0$ for $k \leq \ell$ and then
we have $x_k \in \mathfrak{m}_v^\ell$ for any k
So $\pi^\ell \mid x_k$ and $x_k \pi^{-\ell} \in \mathcal{O}_v$
Let $y = (\pi^{-\ell} x_{k+\ell})_{k\geq 1}$ we have $\pi^\ell y = x$
so $\hat{v}(x) \geq \ell$
Conversely if $x = \pi^m y$, $y = (y_k)_{k\geq 1}$
then
$$\overline{x_k}^{\,k} = \pi^m \overline{y_k}^{\,k} = 0 \text{ for } k \leq m$$
So $\ell = \hat{v}(x)$.
- for $x \neq 0$, $\pi^{-\hat{v}(x)} x \in \widehat{\mathcal{O}}_v^*$
Let $x \in \widehat{\mathbb{K}}_v$, $x = \frac{a}{b}$, $a, b \in \widehat{\mathcal{O}}_v$, $b \neq 0$
$\pi^{\hat{v}(b)} x = a\,(b\,\pi^{-\hat{v}(b)})^{-1} \in \widehat{\mathcal{O}}_v$
so $\hat{v}$ is well defined
and from the description of $\hat{v}$ on $\widehat{\mathcal{O}}_v$
$\{x \in \widehat{\mathbb{K}}_v \mid v(x) = +\infty\} = \{0\}$
Thus $\hat{v}$ is a discrete valuation on $\widehat{\mathbb{K}}_v$
Moreover $\hat{v}$ induces v on $\mathcal{O}_v$
and therefore on $\mathbb{K} = \mathrm{Fr}(\mathcal{O}_v)$.

(iii) Let us show that $\widehat{\mathbb{K}}_v$ is complete
Let $(x_n)_{n\in\mathbb{N}}$ be a Cauchy sequence in $\widehat{\mathbb{K}}_v$
that is for any N there exists M so that
$$\forall p, q \geq M, \quad \hat{v}(x_p - x_q) \geq N$$
By removing the first terms of the sequence if necessary, we may assume that
$$y_k = x_k - x_0 \in \widehat{\mathcal{O}}_v \text{ for } k \in \mathbb{N}$$
and $(y_k)_{k\in\mathbb{N}}$ is a Cauchy sequence as well

for $j \geq 1$
let $k_j = \min\{M \mid \forall p, q \geq M \ \hat{v}(y_p - y_q) \geq j\}$
and put z_j = the image of y_{k_j} in $\mathcal{O}_v / m_v^j$

$(\hat{\mathcal{O}}_v = \varprojlim_{k \geq 1} \mathcal{O}_v / m_v^k)$

we have $z = (z_k)_{k \geq 1} \in \hat{\mathcal{O}}_v$

and $\hat{v}(z - y_n) \geq j$ for $n \geq k_j$
so

$$y_n \xrightarrow[n \to +\infty]{} z \quad \text{so} \quad x_n = y_n + x_0 \xrightarrow[n \to +\infty]{} z + x_0$$

so $\hat{\mathbb{K}}_v$ is complete
. Moreover if $x = (\overline{x_k}^{\,\ell})_{k \geq 1}$ in $\hat{\mathcal{O}}_v$

$$\text{Then } x_k \xrightarrow[k \to +\infty]{} x \text{ in } \hat{\mathcal{O}}_v$$

So $\hat{\mathcal{O}}_v \subset \overline{\mathcal{O}_v}$ but as $\hat{\mathcal{O}}_v = \{x \in \hat{\mathbb{K}}_v \mid |x|_v \leq 1\}$
it is closed and $\hat{\mathcal{O}}_v = \overline{\mathcal{O}_v}$
Since any element of $\hat{\mathbb{K}}_v$ may be
written as $\frac{a}{\pi^k}$ with $a \in \hat{\mathcal{O}}_v$, $\mathbb{K}$ is dense in $\hat{\mathbb{K}}_v$.

