Practical work in mathematics

An approach to projective geometry

Author :
Thomas Rüd

Supervisor :
Prof. David McKinnon

April 24^{th} 2014

Contents

1 Introduction

"Chaque objet abstrait est devenu concret par l'usage [...] un objet concret est un objet abstrait auquel on a fini par s'habituer." Laurent Schwartz

Algebraic geometry covers a lot of topics, and takes some time to get used to. However it is a very powerful tool in mathematics, for geometry but also arithmetic and commutative algebra. In order to have a first glance at this subject we will work on a conjecture, try to bring basic definitions to understand it and study a few simple cases.

This conjecture is about density of a kind of point in projective spaces. We'll see that simple examples of such points characterize the integers and give a motivation in section 2.

In section 3 we will just state the conjecture, then in the 4^{th} we will take a look at a special dimension two space over the rational numbers and, starting with a special case, we will try to broaden our example towards a construction of a strategy. Then we'll prove the general case for this space.

After that we'll move to a similar space but of dimension 3. Throughout section 5 we will try to see problems that arise and what we can adapt from our previous strategy and the results we need to prove in order to make it work. Once this is clear, we will establish a new strategy and proceed to the proof.

Eventually we'll see in section 6 that the proof we constructed can be adapted to those spaces for any dimension, so we will have the general case for all such projective spaces over rational numbers.

2 Motivation

Let's take a very simple example. Take $r \in \mathbb{Q}$ and write $r = \frac{a}{b}$, $\gcd(a,b) = 1$. Then $r \in \mathbb{Z}$ if and only if $b = 1$, so r is an integer if and only if p does not divide b for every prime p.

We can embed $\mathbb{Q}$ in $\mathbb{P}^1(\mathbb{Q})$ by $r = \frac{a}{b} \leftrightarrow [a : b] = [r : 1]$, hence another way of writing the situation is : an integer corresponds to a point $[a : b] \in \mathbb{P}^1(\mathbb{Q})$ such that $[a : b] \not\equiv [1 : 0] \bmod p$ for all prime p. We want to broaden the problem, first changing $[1 : 0]$ to other points and see what points we end up describing, and we also want to see what happens in higher dimensions so take the new problem : for some subset $D \subseteq \mathbb{P}^n(\mathbb{Q})$ find points $P \in \mathbb{P}^n(\mathbb{Q})$ such that $P \notin D \bmod p$ for all prime p.

This motivates the following definition :

Definition 1. Let $D \subseteq \mathbb{P}^n(\mathbb{Q})$, let $P \in \mathbb{P}^n(\mathbb{Q})$ we say P is **D–integral** if

$$P \notin D \bmod p \text{ for all prime } p.$$

Notation. Whenever we take a point $P \in \mathbb{P}^n(\mathbb{Q})$, if we don't specify otherwise, we write it with integer coprime coefficients.

Example : In $\mathbb{P}^2(\mathbb{Q})$, find points $[a : b : c] \not\equiv [0 : 0 : 1] \bmod p$. Take such a point $[a : b : c] \in \mathbb{P}^2(\mathbb{Q})$, we can write it so that $a, b, c \in \mathbb{Z}$ with $\gcd(a, b, c) = 1$. Let p be a prime, if p divides a then p cannot divide b because otherwise $[a : b : c] \equiv [0 : 0 : c] \equiv$

$[0:0:1]$ mod p, likewise prime divisor of b cannot divide a, hence $\gcd(a,b) = 1$. Conversely if $\gcd(a,b) = 1$ then if $a \equiv 0 \bmod p$ for some prime p then $b \not\equiv 0 \bmod p$ so $[a:b:c] \not\equiv [0:0:1] \bmod p$. So the $[0:0:1]$–integral points are the points $[a:b:c]$ with $\gcd(a,b) = 1$.

In this last example we have an interesting property, which is that the integral points we get are Zariski dense in $P \in \mathbb{P}^2(\mathbb{Q})$. By Zariski dense we mean :

Definition 2 (Zariski topology, Zariski density)**.** In a projective space X we define the **Zariski topology** by taking the algebraic subsets as the closed sets.

Hence a set $S \subseteq X$ is not **Zariski dense** if it is contained in some proper algebraic subvariety of X.

We will prove later that the $[0:0:1]$–integral points are Zariski dense in $\mathbb{P}^2(\mathbb{Q})$, but first we will state the conjecture.

3 Conjecture

Conjecture. *Let X be an n–dimensional variety with $n \geq 2$ and let $D \subset X$ with $dim D \leq n-2$. If the rational points on X are Zariski dense, then the D–integral points on X are also potentially Zariski dense.*

Definition 3. If X is a projective variety over a field F, we say $D \subset X$ is **potentially** Zariski dense in X if there is a finite field extension K/F such that D is Zariski dense in X over the field K.

Here we will only study the cases of the projective varieties $X = \mathbb{P}^n(\mathbb{Q})$ so the rational points are automatically dense in X.

4 2-dimensional case.

4.1 $[0:0:1]$-integral points

We go back to our previous example. We are in $\mathbb{P}^2(\mathbb{Q})$ and we know that the $[0:0:1]$–integral points are the points $[a:b:c]$ with $\gcd(a,b) = 1$. Let N be the set of those points. Suppose, for the sake of contradiction, that $N \subseteq C$ for some algebraic curve C. For all $\alpha \in \mathbb{Z}$ define the line

$$V_\alpha : z - \alpha y = 0.$$

Easily the elements of $\{V_\alpha : \alpha \in \mathbb{Z}\}$ are distinct lines, and for a line V_α, we have $\{[x:1:\alpha] : x \in \mathbb{N}\} \in V_\alpha \cap N$, so $\infty = |V_\alpha \cap N| \leq |V_\alpha \cap C|$ hence $|V_\alpha \cap C| = \infty$ for all $\alpha \in \mathbb{Z}$.

