Plans projectifs, arithmétique modulaire et Dobble

M. Deléglise

27 février 2013
révisé le 19 octobre 2026

Résumé

Le jeu de Dobble édité par Asmodée est une excellente occasion d'introduire des objets mathématiques importants : les plans projectifs, l'arithmétique modulaire et les nombres premiers. C'est le sujet de ce texte élémentaire à la portée d'un élève des classes secondaires.

1 Le plan projectif, et le plan affine réel

1.1 Le plan affine réel

Le choix d'une origine O du plan réel et de deux axes Ox et Oy permet d'associer à tout point M du plan deux nombres réels appelés l'abscisse et l'ordonnée de M. Dans la suite on écrira le point (x, y) pour désigner le point M d'abscisse x et d'ordonnée y.

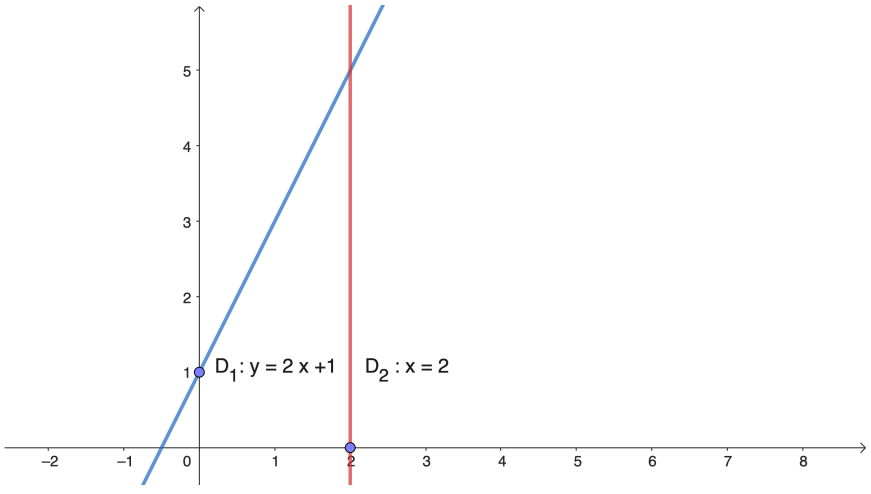


FIGURE 1 – Les droites du plan affine d'équations $y = 2x + 1$ et $x = 2$

Une droite non verticale D est définie par son équation $y = ax + b$. Le nombre a est la pente de cette droite.

Une droite verticale est une droite d'équation $x = x_0$, où x_0 est l'abscisse de son point d'intersection avec l'axe des x. On dira qu'elle a une pente infinie que l'on notera ∞. On notera $\overline{\mathbb{R}}$ l'ensemble $\mathbb{R} \cup \{\infty\}$ de sorte que la pente d'une droite soit, dans tous les cas, un élément de $\overline{\mathbb{R}}$.

Définition 1. *On dit que deux droites sont parallèles si elles ont la même pente.*

Proposition 1. *Soient deux droites distinctes D et D'. Si elles sont parallèles elles n'ont pas de point commun, sinon elles se rencontrent en un unique point.*

Démonstration:

1. Si elles sont parallèles elles ont la même pente. Alors, ou bien,
   — Ce sont deux verticales distinctes donc sans point commun.
   — Elles sont de même pente finie a et donc d'équations respectives $y = ax + b$ et $y = ax + b'$, avec $b \neq b'$. Leurs points communs sont les points dont l'abscisse est solution de l'équation $ax+b = ax+b'$. Cette égalité implique $b = b'$ et n'admet pas de solution.
2. Si elles ne sont pas parallèles, ou bien
   — Aucune des deux n'est verticale, leurs équations sont $y = ax + b$, $y = a'x + b'$ avec $a \neq a'$. Leurs points communs sont les points d'abscisse x satisfaisant $ax + b = a'x + b'$. Cette équation s'écrit :

   $$(a - a')x = b' - b. \tag{1}$$

   Puisque $a - a'$ n'est pas nul il admet un inverse $1/(a - a')$ et en multipliant les deux termes de (1) par cet inverse on voit que cette équation implique $x = (b' - b)/(a - a')$. Et, réciproquement, cette égalité, en la multipliant par $(a - a')$ implique (1). Donc D et D' n'ont qu'un point commun, le point d'abscisse $(b' - b)/(a - a')$.
   — Si D', par exemple, est la verticale définie par $x = x_0$, alors D n'est pas verticale, donc d'équation $y = ax + b$ et l'unique point commun à D et D' est le point de D d'abscisse x_0, c'est à dire $(x_0, ax_0 + b)$.

□

1.2 Le plan projectif réel

On construit le plan projectif réel de la manière suivante : Pour chaque direction de droite on ajoute un nouveau point, qu'on appelle le point à l'infini de cette direction. Deux droites parallèles définissent donc le même point à l'infini.

