Des tables de soustraction à la géométrie projective finie

Benoit Loisel

ENS de Lyon

Mercredi 2 octobre 2019

Outline

1 Un problème d'ITYM

2 Ensembles à différence

3 Géométrie projective

4 Plans projectifs finis

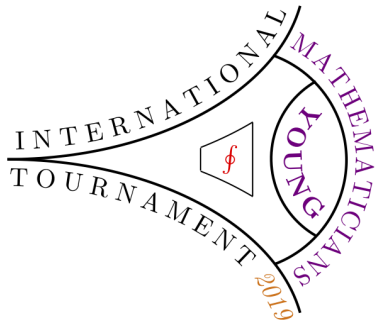
Qu'est-ce que l'ITYM ?

International Tournament of Young Mathematicians

- créé en 2009, *à Orsay,* 6 équipes

  Biélorussie, Bulgarie (2), France (2), Russie ; idée de David Zmiaikou
- chaque année : 10 problèmes ouverts inédits ;
- en 2019, *à Barcelona,* 15 équipes

  Allemagne (2), Biélorussie (2), Bulgarie, France (2), Géorgie, Pologne, Roumanie (2), Russie (2), Thaïlande, Ukraine.



Qu'est-ce que l'ITYM ?

International Tournament of Young Mathematicians

- créé en 2009, *à Orsay,* 6 équipes

  Biélorussie, Bulgarie (2), France (2), Russie ; idée de David Zmiaikou
- chaque année : 10 problèmes ouverts inédits ;
- en 2019, *à Barcelona,* 15 équipes

  Allemagne (2), Biélorussie (2), Bulgarie, France (2), Géorgie, Pologne, Roumanie (2), Russie (2), Thaïlande, Ukraine.

Sélection française : $\mathbb{TFJM}^2$ (Tournoi Français des Jeunes Mathématicien.ne.s)

- créé en 2011 ; soutenu par Animath ;

  avec l'aide d'Igor Kortchemski
- tournois régionaux depuis 2015 ($\sim$ 12 en 2020) :

  à Avignon, Bordeaux, Lille, Lyon, Nancy, Paris (4), Rennes, Toulouse, Tours

De bons résultats pour la France en 2019

Équipe France 1

lycée Victor Hugo

Colomiers, académie de Toulouse

1ère place, Grand 1er prix

De bons résultats pour la France en 2019

Équipe France 1

lycée Victor Hugo

Colomiers, académie de Toulouse

1ère place, Grand 1er prix

Équipe France 2

lycée David d'Angers

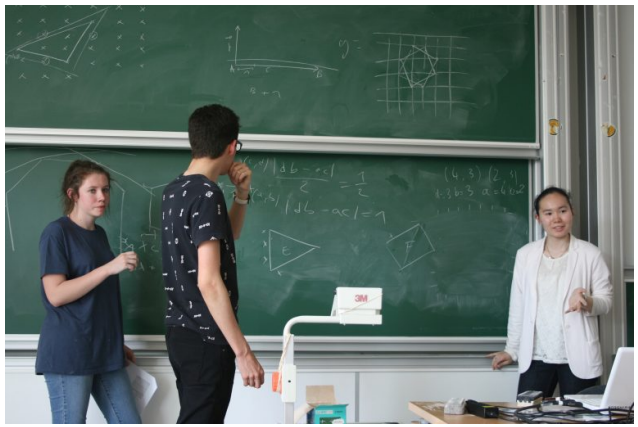
Angers, académie de Rennes

6ème place, 3ème prix

Format de l'ITYM ($\mathbb{TFJM}^2$ assez similaire)

- 6 lycéens par équipe ; 1 (ou 2) encadrant.e bénévole
- 10 problèmes ouverts difficiles mais accessibles
- quelques mois de recherche encadrée

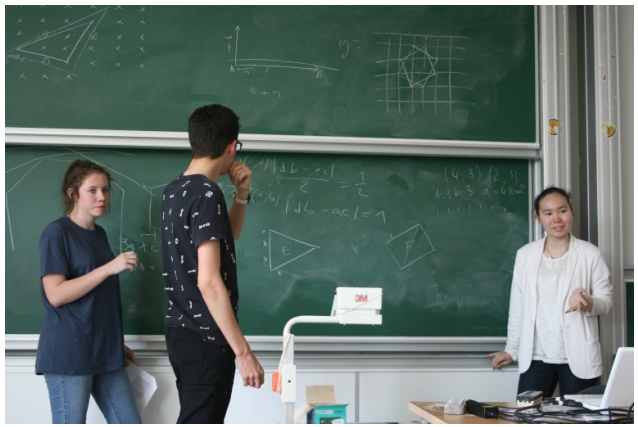
Format de l'ITYM ($\mathbb{TFJM}^2$ assez similaire)



- 6 lycéens par équipe ; 1 (ou 2) encadrant.e bénévole
- 10 problèmes ouverts difficiles mais accessibles
- quelques mois de recherche encadrée
- des débats (30 min par débat + 10 min jury) confrontant

  1 Défeuseur.e ($<$ 10 min), 1 Opposant.e ($\sim$ 8 min), 1 Rapporteur.e ($\sim$ 7 min), 1 Observateur.e

Format de l'ITYM ($\mathbb{TFJM}^2$ assez similaire)



- 6 lycéens par équipe ; 1 (ou 2) encadrant.e bénévole
- 10 problèmes ouverts difficiles mais accessibles
- quelques mois de recherche encadrée
- des débats (30 min par débat + 10 min jury) confrontant

  1 Défeuseur.e ($<$ 10 min), 1 Opposant.e ($\sim$ 8 min), 1 Rapporteur.e ($\sim$ 7 min), 1 Observateur.e
- un jury de mathématicien.ne.s constitué de :

  Doctorant.e.s, Chercheur.e.s, Enseignant.e.s, Ancien.ne.s participant.e.s, Encadrant.e.s

Un problème d'ITYM : Tables d'opération – I

Let $q \geqslant 2$ be an integer. Denote by $[\![0, q-1]\!]$ the set of integers from 0 to $q-1$. A function $\star : [\![0, q-1]\!] \times [\![0, q-1]\!] \to [\![0, q-1]\!]$ is called a q-operation, if there exists an element $e \in [\![0, q-1]\!]$ such that :

- for all $x \in [\![0, q-1]\!]$, we have $\star(x, e) = x$;
- for any $x, y \in [\![0, q-1]\!]$, we have $\star(e, \star(y, x))) = \star(x, y)$

If $\star$ is a q-operation, we shall write $x \star y$ instead of $\star(x, y)$. For any function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ we can construct a function

$$f_q : [\![0, q-1]\!] \times [\![0, q-1]\!] \to [\![0, q-1]\!], \qquad (x, y) \mapsto f(x, y) \mod q.$$

For example, for $f(x, y) = x - y$ and $q = 10$ we have $f_q(2, 5) = 7$, since $2 - 5 = -3 \equiv 7 \mod 10$. For simplicity, we shall use the notation $+_q$, $-_q$, $\times_q$, $\gcd_q$ for functions $x + y$, $x - y$, $x \times y$, $\gcd(x, y)$.

Un problème d'ITYM : Tables d'opération – I

Let $q \geqslant 2$ be an integer. Denote by $[\![0, q-1]\!]$ the set of integers from 0 to $q-1$. A function $\star : [\![0, q-1]\!] \times [\![0, q-1]\!] \to [\![0, q-1]\!]$ is called a q-operation, if there exists an element $e \in [\![0, q-1]\!]$ such that :

- for all $x \in [\![0, q-1]\!]$, we have $\star(x, e) = x$;
- for any $x, y \in [\![0, q-1]\!]$, we have $\star(e, \star(y, x))) = \star(x, y)$

If $\star$ is a q-operation, we shall write $x \star y$ instead of $\star(x, y)$. For any function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ we can construct a function

$$f_q : [\![0, q-1]\!] \times [\![0, q-1]\!] \to [\![0, q-1]\!], \qquad (x, y) \mapsto f(x, y) \mod q.$$

For example, for $f(x, y) = x - y$ and $q = 10$ we have $f_q(2, 5) = 7$, since $2 - 5 = -3 \equiv 7 \mod 10$. For simplicity, we shall use the notation $+_q$, $-_q$, $\times_q$, $\gcd_q$ for functions $x + y$, $x - y$, $x \times y$, $\gcd(x, y)$.

1. Verify that $+_q$, $-_q$, $\times_q$ and $\gcd_q$ are q-operations and find the corresponding element e for each of them. Can you find other examples of q-operations ?

2. Find the number of possible q-operations as a function of q.

Un problème d'ITYM : Tables d'opération – II

We say that a subset $D \subset [\![0, q-1]\!]$ is $\star$-complete, if for any $z \in [\![0, q-1]\!]$ there exist elements $x, y \in D$ such that $x \star y = z$. Define
$c_q(\star) = \min\{\#D,\ D \text{ is } \star\text{-complete}\}$.

3. Estimate $c_q(\mathrm{gcd}_q)$, $c_q(-_q)$, $c_q(+_q)$, $c_q(\times_q)$ as functions of q.

4. What can you say about $c_{q+1}(\star_{q+1}) - c_q(\star_q)$ for $\star \in \{\mathrm{gcd}, +, -, \times\}$?

Un problème d'ITYM : Tables d'opération – II

We say that a subset $D \subset [\![0, q-1]\!]$ is $\star$-complete, if for any $z \in [\![0, q-1]\!]$ there exist elements $x, y \in D$ such that $x \star y = z$. Define
$c_q(\star) = \min\{\#D,\ D \text{ is } \star\text{-complete}\}$.

3. Estimate $c_q(\gcd_q)$, $c_q(-_q)$, $c_q(+_q)$, $c_q(\times_q)$ as functions of q.

4. What can you say about $c_{q+1}(\star_{q+1}) - c_q(\star_q)$ for $\star \in \{\gcd, +, -, \times\}$?

For any q-operation $\star$ consider the number of smallest $\star$-complete subsets
$d_q(\star) = \#\{D \subset [\![0, q-1]\!],\ D \text{ is } \star\text{-complete and } \#D = c_q(\star)\}$.

5. Study the numbers $d_q(\star)$ for $\star \in \{\gcd, +, -, \times\}$. In particular, try answering the following questions :

(a) When q divides $d_q(\star)$?

(b) Can you give an estimate for $d_q(\star)$?

(c) Are there subsequences of $d_q(\star)$ that form (infinite) arithmetic sequences ?

6. Investigate other interesting operations $\star$ or explore other tracks of research.

Un problème d'ITYM : Tables d'opération – III

Ici pour se détendre !

Un problème d'ITYM : Tables d'opération – III

Ici pour se détendre !

Au programme :

- des tables de soustraction,

–	0	1	4	14	16
0	0	20	17	7	5
1	1	0	18	8	6
4	4	3	0	11	9
14	14	13	10	0	19
16	16	15	12	2	0

Table de soustraction modulo 21

Un problème d'ITYM : Tables d'opération – III

Ici pour se détendre !

Au programme :

- des tables de soustraction,
- de la géométrie projective,

–	0	1	4	14	16
0	0	20	17	7	5
1	1	0	18	8	6
4	4	3	0	11	9
14	14	13	10	0	19
16	16	15	12	2	0

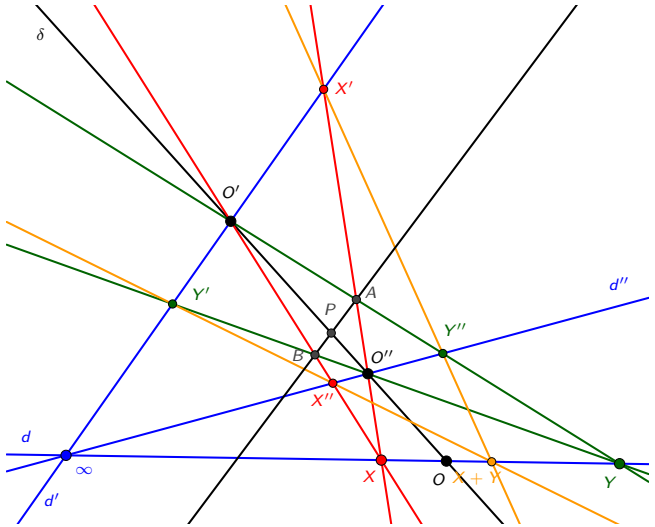
Table de soustraction modulo 21

Un problème d'ITYM : Tables d'opération – III

Ici pour se détendre !

Au programme :

- des tables de soustraction,
- de la géométrie projective,
- des dessins de plans (finis).



—	0	1	4	14	16
0	0	20	17	7	5
1	1	0	18	8	6
4	4	3	0	11	9
14	14	13	10	0	19
16	16	15	12	2	0

Table de soustraction modulo 21

Outline

1 Un problème d'ITYM

2 Ensembles à différence

3 Géométrie projective

4 Plans projectifs finis

Ce que le problème d'ITYM nous invite à étudier

We say that a subset $D \subset [\![0, q-1]\!]$ *is* $\star$*-complete, if for any* $z \in [\![0, q-1]\!]$ *there exist elements* $x, y \in D$ *such that* $x \star y = z$*. Define* $c_q(\star) = \min\{\#D,\ D \text{ is } \star\text{-complete}\}$.

3. *Estimate* $c_q(\mathrm{gcd}_q)$, $c_q(-_q)$, $c_q(+_q)$, $c_q(\times_q)$ *as functions of* q.

Ce que le problème d'ITYM nous invite à étudier

We say that a subset $D \subset [\![0, q-1]\!]$ *is* $\star$*-complete, if for any* $z \in [\![0, q-1]\!]$ *there exist elements* $x, y \in D$ *such that* $x \star y = z$*. Define* $c_q(\star) = \min\{\#D,\ D \text{ is } \star\text{-complete}\}$.

3. *Estimate* $c_q(\mathrm{gcd}_q)$, $c_q\big(-_q\big)$, $c_q(+_q)$, $c_q(\times_q)$ *as functions of* q.

Définition

Une partie $D \subset \mathbb{Z}/q\mathbb{Z}$ est un *ensemble à différence* (planaire, modulo q) si

$$\forall x \in \mathbb{Z}/q\mathbb{Z},\ \exists (y,z) \in D^2,\ x = y - z.$$

Ce que le problème d'ITYM nous invite à étudier

We say that a subset $D \subset [\![0, q-1]\!]$ *is* $\star$*-complete, if for any* $z \in [\![0, q-1]\!]$ *there exist elements* $x, y \in D$ *such that* $x \star y = z$*. Define* $c_q(\star) = \min\{\#D,\ D \text{ is } \star\text{-complete}\}$.

3. *Estimate* $c_q(\gcd_q)$, $c_q(-_q)$, $c_q(+_q)$, $c_q(\times_q)$ *as functions of* q.

Définition

Une partie $D \subset \mathbb{Z}/q\mathbb{Z}$ est un *ensemble à différence* (planaire, modulo q) si

$$\forall x \in \mathbb{Z}/q\mathbb{Z},\ \exists (y,z) \in D^2,\ x = y - z.$$

Un ensemble à différence D est *parfait* si

$$\forall x \in \mathbb{Z}/q\mathbb{Z} \setminus \{0\},\ \exists! (y,z) \in D^2,\ x = y - z.$$

Généralisation : Remplacer $(\mathbb{Z}/q\mathbb{Z}, +)$ par $(G, \cdot)$ groupe et $y - z$ par $y \cdot z^{-1}$.

Ce que le problème d'ITYM nous invite à étudier

We say that a subset $D \subset [\![0, q-1]\!]$ *is* $\star$*-complete, if for any* $z \in [\![0, q-1]\!]$ *there exist elements* $x, y \in D$ *such that* $x \star y = z$. *Define* $c_q(\star) = \min\{\#D,\ D \text{ is } \star\text{-complete}\}$.

3. *Estimate* $c_q(\mathrm{gcd}_q)$, $c_q(-_q)$, $c_q(+_q)$, $c_q(\times_q)$ *as functions of* q.

Définition

Une partie $D \subset \mathbb{Z}/q\mathbb{Z}$ est un *ensemble à différence* (planaire, modulo q) si

$$\forall x \in \mathbb{Z}/q\mathbb{Z},\ \exists (y,z) \in D^2,\ x = y - z.$$

Un ensemble à différence D est *parfait* si

$$\forall x \in \mathbb{Z}/q\mathbb{Z} \setminus \{0\},\ \exists! (y,z) \in D^2,\ x = y - z.$$

Généralisation : Remplacer $(\mathbb{Z}/q\mathbb{Z}, +)$ par $(G, \cdot)$ groupe et $y - z$ par $y \cdot z^{-1}$.

Notation

$c(q) = \min\{\mathrm{Card}(D),\ D \text{ ensemble à différence modulo } q\}$

Tables de soustraction modulo q

On choisit $q = 7 = 1 + \ell + \ell^2$ avec $\ell = 2$.
On se place dans $\mathbb{Z}/7\mathbb{Z}$. On choisit $D \subset \mathbb{Z}/7\mathbb{Z}$.

$$D_1 = \{0, 1, 2, 3, 4, 5, 6\}$$

Tables de soustraction modulo q

On choisit $q = 7 = 1 + \ell + \ell^2$ avec $\ell = 2$.
On se place dans $\mathbb{Z}/7\mathbb{Z}$. On choisit $D \subset \mathbb{Z}/7\mathbb{Z}$.

$$D_1 = \{0, 1, 2, 3, 4, 5, 6\}$$

Table de soustraction $x - y \mod 7$ pour $x, y \in D_1$:

$-$	0	1	2	3	4	5	6
0	0	6	5	4	3	2	1
1	1	0	6	5	4	3	2
2	2	1	0	6	5	4	3
3	3	2	1	0	6	5	4
4	4	3	2	1	0	6	5
5	5	4	3	2	1	0	6
6	6	5	4	3	2	1	0

$$c(7) \leqslant \mathrm{Card}(D_1) = 7$$

Tables de soustraction modulo q

On choisit $q = 7 = 1 + \ell + \ell^2$ avec $\ell = 2$.
On se place dans $\mathbb{Z}/7\mathbb{Z}$. On choisit $D \subset \mathbb{Z}/7\mathbb{Z}$.

$$D_2 = \{0, 1, \ , 3, \ , \ , \ \}$$

Table de soustraction $x - y \mod 7$ pour $x, y \in D_2$:

$-$	0	1	3	
0	0	6	4	
1	1	0	5	
3	3	2	0	

$$c(7) \leqslant \mathrm{Card}(D_1) = 7$$

$$c(7) \leqslant \mathrm{Card}(D_2) = 3$$

Tables de soustraction modulo q

On choisit $q = 7 = 1 + \ell + \ell^2$ avec $\ell = 2$.
On se place dans $\mathbb{Z}/7\mathbb{Z}$. On choisit $D \subset \mathbb{Z}/7\mathbb{Z}$.

$$D_3 = \{0, 1, 2, \ , \ , 5, \ \}$$

Table de soustraction $x - y \mod 7$ pour $x, y \in D_3$:

$-$	0	1	2		5
0	0	6	5		2
1	1	0	6		3
2	2	1	0		4
5	5	4	3		0

$$c(7) \leqslant \mathrm{Card}(D_1) = 7$$

$$c(7) \leqslant \mathrm{Card}(D_2) = 3$$

D_3 pas minimale

$$c(7) \leqslant 3 < \mathrm{Card}(D_3) = 4$$

Tables de soustraction modulo q

On choisit $q = 7 = 1 + \ell + \ell^2$ avec $\ell = 2$.
On se place dans $\mathbb{Z}/7\mathbb{Z}$. On choisit $D \subset \mathbb{Z}/7\mathbb{Z}$.

$$D_4 = \{0, \ , 2, \ , \ , 5, \ \}$$

Table de soustraction $x - y \mod 7$ pour $x, y \in D_4$:

$-$	0	2	5
0	0	5	2
2	2	0	4
5	5	3	0

$c(7) \leqslant \mathrm{Card}(D_1) = 7$

$c(7) \leqslant \mathrm{Card}(D_2) = 3$

D_3 pas minimale
$c(7) \leqslant 3 < \mathrm{Card}(D_3) = 4$

D_4 pas assez de différences.

Cardinal d'un ensemble à différence

Voici un résultat obtenu par des lycéens :

Proposition

On a :

$$\frac{1+\sqrt{4q-3}}{2} \leqslant c(q) \leqslant \sqrt{2(q+1)}+1.$$

Borne inférieure en $\sim \sqrt{q}$

Borne supérieure en $\sim \sqrt{2q}$.

Borne inférieure $\frac{1+\sqrt{4q-3}}{2} \leqslant c(q)$

Borne inférieure $\frac{1+\sqrt{4q-3}}{2} \leqslant c(q)$

Soit $D = \{d_1, \ldots, d_k\}$ ensemble à différence modulo q de cardinal k. Sur la table de soustraction de D, il y a :

	d_1	$\cdots$	d_k
d_1			
$\vdots$			
d_k			

Borne inférieure $\frac{1+\sqrt{4q-3}}{2} \leqslant c(q)$

Soit $D = \{d_1, \ldots, d_k\}$ ensemble à différence modulo q de cardinal k. Sur la table de soustraction de D, il y a :

- k fois 0 sur la diagonale

	d_1	$\cdots$	d_k
d_1	0		
$\vdots$		0	
d_k			0

Borne inférieure $\frac{1+\sqrt{4q-3}}{2} \leqslant c(q)$

Soit $D = \{d_1, \ldots, d_k\}$ ensemble à différence modulo q de cardinal k. Sur la table de soustraction de D, il y a :

- k fois 0 sur la diagonale
- $\leqslant k^2 - k$ valeurs hors diagonale

	d_1	$\cdots$	d_k
d_1		$*$	$*$
$\vdots$	$*$		$*$
d_k	$*$	$*$	

Borne inférieure $\frac{1+\sqrt{4q-3}}{2} \leqslant c(q)$

Soit $D = \{d_1, \ldots, d_k\}$ ensemble à différence modulo q de cardinal k. Sur la table de soustraction de D, il y a :

- k fois 0 sur la diagonale
- $\leqslant k^2 - k$ valeurs hors diagonale

Ainsi $q \leqslant k^2 - k + 1$.

	d_1	$\cdots$	d_k
d_1	0	$*$	$*$
$\vdots$	$*$	0	$*$
d_k	$*$	$*$	0

Borne inférieure $\frac{1+\sqrt{4q-3}}{2} \leqslant c(q)$

Soit $D = \{d_1, \ldots, d_k\}$ ensemble à différence modulo q de cardinal k. Sur la table de soustraction de D, il y a :

- k fois 0 sur la diagonale
- $\leqslant k^2 - k$ valeurs hors diagonale

	d_1	$\cdots$	d_k
d_1	0	$*$	$*$
$\vdots$	$*$	0	$*$
d_k	$*$	$*$	0

Ainsi $q \leqslant k^2 - k + 1$.

$\rightsquigarrow \quad \frac{1+\sqrt{4q-3}}{2} \leqslant k.$

Borne inférieure $\frac{1+\sqrt{4q-3}}{2} \leqslant c(q)$

Soit $D = \{d_1, \ldots, d_k\}$ ensemble à différence modulo q de cardinal k. Sur la table de soustraction de D, il y a :

- k fois 0 sur la diagonale
- $\leqslant k^2 - k$ valeurs hors diagonale

	d_1	$\cdots$	d_k
d_1	0	$*$	$*$
$\vdots$	$*$	0	$*$
d_k	$*$	$*$	0

Ainsi $q \leqslant k^2 - k + 1$.

$\rightsquigarrow \quad \frac{1+\sqrt{4q-3}}{2} \leqslant k.$

Fait

D ensemble à différence parfait modulo q $\iff \mathrm{Card}(D) = \frac{1+\sqrt{4q-3}}{2}$.

Si D parfait mod q avec $\mathrm{Card}(D) = \ell + 1$, alors $q = 1 + \ell + \ell^2$.

Recherche d'ensembles à différence parfaits

Exemple

Pour $\ell = 7$, soit $q = 1 + 7 + 49 = 57$,
on trouve $D = \{0, 1, 3, 13, 32, 36, 43, 52\}$.

57	0	1	3	13	32	36	43	52
0	0	56	54	44	25	21	14	5
1	1	0	55	45	26	22	15	6
3	3	2	0	47	28	24	17	8
13	13	12	10	0	38	34	27	18
32	32	31	29	19	0	53	46	37
36	36	35	33	23	4	0	50	41
43	43	42	40	30	11	7	0	48
52	52	51	49	39	20	16	9	0

Borne supérieure pour $c(q)$

Stratégie : exhiber des familles d'ensembles à différence modulo q.

Lemme

$D_n = \{0, 1, \ldots, n-1, 2n-1, 3n-1, \ldots, \left\lceil \frac{q}{2n} \right\rceil n - 1\}$ est un ensemble à différence modulo q.

Preuve : faire la division euclidienne.

Borne supérieure pour $c(q)$

Stratégie : exhiber des familles d'ensembles à différence modulo q.

Lemme

$D_n = \{0, 1, \ldots, n-1, 2n-1, 3n-1, \ldots, \left\lceil \frac{q}{2n} \right\rceil n - 1\}$ est un ensemble à différence modulo q.

Preuve : faire la division euclidienne.

Ainsi $c(q) \leqslant \mathrm{Card}(D_n) = n + \left\lceil \frac{q}{2n} \right\rceil - 1$.

Minimum en $\simeq \sqrt{\frac{q}{2}}$ donne une borne supérieure en $\sim \sqrt{2q}$.

Borne supérieure pour $c(q)$

Stratégie : exhiber des familles d'ensembles à différence modulo q.

Lemme

$D_n = \{0, 1, \ldots, n-1, 2n-1, 3n-1, \ldots, \left\lceil \frac{q}{2n} \right\rceil n - 1\}$ est un ensemble à différence modulo q.

Preuve : faire la division euclidienne.
Ainsi $c(q) \leqslant \mathrm{Card}(D_n) = n + \left\lceil \frac{q}{2n} \right\rceil - 1$.
Minimum en $\simeq \sqrt{\frac{q}{2}}$ donne une borne supérieure en $\sim \sqrt{2q}$.

Remarque

Banakh-Gavrylkiv (mai 2019) trouvent la borne supérieure :

- $\sim \frac{12}{\sqrt{73}} \sqrt{q}$ pour q quelconque ;
- $\sim \frac{2}{\sqrt{3}} \sqrt{q}$ pour $q > 2.10^{15}$.