(iv) If $x = (\overline{x_k}^{\,k})_{k \geq 1}$ then $x - x_\ell \in \hat{m}_v^\ell$

so $\mathcal{O}_v / m_v^\ell \longrightarrow \hat{\mathcal{O}}_v / \hat{m}_v^\ell$ is surjective
it is injective since

$$\begin{aligned} \mathcal{O}_v \cap \hat{m}_v^\ell &= \{x \in \mathcal{O}_v \mid \hat{v}(x) \geq \ell\} \\ &= \{x \in \mathcal{O}_v \mid v(x) \geq \ell\} \\ &= m_v^\ell . \ \square] \end{aligned}$$

We may put $\mathbb{K}_v = \hat{\mathbb{K}}_v$

北京大学

Corollary

If K_v is a finite field, then $\widehat{G_v}$ is profinite, compact and $\widehat{K}_v$ locally compact

Proof

- (π^k) is a basis of the K_v vector space $\mathfrak{m}_v^k / \mathfrak{m}_v^{k+1}$

  So $G_v / \mathfrak{m}_v^k$ is finite for any k which, by definition, says that $\widehat{G_v}$ is profinite
- The topology on $\widehat{G_v}$ coincide with the topology induced by the product of the discrete topology on $G_v / \mathfrak{m}_v^k$:

Indeed the topology on $\widehat{G_v}$ is generated by the open subsets of the form

$$\{y \mid \hat{v}(y-x) \geq k\} \text{ for some } x \in \widehat{G_v}, k \in \mathbb{N}$$
$$\shortparallel$$
$$pr_k^{-1}(pr_k(x))$$

where $pr_k : \widehat{G_v} \to G_v / \mathfrak{m}_v^k$

and the topology induced by the product topology is precisely generated by open subsets of this form. Then we apply Tychonov's theorem to get that

$$\widehat{G_v} \text{ is compact}$$

for any $x \in \widehat{K}_v$ $x + \pi^k \widehat{G_v}$ is a compact neighbourhood of x, so $\widehat{K}_v$ is locally compact

Remark

You should think of $\widehat{G_v}$ as a Cantor set:

let $E_0 = \bigcup_{n \in \mathbb{N}} [2n, 2n+1] \subset \mathbb{R}$

Let $q = \# K_v$

$$K_0 = [0,1]$$

$$K_n = K_{n-1} \cap (2q-1)^{-n} E_0 \text{ for } n \geq 1$$

$$K = \bigcap_{n \in \mathbb{N}} K_n$$

write $K_v = \{\bar{x}_1, \dots, \bar{x}_q\}$

Then any element in $\hat{G}_v$ may be uni written as

$$a = \lim_{k \to +\infty} \left(\sum_{i=0}^{k} x_{i_k} \pi^i \right)$$

with $(i_k)_{k \in \mathbb{N}} \in \{1, \dots, q\}^{\mathbb{N}}$

(Indeed $\overline{\sum_{i=0}^{k} x_{i_k} \pi^i}^{\,k+1} = p_{k+1}(a)$ determine $i_0, \dots, i_k$)

and
$$\begin{aligned} \hat{G}_v &\longrightarrow K \\ a &\longmapsto \sum_{k \in \mathbb{N}} \frac{2 i_k - 2}{(2q-1)^{k+1}} \end{aligned}$$
is a homeomorphism

(I leave it as an exercise, write numbers in $[0,1]$ using $(2q+1)$ as a numeration basis).

In fact there is a very general result

<u>Proposition</u>

Let K be a compact non empty metric space such that

(i) K is <u>totally disconnected</u>: For any $x, y \in K$ there exist open subsets U and V such that

$$x \in U, \ y \in V, \ U \cap V = \emptyset$$

(ii) K is perfect : For any non empty open subset U in V, $\# U \geq 2$.
Then there is an homeomorphism from K to the usual dyadic Cantor set

Definition
The v-adic topology on $\mathbb{P}^n(\mathbb{K}_v)$ is the quotient topology for the projection $\pi : \mathbb{K}_v^{n+1} - \{0\} \longrightarrow \mathbb{P}^n(\mathbb{K}_v)$
If V is a projective variety $/\mathbb{K}$ the v-adic topology on $V(\mathbb{K}_v)$ is the one induced topology.

Example
$\mathbb{P}^n(\mathbb{R})$ is compact since the continuous map
$$\mathbb{S}^n \longrightarrow \mathbb{P}^n(\mathbb{R}) \text{ is surjective}$$
where
$$\mathbb{S}^n = \left\{(x_0, \dots, x_n) \in \mathbb{R}^{n+1} \;\middle|\; \sum_{i=0}^{n} x_i^2 = 1\right\} \text{ is}$$
compact

Proposition
Assume that v is a place defined by a discrete valuation v and K_v finite
We have $\mathbb{P}^n(\mathbb{K}_v) = \mathbb{P}^n(\hat{\mathcal{O}}_v)$
is a compact topological space
(it is totally disconnected and perfect as well).
More generally, if V is a projective variety over $\mathbb{K}$, $V(\mathbb{K}_v)$ is compact.