To conclude, we need :

Theorem 1 (Bezout theorem)**.** *Let F and G be projective plane curves of degree m and n respectively. Assume F and G have no common component. Then $F \cap G$ has mn points, counting multiplicity.*

For a proof, see [1, 12.31].

Then V_α is a component of C for all $\alpha \in \mathbb{Z}$, so C has an infinite number of components, which is absurd ↯ So the $[0:0:1]$–integral points are Zariski dense over $\mathbb{P}^2(\mathbb{Q})$, as we wanted.

4.2 $[\alpha:\beta:\gamma]$-integral points

Let $[\alpha:\beta:\gamma] \in \mathbb{P}^2(\mathbb{Q})$, $\alpha,\beta,\gamma \in \mathbb{Z}$, $\gcd(\alpha,\beta,\gamma) = 1$. We want to use the previous fact to see that $[\alpha:\beta:\gamma]$–integral points are Zariski dense. A way to do that is to find an integer matrix with determinant one, say P, such that

$$P[\alpha:\beta:\gamma] = [0:0:1].$$

Such a P gives us a new basis and sends $[\alpha:\beta:\gamma]$ to $[0:0:1]$. If we take the lines we used in the previous part and then go back to our original basis, we'll get an infinite number of distinct lines that will help us conclude thanks to Bezout's Theorem as before. The determinant one condition is to ensure that P^{-1} has integer entries, which will be useful for the general case.

The only thing we really need to prove is the existence of such a matrix. This will be a key argument in our general proof.

4.3 Finding a special kind of matrix

Now let's focus on finding the previously described matrix P. It is actually easier to look for P^{-1}; we will state its existence as a theorem.

Theorem 2. *Given $\alpha,\beta,\gamma \in \mathbb{Z}$ with $\gcd(\alpha,\beta,\gamma) = 1$ there exists $P \in GL_n(\mathbb{Z})$ such that $P\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}$ and $|det(P)| = 1$.*

Note that by $\mathrm{GL}_3(\mathbb{Z})$ we mean the group of invertible 3×3 matrices with integer entries. The inverse of a matrix with integer entries in general need not have integer entries, but it is the case if and only if its determinant is ± 1, hence the condition $|det(P)| = 1$.

As we'll see later, we don't really need to know the matrix, we just need to know it exists. Finding one explicitly can be tricky, so we'll first give a nonconstructive proof before trying to actually build one.

4.3.1 Nonconstructive proof

We start with our vector $v := \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} \in \mathbb{Z}^3$. Consider $S := \mathrm{span}(v)$. It is a $\mathbb{Z}$–submodule of $\mathbb{Z}^3$. Suppose we proved that $\mathbb{Z}^3/S \cong \mathbb{Z}^2$. We can take $\left\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right\}$ a basis for $\mathbb{Z}^2$, then there are $v_1, v_2 \in \mathbb{Z}^3$ such that $\{v_1 + S, v_2 + S\}$ is a basis for $\mathbb{Z}^3/S$.

It follows from the construction that $\{v, v_1, v_2\}$ is a basis for $\mathbb{Z}^3$ as a free $\mathbb{Z}$-module. So we can write :

$$\begin{cases} e_1 = (1,0,0) = a_{11}v_1 + a_{21}v_2 + a_{31}v \\ e_2 = (0,1,0) = a_{12}v_1 + a_{22}v_2 + a_{32}v \\ e_3 = (0,0,1) = a_{13}v_1 + a_{23}v_2 + a_{33}v \end{cases}$$

So if $N = (a_{ij})_{i,j=1}^3$, it has integer coefficients and $Nv_1 = e_1$, $Nv_2 = e_2$, $Nv_3 = e_3$, and $M = N^{-1} = \begin{pmatrix} v_1 & v_2 & v \end{pmatrix}$, so $Pe_3 = v$, what we wanted, P is invertible, its inverse, N, has integer coefficients, so $\det(P) = \pm 1$.

Why do we have $\mathbb{Z}^3/S \cong \mathbb{Z}^2$? S has rank one and the rank of $\mathbb{Z}^3$ is 3. Then $\mathbb{Z}^3/S$ is a $\mathbb{Z}$–module of rank 2 so the only way $\mathbb{Z}^3/S$ could fail to be isomorphic to $\mathbb{Z}^2$ is if it contains some torsion submodule.

If it weren't torsion free, there would be $m = \begin{pmatrix} a \\ b \\ c \end{pmatrix} \notin S$ and $k \in \mathbb{Z}$, $k \neq 0$ such that $km \in S$, so $kP = \lambda v = km$, i.e.

$$\begin{pmatrix} ka \\ kb \\ kc \end{pmatrix} = \begin{pmatrix} \lambda\alpha \\ \lambda\beta \\ \lambda\gamma \end{pmatrix}.$$

$\gcd(\alpha, \beta, \gamma) = 1$ (i.e. $m + S \neq 0$ in $\mathbb{Z}^3/S$ but $km + S = 0$).
So $\gcd(ka, kb, kc) = \gcd(\lambda\alpha, \lambda\beta, \lambda\gamma) = \lambda$. But k divides $\gcd(ka, kb, kc)$ so $k|\lambda$, so

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} \frac{\lambda}{k}\alpha \\ \frac{\lambda}{k}\beta \\ \frac{\lambda}{k}\gamma \end{pmatrix} = \underbrace{\frac{\lambda}{k}}_{\in\mathbb{Z}} \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} \in S$$

which is absurd ↯ Hence $\mathbb{Z}^3/S \cong \mathbb{Z}^2$ so we win.