Un contre-exemple

Pour $\ell = 6$, soit $q = 43$, pas d'ensemble à différence parfait.
Se vérifie par ordinateur :

```
def C(q):
    S=Set(range(0,q))
    for k in range(0,q+1):
        P=S.subsets(k)
        for D in P:
            W=Set(((x-y)%q) for x in D for y in D)
            if(W.cardinality()==q):
                return k
```

donne $C(43) = 8 \neq 1 + 6$.

Exemple d'ensemble à différence modulo 43 minimal mais non parfait :

$$D = \{0, 1, 2, 3, 4, 10, 15, 26\}$$

Construction d'ensembles à différence parfaits : l'énoncé

Théorème (Singer (1938))

Si ℓ une puissance d'un nombre premier et $q = 1 + \ell + \ell^2$, alors il existe un ensemble à différence parfait modulo q.

Construction d'ensembles à différence parfaits : l'énoncé

Théorème (Singer (1938))

Si ℓ une puissance d'un nombre premier et $q = 1 + \ell + \ell^2$, alors il existe un ensemble à différence parfait modulo q.

L'égalité

$$q = 1 + \ell + \ell^2 = \frac{\ell^3 - 1}{\ell - 1}$$

invite à travailler dans $\mathbb{P}^2(\mathbb{F}_\ell)$.

Outline

1 Un problème d'ITYM

2 Ensembles à différence

3 Géométrie projective

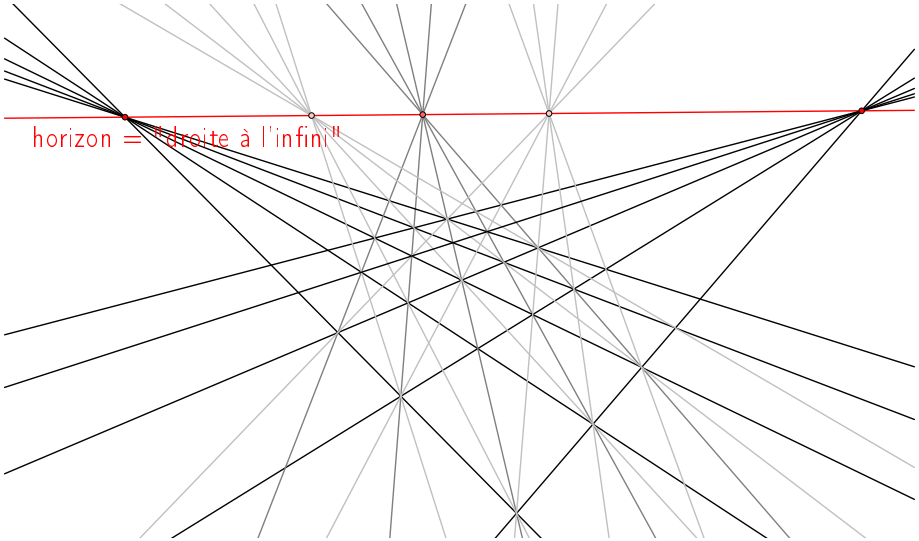
4 Plans projectifs finis

Qu'est-ce que la géométrie projective ?

- attribuée à Girard Desargues, XVIIème siècle, mathématicien et architecte lyonnais ;
- clarifiée par Félix Klein, XIXème siècle, Programme d'Erlangen 1872 : actions de groupes.

Viticulture chilienne, quelque part entre Talca et Santiago, juillet 2018.

Plan projectif réel



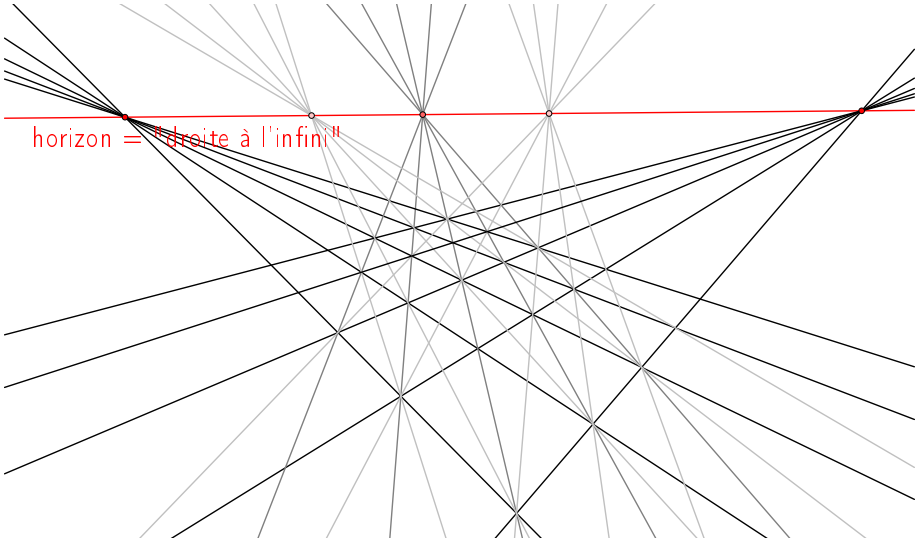
$$\mathbb{P}^2(\mathbb{R}) = \left(\mathbb{R}^3 \setminus \{0\}\right)/\mathbb{R}^*$$

Points $\Pi = \{k \cdot v$ **droites vectorielles**, $v \neq 0\}$

Droites $\Delta = \{W$ **plans vectoriels**, $\dim(W) = 2\}$

Incidence $p = [v] \in \delta = [W] \iff kv \subset W$

Plan projectif réel



$$\mathbb{P}^2(\mathbb{R}) = \left(\mathbb{R}^3 \setminus \{0\}\right)/\mathbb{R}^*$$

Points $\Pi = \{k \cdot v$ **droites vectorielles**, $v \neq 0\}$

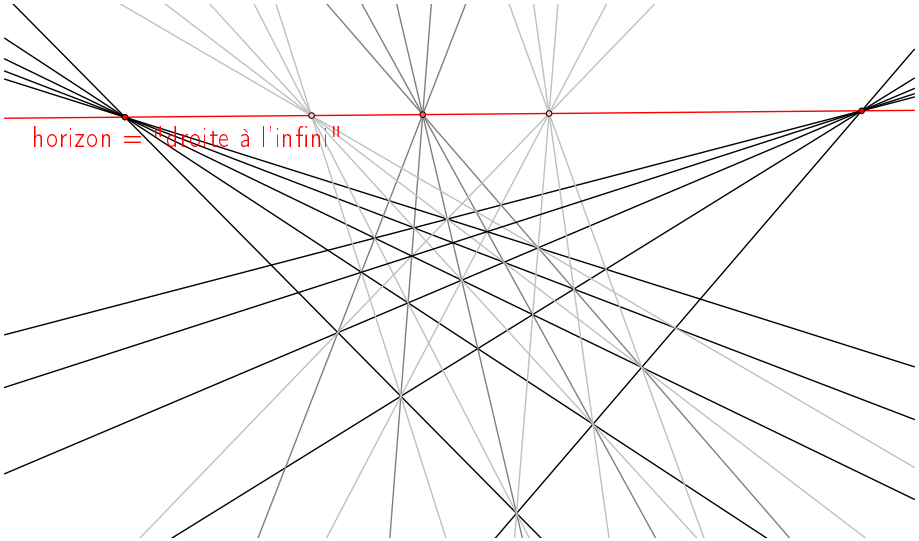
Droites $\Delta = \{W$ **plans vectoriels**, $\dim(W) = 2\}$

Incidence $p = [v] \in \delta = [W] \iff kv \subset W$

Proposition

Deux droites distinctes s'intersectent en un unique point.

Plan projectif réel



$$\mathbb{P}^2(\mathbb{R}) = \left(\mathbb{R}^3 \setminus \{0\}\right)/\mathbb{R}^*$$

Points $\Pi = \{k \cdot v$ **droites vectorielles**, $v \neq 0\}$

Droites $\Delta = \{W$ **plans vectoriels**, $\dim(W) = 2\}$

Incidence $p = [v] \in \delta = [W] \iff kv \subset W$

Proposition

Deux droites distinctes s'intersectent en un unique point.

Preuve : Deux plans vectoriels distincts s'intersectent en une droite vectorielle.

Théorème de Desargues

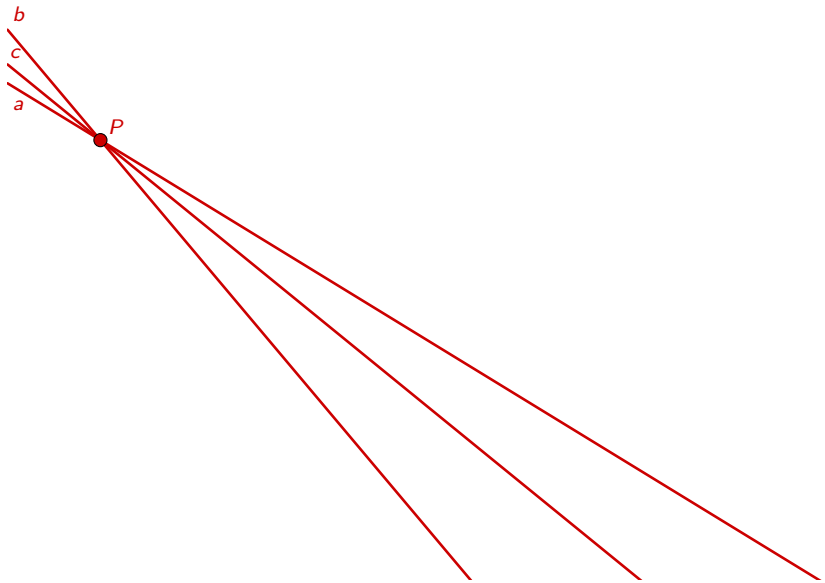
Théorème (Desargues)

Dans $\mathbb{P}^2(K)$ sur K **corps gauche**, *étant donnés deux triangles $A_1B_1C_1$ et $A_2B_2C_2$, si les trois droites $a = (A_1A_2)$, $b = (B_1B_2)$ et $c = (C_1C_2)$ sont concourantes, alors les trois points d'intersection $A = (B_1C_1) \cap (B_2C_2)$, $B = (C_1A_1) \cap (C_2A_2)$ et $C = (A_1B_1) \cap (A_2B_2)$ sont alignés.*

Théorème de Desargues

Théorème (Desargues)

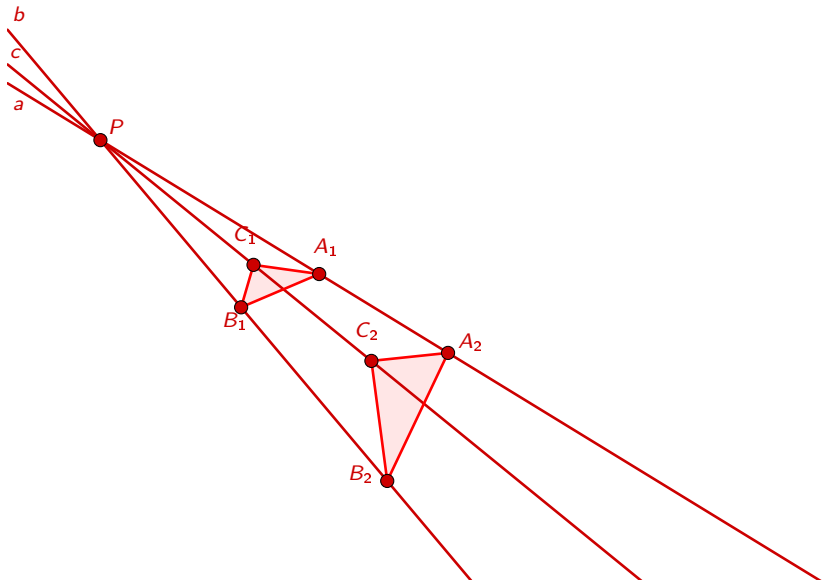
Dans $\mathbb{P}^2(K)$ sur K **corps gauche**, *étant donnés deux triangles $A_1B_1C_1$ et $A_2B_2C_2$, si les trois droites $a = (A_1A_2)$, $b = (B_1B_2)$ et $c = (C_1C_2)$ sont concourantes, alors les trois points d'intersection $A = (B_1C_1) \cap (B_2C_2)$, $B = (C_1A_1) \cap (C_2A_2)$ et $C = (A_1B_1) \cap (A_2B_2)$ sont alignés.*



Théorème de Desargues

Théorème (Desargues)

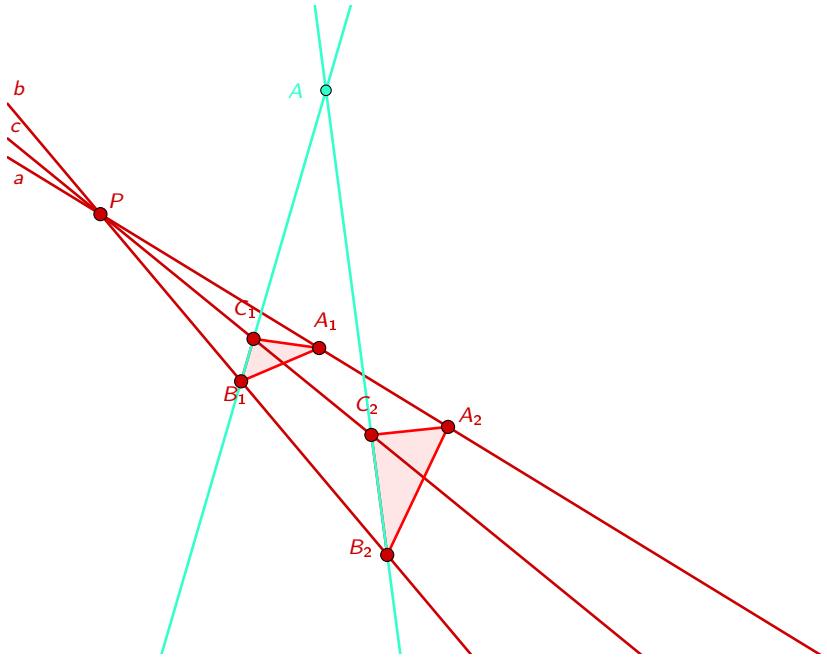
Dans $\mathbb{P}^2(K)$ sur K **corps gauche**, *étant donnés deux triangles $A_1B_1C_1$ et $A_2B_2C_2$, si les trois droites $a = (A_1A_2)$, $b = (B_1B_2)$ et $c = (C_1C_2)$ sont concourantes, alors les trois points d'intersection $A = (B_1C_1) \cap (B_2C_2)$, $B = (C_1A_1) \cap (C_2A_2)$ et $C = (A_1B_1) \cap (A_2B_2)$ sont alignés.*



Théorème de Desargues

Théorème (Desargues)

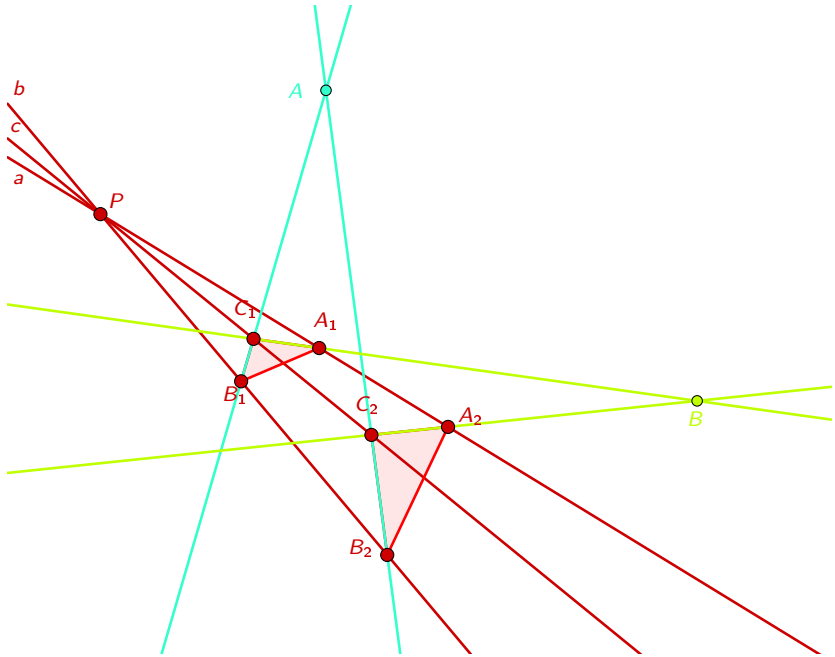
Dans $\mathbb{P}^2(K)$ sur K **corps gauche**, *étant donnés deux triangles $A_1B_1C_1$ et $A_2B_2C_2$, si les trois droites $a = (A_1A_2)$, $b = (B_1B_2)$ et $c = (C_1C_2)$ sont concourantes, alors les trois points d'intersection $A = (B_1C_1) \cap (B_2C_2)$, $B = (C_1A_1) \cap (C_2A_2)$ et $C = (A_1B_1) \cap (A_2B_2)$ sont alignés.*



Théorème de Desargues

Théorème (Desargues)

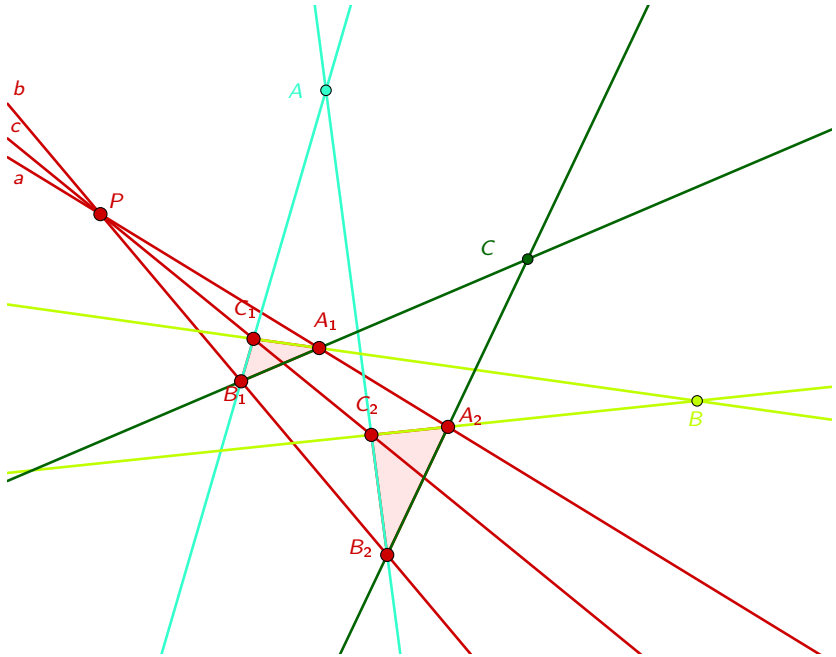
Dans $\mathbb{P}^2(K)$ sur K **corps gauche**, *étant donnés deux triangles $A_1B_1C_1$ et $A_2B_2C_2$, si les trois droites $a = (A_1A_2)$, $b = (B_1B_2)$ et $c = (C_1C_2)$ sont concourantes, alors les trois points d'intersection $A = (B_1C_1) \cap (B_2C_2)$, $B = (C_1A_1) \cap (C_2A_2)$ et $C = (A_1B_1) \cap (A_2B_2)$ sont alignés.*



Théorème de Desargues

Théorème (Desargues)

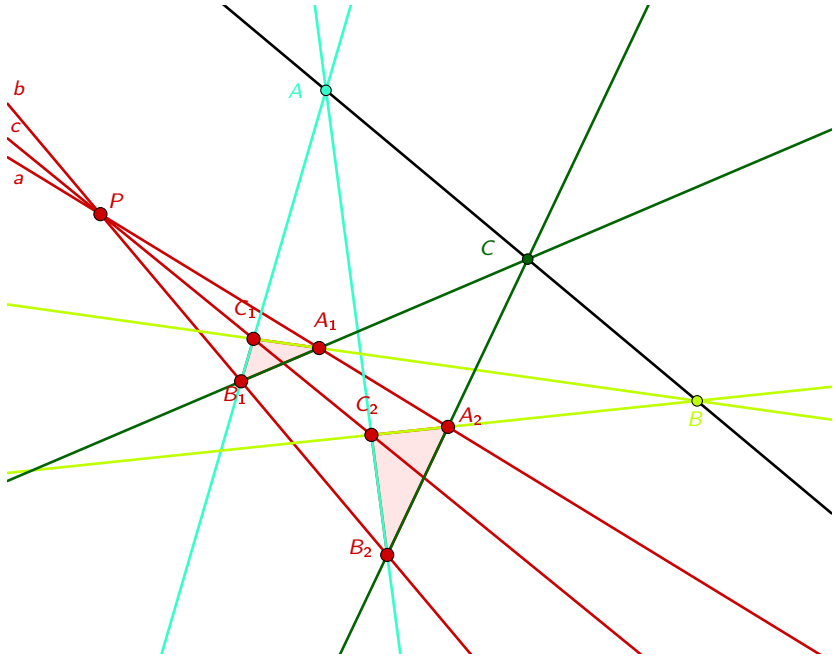
Dans $\mathbb{P}^2(K)$ sur K **corps gauche**, *étant donnés deux triangles $A_1B_1C_1$ et $A_2B_2C_2$, si les trois droites $a = (A_1A_2)$, $b = (B_1B_2)$ et $c = (C_1C_2)$ sont concourantes, alors les trois points d'intersection $A = (B_1C_1) \cap (B_2C_2)$, $B = (C_1A_1) \cap (C_2A_2)$ et $C = (A_1B_1) \cap (A_2B_2)$ sont alignés.*



Théorème de Desargues

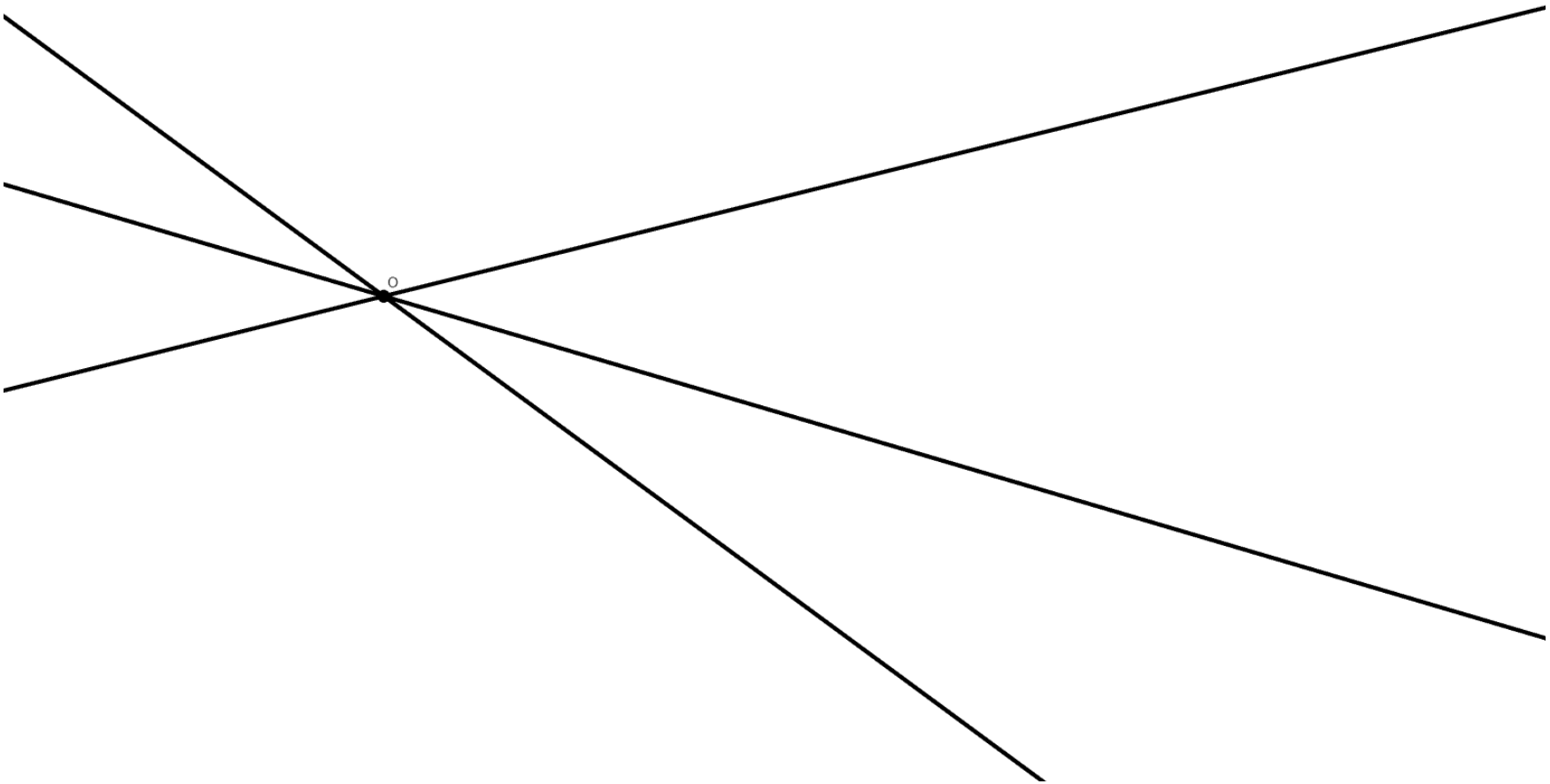
Théorème (Desargues)

Dans $\mathbb{P}^2(K)$ sur K **corps gauche**, *étant donnés deux triangles $A_1B_1C_1$ et $A_2B_2C_2$, si les trois droites $a = (A_1A_2)$, $b = (B_1B_2)$ et $c = (C_1C_2)$ sont concourantes, alors les trois points d'intersection $A = (B_1C_1) \cap (B_2C_2)$, $B = (C_1A_1) \cap (C_2A_2)$ et $C = (A_1B_1) \cap (A_2B_2)$ sont alignés.*



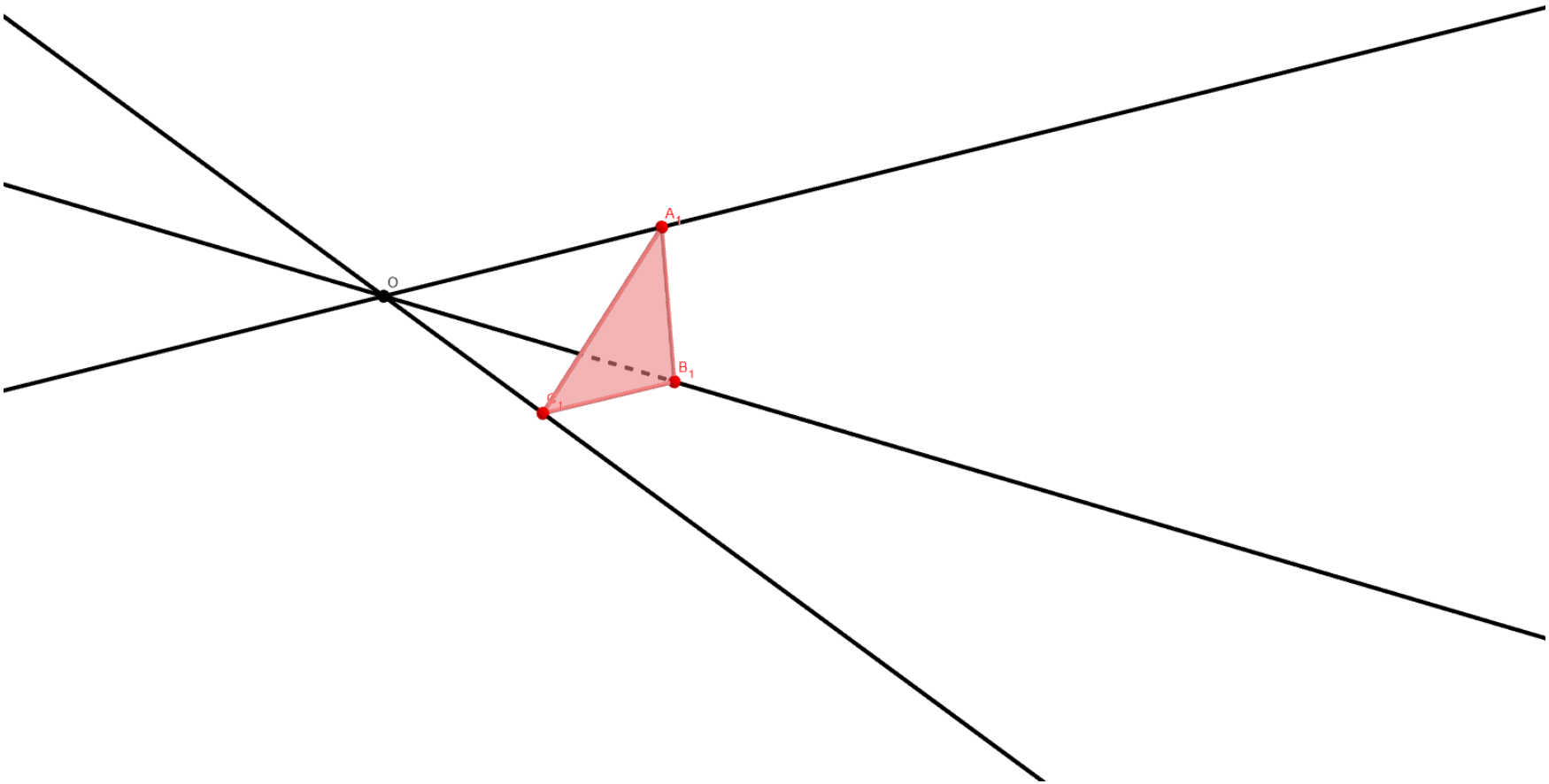
Interprétation en dimension supérieure

Le théorème de Desargues est vrai en dimension $\geqslant 3$, et ça se voit !