Définition 2. *Le plan projectif réel est obtenu en ajoutant au plan affine, pour toute direction de droite, un nouveau point, appelé le point à l'infini dans cette direction.*

Définition 3. *L'ensemble des droites du plan projectif réel est, par définition, l'ensemble dont les éléments sont :*

1. *Toutes les droites du plan affine, chacune enrichie du point à l'infini dans sa direction, qu'on appellera les droites ordinaires du plan projectif.*
2. *Une dernière droite, la droite à l'infini, dont les points sont les points à l'infini de toutes les directions.*

Chaque droite du plan projectif, à l'exception de la droite à l'infini, est ainsi une droite ordinaire bien définie par son équation.

Il est impossible de représenter graphiquement le plan projectif avec sa droite à l'infini. La figure 2 en donne une idée : c'est l'image en perspective d'une mer infinie sur une terre supposée plate ! La droite à l'infini est la ligne d'horizon.

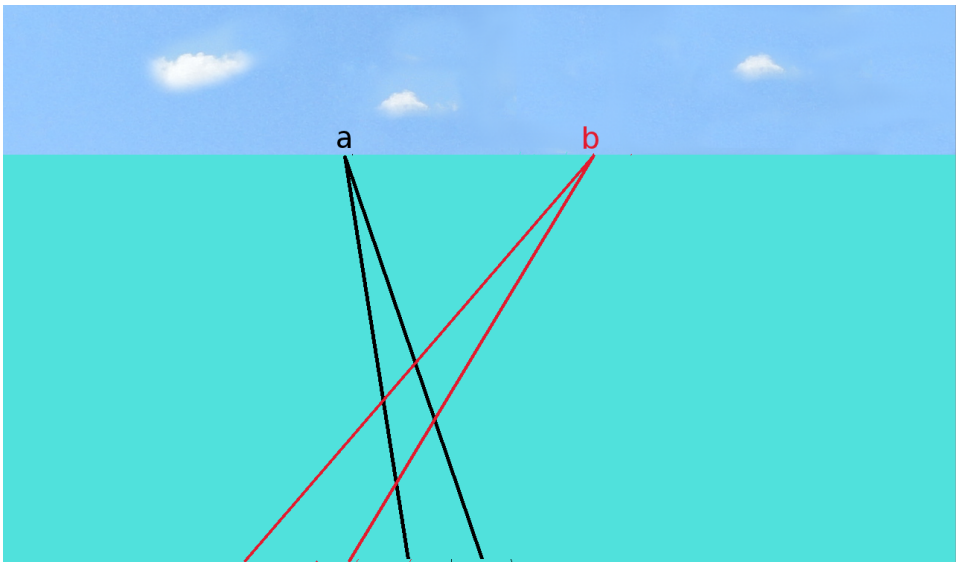


FIGURE 2 – Le plan affine complété par la droite à l'infini. Les deux droites noires (resp. rouges) sont parallèles et ne se rencontrent qu'en le point à l'infini de leur direction, le point a (resp. b)

Proposition 2. *Deux droites distinctes D, D' du plan projectif réel se coupent toujours en exactement un point.*

Démonstration:

— Si D, par exemple, est la droite à l'infini, D' est une droite ordinaire. D ne contient que les points à l'infini, et D' n'en contient qu'un, celui de sa direction.
— Sinon ce sont deux droites ordinaires, chacune d'entre elles est une droite affine à laquelle on a rajouté le point à l'infini dans sa direction. Alors, grâce à la proposition 1,
  — Si elles sont parallèles, elles n'ont pas de point commun dans le plan affine mais elles partagent leur unique point à l'infini, celui de leur direction.
  — Sinon, elles se rencontrent en un unique point du plan affine, et elles n'ont pas de point commun à l'infini car leurs directions ne sont pas les mêmes.

□

2 Le corps $\mathbb{F}_p$.

Rappelons qu'un nombre entier positif p est premier si il n'a pas d'autre diviseur que 1 et p. Le nombre 5 est premier car il n'est divisible que par 1 et 5, 6 ne l'est pas car il a 4 diviseurs $1, 2, 3, 6$.

Pour tout nombre premier p, on note $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ l'ensemble des entiers naturels plus petits que p. On le munit de deux opérations, une addition et une multiplication. L'addition est définie de la manière suivante : Pour calculer $a+b$ on calcule la somme ordinaire $a+b$, mais si le résultat est supérieur ou égal à p on en retranche p. Pour $p = 5$ par exemple, $1 + 2 = 3$ et $3 + 4 = 7 - 5 = 2$. Cette opération est appelée l'addition modulo p. On définit la multiplication sur $\mathbb{F}_p$ de manière semblable : Pour calculer le produit de a par b on calcule d'abord le produit ordinaire, et, si le résultat est supérieur ou égal à p on le remplace par le reste de sa division par p. Ainsi, dans le cas $p = 5$, $3 \times 4 = 12 - 10 = 2$. On appelle cette opération la multiplication modulo p. La figure 3 montre la table d'addition et la table de multiplication de $\mathbb{F}_5$.