Proof
- The ring $\hat{\mathcal{O}}_v$ is a principal domain, so

$\mathbb{P}^n(\hat{\mathcal{O}}_v) \xleftarrow{\sim} \{\text{primitive elements in } \hat{\mathcal{O}}_v^{n+1}\}/\hat{\mathcal{O}}_v^*$

- If $[x_0 : \ldots : x_n] \in \mathbb{P}^n(\mathbb{K}_v)$,
  $(x_0, \ldots, x_n) \neq 0$
  so $k_0 = \min(v(x_0), \ldots, v(x_n)) \in \mathbb{Z}$.
  $[x_0 : \ldots : x_n] = [x_0 \pi^{-k_0} : \ldots : x_0 \pi^{-k_0}]$
  For $(y_0, \ldots, y_n) \in \mathbb{K}_v^{n+1}$
  $(y_0, \ldots, y_n)$ is a primitive element in $\mathcal{O}_v^{n+1}$
  if and only if $\min(v(y_0), \ldots, v(y_n)) = 0$.
  Here we have
  $$\min_{0 \leq i \leq n} v(x_i \pi^{-k_0}) = 0$$
  so $[x_0 : \ldots : x_n]$ is in the image of $\mathbb{P}^n(\hat{\mathcal{O}}_v)$,
- $\{\text{primitive elements in } \hat{\mathcal{O}}_v^{n+1}\}$
  $= \{(x_0, \ldots, x_n) \in \mathbb{Z}^{n+1} \mid \max\{|x_0|, \ldots, |x_n|\} = 1\}$
  is compact (closed in $\hat{\mathcal{O}}_v^{n+1}$)
  So $\mathbb{P}^n(\hat{\mathcal{O}}_v) = \mathbb{P}^n(\mathbb{K}_v)$ is compact
- If V is a variety
  $V(\mathbb{K}_v) \subset \mathbb{P}^n(\mathbb{K}_v)$ is closed. $\square$

c) Adele ring, local-global principle

Remember

$$Pl(\mathbb{Q}) = \underset{\text{set of primes}}{\mathcal{P}} \cup \{\infty\}$$
$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z} \quad \text{for } p \text{ prime}$$
$$\mathbb{Q}_p = Fr(\mathbb{Z}_p)$$
$$\mathbb{Q}_\infty = \mathbb{R}$$

<u>Definition</u>

$$\mathbb{A}_\mathbb{Q} = \{(x_v) \in \prod_{v \in Pl(\mathbb{Q})} \mathbb{Q}_v \mid \{p \in \mathcal{P} \mid x_p \notin \mathbb{Z}_p\} \text{ is finite}\}$$

$$= \bigcup_{\substack{S \subset Pl(\mathbb{Q}) \\ S \text{ finite}, \infty \in S}} \left(\prod_{v \in S} \mathbb{Q}_v \right) \times \prod_{v \notin S} \mathbb{Z}_v$$

it is a subring of $\prod_{v \in Pl(\mathbb{Q})} \mathbb{Q}_v$ and contains the image of $\mathbb{Q}$

Indeed if $x \in \mathbb{Q}$, $\{ p \in \mathcal{P} \mid v_p(x) \neq 0 \}$ is finite so $\mathbb{Q} \subset \mathbb{A}_\mathbb{Q}$

Remark

The reason to introduce $\mathbb{A}_\mathbb{Q}$ is that this ring is locally compact.

Prop

Let V be a projective variety over $\mathbb{Q}$,

$$V(\mathbb{A}_\mathbb{Q}) = \prod_{v \in Pl(\mathbb{Q})} V(\mathbb{Q}_v)$$

Lemma

Let $\varphi : A \to B$ be an injective morphism of rings then the induced map

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

is injective

Proof

We also denote by φ the map : $A^{n+1} \to B^{n+1}$

$$(a_0, \dots, a_n) \mapsto (\varphi(a_0), \dots, \varphi(a_n))$$

and the map $\mathbb{P}^n(A) \to \mathbb{P}^n(B)$

$$L \longmapsto B\varphi(L) \subset B^{n+1}$$

In fact we are going to prove the more precise

statement: $L = \varphi^{-1}(B\,\varphi(L))$
L is a direct summand of A^{n+1}
so there is a linear map $p : A^{n+1} \to A^{n+1}$
such that $p \circ p = 0$ and $L = \mathrm{Ker}(p)$
Let $p_B : B^{n+1} \to B^{n+1}$ be the map
induced by extension of scalars.
Then $B\varphi(L) \subset \mathrm{Ker}(p_B)$
Thus $\varphi^{-1}(B\varphi(L)) \subset \mathrm{Ker}(p_B \circ \varphi) = \mathrm{Ker}(p) = L$
and $L \subset \varphi^{-1}(B\varphi(L))$ is true $\square$
If φ is an inclusion, we identify $\mathbb{P}^n(A)$ with its image.