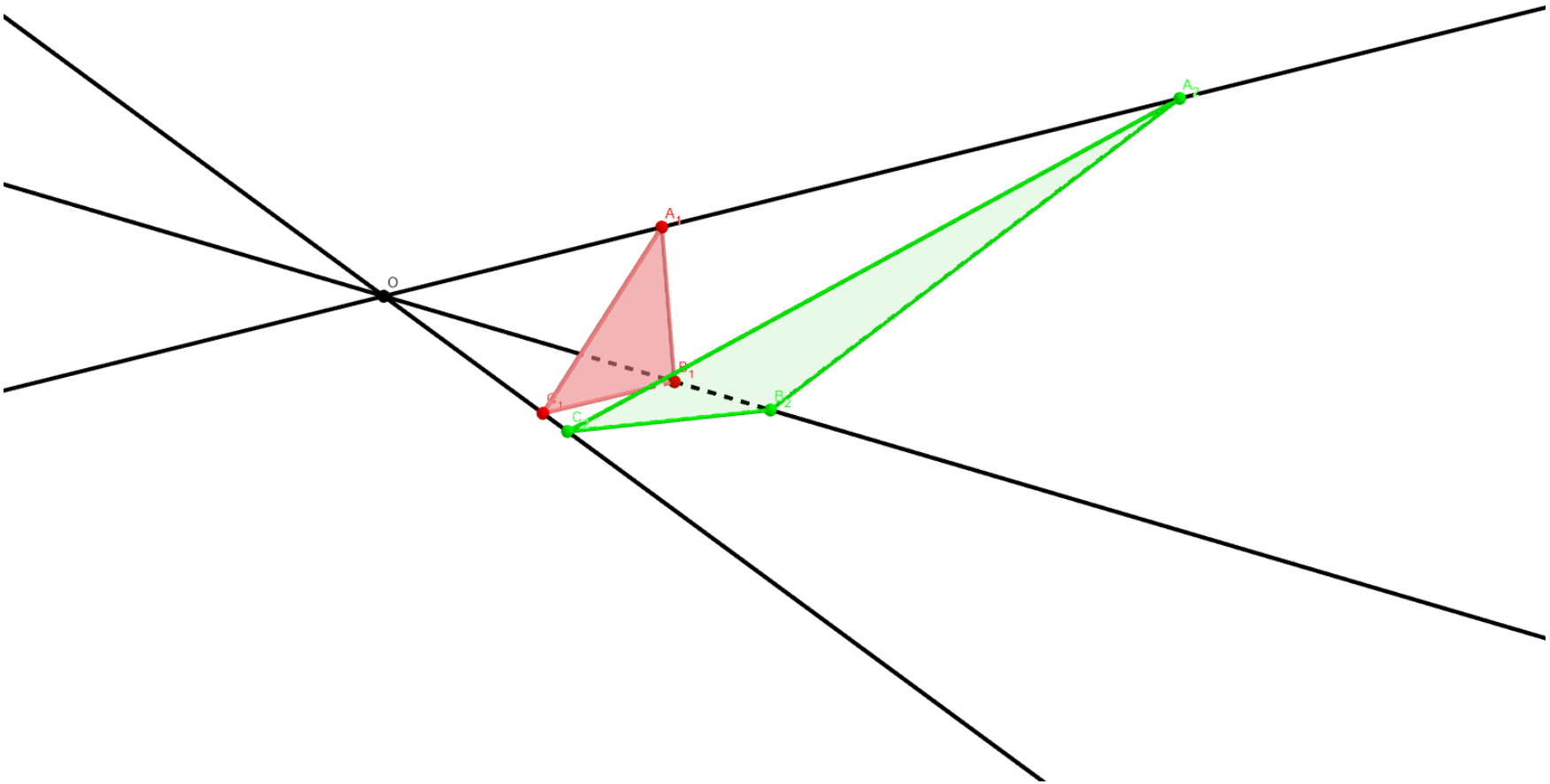
Interprétation en dimension supérieure

Le théorème de Desargues est vrai en dimension $\geqslant 3$, et ça se voit !



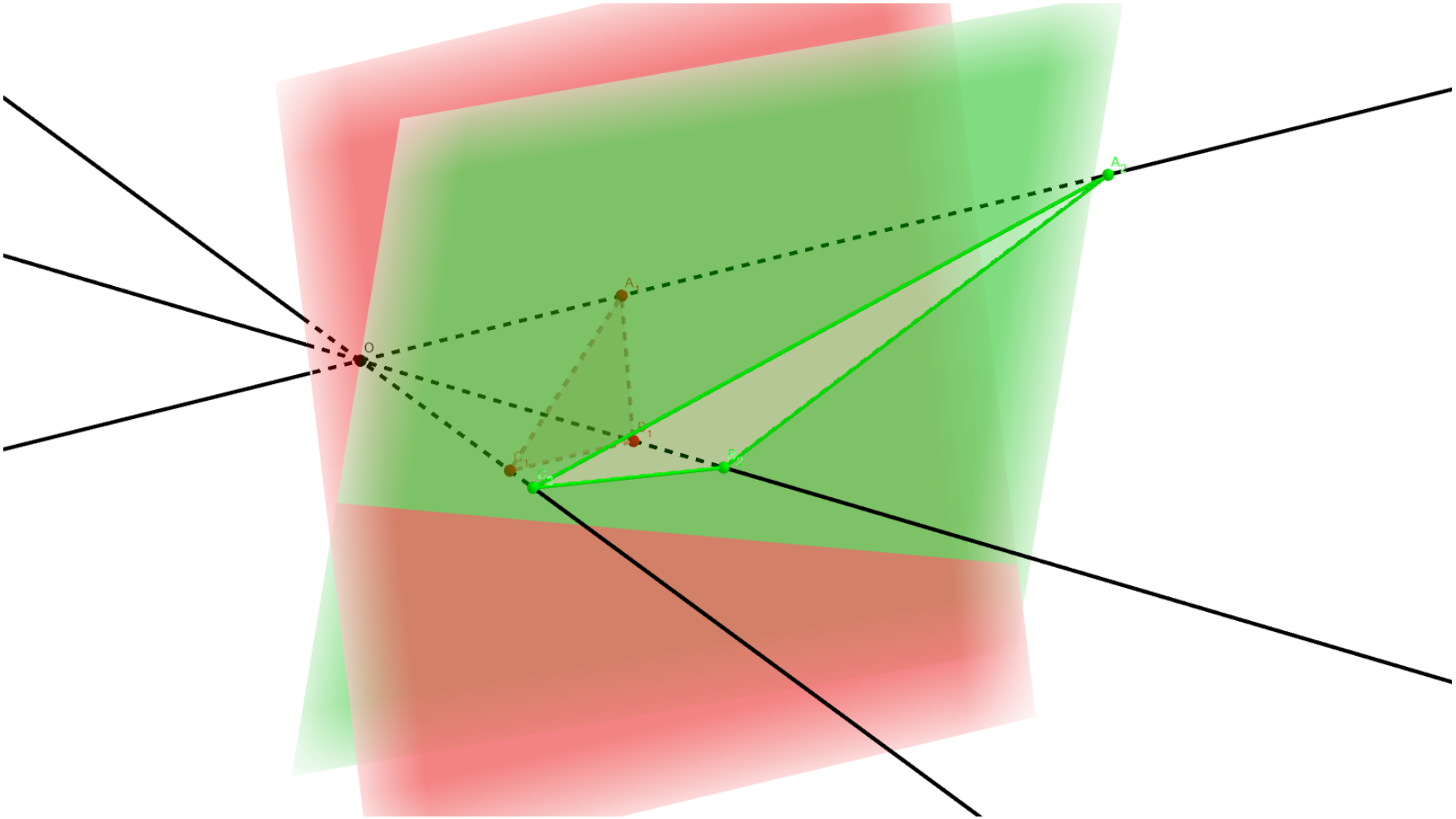
Interprétation en dimension supérieure

Le théorème de Desargues est vrai en dimension $\geqslant 3$, et ça se voit !



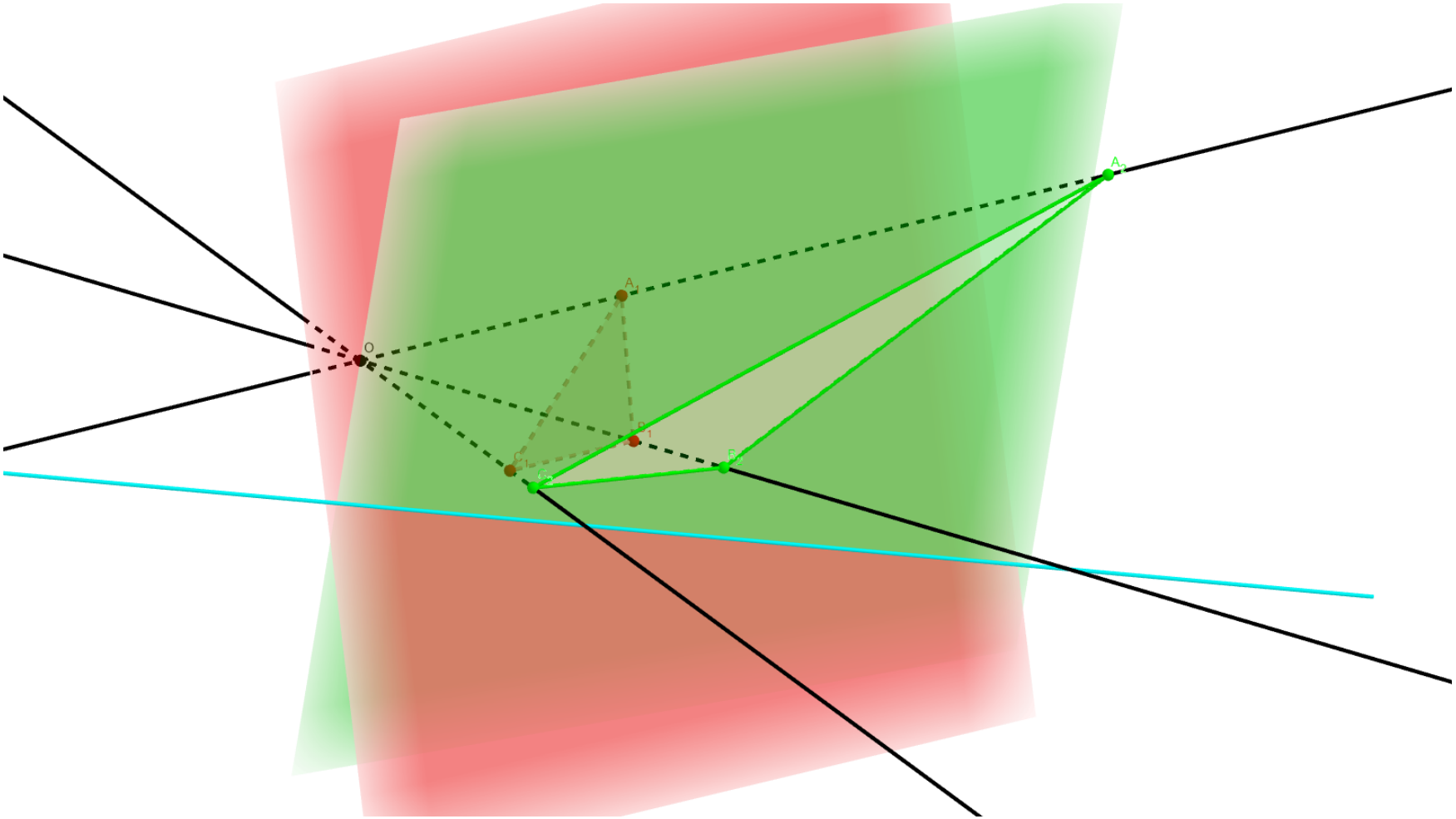
Interprétation en dimension supérieure

Le théorème de Desargues est vrai en dimension $\geqslant 3$, et ça se voit !



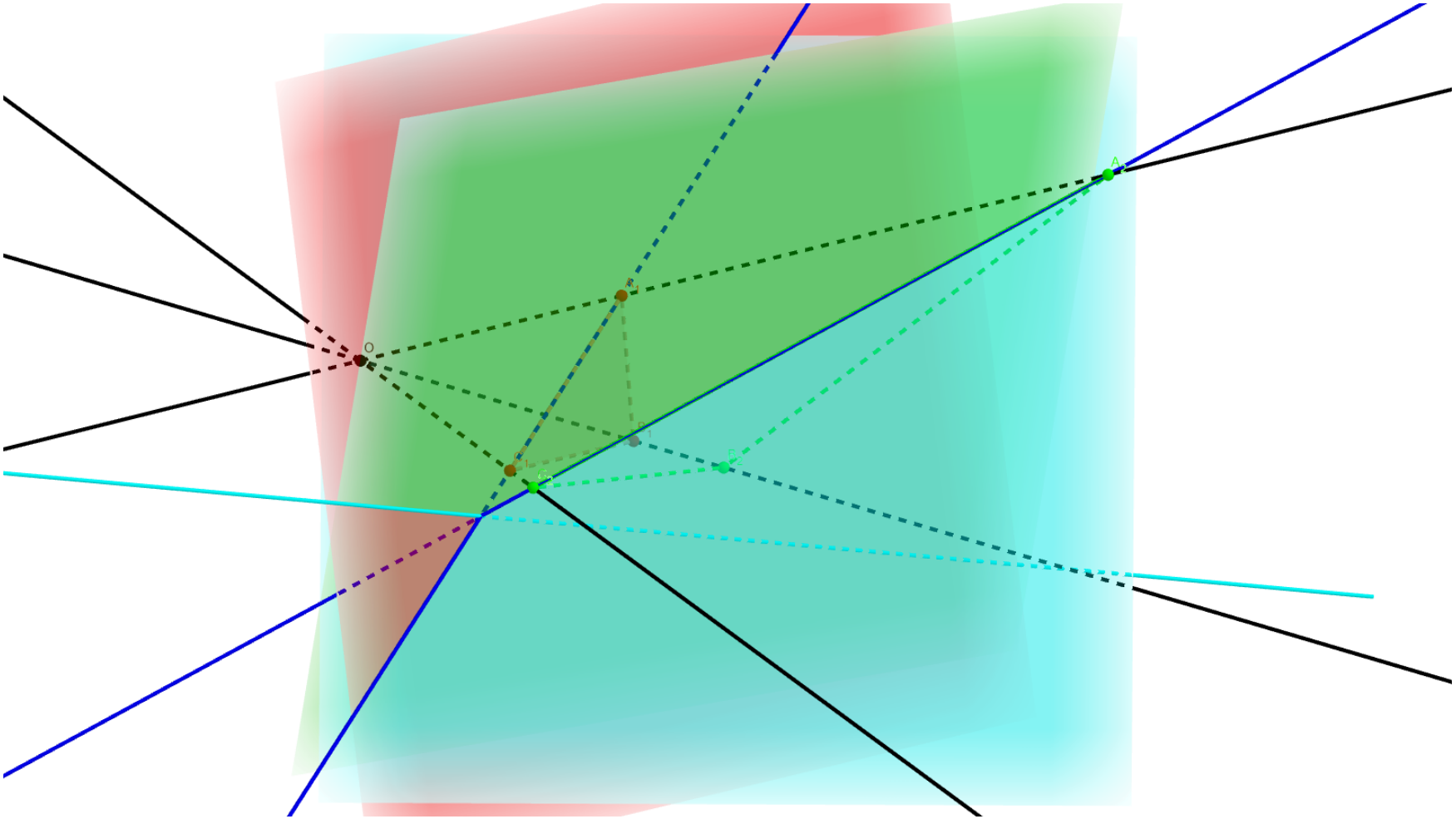
Interprétation en dimension supérieure

Le théorème de Desargues est vrai en dimension $\geqslant 3$, et ça se voit !



Interprétation en dimension supérieure

Le théorème de Desargues est vrai en dimension $\geqslant 3$, et ça se voit !



Théorème de Pappus

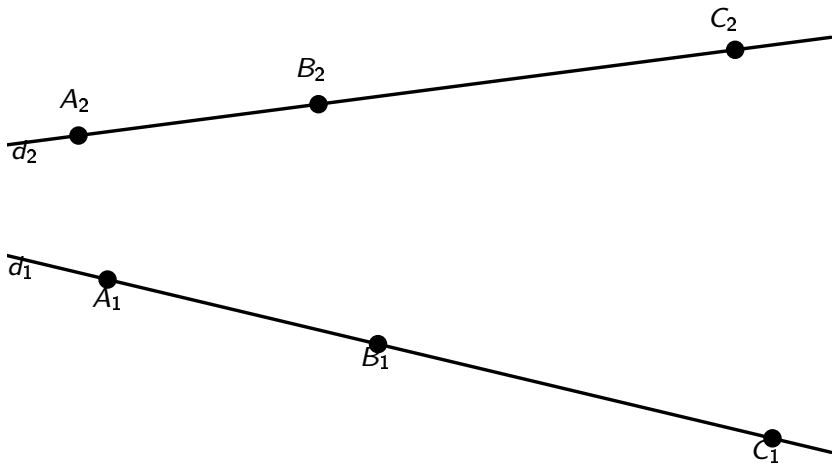
Théorème (Pappus)

Dans $\mathbb{P}^2(K)$ sur K **corps commutatif**, *étant donnés trois points A_1, B_1, C_1 alignés sur une droite d_1 et trois points A_2, B_2, C_2 alignés sur une droite d_2, les trois points d'intersection $A = (B_2C_1) \cap (B_1C_2)$, $B = (C_2A_1) \cap (C_1A_2)$ et $C = (A_2B_1) \cap (A_1B_2)$ sont alignés.*

Théorème de Pappus

Théorème (Pappus)

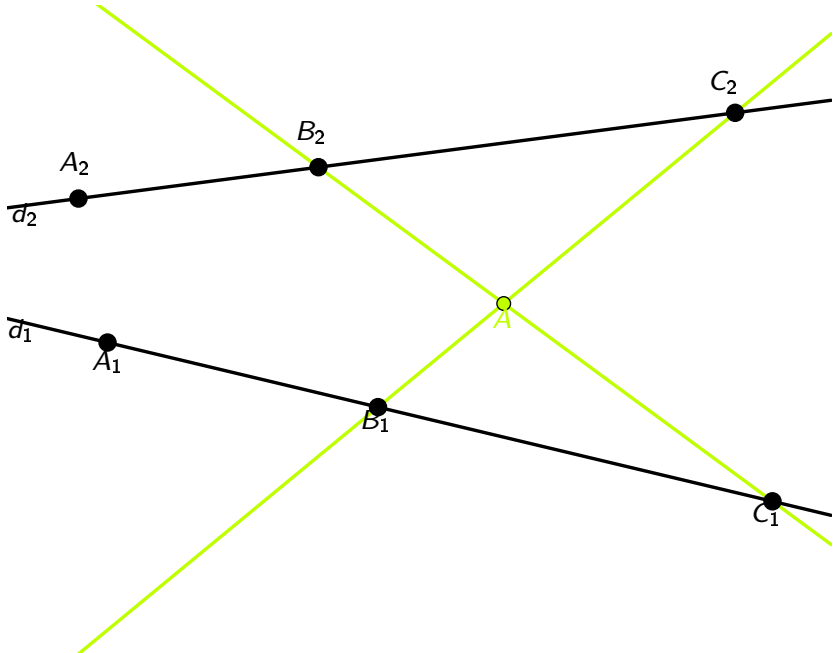
Dans $\mathbb{P}^2(K)$ sur K **corps commutatif**, *étant donnés trois points A_1, B_1, C_1 alignés sur une droite d_1 et trois points A_2, B_2, C_2 alignés sur une droite d_2, les trois points d'intersection $A = (B_2C_1) \cap (B_1C_2)$, $B = (C_2A_1) \cap (C_1A_2)$ et $C = (A_2B_1) \cap (A_1B_2)$ sont alignés.*



Théorème de Pappus

Théorème (Pappus)

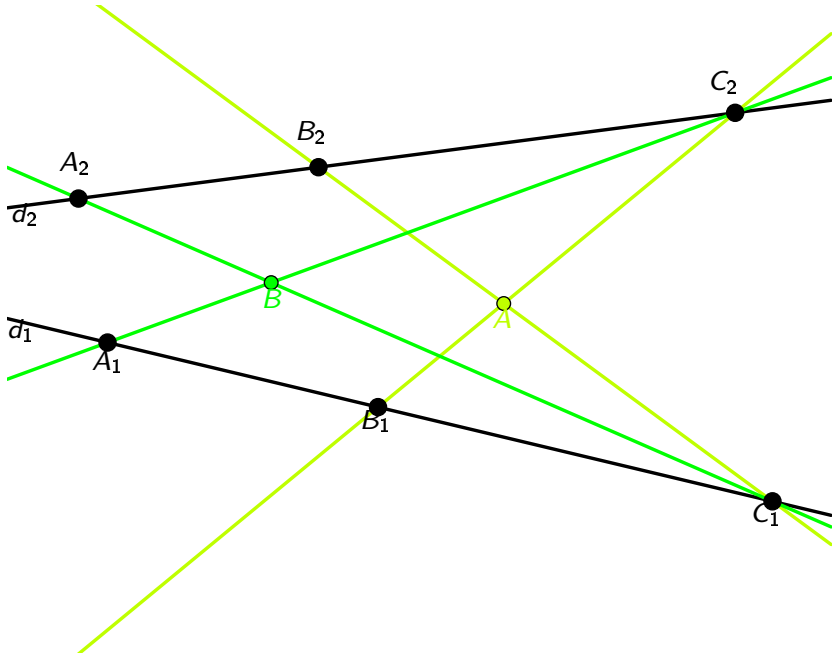
Dans $\mathbb{P}^2(K)$ sur K **corps commutatif**, *étant donnés trois points A_1, B_1, C_1 alignés sur une droite d_1 et trois points A_2, B_2, C_2 alignés sur une droite d_2, les trois points d'intersection $A = (B_2C_1) \cap (B_1C_2)$, $B = (C_2A_1) \cap (C_1A_2)$ et $C = (A_2B_1) \cap (A_1B_2)$ sont alignés.*



Théorème de Pappus

Théorème (Pappus)

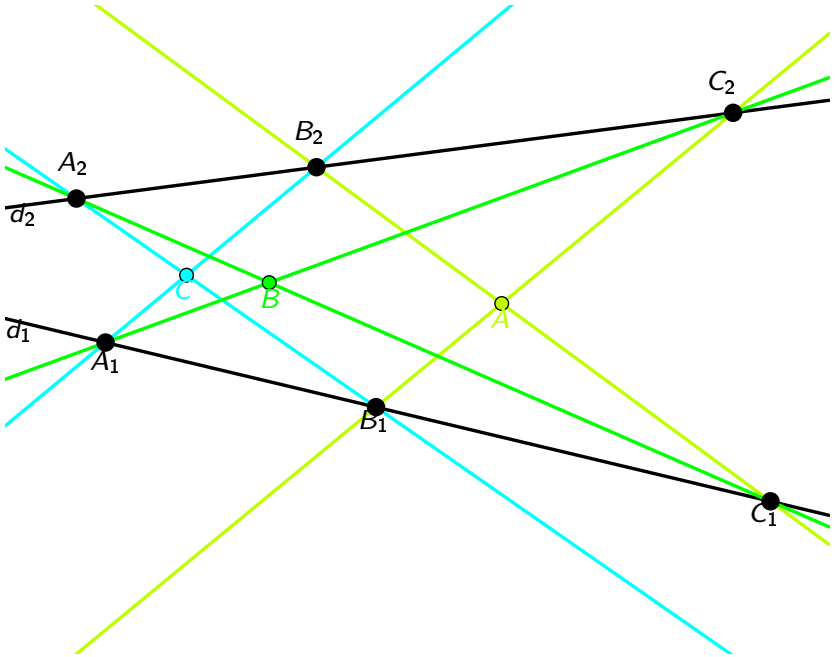
Dans $\mathbb{P}^2(K)$ sur K **corps commutatif**, *étant donnés trois points A_1, B_1, C_1 alignés sur une droite d_1 et trois points A_2, B_2, C_2 alignés sur une droite d_2, les trois points d'intersection $A = (B_2C_1) \cap (B_1C_2)$, $B = (C_2A_1) \cap (C_1A_2)$ et $C = (A_2B_1) \cap (A_1B_2)$ sont alignés.*