4.3.2 Constructive proof

Let's return to finding the matrix P. We know we must have $P\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}$ so we know that the last column of P must be $\begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}$. Let's try to find such a P with determinant 1.

We need to find $a, b, c, \aleph, \beth, \gimel \in \mathbb{Z}$ such that

$$\begin{vmatrix} \aleph & a & \alpha \\ \beth & b & \beta \\ \gimel & c & \gamma \end{vmatrix} = 1 = \begin{pmatrix} \aleph & \beth & \gimel \end{pmatrix} \cdot \left(\begin{pmatrix} a \\ b \\ c \end{pmatrix} \wedge \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} \right) = \begin{pmatrix} \aleph & \beth & \gimel \end{pmatrix} \cdot \begin{pmatrix} b\gamma - c\beta \\ c\alpha - a\gamma \\ a\beta - b\alpha \end{pmatrix}.$$

We will be able to find such $\aleph, \beth, \gimel \in \mathbb{Z}$ if we have

$$\gcd(b\gamma - c\beta, c\alpha - a\gamma, a\beta - b\alpha) = 1.$$

Pick b, c such that $b\gamma - c\beta = \gcd(\gamma, \beta)$. Here we suppose again that $\gamma \neq 0$ so $\gcd(\gamma, \beta) \neq 0$ (if $\gamma = 0$ we can take a, b such that $a\beta - b\alpha = \gcd(\alpha, \beta) \neq 0$). We must

have $\gcd(b,c) = 1$ so there are $m, n \in \mathbb{Z}$ such that $mb + nc = 1$. Set $a = 0$ and call $d := \gcd(b\gamma - c\beta, c\alpha - a\gamma, a\beta - b\alpha) = \gcd(b\gamma - c\beta, c\alpha, -b\alpha)$. Then $d|c\alpha$ and $d|-b\alpha$ so

$$d|n(c\alpha) - m(-b\alpha) = (mb + nc)\alpha = \alpha.$$

So $d|\alpha$ but also by definition $d|(b\gamma - c\beta) = \gcd(\beta, \gamma)$, so $d|\gcd(\alpha, \gcd(\beta, \gamma)) = \gcd(\alpha, \beta, \gamma) = 1$, hence $d = \gcd(b\gamma - c\beta, c\alpha, -b\alpha) = 1$, what we wanted.

So just pick $\aleph, \beth, \gimel \in \mathbb{Z}$ such that $\aleph(b\gamma - c\beta) + \beth(c\alpha) + \gimel(-b\alpha) = \begin{vmatrix} \aleph & 0 & \alpha \\ \beth & b & \beta \\ \gimel & c & \gamma \end{vmatrix} = 1.$

Hence define $P = \begin{pmatrix} \aleph & 0 & \alpha \\ \beth & b & \beta \\ \gimel & c & \gamma \end{pmatrix}$. The calculations above give us the desired result.

4.4 Strategy for the general case.

First remark that if we take $D \subseteq \mathbb{P}^2(\mathbb{Q})$ as in the conjecture, $\dim(D) \leq 0$ so $\dim(D) = 0$ so D is a finite set of points.

We want to adapt our strategy to use Bezout's theorem for the general case in dimension 2, so given a finite set of points D, we want to build infinitely many distinct lines each containing infinitely many $D-$integral points, and then we can conclude as in the previous case. The problem is that we can't construct those lines as easily as before because we need to have lines containing $D-$integral points, and D can have several points not only one as before, so our construction doesn't work.

So we'll go through the following two steps to prove our result.

- **Step 1 :** Prove that if a line that does not intersect D contains one $D-$integral point then it contains infinitely many of them.
- **Step 2 :** Prove that given any finite set of points S and a point m not in S, there is a line containing m and not intersecting S.
- **Step 3 :** Find a $D-$integral point m.

Suppose these facts are proved. We take the point m from step 3 and thanks to step 2 with $S = D$ take a line containing m that does not intersect D ($m \notin D$ because m is $D-$integral). By step 1 we get infinitely many points, say $\{m_n : n \in \mathbb{N}\} \in L$, pairwise distinct and all $D-$integral. Then using step 2 with $S = D \cup \{m_i\}$ we get a line L_{m_i} that does not intersect $D \cup m$ (so $L_{m_i} \neq L$). So by step 1 each L_{m_i} contains infinitely many $D-$integral points and they are pairwise distinct (if $m_j \in L_{m_i}$ for $i \neq j$, then $L_{m_i} = L$).

So we apply the previous argument, suppose the $D-$integral points are contained within a curve C, then $C \cap L_{m_i}$ is infinite for each L_{m_i}. By Bezout's theorem all L_{m_i} are components of C, so C has infinitely many distinct components, which is absurd ↯ So the $D-$integral points are Zariski dense.

Remark 1. *Although it doesn't appear that we need to take field extensions, we will need it in step 3 in the case where D mod $p = \mathbb{P}^2(\mathbb{Q})$ mod p for some prime p. For example if $p = 2$ then $\mathbb{P}^2(\mathbb{Q})$ mod p only contains 7 points, so it is possible that D mod 2 contains all of them. In that case there are no $D-$integral points in $\mathbb{P}^2(\mathbb{Q})$, so we will need to take a field extension of $\mathbb{Q}$ to create one.*

4.4.1 Step 1

Again we'll go back to the case of $D = \{[0:0:1]\}$. Now let $L : ax + by + cz = 0$ be a line with $a, b, c \in \mathbb{Z}$, $\gcd(a, b, c) = 1$. Suppose $[0:0:1] \notin L$ and there is a $D-$integral point $[x_0 : y_0 : z_0] \in L$. Let's show that we can find an infinity of $D-$integral points on the line.