<u>Proof of the proposition</u>
The inclusion map $\mathbb{A}_{\mathbb{Q}} \to \prod_{v \in Pl(\mathbb{Q})} \mathbb{Q}$
gives a map

$$\begin{tikzcd} V(\mathbb{A}_{\mathbb{Q}}) \arrow[r] \arrow[d, hook, "\text{injective}"'] \arrow[dr, phantom, "\circlearrowleft"] & \prod_{v \in Pl(\mathbb{Q})} V(\mathbb{Q}_v) \arrow[d, hook, "\text{injective.}"] \\ \mathbb{P}^n(\mathbb{A}_{\mathbb{Q}}) \arrow[r, hook, "\text{injective}"'] & \prod_{v \in Pl(\mathbb{Q})} \mathbb{P}^n(\mathbb{Q}_v) \end{tikzcd}$$

Assume that V is defined by $f_1, \dots, f_r$
homogeneous in $\mathbb{Q}[T_0, \dots, T_n]$
Let $y = (y_v)_{v \in Pl(\mathbb{Q})} \in \prod_{v \in Pl(\mathbb{Q})} V(\mathbb{Q}_v)$

For any prime p, since $\mathbb{Z}_p$ is principal, we may
take $y_p = [x_0 : \dots : x_p]$ with $(x_0, \dots, x_p) \in \mathbb{Z}_p^{n+1}$
primitive and $f_i(x_0, \dots, x_p) = 0$ for $i \in \{1, \dots, r\}$
thus

$$y \in V(\mathbb{R}) \times \prod_{p \in \mathcal{P}} V(\mathbb{Z}_p) = V\Big(\mathbb{R} \times \prod_{p \in \mathcal{P}} \mathbb{Z}_p\Big) \subset V(\mathbb{A}_{\mathbb{Q}}). \quad \square$$

Corollary

If V is a projective variety $/\mathbb{Q}$ then $V(\mathbb{A}_{\mathbb{Q}})$ is a compact topological space.

We have

$$V(\mathbb{Q}) \subset V(\mathbb{A}_{\mathbb{Q}})$$

The following question

Question

Let V be a nice variety $/\mathbb{Q}$

(nice = projective smooth and geometrically integral variety)

Is the implication

$$V(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset \Rightarrow V(\mathbb{Q})$$

true?

If V is defined by $f_1, \dots, f_r \in \mathbb{Z}[X_0, \dots, X_n]$ homogeneous

This question is equivalent to

Assume that the system of equations

$$f_i(x_0, \dots, x_n) = 0 \quad \text{for } i \in \{1, \dots, r\}$$

(i) has a nonzero solution in $\mathbb{R}^{n+1}$

(ii) has a primitive solution in $(\mathbb{Z}/M\mathbb{Z})^{n+1}$ for any $M \geq 1$

Does it have a primitive solution in $(\mathbb{Z}^{n+1})$?

Terminology

- If V satisfies the implication, one says that V satisfies Hasse principle
- If $V(\mathbb{Q})$ is dense in $V(\mathbb{A}_{\mathbb{Q}})$ then we say that V satisfies weak approximation

16/5/2016 d) Arakelov heights

Remember

1) On $\mathbb{P}^N(\mathbb{Q})$ we have heights given by
$$H_N(\pi(x)) = \|x\|_\infty$$
if x is a primitive element in $\mathbb{Z}^{N+1}$
where $\|\cdot\|_\infty$ is a norm on $\mathbb{R}^{N+1}$
For any morphism of varieties
$$\phi : V \longrightarrow \mathbb{P}^N_{\mathbb{Q}}$$
we get an exponential height
$$H = H_N \circ \phi : V(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0}$$
Let us rewrite this height in a slightly different language

2) If $(x_0, -, x_n) \in \mathbb{Z}^{N+1}$
$(x_0, -, x_n)$ is primitive
iff $\gcd(x_0, -, x_n) = 1$
iff for any prime p, $\min\limits_{0\leq i\leq n}(v_p(x_i)) = 0$

iff prime p, $\max\limits_{0\leq i\leq N} |x_i|_p = 1$

For $(x_0, -, x_n)$ in $\mathbb{Q}_p^{N+1}$ write $\|(x_0, -, x_N\|_p = \max\limits_{0\leq i\leq N} |x_i|_p$
Then for a primitive $(x_0, -, x_N) \in \mathbb{Z}^{N+1}$

we have $\|(x_0, -, x_N)\|_\infty = \prod\limits_{v \in Pl(\mathbb{Q})} \|(x_0, -, x_N)\|_v$