Théorème de Pappus

Théorème (Pappus)

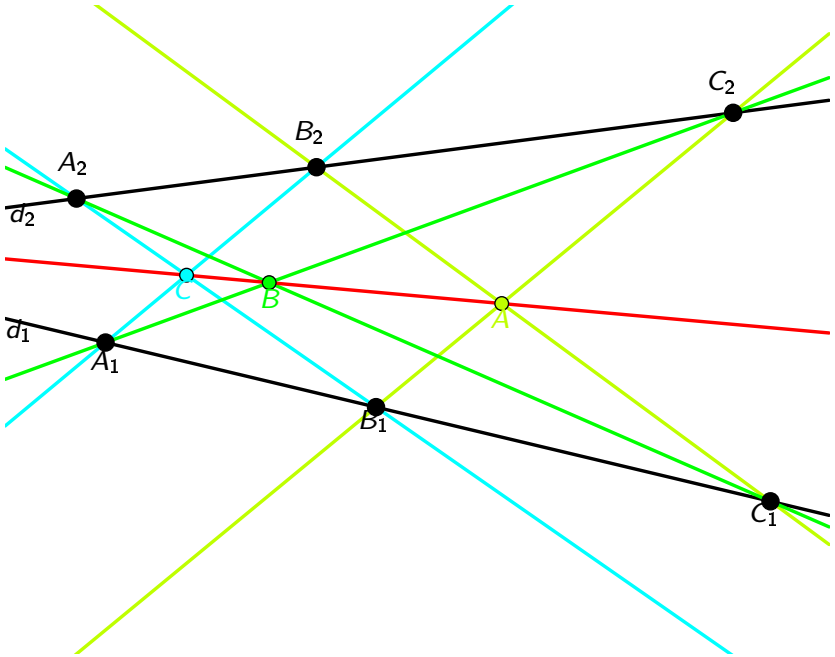
Dans $\mathbb{P}^2(K)$ sur K **corps commutatif**, *étant donnés trois points A_1, B_1, C_1 alignés sur une droite d_1 et trois points A_2, B_2, C_2 alignés sur une droite d_2, les trois points d'intersection $A = (B_2C_1) \cap (B_1C_2)$, $B = (C_2A_1) \cap (C_1A_2)$ et $C = (A_2B_1) \cap (A_1B_2)$ sont alignés.*



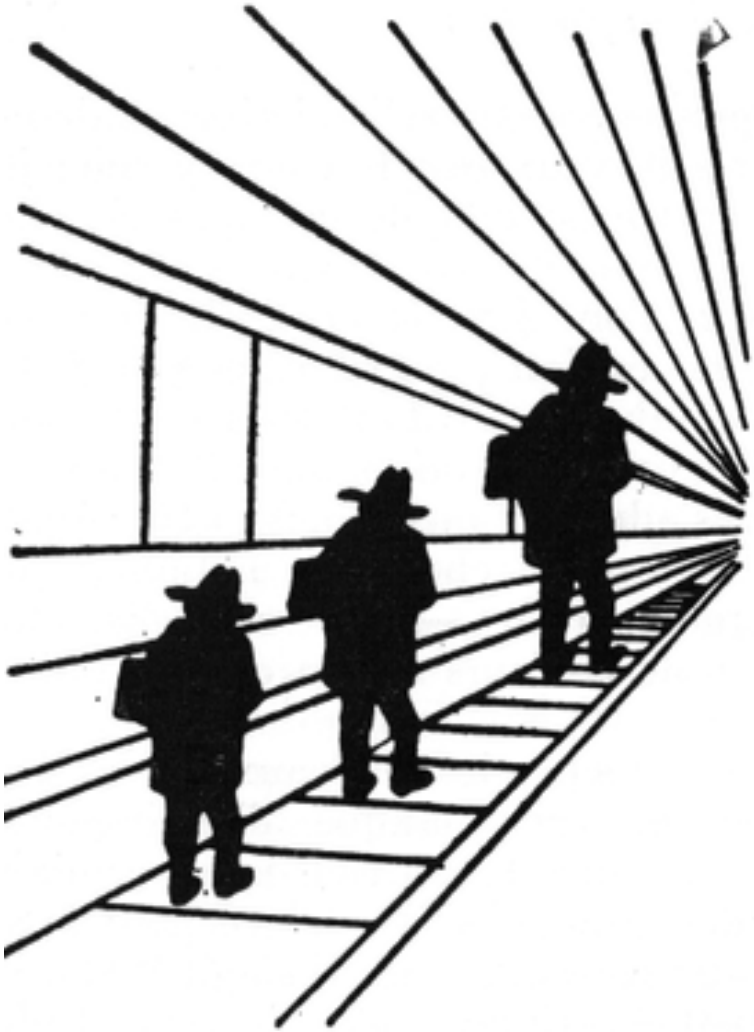
Théorème de Pappus

Théorème (Pappus)

Dans $\mathbb{P}^2(K)$ sur K **corps commutatif**, *étant donnés trois points A_1, B_1, C_1 alignés sur une droite d_1 et trois points A_2, B_2, C_2 alignés sur une droite d_2, les trois points d'intersection $A = (B_2C_1) \cap (B_1C_2)$, $B = (C_2A_1) \cap (C_1A_2)$ et $C = (A_2B_1) \cap (A_1B_2)$ sont alignés.*



Illusions d'optique ?



Axiomes de la géométrie projective

Définition (Whitehead, 1906 ; Veblen-Young, 1917)

Un *espace projectif* $\mathcal{P} = (\Pi, \Delta)$ est la donnée d'un ensemble de points Π, d'un ensemble de droites Δ, qui sont des ensembles de points, telles que :

Axiomes de la géométrie projective

Définition (Whitehead, 1906 ; Veblen-Young, 1917)

Un *espace projectif* $\mathcal{P} = (\Pi, \Delta)$ est la donnée d'un ensemble de points Π, d'un ensemble de droites Δ, qui sont des ensembles de points, telles que :

(EP1) « Par deux points, il passe une unique droite. »

deux points distincts A et B sont contenus dans une unique droite (AB) ;

Axiomes de la géométrie projective

Définition (Whitehead, 1906 ; Veblen-Young, 1917)

Un *espace projectif* $\mathcal{P} = (\Pi, \Delta)$ est la donnée d'un ensemble de points Π, d'un ensemble de droites Δ, qui sont des ensembles de points, telles que :

(EP1) « Par deux points, il passe une unique droite. »

deux points distincts A et B sont contenus dans une unique droite (AB) ;

(EP2) « Deux droites coplanaires s'intersectent en un unique point »

si A et D sont deux points distincts de B et C, si les droites (AB) et (CD) s'intersectent, alors les droites (AC) et (BD) s'intersectent aussi ;

Axiomes de la géométrie projective

Définition (Whitehead, 1906 ; Veblen-Young, 1917)

Un *espace projectif* $\mathcal{P} = (\Pi, \Delta)$ est la donnée d'un ensemble de points Π, d'un ensemble de droites Δ, qui sont des ensembles de points, telles que :

(EP1) « Par deux points, il passe une unique droite. »

deux points distincts A et B sont contenus dans une unique droite (AB) ;

(EP2) « Deux droites coplanaires s'intersectent en un unique point »

si A et D sont deux points distincts de B et C, si les droites (AB) et (CD) s'intersectent, alors les droites (AC) et (BD) s'intersectent aussi ;

(EP3) toute droite contient au moins trois points distincts.

Axiomes de la géométrie projective

Définition (Whitehead, 1906 ; Veblen-Young, 1917)

Un *espace projectif* $\mathcal{P} = (\Pi, \Delta)$ est la donnée d'un ensemble de points Π, d'un ensemble de droites Δ, qui sont des ensembles de points, telles que :

(EP1) « Par deux points, il passe une unique droite. »

deux points distincts A et B sont contenus dans une unique droite (AB) ;

(EP2) « Deux droites coplanaires s'intersectent en un unique point »

si A et D sont deux points distincts de B et C, si les droites (AB) et (CD) s'intersectent, alors les droites (AC) et (BD) s'intersectent aussi ;

(EP3) toute droite contient au moins trois points distincts.

Plan projectif : toutes les droites sont coplanaires.
Non dégénéré : existence d'un quadrangle (4 points qui sont 3 à 3 non alignés).

Place du théorème de Desargues

Théorème (Veblen–Young, 1917)

Si $\mathcal{P}$ est non planaire, alors il vérifie le théorème de Desargues.

Place du théorème de Desargues

Théorème (Veblen–Young, 1917)

Si $\mathcal{P}$ est non planaire, alors il vérifie le théorème de Desargues.

Trois types d'espaces projectifs :

1. les espaces dégénérés : $\mathrm{Card}(\Delta) = 1$;

Place du théorème de Desargues

Théorème (Veblen–Young, 1917)

Si $\mathcal{P}$ est non planaire, alors il vérifie le théorème de Desargues.

Trois types d'espaces projectifs :

1. les espaces dégénérés : $\mathrm{Card}(\Delta) = 1$;
2. les espaces désarguésiens : e.g. $\mathbb{P}^d(K)$ pour K corps gauche ;

Place du théorème de Desargues

Théorème (Veblen–Young, 1917)

Si $\mathcal{P}$ est non planaire, alors il vérifie le théorème de Desargues.

Trois types d'espaces projectifs :

1. les espaces dégénérés : $\mathrm{Card}(\Delta) = 1$;
2. les espaces désarguésiens : e.g. $\mathbb{P}^d(K)$ pour K corps gauche ;
3. les plans non-désarguésiens : e.g. $\mathbb{P}^2(\mathbb{O})$.

Place du théorème de Desargues

Théorème (Veblen–Young, 1917)

Si $\mathcal{P}$ est non planaire, alors il vérifie le théorème de Desargues.

Trois types d'espaces projectifs :

1. les espaces dégénérés : $\mathrm{Card}(\Delta) = 1$;
2. les espaces désarguésiens : e.g. $\mathbb{P}^d(K)$ pour K corps gauche ;
3. les plans non-désarguésiens : e.g. $\mathbb{P}^2(\mathbb{O})$.

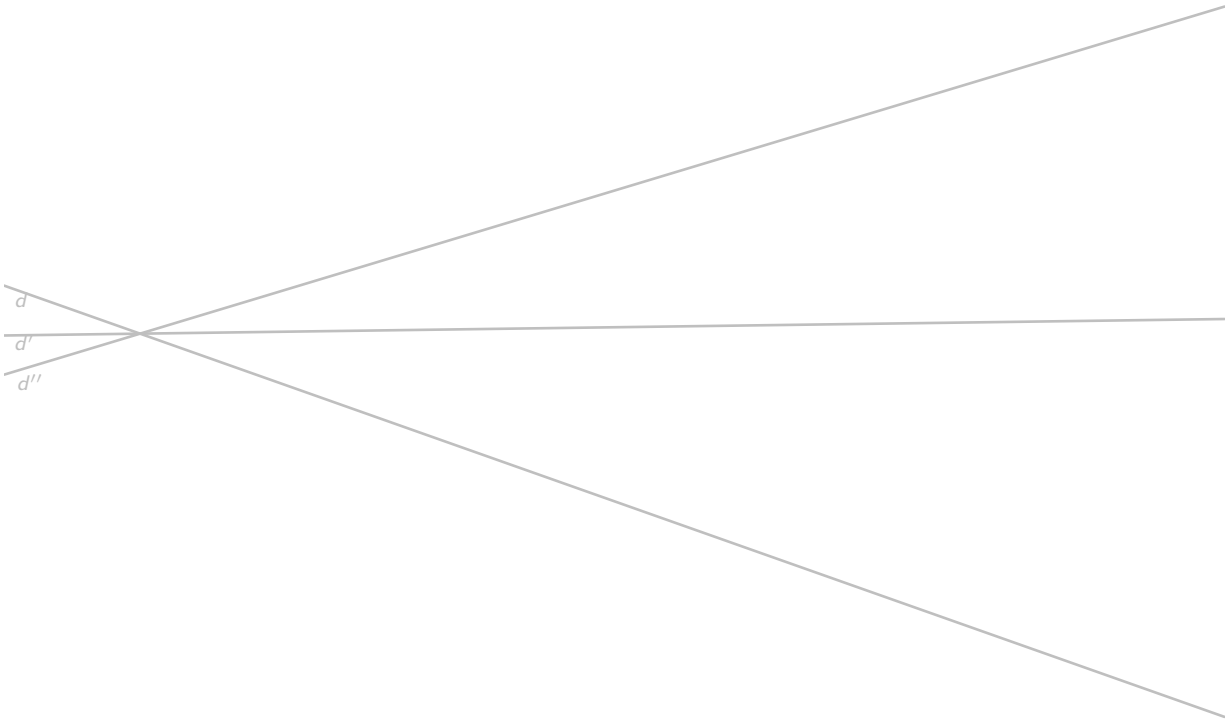
Théorème (Hilbert, 1899)

Un plan projectif :

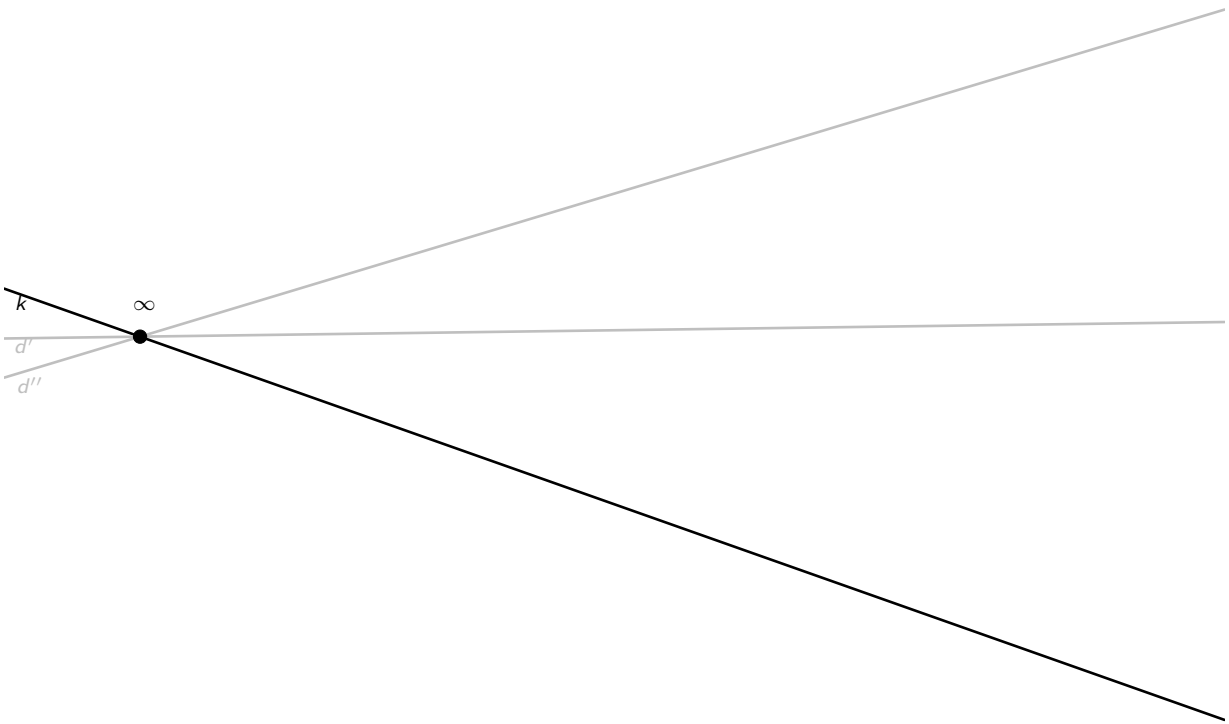
1. *vérifie le théorème de Desargues si, et seulement si, il est isomorphe au plan projectif sur un corps gauche ;*
2. *vérifie le théorème de Pappus si, et seulement si, il est isomorphe au plan projectif sur un corps commutatif.*

Réalisation géométrique de l'addition

Soient $d, d', d'' \in \Delta$ distinctes concourantes

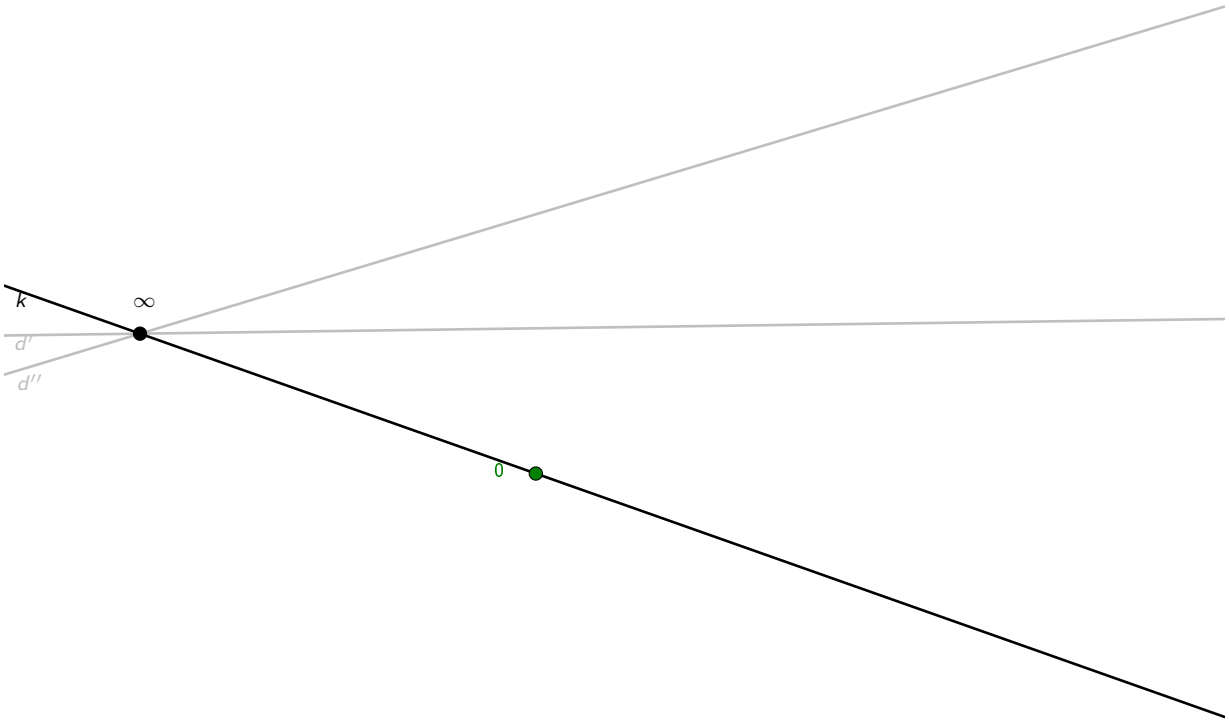


Réalisation géométrique de l'addition



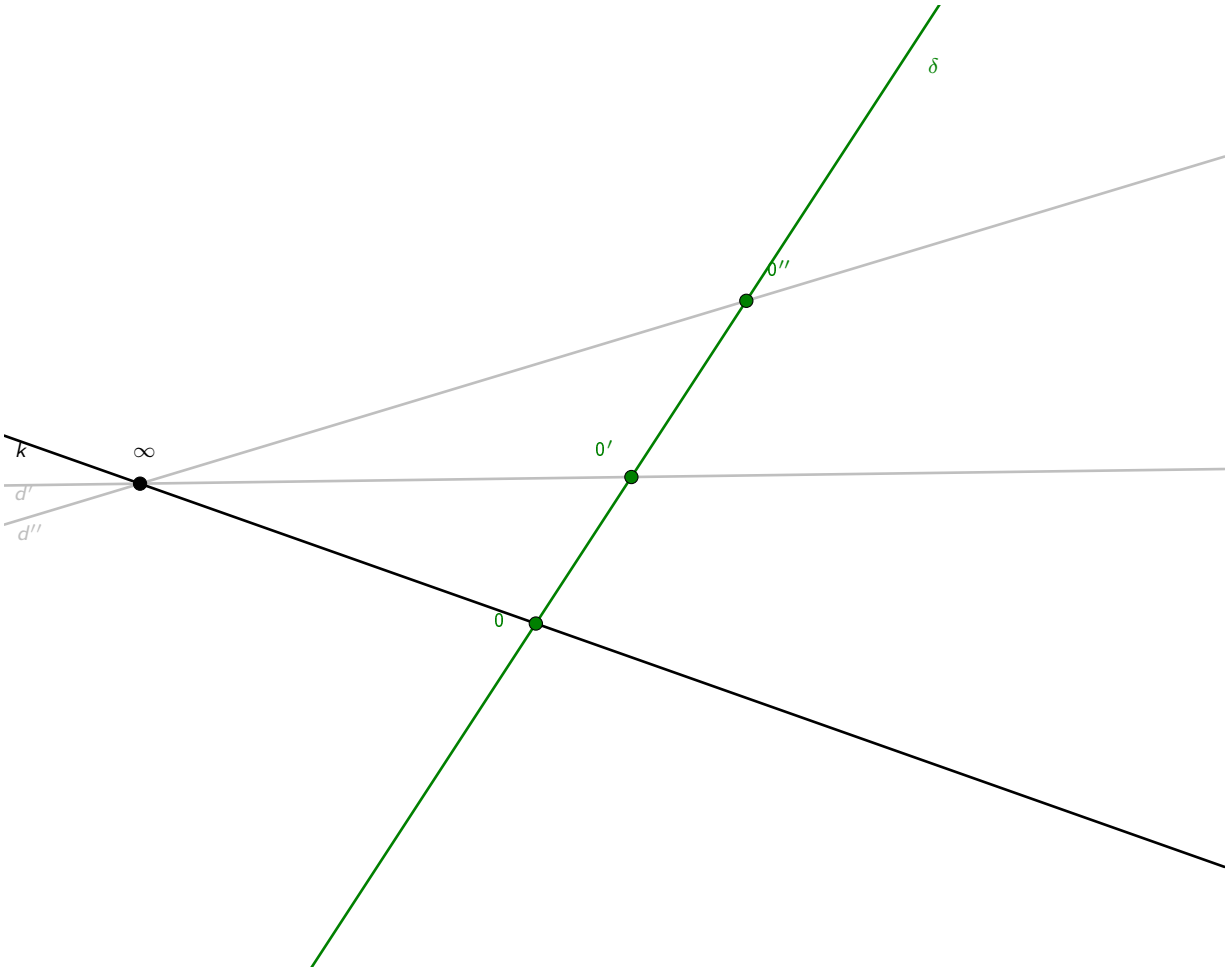
Soient $d, d', d'' \in \Delta$ distinctes concourantes en ∞.
Soit $k = d \setminus \{\infty\}$.

Réalisation géométrique de l'addition



Soient $d, d', d'' \in \Delta$ distinctes concourantes en ∞.
Soit $k = d \setminus \{\infty\}$.
Soit $0 \in k$.

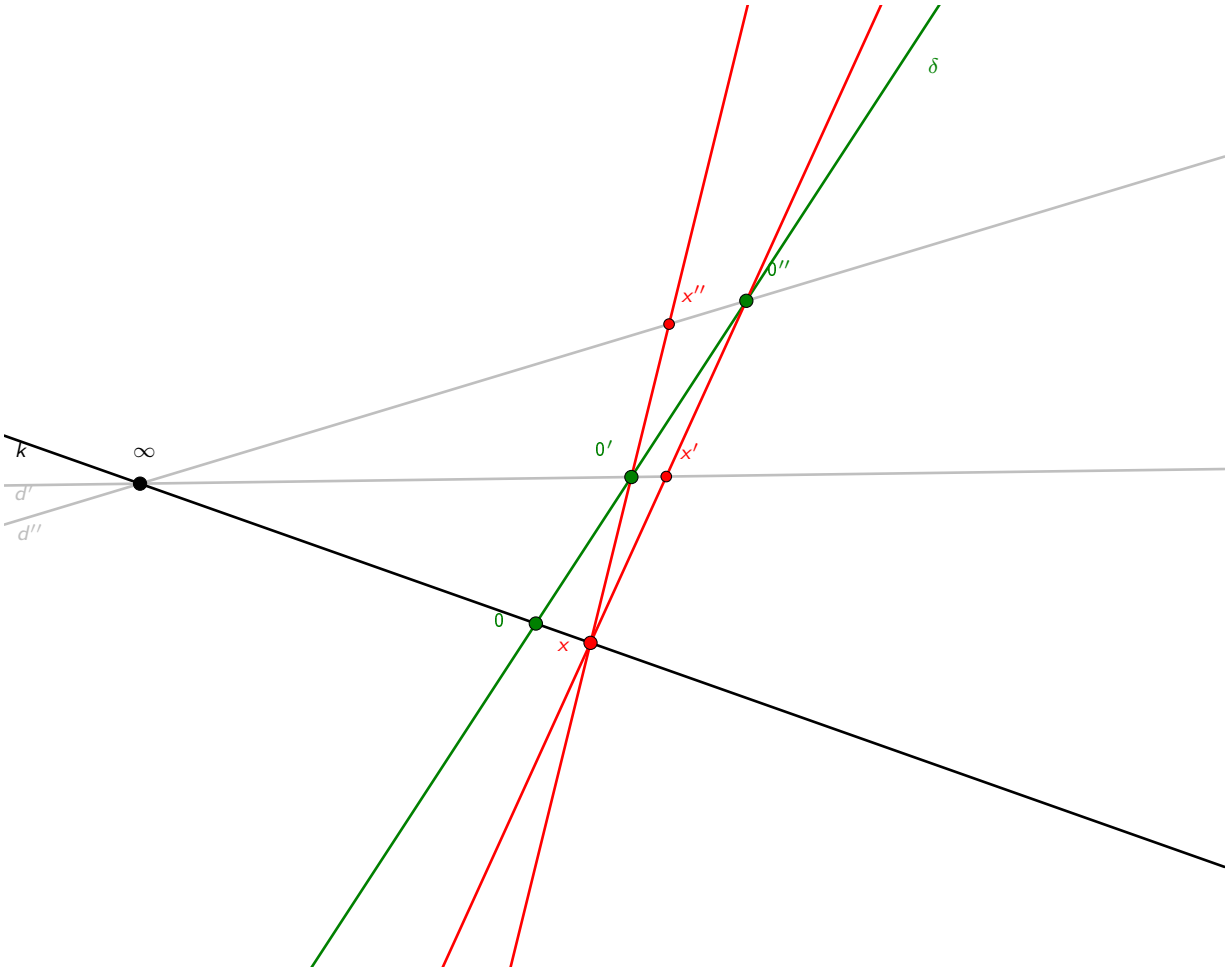
Réalisation géométrique de l'addition



Soient $d, d', d'' \in \Delta$ distinctes concourantes en ∞.
Soit $k = d \setminus \{\infty\}$.
Soit $0 \in k$.
Soit $\delta \in \Delta$ telle que $0 \in \delta \neq d$.