$[0:0:1] \notin L$ so $c \neq 0$, let $[x:y:z] \in L$, $x, y, z \in \mathbb{Z}$, $\gcd(x, y, z) = 1$.

Remark 2. *$[x:y:z]$ is not $D-$integral iff there is a prime p such that $p|x$ and $p|y$. Suppose there is such a p. Then $p|ax + by = -zc$ but $\gcd(x, y, z) = 1$ so $p \nmid z$ so $p|c$. So if we stay on the line L, we only need to check that,*

$$[x:y:z] \notin D \text{ mod } p \text{ for all } p \text{ dividing } c.$$

We're now reduced to a finite number of constraints.

We want to find other $D-$integral points in L of the form $[x:y:z_0]$. Such a point $[x:y:z_0]$ must belong to the line, so $ax + by + cz_0 = 0 = ax_0 + by_0 + cz_0$. Thus $a(x - x_0) + b(y - y_0) = 0$ and hence $a(x - x_0) = b(y_0 - y)$.

We have that for all $k \in \mathbb{N}$, $[x:y:z_0] \in L$ where $x = x_0 + kb$, $y = y_0 - ka$, and we have an infinity of them. That's because

$$a(x_0 + kb) + b(y_0 - ka) + cz_0 = ax_0 + by_0 + cz_0 + kab - kab = ax_0 + by_0 + cz_0 = 0.$$

Also suppose $c|k$. Then if $p|c$,

$$x \equiv x_0 + kb \bmod p \equiv x_0 \bmod p \qquad y \equiv y_0 + kb \bmod p \equiv y_0 \bmod p,$$

$$\text{so } [x:y:z_0] \equiv [x_0 : y_0 : z_0] \bmod p \text{ for all } p|c.$$

By the previous remark, $[x:y:z_0]$ is $D-$integral, so if $k \in N$, define

$$m_k \coloneqq [x_k : y_k : z_k] \coloneqq [x_0 + kcb : y_0 - kca : z_0],$$

then $P_k \in L$ and it is $D-$integral, so we found infinitely many $D-$integral points on L.

Now we suppose $D = \{[\alpha : \beta : \gamma]\}$, $\alpha, \beta, \gamma \in \mathbb{Z}$, $\gcd(\alpha, \beta, \gamma) = 1$. Let $L : ax+by+cz$, $a, b, c \in \mathbb{Z}$ $\gcd(a, b, c) = 1$, a line such that $[\alpha : \beta : \gamma] \notin L$ and $[x_0 : y_0 : z_0]$ be $D-$integral and on L. Take the matrix P like in Theorem 2, and write $N = P^{-1}$ and L' the image of L under N.

Let's write $P = \begin{pmatrix} \text{א} & 0 & \alpha \\ \text{ב} & i & \beta \\ \text{ג} & j & \gamma \end{pmatrix}$; then

$$\begin{aligned}
[x:y:z] \in L' &\Leftrightarrow P[x:y:z] \in L \\
&\Leftrightarrow \begin{pmatrix} \text{א} & 0 & \alpha \\ \text{ב} & i & \beta \\ \text{ג} & j & \gamma \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in L \\
&\Leftrightarrow \underbrace{(a\text{א} + b\text{ב} + c\text{ג})}_{=A} x + \underbrace{(ib + jc)}_{=B} y + \underbrace{(a\alpha + b\beta + c\gamma)}_{=C} z = 0 \\
&\Leftrightarrow Ax + By + Cz = 0
\end{aligned}$$

So the equation of L' in the new system is $Ax + By + Cz = 0$, and by hypothesis $C = a\alpha + b\beta + c\gamma \neq 0$ because $[\alpha : \beta : \gamma] \notin L$. Write $[x_1 : y_1 : z_1] = P^{-1}[x_0 : y_0 : z_0]$. We follow the same scheme as previously now that our point is $[0 : 0 : 1]$ in this new basis, and we get our points $[x_1 + kCB : y_1 - kCA : z_1] = [x_1 : y_1 : z_1] + kC[B : -A : 0]$. We get the points

$$[x_1 : y_1 : z_1] + kC[B : -A : 0] \text{ for all } k \in \mathbb{N}.$$

We now go back in our original basis,

$$\begin{aligned}[x_k : y_k : z_k] &= P([x_1 : y_1 : z_1] + kC[B : -A : 0]) \\ &= P[x_1 : y_1 : z_1] + kCP[B : -A : 0] \\ &= [x_0 : y_0 : z_0] + kC[b : -a : 0].\end{aligned}$$

Our points therefore have the form

$$[x_k : y_k : z_k] = [x_0 + k(a\alpha + b\beta + c\gamma)b : y_0 - k(a\alpha + b\beta + c\gamma)a : z_0].$$

Keep in mind that we just need points of the form $[x_0 + Kb : y_0 - Ka : z_0]$ with $(a\alpha + b\beta + c\gamma)|K$.