But $\forall \lambda \in \mathbb{Q}_p$, $\forall x \in \mathbb{Q}_p^{N+1}$ $\quad \|\lambda x\|_p = |\lambda|_p \|x\|_p$

So if $\lambda \in \mathbb{Q}^*$ and $(y_0, -, y_N) = \lambda(x_0, -, x_N)$
$$\prod_{v\in Pl(\mathbb{Q})} \|(y_0, -, y_N)\|_v = \underbrace{\prod_{v \in Pl(\mathbb{Q})} |\lambda|_v}_{=1} \times \|(x_0, -, x_N)\|_\infty$$

北京大学

Conclusion

For any $(y_0, -, y_N)$ in $\mathbb{Q}^{N+1}$

$$H([y_0 : - : y_N]) = \prod_{v \in Pl(\mathbb{Q})} \|(y_0, -, y_N)\|_v$$

But we would like an expression of the height which does not depends on the choice of the embedding but is more intrinsic, although one has to make choice to define a height. For that let us consider

$L = \phi^*(\mathcal{O}_{\mathbb{P}^n}(1))$ which is a line bundle over V.

If $x \in V(\mathbb{Q})$

$$L(x) = \mathcal{O}_{\mathbb{P}^n}(1)(\phi(x)) = \mathcal{O}_{\mathbb{P}^n}(-1)(\phi(x))^\vee$$

which is the 1 dimensional vector space in $\mathbb{Q}^{n+1}$ corresponding to $\phi(x)$ that is

if $\phi(x) = (y_0 : - : y_N)$ then $L(x) = \mathbb{Q}(y_0, -, y_N)^\vee$!

But

$\|\cdot\|_v$, by restriction defines a norm on $L(x)^\vee$

we get a map

$$\|\cdot\|_v : L^\vee(\mathbb{Q}_v) \longrightarrow \mathbb{R}_{\geq 0}$$

which is continuous and such that

$$\forall\, y \in L^\vee(\mathbb{Q}_v)\ \forall \lambda \in \mathbb{Q}_v\ \|\lambda y\|_v = |\lambda|_v \|y\|_v$$

and

$$\forall x \in V(\mathbb{Q}), \forall y \in L^\vee(x)\quad H(x) = \prod_{v \in Pl(\mathbb{Q})} \|y\|_v$$

Now the tradition is to define in terms of L not $L^\vee$

For $v \in Pl(\mathbb{Q})$ there exists a unique $\|\cdot\|_v : L(\mathbb{Q}_v) \to \mathbb{R}_{\geq 0}$

such that

$$\forall x \in V(\mathbb{Q}_v)\ \forall y \in L(x), \forall y' \in L(x)^\vee$$
$$\|y'\|_v \, \|y\|_v = |\langle y', y\rangle|_v$$

duality

If $x \in V(\mathbb{Q})$ $y \in L(x)$, $y' \in L(x)^\vee$ bilinear form

$$\Big(\prod_{v \in Pl(\mathbb{Q})} \|y'\|_v\Big) \times \Big(\prod_{v \in Pl(\mathbb{Q})} \|y\|_v\Big) = \prod_{v \in Pl(\mathbb{Q})} |\underbrace{\langle y', y\rangle}_{\in \mathbb{Q}}|_v$$

By the product formula $= 1$

Conclusion

We have written
$$H(x) = \prod_{v \in Pl(\mathbb{Q})} \|y\|_v^{-1} \quad \text{for } y \in L(x)^\vee$$

where $\|\cdot\|_v : L(\mathbb{Q}_v) \to \mathbb{R}_{>0}$ is continuous and defines a norm in each fibre

This is the setting we are going to generalize in the next chapter before we speak of interpretation.

Example

On $\mathbb{P}^n(\mathbb{Q})$, for $\phi = Id_{\mathbb{P}^n}$
X_i is a section of $L = \mathcal{O}_{\mathbb{P}^n}(1)$

we have

$$\|X_i(x_0 : \dots : x_n)\| = \begin{cases} \dfrac{|x_i|_v}{\max\limits_{0 \le i \le n} |x_i|_v} & \text{if } v \neq \infty \\[2ex] \dfrac{|x_i|_\infty}{\|(x_0, \dots, x_n)\|_\infty} & \text{if } v = \infty \end{cases}$$

the quotient does not depend on the choices of the homogeneous coordinats, so it is well defined.