Posons $0' = \delta \cap d'$ et $0'' = \delta \cap d''$.

Réalisation géométrique de l'addition

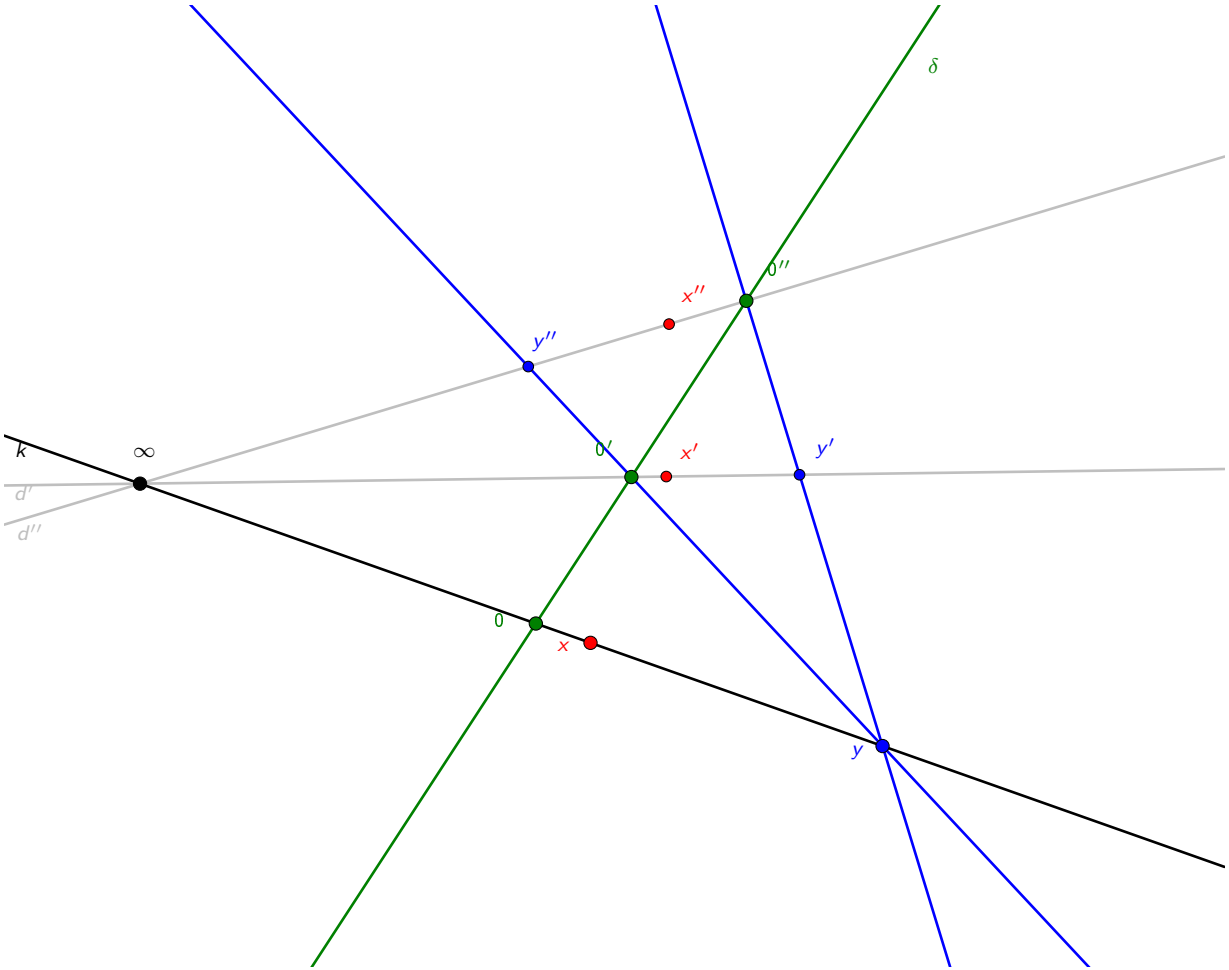


Soient $d, d', d'' \in \Delta$ distinctes concourantes en ∞.
Soit $k = d \setminus \{\infty\}$.
Soit $0 \in k$.
Soit $\delta \in \Delta$ telle que $0 \in \delta \neq d$.

Posons $0' = \delta \cap d'$ et $0'' = \delta \cap d''$.

Pour $x \in k$, on pose :
$x' = (x0'') \cap d'$,
$x'' = (x0') \cap d''$.

Réalisation géométrique de l'addition

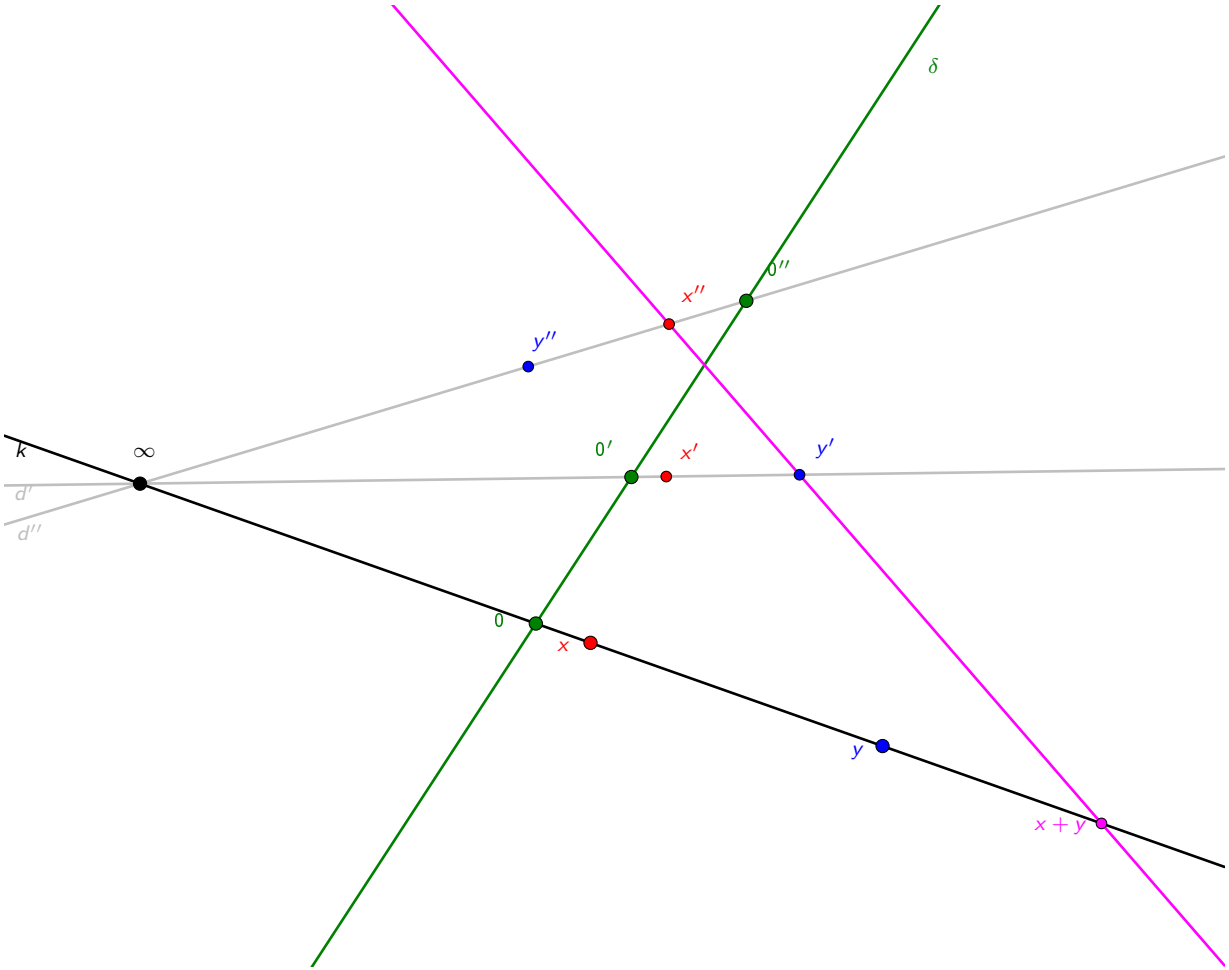


Soient $d, d', d'' \in \Delta$ distinctes concourantes en ∞.
Soit $k = d \setminus \{\infty\}$.
Soit $0 \in k$.
Soit $\delta \in \Delta$ telle que $0 \in \delta \neq d$.

Posons $0' = \delta \cap d'$ et $0'' = \delta \cap d''$.

Pour $x \in k$, on pose :
$x' = (x0'') \cap d'$,
$x'' = (x0') \cap d''$.

Réalisation géométrique de l'addition



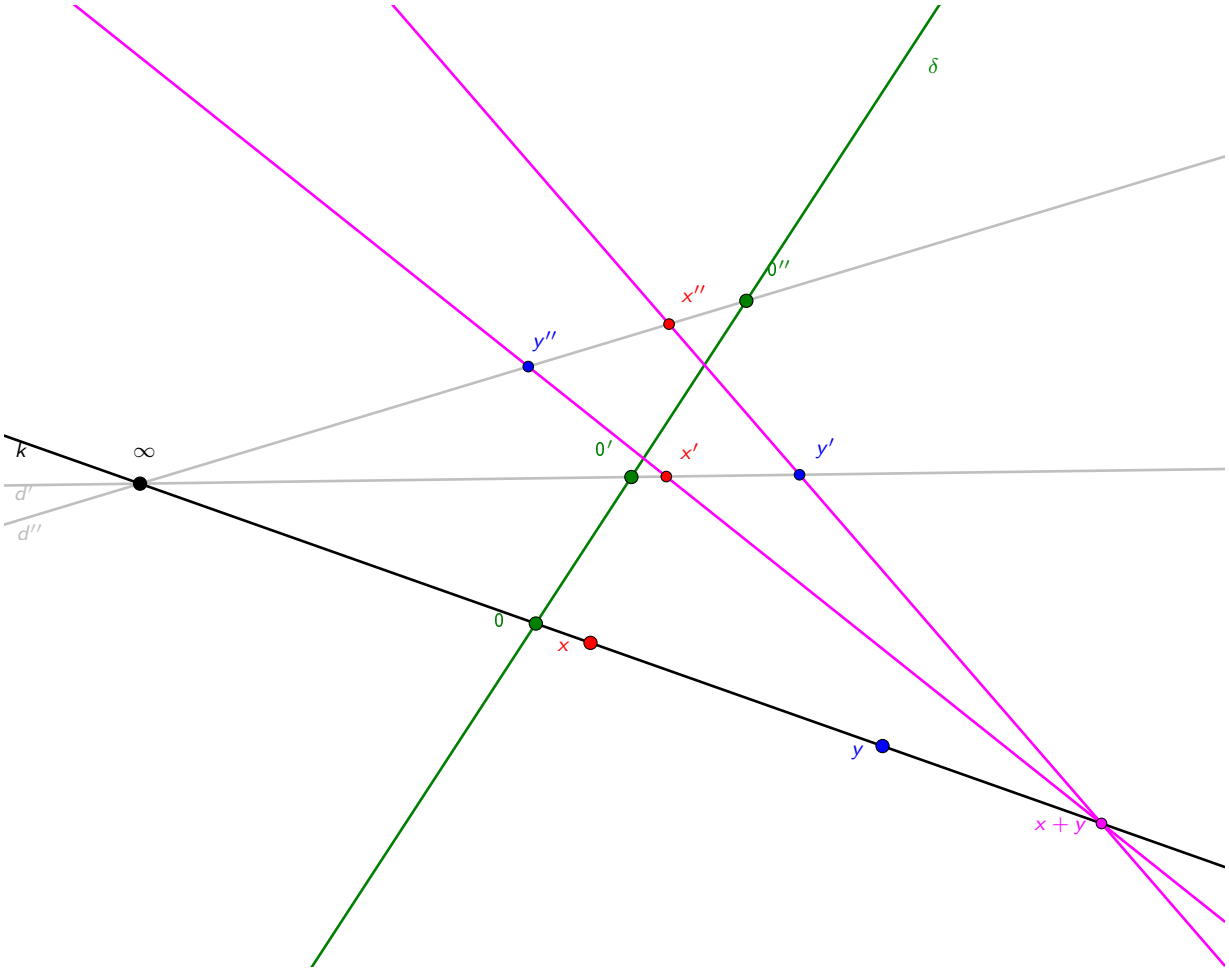
Soient $d, d', d'' \in \Delta$ distinctes concourantes en ∞.
Soit $k = d \setminus \{\infty\}$.
Soit $0 \in k$.
Soit $\delta \in \Delta$ telle que $0 \in \delta \neq d$.

Posons $0' = \delta \cap d'$ et $0'' = \delta \cap d''$.

Pour $x \in k$, on pose :
$x' = (x0'') \cap d'$,
$x'' = (x0') \cap d''$.

$\forall x, y \in k$,
$x + y = (x'y'') \cap d$

Réalisation géométrique de l'addition



Soient $d, d', d'' \in \Delta$ distinctes concourantes en ∞.
Soit $k = d \setminus \{\infty\}$.
Soit $0 \in k$.
Soit $\delta \in \Delta$ telle que $0 \in \delta \neq d$.

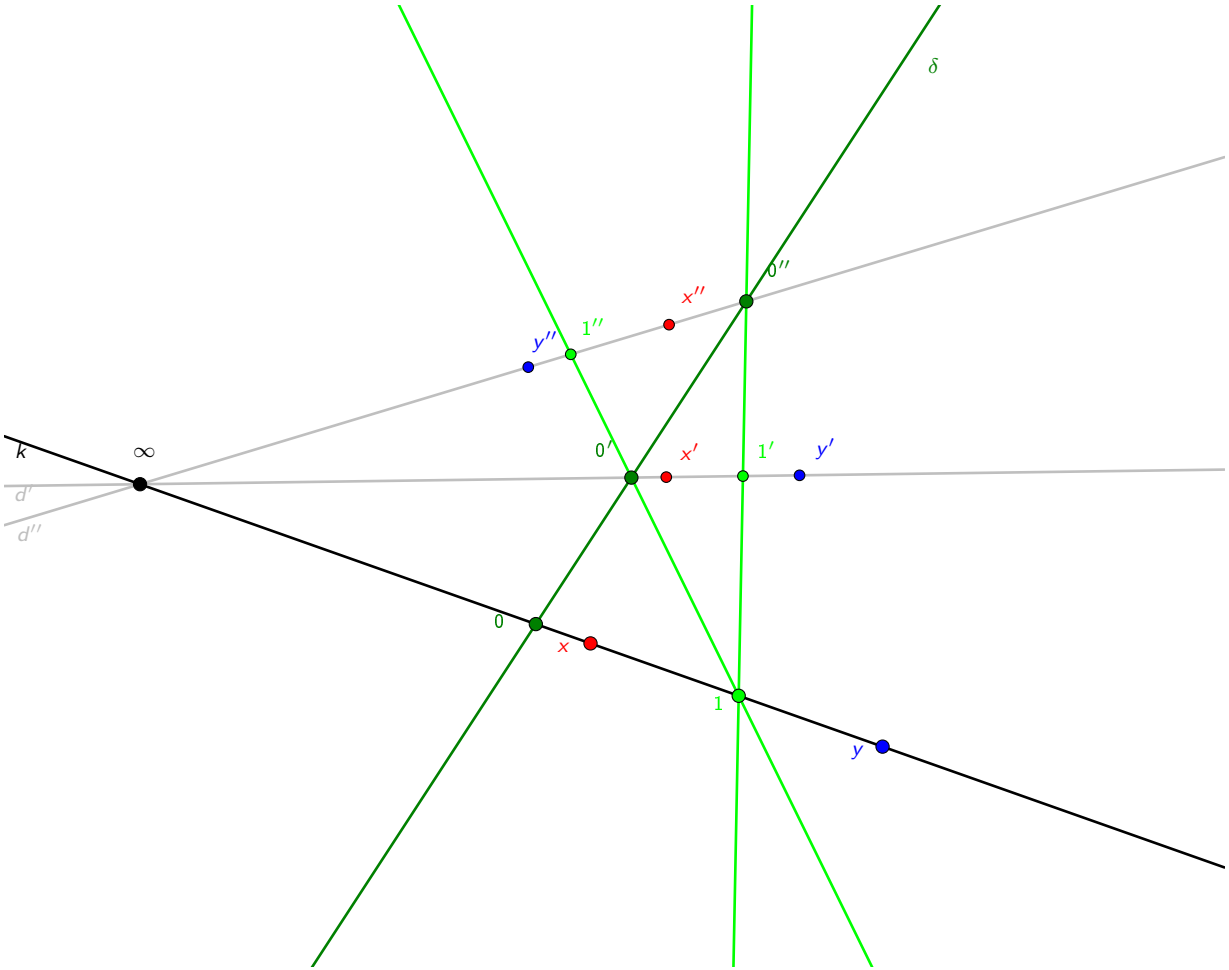
Posons $0' = \delta \cap d'$ et $0'' = \delta \cap d''$.

Pour $x \in k$, on pose :
$x' = (x0'') \cap d'$,
$x'' = (x0') \cap d''$.

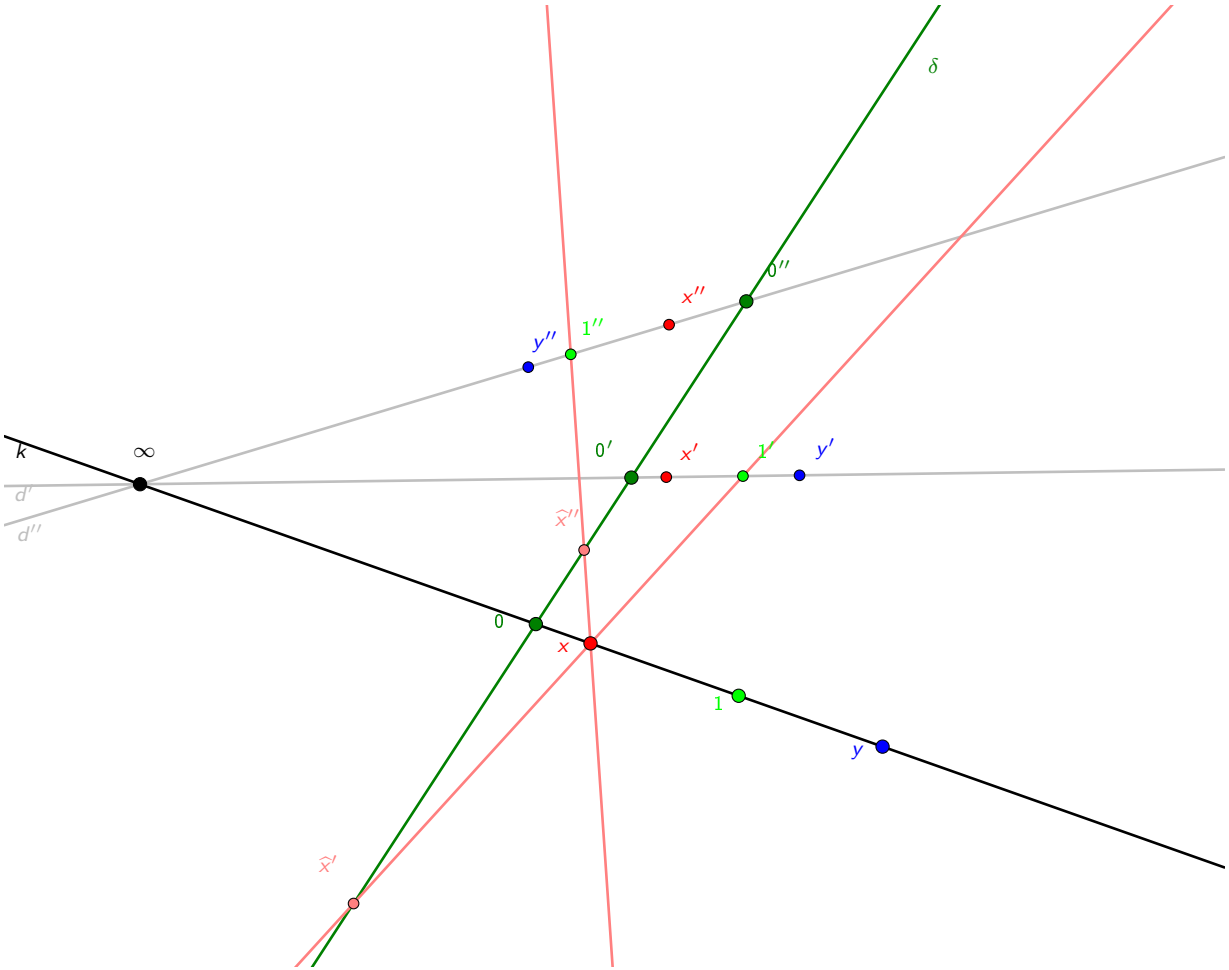
$\forall x, y \in k$,
$x + y = (x'y'') \cap d$
$= y + x = (x''y') \cap d$

et de la multiplication

Soit $1 \in k^* = k \setminus \{0\}$



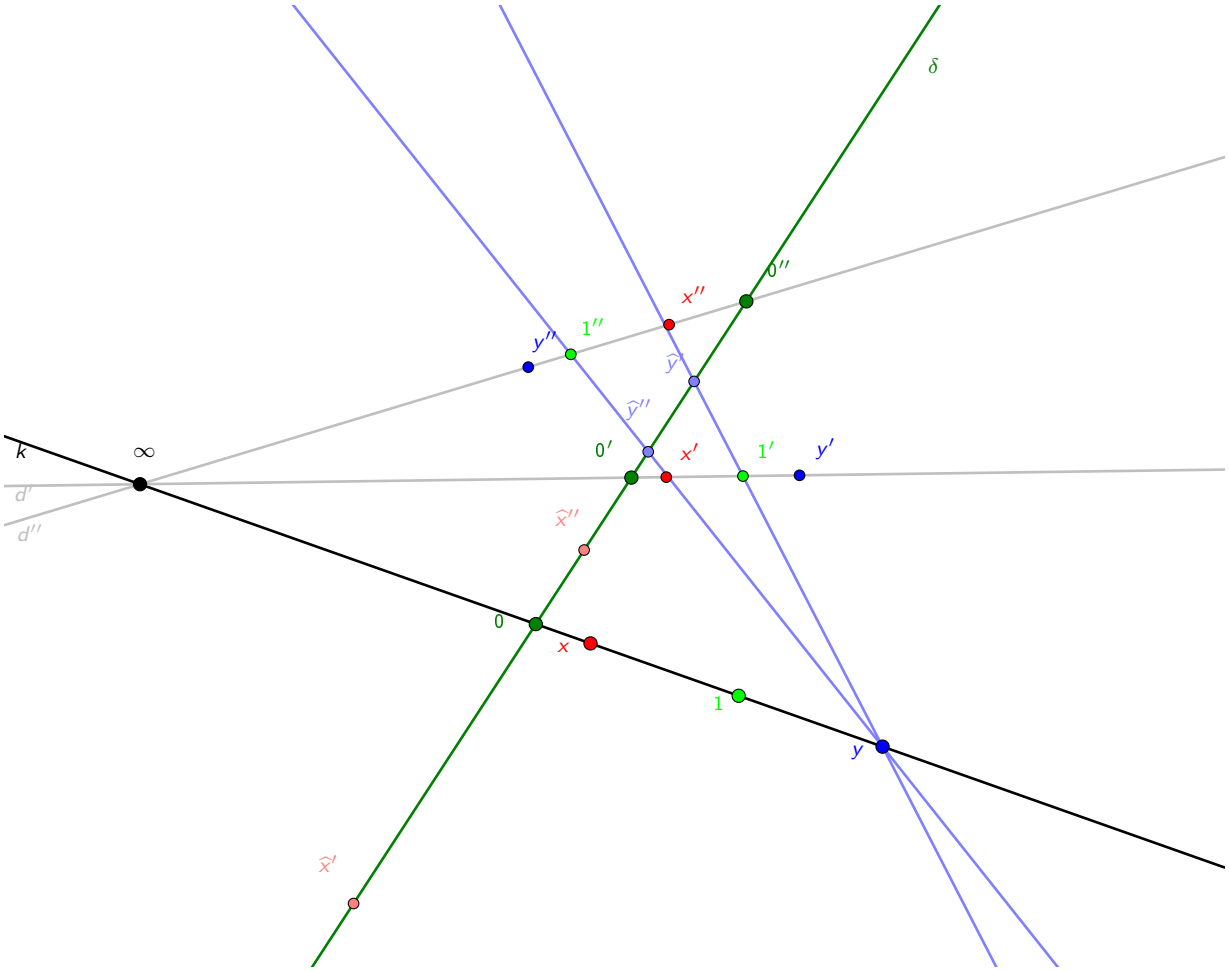
et de la multiplication



Soit $1 \in k^* = k \setminus \{0\}$

Pour $x \in d$, on pose :
$\widehat{x}' = (x1') \cap \delta$,
$\widehat{x}'' = (x1'') \cap \delta$.