Now starting from any set $D = \{[\alpha_s : \beta_s : \gamma_s] | 1 \leq s \leq n\}$, write $L : ax + by + cz = 0$. Suppose that $L \cap D = \varnothing$, and there is $[x_0 : y_0 : z_0] \in L$ that is $D-$integral. Let $k \in \mathbb{N}$ and build

$$[x_k : y_k : z_k] = [x_0 + kNb : y_0 - kNa : z_0]$$

where $N = \prod_{s=1}^{n}(a\alpha_s + b\beta_s + c\gamma_s)$. We can check that $[x_k : y_k : z_k] \in L$ and also given any $s \in \{1, \cdots, n\}$, $a\alpha_s + b\beta_s + c\gamma_s \neq 0$ and $(a\alpha_s + b\beta_s + c\gamma_s)|N$ so by previous construction $[x_k : y_k : z_k]$ is $[\alpha_s : \beta_s : \gamma_s]$-integral and thus $[x_k : y_k : z_k]$ is $D-$integral. So we won; we just constructed infinitely many $D-$integral points on L. □

4.4.2 Step 2.

This step is pretty straightforward. Take a point $m \in \mathbb{P}^2(\mathbb{Q})$ and S a finite set of points such that $m \notin S$. Given two points there is exactly one line going through them both, so there are only finitely many lines containing m and points of S, but there are infinitely many lines containing m so we can take one not intersecting S. □

4.4.3 Step 3.

Take any point in $\mathbb{P}^2(\mathbb{Q}) \setminus D$ which is nonempty because D is finite. Then use step 2 to take a line $L : ax + by + cz$ such that $D \cap L = \varnothing$. If L contains a $D-$integral point, call it m, and we're done. Suppose not, we want to find a $D-$integral point $m = [x_0 : y_0 : z_0]$ on L.

Suppose without loss of generality that $c \neq 0$. We want to look for x_0 such that $x_0 \not\equiv \alpha_s \bmod p$ for all $s \in \{1, \cdots, n\}$, for all p prime, but as we showed in step 1,

we can restrict ourselves to $p|c$. If we find such a x_0, we take any y_0, z_0 such that $[x_0 : y_0 : z_0] \in L$ (if $c = 0$ we can look for $z_0 \not\equiv \gamma_s \bmod p$ and then take any x_0, z_0 such that $[x_0 : y_0 : z_0] \in L$).

"Simple" case: c has only one prime divisor p. If there is $q \in \mathbb{N}$ such that $q \not\equiv \alpha_s \bmod p$ for all $s \in \{1, \cdots, n\}$, take $x_0 = q$, and then $y_0 = 1$ and $z_0 = \frac{-(ax_0+by_0)}{c}$. Then for all s, we cannot have p such that $[x_0 : y_0 : z_0] \equiv [\alpha_s : \beta_s : \gamma_i] \bmod p$ because $x_0 \not\equiv \alpha_s \bmod p$ for all s.

If there is no such q, note that the polynomial $x^{p^2} - x$ has an irreducible factor in $\mathbb{F}_p[x]$ that doesn't divide $x^p - x$. Let $f(x) \in \mathbb{Z}[x]$ whose reduction mod p is that irreducible factor, then it is irreducible in $\mathbb{Z}[x]$ and by Gauss lemma it is irreducible as a polynomial of $\mathbb{Q}[x]$. So we can extend the field with this polynomial and take θ a root of $f(x)$. So $\theta^{p^2} = \theta$ and

$$\theta \notin \mathbb{N} \bmod p.$$

Why ? Suppose otherwise, then there is $r \in \{1, \cdots, p\}$ such that $\theta \equiv r \bmod p$ so $\theta^p \equiv r^p \equiv r \equiv \theta \bmod p$, because if $r \in \{1, \cdots, p\}$, it is a root of $x^p - x$ in $\mathbb{F}_p$, so θ is a root of $x^p - x$ in $\mathbb{F}_p$, but we constructed θ to not be a root of this polynomial (our polynomial does not divide $x^p - x$).

So take $x_0 = \theta$, $y_0 = 1$ and $z_0 = \frac{-(ax_0+by_0)}{c}$.

General case : Let p a prime divisor of c, and suppose there is $\omega_p \in \mathbb{Q}$ such that for all i, $\alpha_i \not\equiv \omega_p \bmod p$. We want to find x_0 such that

$$x_0 \equiv \omega_p \bmod p \quad p \text{ is a prime divisor of } N.$$

By the Chinese remainder theorem, we can find such a x_0, then take $y_0 = 1$ and $z_0 = \frac{-(ax_0+by_0)}{c}$ and so for all $p|c$, p prime, $[x_0, y_0, z_0] \not\equiv [\alpha_i : \beta_i : \gamma_i] \bmod p$ because $x_0 \equiv \omega_p \not\equiv \alpha_i \bmod p$.

Suppose there is a p, prime divisor of c such that there is no ω_p such that $\alpha_i \not\equiv \omega_p \bmod p$ for all i. Then take a field extension of $\mathbb{Q}$ that induces a nontrivial extension of $\mathbb{F}_p$. Like we did before, we know that we we can take an irreducible polynomial in $\mathbb{Q}[x]$ whose root generates a nontrivial extension of $\mathbb{F}_p$, so we can extend $\mathbb{Q}$ with this polynomial and take one of its roots. We proved it cannot be congruent to any $n \in \mathbb{N} \bmod p$, so in particular we have an element ω_p not congruent to any $\alpha_i \bmod p$. We extend our field for every p where we have such a problem, and then take $x_0 \equiv \omega_p \bmod p$ for every prime divisor p of c thanks to the Chinese Remainder Theorem and conclude as before. □

4.5 Extending the strategy

We just all proved the three steps so we can conclude that the conjecture is true for $X = \mathbb{P}^2(\mathbb{Q})$. However we didn't solve the problem for 2-dimensional projective varieties. Also during our research we saw that it was very comfortable to work with $\mathbb{P}^2(\mathbb{Q})$ so we might want to prove the conjecture for $\mathbb{P}^n(\mathbb{Q})$ with $n \geq 3$ and try to adapt the strategy we build for dimension 2. In the next part we'll see how we can adapt the strategy for 3-dimensional spaces.

5 3-dimensional case

Now we work in $\mathbb{P}^3(\mathbb{Q})$, what in our previous strategy fails in dimension 3 ?

Problems : The first problem we have is, even if we find infinitely many lines with infinitely many $D-$integral points each, it it possible that all those lines are contained in some 2-dimensional algebraic surface in $\mathbb{P}^3(\mathbb{Q})$ so it is possible that all our lines are contained in a subvariety. Also now we have $\dim(D) \leq 1$ so D need not contain only points, it may contain some curves, and we would need to prove that we can find lines going through some point outside of D and that does not intersect D.

We will proceed as we did in dimension 2, using Bezout's Theorem to conclude, as it is true in any dimension.

5.1 Strategy for the 3 dimensional case

Let D be a finite set of points and curves, suppose the set of D-integral points in $\mathbb{P}^3(\mathbb{Q})$ is not Zariski dense. So it is contained in a 2-dimensional algebraic variety, call it $\mathcal{S}$.

We will write N_D the set of all $D-$integral points. Here are the steps for the strategy of our proof :

- **Step 1 :** Given any point, there exists a line that goes through this point and does not intersect D.
- **Step 1' :** With the same setup as step 1, we can ensure our line is not contained in $\mathcal{S}$.
- **Step 2 :** If L is a line such that $L \cap D = \varnothing$ and $L \cap N_D \neq \varnothing$ then $|L \cap N_D| = \infty$.
- **Step 3 :** There exists a $D-$integral point.

Once we prove these steps, we can proceed in the following way : We find a point $m \in N_D$ by step 3; by hypothesis $m \in \mathcal{S}$. With step 1' we take a line L that contains m, does not intersect D and is not contained in $\mathcal{S}$. By step 2, $|L \cap N_D| = \infty$, but $N_D \subset \mathcal{S}$ so $|L \cap \mathcal{S}| = \infty$ but L is not contained in S so by Bezout theorem $|L \cap \mathcal{S}| < \infty$, which is absurd $\lightning$. So we can conclude that the $D-$integral points are Zariski dense in $\mathbb{P}^3(\mathbb{Q})$. □

5.1.1 Step 1

Take a point $P \in \mathbb{P}^3(\mathbb{Q})$ that is not contained in D. Let's prove that there is a line L such that $L \cap D = \varnothing$.

Let's give a definition before proving that.

Definition 4 (Grassmannian)**.** Suppose we are working over a field $\mathbb{K}$; in our case we have $\mathbb{K} = \mathbb{Q}$. Let $N, M \in \mathbb{N}$ with $M < N$, then the Grassmannian $G(N, M)$ is the set of all vector subspaces $\Lambda \subset \mathbb{K}^N$.

And we'll use the following theorem :

Theorem 3. *The Grassmanian $G(N,M)$ carries the structure of an abstract variety. It is irreducible and rational of dimension $M(N-M)$.*

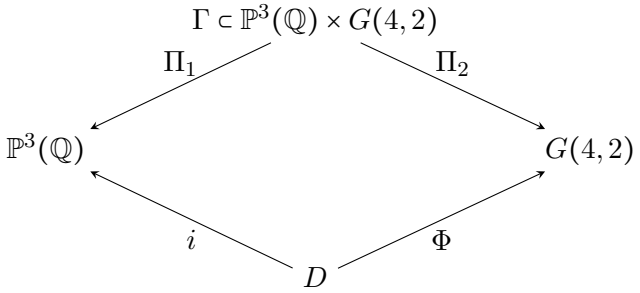
More details are available in [1, 11.13]

Consider the map

$$\Phi : \left| \begin{array}{l} D \longrightarrow G(4,2) \\ Q \longmapsto \overline{PQ} \text{ the line from } P \text{ to } Q. \end{array} \right.$$

$\mathbb{P}^3(\mathbb{Q})$ corresponds to the set of lines in $\mathbb{A}^4(\mathbb{Q})$ so we can see $G(4,2)$ as the set of lines in $\mathbb{P}^3(\mathbb{Q})$.

And now consider the canonical projection maps $\Pi_1 : \mathbb{P}^3(\mathbb{Q}) \times G(4,2) \to \mathbb{P}^3(\mathbb{Q})$ and $\Pi_2 : \mathbb{P}^3(\mathbb{Q}) \times G(3,1) \to G(4,2)$. Also take the inclusion map $i : D \to \mathbb{P}^3(\mathbb{Q})$. We restrict Π_1 and Π_2 to the algebraic subset $\Gamma := \{m \times L \in \mathbb{P}^3(\mathbb{Q}) \times G(4,2) : m \in L\}$ and we get the following diagram :



$\Phi(D)$ corresponds to the set of lines containing P and intersecting D so it is precisely the set of lines we do not want. We want to use our morphisms to find all the points Q in $\mathbb{P}^3(\mathbb{Q})$ such that $\overline{PQ}$ intersects D. We have $\dim(D) = 1$ hence $\dim(\Phi(D)) \leq 1$. Now look at the fibers of Π_2. Fix $L \in G(4,2)$. Then:

$$\Pi_2^{-1}(L) = \{(p,L) : p \in L\} \quad \text{so } \dim(\Pi_2^{-1}(L)) = \dim(L) = 1.$$

Then $\dim\left(\Pi_2^{-1}\left(\Phi(D)\right)\right) = \dim\left(\Phi(D)\right) + 1 \leq 2$, so $\dim\left(\Pi_1\left(\Pi_2^{-1}\left(\Phi(D)\right)\right)\right) \leq 2 < 3$.