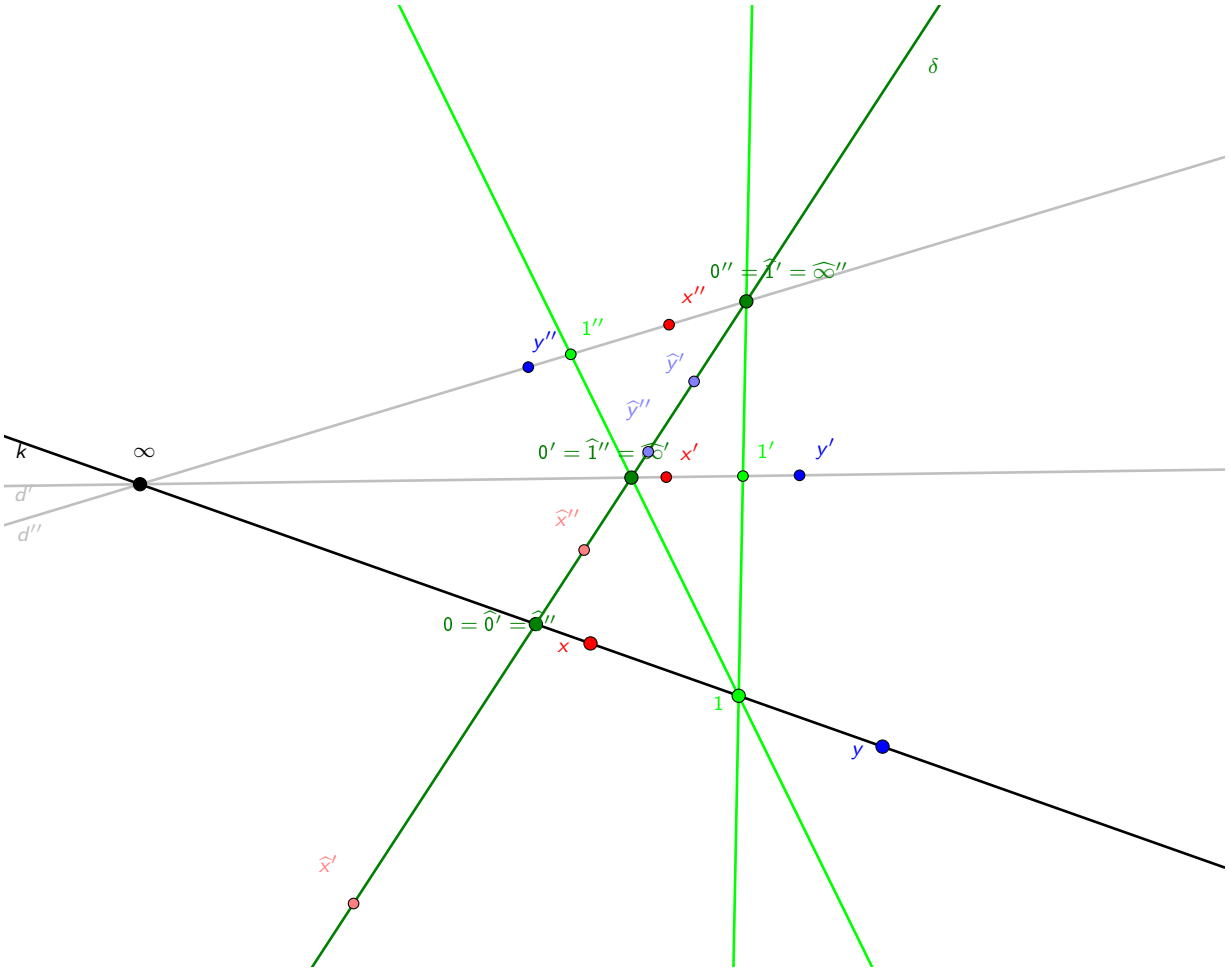
et de la multiplication



Soit $1 \in k^* = k \setminus \{0\}$

Pour $x \in d$, on pose :
$\widehat{x}' = (x1') \cap \delta$,
$\widehat{x}'' = (x1'') \cap \delta$.

et de la multiplication



Soit $1 \in k^* = k \setminus \{0\}$

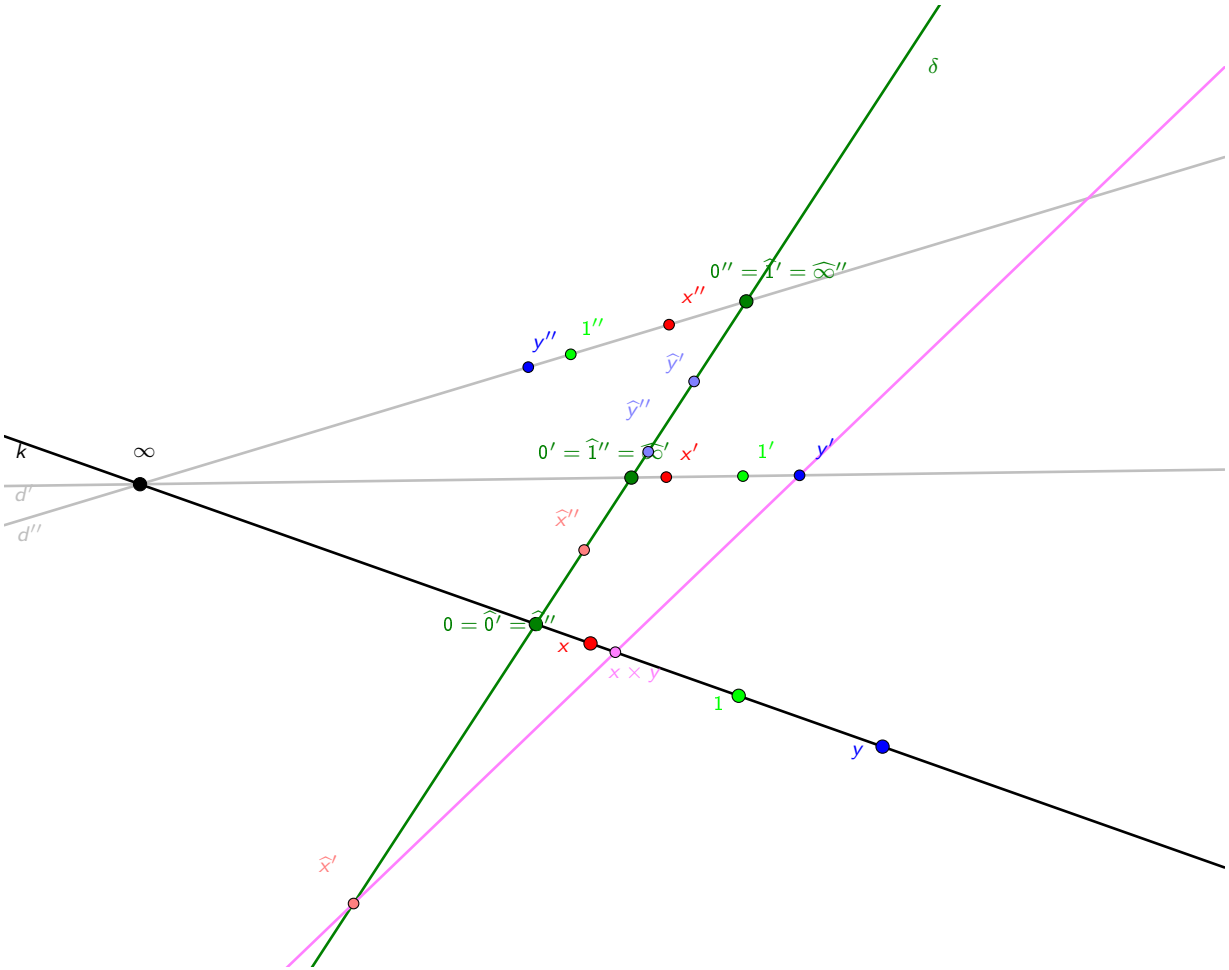
Pour $x \in d$, on pose :

$$\widehat{x}' = (x1') \cap \delta,$$
$$\widehat{x}'' = (x1'') \cap \delta.$$

Remarque :

$$0 = \widehat{0}' = \widehat{0}'',$$
$$0' = \widehat{\infty}' = \widehat{1}'',$$
$$0'' = \widehat{1}' = \widehat{\infty}''.$$

et de la multiplication



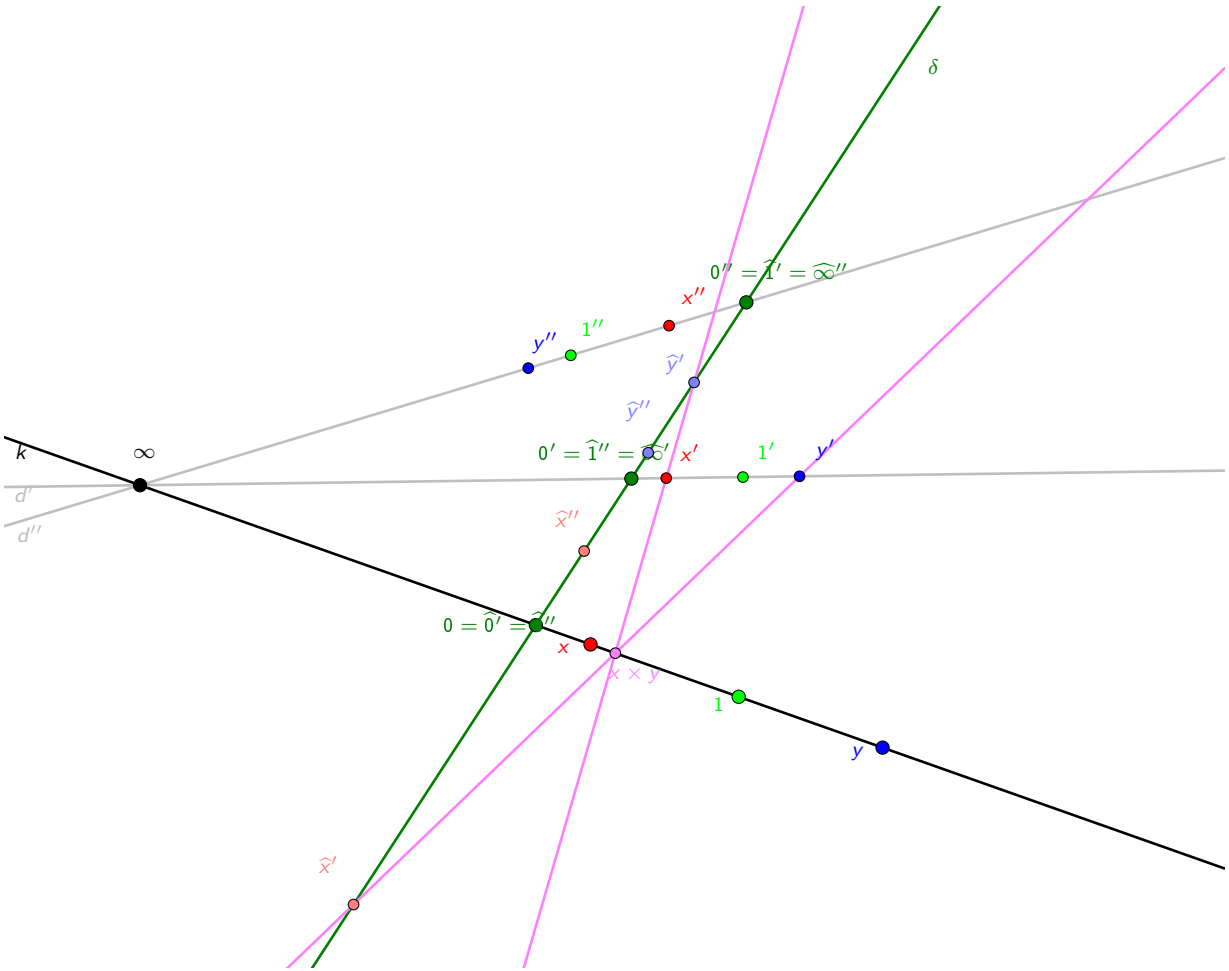
Soit $1 \in k^* = k \setminus \{0\}$

Pour $x \in d$, on pose :
$$\hat{x}' = (x1') \cap \delta,$$
$$\hat{x}'' = (x1'') \cap \delta.$$

Remarque :
$$0 = \hat{0}' = \hat{0}'',$$
$$0' = \hat{\infty}' = \hat{1}'',$$
$$0'' = \hat{1}' = \hat{\infty}''.$$

$\forall x, y \in k$,
$$x \times y = (\hat{x}' y') \cap d$$

et de la multiplication



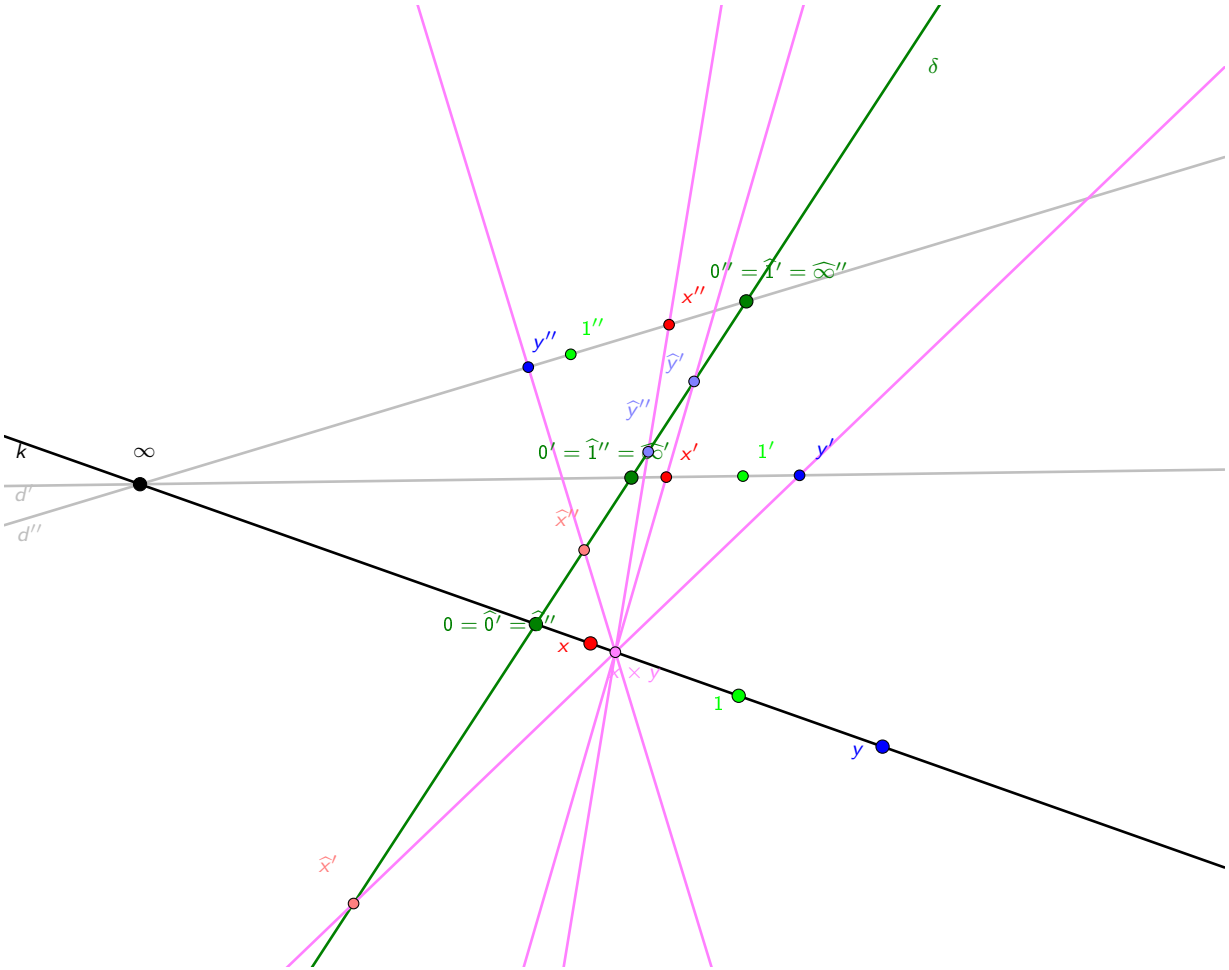
Soit $1 \in k^* = k \setminus \{0\}$

Pour $x \in d$, on pose :
$$\widehat{x}' = (x1') \cap \delta,$$
$$\widehat{x}'' = (x1'') \cap \delta.$$

Remarque :
$$0 = \widehat{0}' = \widehat{0}'',$$
$$0' = \widehat{\infty}' = \widehat{1}'',$$
$$0'' = \widehat{1}' = \widehat{\infty}''.$$

$\forall x, y \in k$,
$$x \times y = (\widehat{x}' y') \cap d$$
$$= y \times x = (\widehat{y}' x') \cap d$$

et de la multiplication



Soit $1 \in k^* = k \setminus \{0\}$

Pour $x \in d$, on pose :
$$\widehat{x}' = (x1') \cap \delta,$$
$$\widehat{x}'' = (x1'') \cap \delta.$$

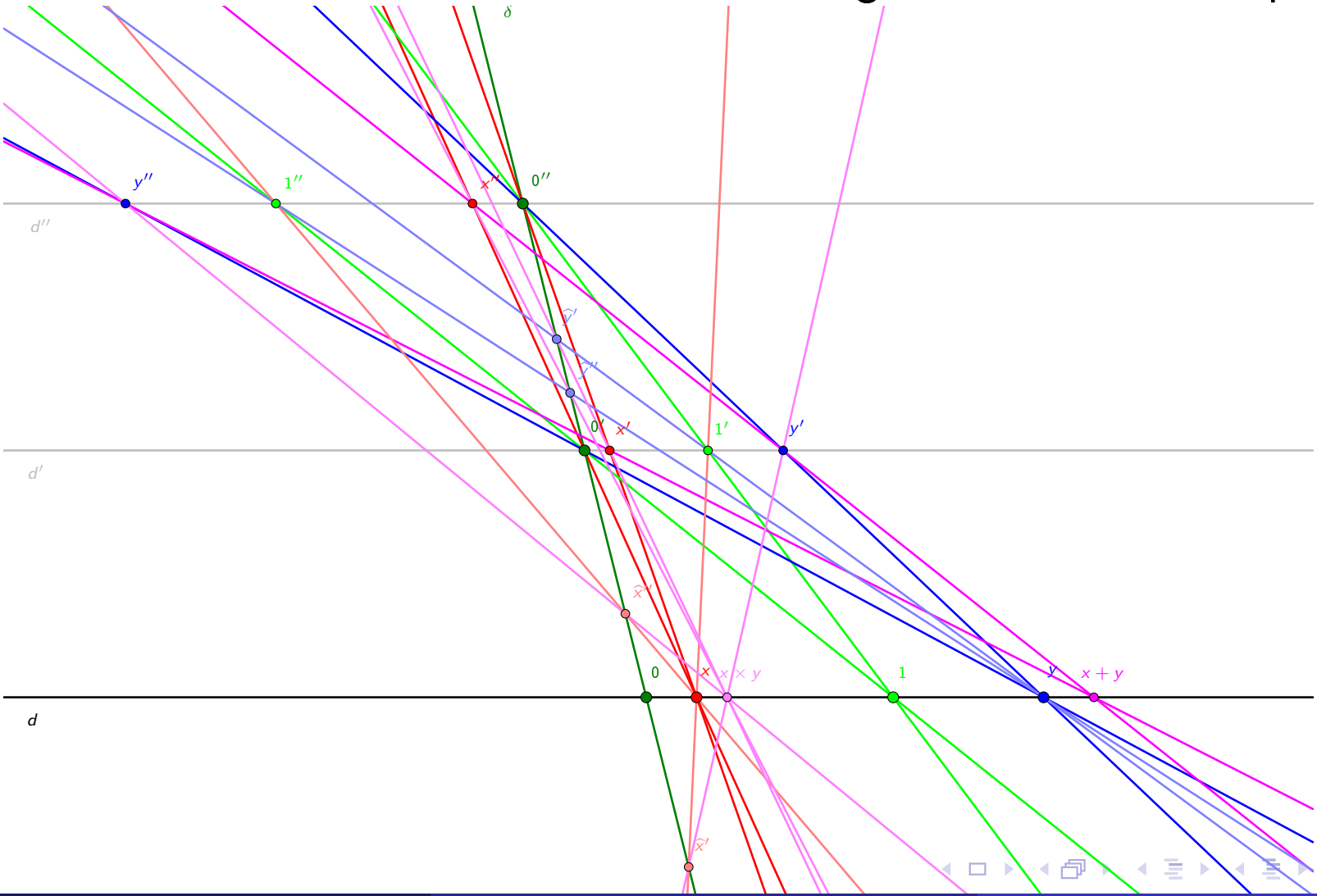
Remarque :
$$0 = \widehat{0}' = \widehat{0}'',$$
$$0' = \widehat{\infty}' = \widehat{1}'',$$
$$0'' = \widehat{1}' = \widehat{\infty}''.$$

$\forall x, y \in k,$
$$\begin{aligned} x \times y &= (\widehat{x}' y') \cap d \\ = y \times x &= (\widehat{y}' x') \cap d \\ &= (\widehat{x}'' y'') \cap d \\ &= (\widehat{y}'' x'') \cap d \end{aligned}$$

Quand on n'a pas de compas...

Quand on n'a pas de compas...

... mais une règle avec deux côtés parallèles !



Outline

1 Un problème d'ITYM

2 Ensembles à différence

3 Géométrie projective

4 Plans projectifs finis

Des espaces finis

Proposition

Soit $\mathcal{P} = (\Pi, \Delta, \Phi)$ *un plan projectif fini (non dégénéré). Il existe un unique entier* $n \in \mathbb{Z}_{\geqslant 2}$, *appelé* ordre *de* $\mathcal{P}$ *tel que :*

Des espaces finis

Proposition

Soit $\mathcal{P} = (\Pi, \Delta, \Phi)$ *un plan projectif fini (non dégénéré). Il existe un unique entier* $n \in \mathbb{Z}_{\geqslant 2}$, *appelé* ordre *de* $\mathcal{P}$ *tel que :*

(1) *toute droite* $d \in \Delta$ *passe par exactement* $n+1$ *points distincts de* $\mathcal{P}$;

(1') *par tout point* $p \in \Pi$ *de* $\mathcal{P}$, *il passe exactement* $n+1$ *droites distinctes ;*

Des espaces finis

Proposition

Soit $\mathcal{P} = (\Pi, \Delta, \Phi)$ *un plan projectif fini (non dégénéré). Il existe un unique entier* $n \in \mathbb{Z}_{\geqslant 2}$, *appelé* ordre *de* $\mathcal{P}$ *tel que :*

(1) *toute droite* $d \in \Delta$ *passe par exactement* $n+1$ *points distincts de* $\mathcal{P}$;

(1') *par tout point* $p \in \Pi$ *de* $\mathcal{P}$, *il passe exactement* $n+1$ *droites distinctes ;*

(2) $\mathcal{P}$ *contient exactement* $\mathrm{Card}(\Pi) = n^2 + n + 1$ *points ;*

(2') $\mathcal{P}$ *contient exactement* $\mathrm{Card}(\Delta) = n^2 + n + 1$ *droites.*

Des espaces finis

Proposition

Soit $\mathcal{P} = (\Pi, \Delta, \Phi)$ *un plan projectif fini (non dégénéré). Il existe un unique entier* $n \in \mathbb{Z}_{\geqslant 2}$, *appelé* ordre *de* $\mathcal{P}$ *tel que :*

(1) *toute droite* $d \in \Delta$ *passe par exactement* $n+1$ *points distincts de* $\mathcal{P}$;

(1') *par tout point* $p \in \Pi$ *de* $\mathcal{P}$, *il passe exactement* $n+1$ *droites distinctes ;*

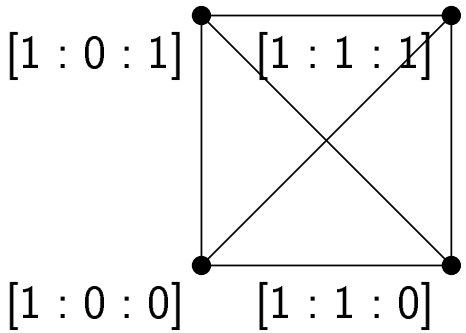
(2) $\mathcal{P}$ *contient exactement* $\mathrm{Card}(\Pi) = n^2 + n + 1$ *points ;*

(2') $\mathcal{P}$ *contient exactement* $\mathrm{Card}(\Delta) = n^2 + n + 1$ *droites.*

Si, de plus, $\mathcal{P}$ *est désarguésien, alors* $\mathcal{P}$ *est isomorphe à* $\mathbb{P}^2(\mathbb{F}_n)$ *et, en particulier,* n *est une puissance d'un nombre premier.*

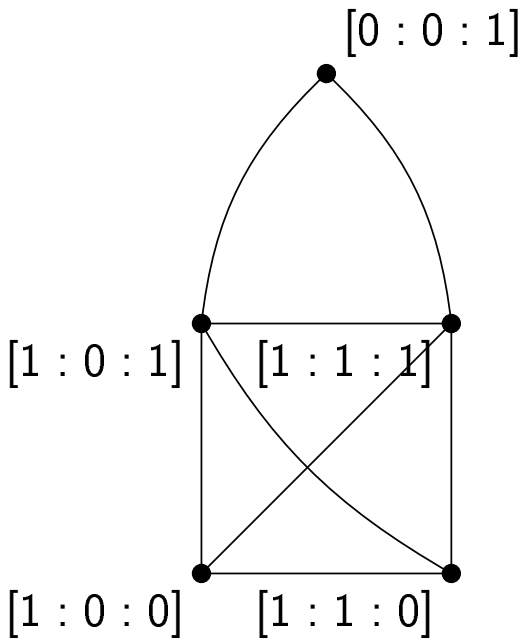
Des dessins finis : $\mathbb{P}^2(\mathbb{F}_2)$

Plan projectif de Fano



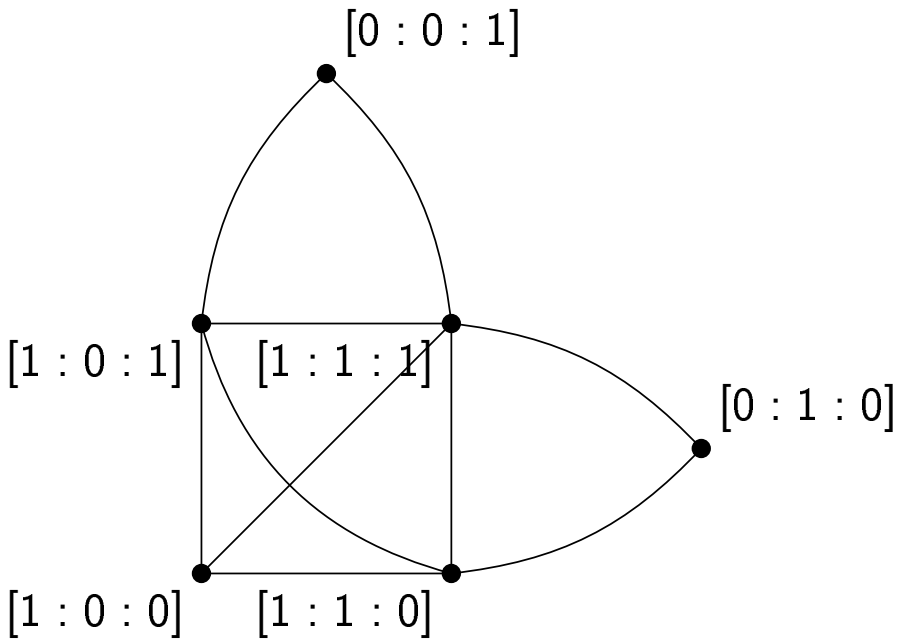
Des dessins finis : $\mathbb{P}^2(\mathbb{F}_2)$

Plan projectif de Fano



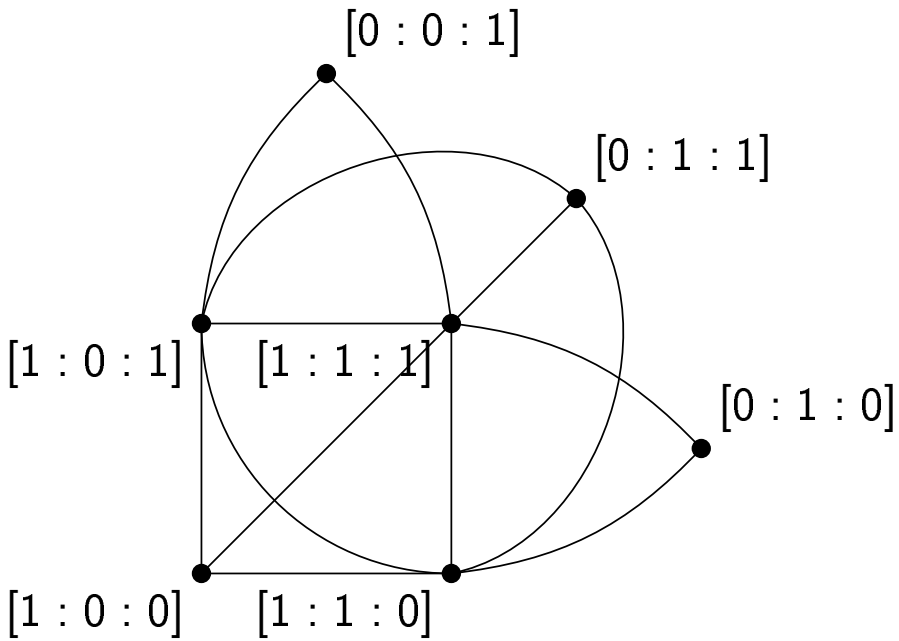
Des dessins finis : $\mathbb{P}^2(\mathbb{F}_2)$

Plan projectif de Fano



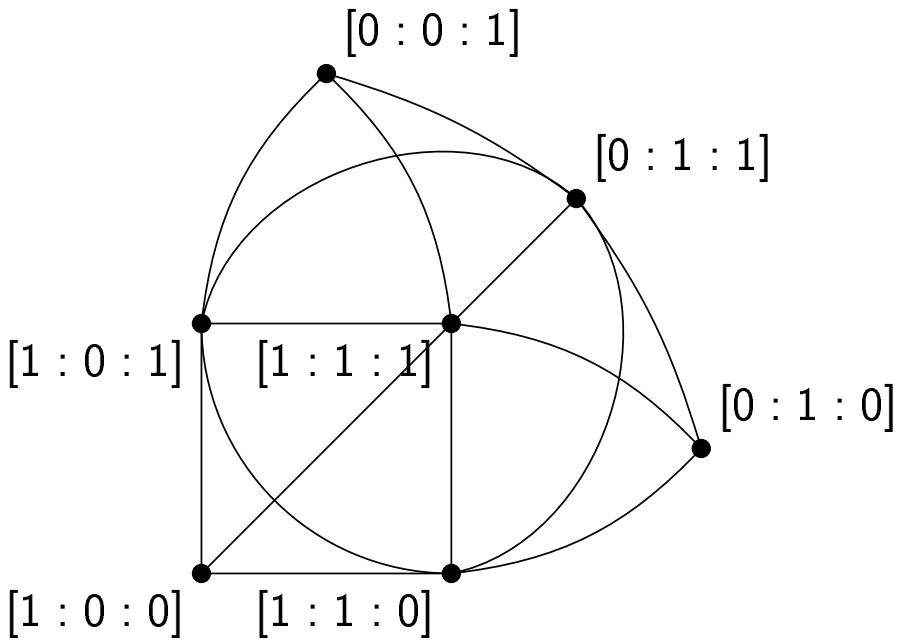
Des dessins finis : $\mathbb{P}^2(\mathbb{F}_2)$

Plan projectif de Fano



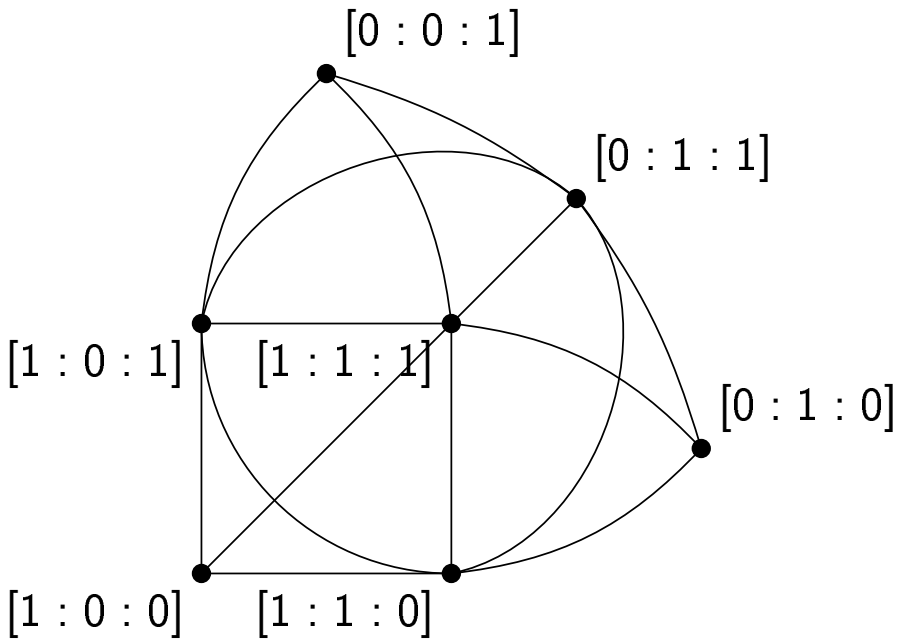
Des dessins finis : $\mathbb{P}^2(\mathbb{F}_2)$

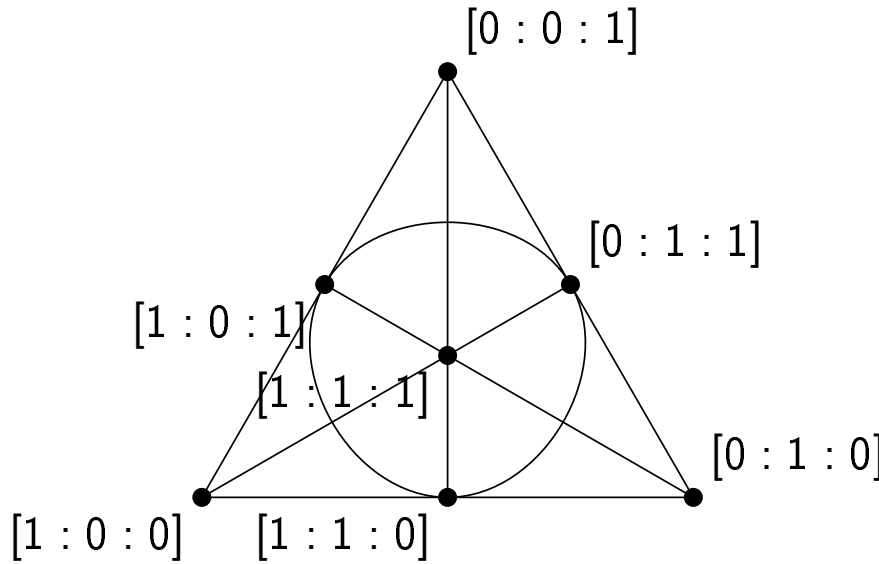
Plan projectif de Fano



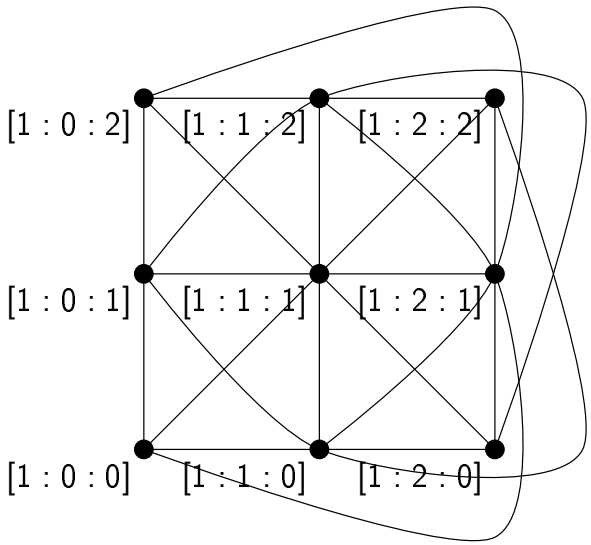
Des dessins finis : $\mathbb{P}^2(\mathbb{F}_2)$

Plan projectif de Fano

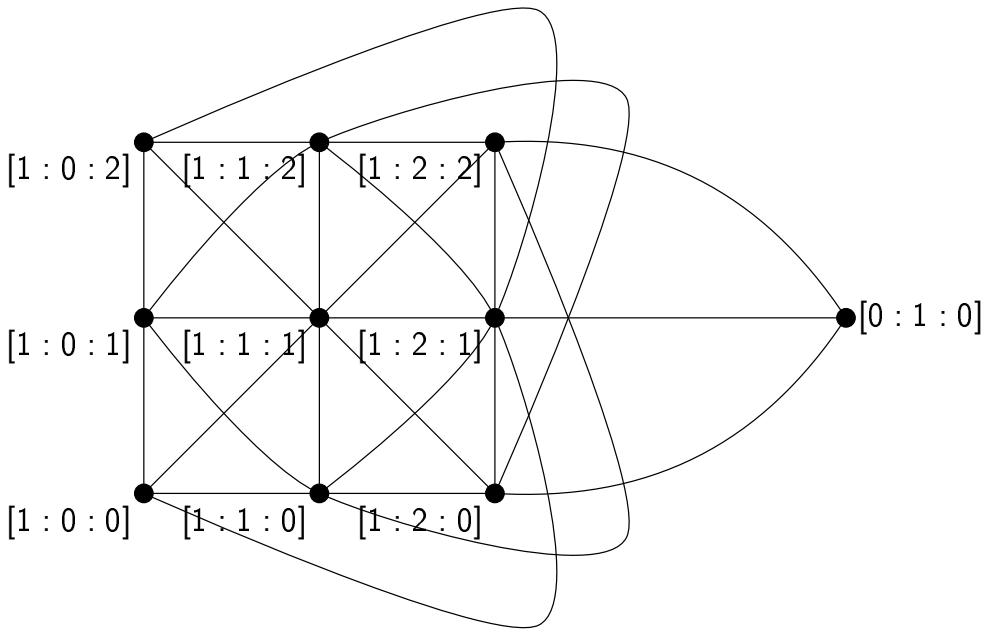




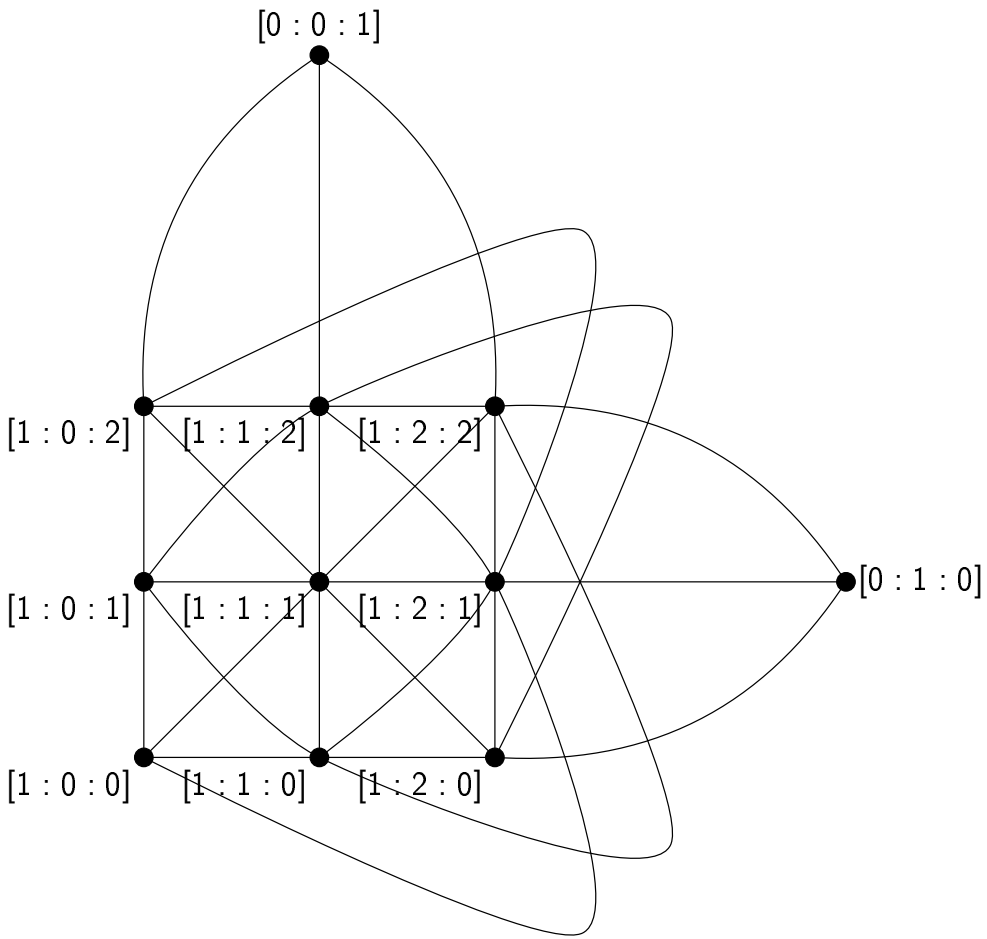
Autre exemple : $\mathbb{P}^2(\mathbb{F}_3)$



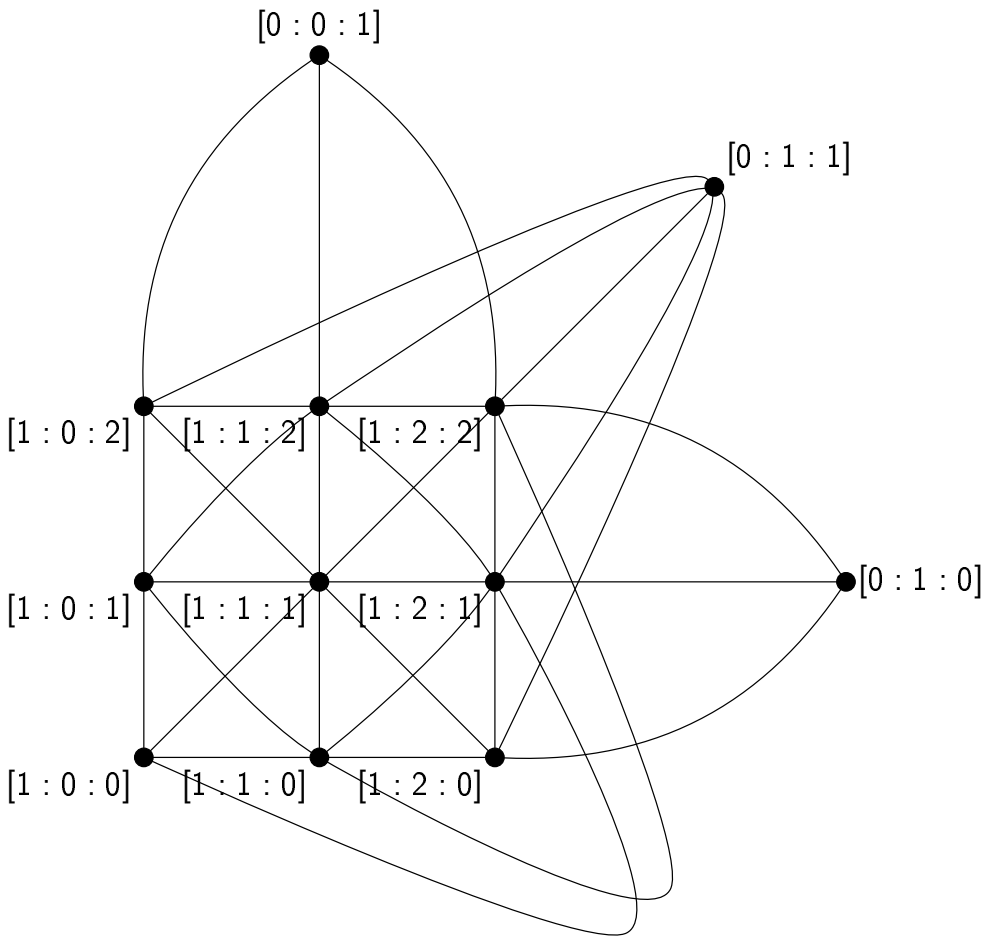
Autre exemple : $\mathbb{P}^2(\mathbb{F}_3)$



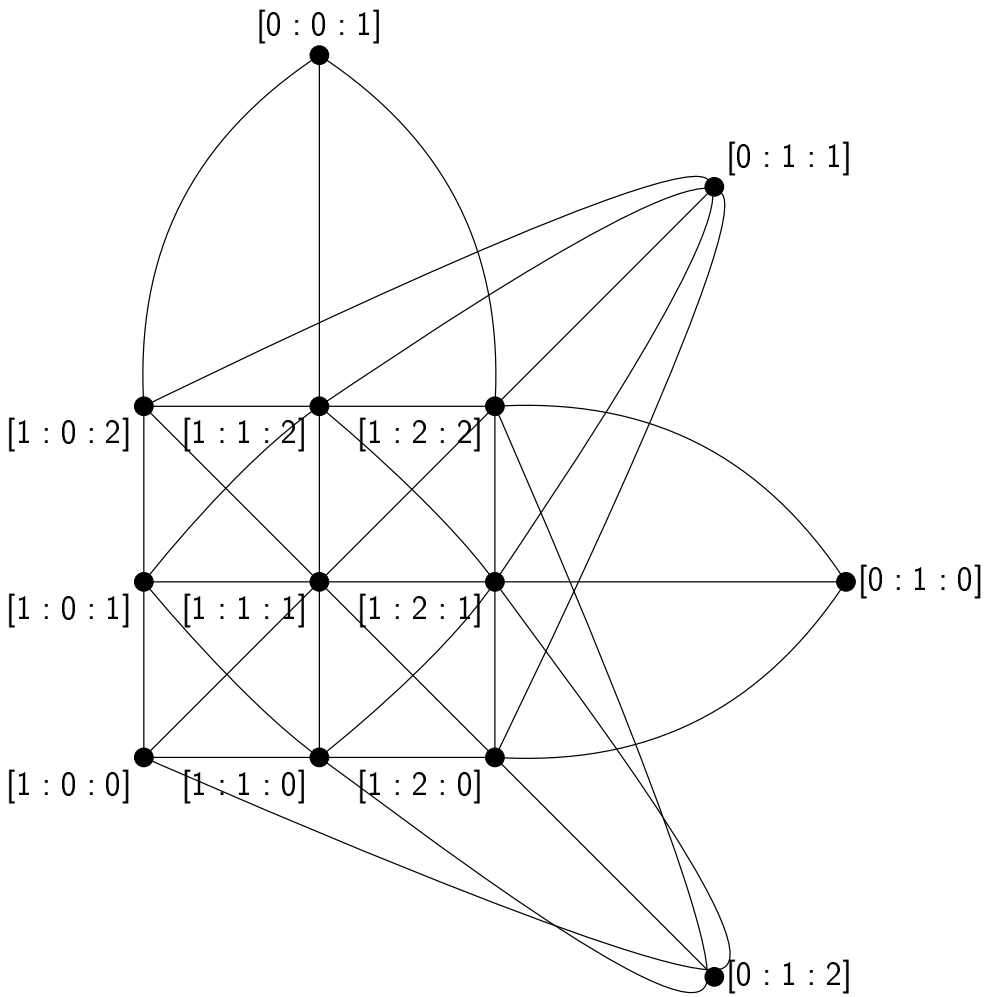
Autre exemple : $\mathbb{P}^2(\mathbb{F}_3)$



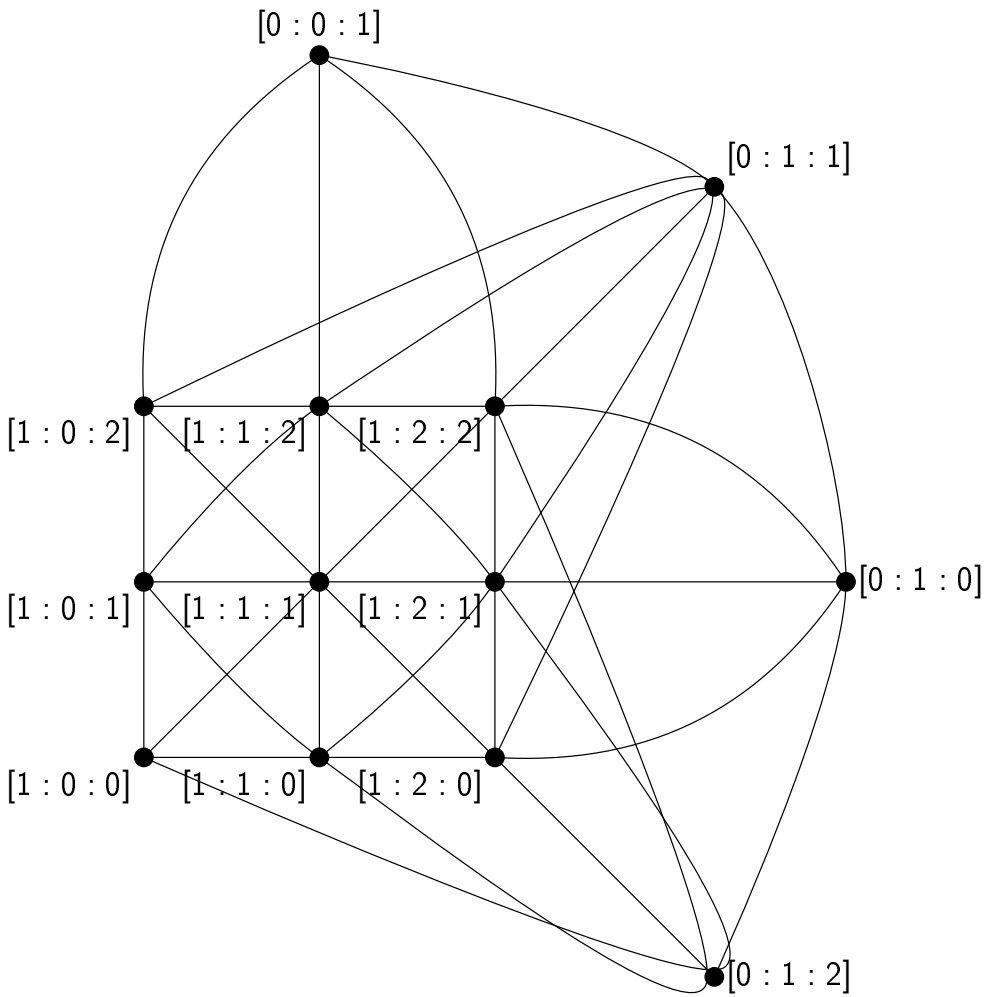
Autre exemple : $\mathbb{P}^2(\mathbb{F}_3)$



Autre exemple : $\mathbb{P}^2(\mathbb{F}_3)$



Autre exemple : $\mathbb{P}^2(\mathbb{F}_3)$



Lien avec les ensembles à différence

Théorème (Singer, 1938)

Soit $\ell \geqslant 2$ et $q = 1 + \ell + \ell^2$. On suppose qu'il existe $D = \{x_0, \ldots, x_\ell\}$ un ensemble à différence modulo q parfait. Pour tout $j \in [\![0, q-1]\!]$, on pose

$$d_j = D + j = \{x_0 + j, \ldots, x_\ell + j\}.$$

Lien avec les ensembles à différence

Théorème (Singer, 1938)

Soit $\ell \geqslant 2$ et $q = 1 + \ell + \ell^2$. On suppose qu'il existe $D = \{x_0, \ldots, x_\ell\}$ un ensemble à différence modulo q parfait. Pour tout $j \in [\![0, q-1]\!]$, on pose

$$d_j = D + j = \{x_0 + j, \ldots, x_\ell + j\}.$$

Soient

- $\Pi = \mathbb{Z}/q\mathbb{Z}$,

Lien avec les ensembles à différence

Théorème (Singer, 1938)

Soit $\ell \geqslant 2$ et $q = 1 + \ell + \ell^2$. On suppose qu'il existe $D = \{x_0, \ldots, x_\ell\}$ un ensemble à différence modulo q parfait. Pour tout $j \in [\![0, q-1]\!]$, on pose

$$d_j = D + j = \{x_0 + j, \ldots, x_\ell + j\}.$$

Soient

- $\Pi = \mathbb{Z}/q\mathbb{Z}$,
- $\Delta = \{d_j,\ 0 \leqslant j \leqslant q-1\}$,

Lien avec les ensembles à différence

Théorème (Singer, 1938)

Soit $\ell \geqslant 2$ et $q = 1 + \ell + \ell^2$. On suppose qu'il existe $D = \{x_0, \ldots, x_\ell\}$ un ensemble à différence modulo q parfait. Pour tout $j \in [\![0, q-1]\!]$, on pose

$$d_j = D + j = \{x_0 + j, \ldots, x_\ell + j\}.$$

Soient

- $\Pi = \mathbb{Z}/q\mathbb{Z}$,
- $\Delta = \{d_j,\ 0 \leqslant j \leqslant q-1\}$,
- $\Phi = \{(p, d) \in \Pi \times \Delta,\ p \in d\}$,

Lien avec les ensembles à différence

Théorème (Singer, 1938)

Soit $\ell \geqslant 2$ et $q = 1 + \ell + \ell^2$. On suppose qu'il existe $D = \{x_0, \dots, x_\ell\}$ un ensemble à différence modulo q parfait. Pour tout $j \in [\![0, q-1]\!]$, on pose

$$d_j = D + j = \{x_0 + j, \dots, x_\ell + j\}.$$

Soient

- $\Pi = \mathbb{Z}/q\mathbb{Z}$,
- $\Delta = \{d_j,\ 0 \leqslant j \leqslant q-1\}$,
- $\Phi = \{(p, d) \in \Pi \times \Delta,\ p \in d\}$,

Alors $\mathcal{P} = (\Pi, \Delta, \Phi)$ est un plan projectif fini d'ordre ℓ.