$\Pi_1\left(\Pi_2^{-1}\left(\Phi(D)\right)\right)$ is the set of points M such that the lines $\overline{PM}$ intersects D. We saw that $\Pi_1\left(\Pi_2^{-1}\left(\Phi(D)\right)\right) \subsetneq \mathbb{P}^3(\mathbb{Q})$ so take $M \in \mathbb{P}^3(\mathbb{Q}) \setminus \Pi_1\left(\Pi_2^{-1}\left(\Phi(D)\right)\right)$, and we win. □

Step 1' : Now we want to be sure we pick a line not contained in $\mathcal{S}$. We have that $\dim(\mathcal{S}) = 2$, so $\dim\left(\mathcal{S} \cup \left(\Pi_2^{-1}\left(\Phi(D)\right)\right)\right) = 2 < 3$ so we can take a point $Q \in \mathbb{P}^3(\mathbb{Q}) \setminus \left(\mathcal{S} \cup \Pi_1\left(\Pi_2^{-1}\left(\Phi(D)\right)\right)\right)$. Our line $\overline{PQ}$ will not be contained in the sets of bad points so it will not intersect D, and it will contain a $Q \notin \mathcal{S}$ so it is not contained in $\mathcal{S}$. □

5.1.2 Step 2.

Suppose we have a line L that contains one point $P = [a : b : c : d]$, $a, b, c, d \in \mathbb{Z}$ and $\gcd(a,b,c,d) = 1$. Also suppose that P is D–integral and $L \cap D = \varnothing$.

Take $\alpha, \beta, \gamma, \delta, \aleph, \beth, \gimel, \daleth \in \mathbb{Z}$ such that $\gcd(\alpha,\beta,\gamma,\delta) = \gcd(\aleph, \beth, \gimel, \daleth) = 1$ and

$$L : \left\{ \begin{array}{l} \alpha x + \beta y + \gamma z + \delta t = 0 \\ \aleph x + \beth y + \gimel z + \daleth t = 0 \end{array} \right. .$$

We need a result to solve this problem.

Claim. There is an integer $N \neq 0$ such that if $P \in L$ and $P \in D \bmod p$ for some prime number p then $p|N$.

Suppose for now that we proved this claim. Fix such an $N \in \mathbb{N}$ and consider the set of points of the form $P_k = [a : b : c : d] + kN[b\beta : -a\gamma : 0 : 0]$. We can check that $P_k \in L$. Suppose there is a $k \in \mathbb{N}$ such that P_k is not $D-$integral, then there is a prime p such that $P_k \in D \bmod p$, by the claim $p|N$ so $P_k \equiv P + kN[b\beta : -a\gamma : 0 : 0] \equiv P \bmod p$ but P is $D-$integral, so it is absurd, hence all P_k are $D-$integral, and $N \neq 0$ so they are pairwise distinct, so we have an infinite set of $D-$integral points in our line, as we wanted.

Let's give a definition and state the projective Nullstellensatz to prove our claim.

Definition 5. A homogeneous $J \subset k[x_0, \cdots, x_n]$ is irrelevant if $J \supset < x_0^N, \cdots, x_n^N >$ for some $N \in \mathbb{N}$.

Theorem 4 (Projective Nullstellensatz)**.** *Let k be algebraically closed and $J \subset k[x_0, \cdots, x_n]$ be a homogeneous ideal. Then $X(J) = \varnothing$ if and only if J is irrelevant.*

For a proof of the projective Nullstellensatz, see [1, 9.25].

Proof of the claim : Since $L \cap D = \varnothing$, then $I(L \cap D)$ is irrelevant, so there is some $d \in \mathbb{N}$ such that every monomial of degree d lies in $I(L \cap D)$. Note that $I(L \cap D) = I(L) + I(D)$ so for any $i \leq 3$, $x_i^d = \sum_{j=1}^{n_i} f_{ij} l_i + g_{ij} d_j$ for some f_{ij}, fg_{ij} homogeneous polynomials and $l_j \in I(L) \subseteq \mathbb{Z}[x_0, x_1, x_2, x_3]$, $d_j \in I(D) \subseteq \mathbb{Z}[x_0, x_1, x_2, x_3]$. In the Nullstellensatz k is an algebraic closed field, so $f_{i,j}$ and $g_{i,j}$ have coefficients in $\overline{\mathbb{Q}}$, but there are finitely many coefficients and each of them are algebraic over $\mathbb{Q}$ so they are all contained in a finite extension $k/\mathbb{Q}$.

Let $\mathcal{O}_k$ be the ring of integers of k.

So for each i there is $\alpha_i \in \mathcal{O}_k$, $n_i \neq 0$ such that

$$\alpha_i x_i^d = \sum_{j=1}^{n_i} F_{ij} L_j + G_{ij} D_j$$

where $F_{ij}, G_{ij}, L_j, D_j \in \mathcal{O}_k[x_0, x_1, x_2, x_3]$.

Suppose $P \in L$ satisfies $P \in D \bmod p$, if $\alpha = \prod_{i=0}^{3} \alpha_i$ and N is the norm of α then

$$\alpha_i x_i(P)^d \equiv 0 \bmod p \text{ for all } i$$

so $N x_i(P)^d \equiv 0 \bmod p$ for all i. Since $x_i(P) \not\equiv 0 \bmod p$ for at least one i, we get that $p|n_i$. By construction, N satisfies our claim. Hence step 2 is proved. □

5.1.3 Step 3

Take any point $P \notin D$, and use step 1 to find a line L that goes through P and does not intersect D, we want to find a $D-$integral point on this line. We want to use the same strategy as in dimension 2, but D may contain curves, and if we extend our base field, we will have more points in those curves so we have to be careful.

By our claim in step 2 proof, there is $N \neq 0$ such that if $P \in L$ and $P \in D \bmod p$ for some prime number p then $p|N$ so we only need to take care of a finite number of constraints.

Let's state two theorems, but first we have to give a definition.

Definition 6 (Norm)**.** Let ℓ be an algebraic element of a field k. We define the norm of ℓ with respect to k, written $N_k(\ell)$, as the number of elements of the ring $\mathcal{O}_k/(\ell)$

Remark 3. *If ℓ is an element of a field k, then for any finite extension L/k we have $N_L(\ell) = N_k(\ell)^{[L:k]}$. So the norm increases when we increase the base field.*

Theorem 5. *For any curve $\mathcal{C}$ defined over a number field k there is a constant α such that for any prime ℓ of $\mathcal{O}_k$, $\mathcal{C}$ has at most $\alpha N_k(\ell)$ points over $\mathcal{O}_k(\ell)$.*

Theorem 6. *For any curve $\mathcal{C}$ defined over a number field k and for any prime ℓ of $\mathcal{O}_k$ there is a constant α such that for any finite extension L/k, $\mathcal{C}$ has at most $\alpha N_L(\ell)$ points defined over the extension of $\mathcal{O}_L/(\ell)$.*

Proof. We will prove this fact for all $\mathbb{P}^n$ and not just $\mathbb{P}^3$. Take a number field k and a curve $\mathcal{C}$ defined over $\mathbb{P}^n(k)$. We know that $\mathcal{C}$ contains (at least) two points with different coordinates so we can pick two coordinates that change between the two points, suppose without loss of generality that it is the two first coordinates, x_0 and x_1. Then the projection map f from $\mathcal{C}$ to $\mathbb{P}^1(k)$ on those coordinates defined by $f(x0 : ... : xn) = [x0 : x1]$ is not constant. The map f is a rational map between two curves so it has a finite degree, say d. Now fix $\ell \in \mathcal{O}_k$, then $\mathbb{P}^1(k)$ contains $N_k(\ell) + 1$ points mod ℓ so there can't be more than $d(N(\ell) + 1) \leq 2dN_k(\ell)$ points on $\mathcal{C}$ over $\mathcal{O}_k/(\ell)$. Define $\alpha = 2d$ and we get the desired result. □

We can now proceed to proving step 3.

Note that $\mathbb{P}^3(\mathbb{Q})$ mod p contains $\frac{p^4-1}{p-1} = p^3 + p^2 + p + 1$ points, because for each entry we get p values to chose from, so we get $p^4 - 1$ points (-1 to avoid $[0 : 0 : 0 : 0]$). We then divide by $p - 1$ to get rid of all the multiples, another way to say this is that we force one of the entries to be 1, which we can because we are over a field. If k is an algebraic field extension of $\mathbb{Q}$, then for each entry we'll have $N_k(p)$ values to chose from, so $\mathbb{P}^3(k)$ mod p contains $\frac{N_k(p)^4-1}{N_k(p)-1} = N_k(p)^3 + N_k(p)^2 + N_k(p) + 1$ points.

D contains a finite number of curves and for each curve $\mathcal{C}$ and each prime $p|N$ there is $\alpha_p^{\mathcal{C}} N(p)$ such that if we take a finite extension k, $\mathcal{C}$ contains at most $\alpha_p^{\mathcal{C}} N_k(p)$ points in $\mathbb{P}^3(k)$ mod p.

Define $\alpha = \max\{\alpha_p^{\mathcal{C}} N(p) | \quad \mathcal{C} \in D \text{ and } p|N\}$, then for all finite extension extension $k/\mathbb{Q}$, all prime number $p|N$ and any $\mathcal{C} \in D$, the latter will contain at most $\alpha N_k(p)$ points mod p.

Take a field extension $k/\mathbb{Q}$ of degree d big enough such that we ensure that for all prime $p|N$, $\frac{N_k(p)^4-1}{N_k(p)-1} > \alpha N_k(p)$ and so there is a point in the extension that is not contained in any $\mathcal{C} \in D$. It is possible by remark 3 because $N_k(p) = N_{\mathbb{Q}}(p)^{[k:\mathbb{Q}]} = p^d$.

For each of the finitely many remaining points of D, we take a curve containing these points, and apply previous argument to get an extension containing a point P_p that is not in D mod p for all $p|N$.

By the Chinese remainder theorem we can get P such that $P \equiv P_p$ mod p for all $p|N$, so this point is $D-$integral, which proves Step 3. □

The conjecture is now proved for $X = \mathbb{P}^3(\mathbb{Q})$, so let's see about higher dimensions.

6 n-dimensional case

If we take a look at our proof for the case $n = 3$, all the theorems used such as Bezout's Theorem, or the Nullstellensatz are true in any dimension so the proof for $\mathbb{P}^3(\mathbb{Q})$ will generalise to arbitrary dimensions general proof for $\mathbb{P}^n(\mathbb{Q})$ is the latter one. So the conjecture is true for $\mathbb{P}^n(\mathbb{Q})$ for all $n \geq 2$.

However the general case is not proved. Even the general case for 2-dimensional varieties such that rational points are Zariski dense is still open.

7 Conclusion

We covered basic notions of projective geometry, started this project with very little notions about algebraic geometry and managed to tackle a hard problem finding for a solution in some particular cases.

Algebraic geometry is a very broad and useful topic, and this discussion hopefully made some aspects clear and gave more tools and a better intuition in this domain.

Acknowledgements

I would like to thank Prof. David McKinnon, who kindly agreed to supervise the project. He proposed this very interesting topic and helped me weeks after weeks understand the subject and gave me very good directions and enlightening discussions. My only regret is not having been able to work further on this topic and see other problems around the conjecture.

References

[1] Brendan Hassett. *Introduction to Algebraic Geometry.* Cambridge, 2007.