Il existe d'autres constructions de plans projectifs (Marshall Hall, 1943) toutes d'ordre une puissance de p.

Puissances de nombres premiers ?

Conjecture (Prime Power Conjecture)

On se demande si l'ordre d'un plan projectif $\mathcal{P}$ est toujours une puissance d'un nombre premier.

Puissances de nombres premiers ?

Conjecture (Prime Power Conjecture)

On se demande si l'ordre d'un plan projectif $\mathcal{P}$ est toujours une puissance d'un nombre premier.

Vraie si l'ordre ℓ :

- $\ell \equiv 1$ ou $2 \mod 4$ et n'est pas la somme de deux carrés (Bruck-Ryser, 1949) ;

Puissances de nombres premiers ?

Conjecture (Prime Power Conjecture)

On se demande si l'ordre d'un plan projectif $\mathcal{P}$ est toujours une puissance d'un nombre premier.

Vraie si l'ordre ℓ :

- $\ell \equiv 1$ ou $2 \mod 4$ et n'est pas la somme de deux carrés (Bruck-Ryser, 1949) ;
- $\ell = 10$ (Lam-Swiercz-Thiel, 1989).

Puissances de nombres premiers ?

Conjecture (Prime Power Conjecture)

On se demande si l'ordre d'un plan projectif $\mathcal{P}$ est toujours une puissance d'un nombre premier.

Vraie si l'ordre ℓ :

- $\ell \equiv 1$ ou $2 \mod 4$ et n'est pas la somme de deux carrés (Bruck-Ryser, 1949) ;
- $\ell = 10$ (Lam-Swiercz-Thiel, 1989).

Version faible :

Conjecture

On conjecture que l'ordre ℓ d'un ensemble à différence D parfait modulo $q = 1 + \ell + \ell^2$ est toujours une puissance d'un nombre premier.

On a vu que c'est vrai jusqu'à $\ell = 11$; Baumert-Gordon (2003) $\ell \leqslant 2.10^9$.

Existence de certains ensembles à différence

Théorème (Singer (1938))

Soit ℓ une puissance d'un nombre premier et $q = 1 + \ell + \ell^2$. Il existe un ensemble à différence parfait modulo q.

Soit $F = \mathbb{F}_{\ell^3}$ corps fini à ℓ^3 éléments, $\mathbb{F}_\ell$-espace vectoriel de dimension 3.
$\mathbb{F}_{\ell^3}^\times = \langle \beta \rangle$ groupe cyclique d'ordre $\ell^3 - 1 = (\ell^2 + \ell + 1) \cdot (\ell - 1)$

Existence de certains ensembles à différence

Théorème (Singer (1938))

Soit ℓ une puissance d'un nombre premier et $q = 1 + \ell + \ell^2$. Il existe un ensemble à différence parfait modulo q.

Soit $F = \mathbb{F}_{\ell^3}$ corps fini à ℓ^3 éléments, $\mathbb{F}_\ell$-espace vectoriel de dimension 3.
$\mathbb{F}_{\ell^3}^\times = \langle \beta \rangle$ groupe cyclique d'ordre $\ell^3 - 1 = (\ell^2 + \ell + 1) \cdot (\ell - 1)$
Structure de groupe cyclique sur $\mathbb{P}^2(\mathbb{F}_\ell) \simeq \mathbb{F}_{\ell^3}^\times / \mathbb{F}_\ell^\times$ via :

$$\begin{array}{rccc} \Phi : & \mathbb{F}_{\ell^3}^\times / \mathbb{F}_\ell^\times & \xrightarrow{\simeq} & \mathbb{Z}/(\ell^2+\ell+1)\mathbb{Z} \\ & \left(\beta \mod \mathbb{F}_\ell^\times\right)^n & \mapsto & n \mod q \end{array}$$

Existence de certains ensembles à différence

Théorème (Singer (1938))

Soit ℓ une puissance d'un nombre premier et $q = 1 + \ell + \ell^2$. Il existe un ensemble à différence parfait modulo q.

Soit $F = \mathbb{F}_{\ell^3}$ corps fini à ℓ^3 éléments, $\mathbb{F}_\ell$-espace vectoriel de dimension 3.
$\mathbb{F}_{\ell^3}^\times = \langle \beta \rangle$ groupe cyclique d'ordre $\ell^3 - 1 = (\ell^2 + \ell + 1) \cdot (\ell - 1)$
Structure de groupe cyclique sur $\mathbb{P}^2(\mathbb{F}_\ell) \simeq \mathbb{F}_{\ell^3}^\times / \mathbb{F}_\ell^\times$ via :

$$\begin{array}{rccc} \Phi \ : & \mathbb{F}_{\ell^3}^\times / \mathbb{F}_\ell^\times & \xrightarrow{\simeq} & \mathbb{Z}/(\ell^2+\ell+1)\mathbb{Z} \\ & \left(\beta \mod \mathbb{F}_\ell^\times\right)^n & \mapsto & n \mod q \end{array}$$

Lemme

Si W plan vectoriel de $\mathbb{F}_{\ell^3}$, $\rightsquigarrow d = \mathbb{P}(W)$ droite de $\mathbb{P}^2(\mathbb{F}_\ell)$, alors $D = \Phi(d)$ ensemble à différence parfait modulo q.

Conséquence : $d(q) = \mathrm{Card}\{D \text{ parfait}\} \geqslant q$. En fait, $q | d(q)$.

Algorithme de construction de ces ensembles à différence (exemple : $\ell = 3$ et $q = 13$)

$\mathbb{F}_{\ell^3} = \mathbb{F}_{27} = \mathbb{F}_3[\zeta]$ avec ζ racine du polynôme cyclotomique Φ_{26}.

Algorithme de construction de ces ensembles à différence (exemple : $\ell = 3$ et $q = 13$)

$\mathbb{F}_{\ell^3} = \mathbb{F}_{27} = \mathbb{F}_3[\zeta]$ avec ζ racine du polynôme cyclotomique Φ_{26}.
Algorithme de Berlekamp $\rightsquigarrow$ facteur irréductible P de Φ_{26} sur $\mathbb{F}_3$

$$P = X^3 - X + 1 \text{ donc } \mathbb{F}_{27} \simeq \mathbb{F}_3[X]/(P)$$

Algorithme de construction de ces ensembles à différence (exemple : $\ell = 3$ et $q = 13$)

$\mathbb{F}_{\ell^3} = \mathbb{F}_{27} = \mathbb{F}_3[\zeta]$ avec ζ racine du polynôme cyclotomique Φ_{26}.
Algorithme de Berlekamp $\rightsquigarrow$ facteur irréductible P de Φ_{26} sur $\mathbb{F}_3$

$$P = X^3 - X + 1 \text{ donc } \mathbb{F}_{27} \simeq \mathbb{F}_3[X]/(P)$$

Soit $\xi = \{\pm\zeta\}$ classe de $\zeta = (X \mod P)$ dans $\mathbb{F}_{27}^\times/\mathbb{F}_3^\times \simeq \mathbb{Z}/13\mathbb{Z}$.

Algorithme de construction de ces ensembles à différence (exemple : $\ell = 3$ et $q = 13$)

$\mathbb{F}_{\ell^3} = \mathbb{F}_{27} = \mathbb{F}_3[\zeta]$ avec ζ racine du polynôme cyclotomique Φ_{26}.
Algorithme de Berlekamp $\rightsquigarrow$ facteur irréductible P de Φ_{26} sur $\mathbb{F}_3$

$$P = X^3 - X + 1 \text{ donc } \mathbb{F}_{27} \simeq \mathbb{F}_3[X]/(P)$$

Soit $\xi = \{\pm\zeta\}$ classe de $\zeta = (X \mod P)$ dans $\mathbb{F}_{27}^\times/\mathbb{F}_3^\times \simeq \mathbb{Z}/13\mathbb{Z}$.

Plan vectoriel de $\mathbb{F}_{27}$:

$$\begin{aligned} W &= \mathrm{Vect}_{\mathbb{F}_3}(1, \zeta) \\ &= \{0, 1, -1, \zeta, \zeta+1, \zeta-1, \\ &\qquad -\zeta, -\zeta+1, -\zeta-1\} \\ &= \{0, \zeta^0, \zeta^{13}, \zeta^1, \zeta^9, \\ &\qquad \zeta^3, \zeta^{14}, \zeta^{16}, \zeta^{22}\} \end{aligned}$$

Algorithme de construction de ces ensembles à différence (exemple : $\ell = 3$ et $q = 13$)

$\mathbb{F}_{\ell^3} = \mathbb{F}_{27} = \mathbb{F}_3[\zeta]$ avec ζ racine du polynôme cyclotomique Φ_{26}.
Algorithme de Berlekamp $\rightsquigarrow$ facteur irréductible P de Φ_{26} sur $\mathbb{F}_3$

$$P = X^3 - X + 1 \text{ donc } \mathbb{F}_{27} \simeq \mathbb{F}_3[X]/(P)$$

Soit $\xi = \{\pm\zeta\}$ classe de $\zeta = (X \mod P)$ dans $\mathbb{F}_{27}^\times/\mathbb{F}_3^\times \simeq \mathbb{Z}/13\mathbb{Z}$.

Plan vectoriel de $\mathbb{F}_{27}$:

$$\begin{aligned} W &= \mathrm{Vect}_{\mathbb{F}_3}(1, \zeta) \\ &= \{0, 1, -1, \zeta, \zeta+1, \zeta-1, \\ &\qquad -\zeta, -\zeta+1, -\zeta-1\} \\ &= \{0, \zeta^0, \zeta^{13}, \zeta^1, \zeta^9, \\ &\qquad \zeta^3, \zeta^{14}, \zeta^{16}, \zeta^{22}\} \\ \mathbb{P}(W) &= \{\xi^0, \xi^1, \xi^3, \xi^9\} \end{aligned}$$

Algorithme de construction de ces ensembles à différence (exemple : $\ell = 3$ et $q = 13$)

$\mathbb{F}_{\ell^3} = \mathbb{F}_{27} = \mathbb{F}_3[\zeta]$ avec ζ racine du polynôme cyclotomique Φ_{26}.
Algorithme de Berlekamp $\rightsquigarrow$ facteur irréductible P de Φ_{26} sur $\mathbb{F}_3$

$$P = X^3 - X + 1 \text{ donc } \mathbb{F}_{27} \simeq \mathbb{F}_3[X]/(P)$$

Soit $\xi = \{\pm\zeta\}$ classe de $\zeta = (X \mod P)$ dans $\mathbb{F}_{27}^\times/\mathbb{F}_3^\times \simeq \mathbb{Z}/13\mathbb{Z}$.

Plan vectoriel de $\mathbb{F}_{27}$:

$$\begin{aligned} W &= \mathrm{Vect}_{\mathbb{F}_3}(1, \zeta) \\ &= \{0, 1, -1, \zeta, \zeta+1, \zeta-1, \\ &\qquad -\zeta, -\zeta+1, -\zeta-1\} \\ &= \{0, \zeta^0, \zeta^{13}, \zeta^1, \zeta^9, \\ &\qquad \zeta^3, \zeta^{14}, \zeta^{16}, \zeta^{22}\} \\ \mathbb{P}(W) &= \{\xi^0, \xi^1, \xi^3, \xi^9\} \\ \Phi(\mathbb{P}(W)) &= \{0, 1, 3, 9\} \end{aligned}$$

Algorithme de construction de ces ensembles à différence (exemple : $\ell = 3$ et $q = 13$)

$\mathbb{F}_{\ell^3} = \mathbb{F}_{27} = \mathbb{F}_3[\zeta]$ avec ζ racine du polynôme cyclotomique Φ_{26}.
Algorithme de Berlekamp $\rightsquigarrow$ facteur irréductible P de Φ_{26} sur $\mathbb{F}_3$

$$P = X^3 - X + 1 \text{ donc } \mathbb{F}_{27} \simeq \mathbb{F}_3[X]/(P)$$

Soit $\xi = \{\pm\zeta\}$ classe de $\zeta = (X \mod P)$ dans $\mathbb{F}_{27}^\times/\mathbb{F}_3^\times \simeq \mathbb{Z}/13\mathbb{Z}$.

Plan vectoriel de $\mathbb{F}_{27}$:

$$\begin{aligned} W &= \mathrm{Vect}_{\mathbb{F}_3}(1, \zeta) \\ &= \{0, 1, -1, \zeta, \zeta+1, \zeta-1, \\ &\qquad -\zeta, -\zeta+1, -\zeta-1\} \\ &= \{0, \zeta^0, \zeta^{13}, \zeta^1, \zeta^9, \\ &\qquad \zeta^3, \zeta^{14}, \zeta^{16}, \zeta^{22}\} \\ \mathbb{P}(W) &= \{\xi^0, \xi^1, \xi^3, \xi^9\} \\ \Phi(\mathbb{P}(W)) &= \{0, 1, 3, 9\} \end{aligned}$$

Donc $D = \{0, 1, 3, 9\}$ ensemble à différence parfait modulo 13 :

	0	1	3	9
0	0	12	10	4
1	1	0	11	5
3	3	2	0	7
9	9	8	6	0

Bibliographie I

Taras O. Banakh et Volodymyr M. Gavrylkiv.

Difference bases in cyclic groups.

Journal of Algebra and Its Applications, 18(05), mai 2019.

Richard H. Bruck et Herbert J. Ryser.

The nonexistence of certain finite projective planes.

Canadian Journal of Mathematics, 1(1) :88–93, 1949.

Marshall Hall.

Projective planes.

Transactions of the American Mathematical Society, 54 :229–277, 1943.

David Hilbert.

Grundlagen der geometrie.

Leipzig, B.G. Teubner, 1903.

Bibliographie II

Clement W. H. Lam, Larry Thiel, et Stanley Swiercz.

The non-existence of finite projective planes of order 10.

Canadian Journal of Mathematics, 41(6) :1117—-1123, 1989.

James Singer.

A theorem in finite projective geometry and some applications to number theory.

Transactions of the American Mathematical Society, 43(3) :377–385, 1938.

Oswald Veblen et John W. Young.

Projective Geometry Volume II.

Blasidell Publishing Company, 1946.

Alfred N. Whitehead.

The axioms of projective geometry.

Cambridge : At the University Press, 1906.

Démonstration du Lemme de Singer I

Lemme

Pour toute droite projective $d \in \mathbb{P}(\mathbb{F}_{\ell^3}) \simeq \mathbb{P}^2(\mathbb{F}_\ell)$, tout élément non trivial du groupe $\mathbb{F}_{\ell^3}^\times/\mathbb{F}_\ell^\times$ s'écrit de manière unique comme différence $\zeta \cdot \xi^{-1}$ avec $\zeta, \xi \in d \subset \mathbb{F}_{\ell^3}^\times/\mathbb{F}_\ell^\times$.

Soit ζ une racine primitive $\ell^3 - 1$-ème de l'unité, de sorte que $\mathbb{F}_{\ell^3} = \mathbb{F}_\ell[\zeta] \simeq \mathbb{F}_\ell[X]/(Q)$ avec $Q = \alpha + \beta X + \gamma X^2 \in \mathbb{F}_\ell[X]$ irréductible.
Soit d une droite projective. Comme $\mathrm{PGL}_3(\mathbb{F}_\ell)$ agit transitivement sur l'ensemble des droites projectives, c'est-à-dire sur l'ensemble des sous-$\mathbb{F}_\ell$-espaces vectoriels de dimension 2 de $\mathbb{F}_{\ell^3}$, on peut supposer, sans restriction, que $d = \mathbb{P}(W)$ avec $W = \mathrm{Vect}_{\mathbb{F}_\ell}(1, \zeta)$.
Ainsi, tout élément ξ de d peut s'écrire $\xi = \xi \cdot 1^{-1}$.

Démonstration du Lemme de Singer II

De plus, pour tout élément $(u, v, w) \in \mathbb{F}_\ell^3 \setminus \{(0,0,0)\}$, et tout $(a, b) \in \mathbb{F}_\ell^2$, on a

$$\begin{aligned}(u + v\zeta + w\zeta^2) \cdot (a + b\zeta) =& au + (av + bu)\zeta + (aw + vb)\zeta^2 + bw\zeta^3 \\ =& (au + \alpha bw) + (av + bu + \beta bw)\zeta \\ &+ (aw + bv + \gamma bw)\zeta^2\end{aligned}$$

Pour que ce produit soit dans W, il suffit que $aw + b(v + \gamma w) = 0$.

- Si $w = 0$, on prend $(a, b) = (1, 0)$.
- Sinon, on prend $(a, b) = (\frac{-v-\gamma w}{w}, 1)$.

Ainsi, on a écrit tout point de $\mathbb{F}_{\ell^3}$ comme quotient de deux points de W.
Ce qui démontre l'existence.
L'unicité découle immédiatement de la minimalité du cardinal.

Aux origines de la géométrie

Les Éléments (d'Euclide) :

- $\sim$ IIIème siècle avant J.-C.,
- 13 livres,
- raisonnement mathématique articulé en :
  - axiomes,
  - définitions,
  - théorèmes,
  - démonstrations.
- instaure les bases de la géométrie (euclidienne) : constructions à la règle et au compas

Axiomes de la géométrie euclidienne

Les cinq axiomes de la géométrie euclidienne :

(A1) un segment de droite peut être tracé en joignant deux points quelconques distincts ;

(A2) un segment de droite peut être prolongé indéfiniment en une ligne droite ;

(A3) étant donné un segment de droite quelconque, un cercle peut être tracé en prenant ce segment comme rayon et l'une de ses extrémités comme centre ;

(A4) tous les angles droits sont congruents ;

Axiomes de la géométrie euclidienne

Les cinq axiomes de la géométrie euclidienne :

(A1) un segment de droite peut être tracé en joignant deux points quelconques distincts ;

(A2) un segment de droite peut être prolongé indéfiniment en une ligne droite ;

(A3) étant donné un segment de droite quelconque, un cercle peut être tracé en prenant ce segment comme rayon et l'une de ses extrémités comme centre ;

(A4) tous les angles droits sont congruents ;

(A5) si deux lignes sont sécantes avec une troisième de telle façon que la somme des angles intérieurs d'un côté est strictement inférieure à deux angles droits, alors ces deux lignes sont forcément sécantes de ce côté.

Espace projectif de dimension d sur un corps (gauche) k

Notation

$$\mathbb{P}^d(k) = \left(k^{d+1} \setminus \{0\}\right)/k^*$$
$$= \left\{[x_0 : \ldots : x_d],\ (x_0, \ldots, x_d) \in k^{d+1} \setminus \{0\}\right\}$$

Définition

Homographies = action du groupe $\mathrm{PGL}_{d+1}(k)$ sur l'espace $\mathbb{P}^d(k)$.

Exemple

$d = \{[0 : y : z], (y, z) \neq (0, 0)\}$ droite à l'infini de
$A = \{[1 : y : z], (y, z) \in k^2\}$ réalisation d'un plan affine le plan projectif.

Axiomes des plans projectifs

Définition (Hall, 1943)

Un *plan projectif* (non dégénéré) est la donnée d'un ensemble de points Π, d'un ensemble de droites Δ et d'une relation d'incidence entre points et droites $\Phi \subset \Pi \times \Delta$ tels que :

Axiomes des plans projectifs

Définition (Hall, 1943)

Un *plan projectif* (non dégénéré) est la donnée d'un ensemble de points Π, d'un ensemble de droites Δ et d'une relation d'incidence entre points et droites $\Phi \subset \Pi \times \Delta$ tels que :

(P1) deux points distincts A, B sont contenus dans une unique droite (AB) ;

Axiomes des plans projectifs

Définition (Hall, 1943)

Un *plan projectif* (non dégénéré) est la donnée d'un ensemble de points Π, d'un ensemble de droites Δ et d'une relation d'incidence entre points et droites $\Phi \subset \Pi \times \Delta$ tels que :

(P1) deux points distincts A, B sont contenus dans une unique droite (AB) ;

(P2) deux droites distinctes s'intersectent toujours en un unique point ;

Axiomes des plans projectifs

Définition (Hall, 1943)

Un *plan projectif* (non dégénéré) est la donnée d'un ensemble de points Π, d'un ensemble de droites Δ et d'une relation d'incidence entre points et droites $\Phi \subset \Pi \times \Delta$ tels que :

(P1) deux points distincts A, B sont contenus dans une unique droite (AB) ;

(P2) deux droites distinctes s'intersectent toujours en un unique point ;

(P3) il existe au moins un quadrangle, c'est-à-dire quatre points distincts qui sont trois à trois non alignés.

Axiomes des plans projectifs

Définition (Hall, 1943)

Un *plan projectif* (non dégénéré) est la donnée d'un ensemble de points Π, d'un ensemble de droites Δ et d'une relation d'incidence entre points et droites $\Phi \subset \Pi \times \Delta$ tels que :

(P1) deux points distincts A, B sont contenus dans une unique droite (AB) ;

(P2) deux droites distinctes s'intersectent toujours en un unique point ;

(P3) il existe au moins un quadrangle, c'est-à-dire quatre points distincts qui sont trois à trois non alignés.

Remarque

On peut remplacer (P3) par

(P3') toute droite contient au moins trois points distincts et

(P3'') il existe au moins trois points non alignés,

pour faire apparaître une dualité points $\leftrightarrow$ droites.

Démonstration du théorème de Veblen-Young

Il s'agit de démontrer le théorème de Desargues pour des espaces projectifs non planaires. Supposons donnés deux triangles $A_1B_1C_1$ et $A_2B_2C_2$, tels que les trois droites $a = (A_1A_2)$, $b = (B_1B_2)$ et $c = (C_1C_2)$ sont concourantes.

Démonstration du théorème de Veblen-Young

Il s'agit de démontrer le théorème de Desargues pour des espaces projectifs non planaires. Supposons donnés deux triangles $A_1B_1C_1$ et $A_2B_2C_2$, tels que les trois droites $a = (A_1A_2)$, $b = (B_1B_2)$ et $c = (C_1C_2)$ sont concourantes.
Comme les droites a et b s'intersectent par hypothèse, on en déduit que les quatre points A_1, A_2, B_1, B_2 sont coplanaires. En particulier, les droites (A_1B_1) et (A_2B_2) s'intersectent nécessairement. De plus, si les deux triangles $A_1B_1C_1$ et $A_2B_2C_2$ sont dans des plans distincts, alors le point d'intersection $C = (A_1B_1) \cap (A_2B_2)$ est dans l'intersection de ces deux plans.

Démonstration du théorème de Veblen-Young

Il s'agit de démontrer le théorème de Desargues pour des espaces projectifs non planaires. Supposons donnés deux triangles $A_1B_1C_1$ et $A_2B_2C_2$, tels que les trois droites $a = (A_1A_2)$, $b = (B_1B_2)$ et $c = (C_1C_2)$ sont concourantes.

Comme les droites a et b s'intersectent par hypothèse, on en déduit que les quatre points A_1, A_2, B_1, B_2 sont coplanaires. En particulier, les droites (A_1B_1) et (A_2B_2) s'intersectent nécessairement. De plus, si les deux triangles $A_1B_1C_1$ et $A_2B_2C_2$ sont dans des plans distincts, alors le point d'intersection $C = (A_1B_1) \cap (A_2B_2)$ est dans l'intersection de ces deux plans.

Par un argument analogue, on montre que les points d'intersection $A = (B_1C_1) \cap (B_2C_2)$ et $B = (C_1A_1) \cap (C_2A_2)$ existent et sont dans l'intersection des deux plans contenant les triangles $A_1B_1C_1$ et $A_2B_2C_2$. Ainsi, l'intersection de ces deux plans est une droite qui contient les trois points d'intersection A, B et C.

Lemmes, laissés en exercice

Pour démontrer la proposition sur l'existence de l'ordre d'un plan projectif fini, on montre successivement que :

Lemme

Un plan projectif $\mathcal{P}$ n'est pas la réunion de deux droites.

Lemmes, laissés en exercice

Pour démontrer la proposition sur l'existence de l'ordre d'un plan projectif fini, on montre successivement que :

Lemme

Un plan projectif $\mathcal{P}$ n'est pas la réunion de deux droites.

Lemme

Soit $\mathcal{P} = (\Pi, \Delta, \Phi)$ un plan projectif. Soient $d_1, d_2 \in \Delta$ deux droites distinctes. Pour tout $p \in \Pi \setminus (d_1 \cup d_2)$, l'application $f_p : d_1 \to d_2$ qui à un point $x \in d_1$ associe l'unique point d'intersection de d_2 et de la droite (xp) est une bijection de d_1 sur d_2

Lemmes, laissés en exercice

Pour démontrer la proposition sur l'existence de l'ordre d'un plan projectif fini, on montre successivement que :

Lemme

Un plan projectif $\mathcal{P}$ n'est pas la réunion de deux droites.

Lemme

Soit $\mathcal{P} = (\Pi, \Delta, \Phi)$ un plan projectif. Soient $d_1, d_2 \in \Delta$ deux droites distinctes. Pour tout $p \in \Pi \setminus (d_1 \cup d_2)$, l'application $f_p : d_1 \to d_2$ qui à un point $x \in d_1$ associe l'unique point d'intersection de d_2 et de la droite (xp) est une bijection de d_1 sur d_2

Lemme

Soit $\mathcal{P} = (\Pi, \Delta, \Phi)$ un plan projectif. Si $p \in \Pi$ et $d \in \Delta$ sont tels que $p \notin d$, alors les droites passant par p sont en bijection avec les points de d.