FIGURE 3 – Tables d'addition et de multiplication de $\mathbb{F}_5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Nous admettrons la proposition suivante [1]

Proposition 3. *Soit p un nombre premier arbitraire et l'ensemble $\mathbb{F}_p$ muni de l'addition et de la multiplication modulo p. Alors*

1. *Chaque nombre x a un unique opposé, c'est-à-dire un nombre qui, ajouté à x, donne 0. On note ce nombre $-x$.*
2. *Chaque x non nul a un unique inverse, c'est-à-dire un nombre qui, multiplié par x, donne 1. On note ce nombre $1/x$.*

FIGURE 4 – Tables des opposés et des inverses dans $\mathbb{F}_5$

x	0	1	2	3	4
$-x$	0	4	3	2	1

x	1	2	3	4
$1/x$	1	3	2	4

Division et soustraction dans $\mathbb{F}_p$.

1. On définit $a - b$ comme la somme de a et de l'opposé de b.
2. Lorsque b n'est pas nul on définit $\frac{a}{b}$ comme le produit $a \times (1/b)$ de a par l'inverse de b. Pour $p = 5$, par exemple $a = 2$ et $b = 3$. La table des inverses de la figure 4 nous dit que l'inverse de 3 est 2. Donc

$$\frac{2}{3} = 2 \times \frac{1}{3} = 2 \times 2 = 4.$$

Remarque. Rien n'empêche de définir l'addition et la multiplication modulo n lorsque n n'est pas premier, mais, dans ce cas, la propriété 2 de la proposition 3 est fausse. Par exemple, pour $n = 6$ qui n'est pas premier, puisque $6 = 2 \times 3$, dressons les tables d'addition et de multiplication modulo 6 (cf. figure 5). On voit sur la table de multiplication que seuls 1 et 5 admettent un inverse. En particulier, modulo 6, on ne peut pas diviser par $2, 3$ et 4 parce que ces nombres n'ont pas d'inverse.

3 Le plan affine et le plan projectif sur $\mathbb{F}_p$

3.1 Le plan affine sur $\mathbb{F}_p$

Comme nous l'avons fait dans le cas des nombres réels (cf. figure 1), à tout couple (x, y) d'éléments de $\mathbb{F}_p$ on associe un point du plan affine sur $\mathbb{F}_p$. Puisque $\mathbb{F}_p$ a p éléments, le plan affine sur $\mathbb{F}_p$ a $p \times p = p^2$ points représentés sur la figure 6 dans le cas $p = 5$.

1. Pour ceux qui connaissent un peu d'arithmétique, c'est la démonstration du point 2 qui nécessite la primalité de p. On la démontre généralement en utilisant le théorème de Bezout.

FIGURE 5 – Tables d'addition et de multiplication modulo 6

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(0,4)	(1,4)	(2,4)	(3,4)	(4,4)
(0,3)	(1,3)	(2,3)	(3,3)	(4,3)
(0,2)	(1,2)	(2,2)	(3,2)	(4,2)
(0,1)	(1,1)	(2,1)	(3,1)	(4,1)
(0,0)	(1,0)	(2,0)	(3,0)	(4,0)

(0,4)	(1,4)	(2,4)	(3,4)	(4,4)
(0,3)	(1,3)	(2,3)	(3,3)	(4,3)
(0,2)	(1,2)	(2,2)	(3,2)	(4,2)
(0,1)	(1,1)	(2,1)	(3,1)	(4,1)
(0,0)	(1,0)	(2,0)	(3,0)	(4,0)

FIGURE 6 – Les points du plan affine sur $\mathbb{F}_5$: à gauche, en bleu, les points de la droite $y = 2x + 1$ et à droite, en jaune, ceux de la droite $x = 2$

Comme dans le cas réel, une droite du plan affine est définie par son équation de la forme $y = ax + b$, ou de la forme $x = x_0$ et on dit dans ce cas qu'elle est verticale. Dans le premier cas elle est de pente a, et dans le deuxième cas de pente infinie ∞.

On dit encore que deux droites sont parallèles si elles ont la même pente. On a alors exactement, comme dans le cas réel :

Proposition 4. *Soient deux droites distinctes D et D' du plan affine sur $\mathbb{F}_p$. Si elles sont parallèles elles n'ont pas de point commun, sinon elles se rencontrent en un unique point.*

Démonstration: La démonstration est la même que dans le cas du plan réel.

1. Si elles sont parallèles elles ont la même pente. Alors, ou bien,
   — Ce sont deux verticales distinctes donc sans point commun.
   — Elles sont de même pente finie a et donc d'équations respectives $y = ax + b$ et $y = ax + b'$, avec $b \neq b'$. Leurs points communs sont les points dont l'abscisse est solution de l'équation $ax+b = ax+b'$. Cette égalité implique $b = b'$ et n'admet pas de solution.
2. Elles ne sont pas parallèles
   — Si aucune des deux n'est verticale, leurs équations sont $y = ax+b$, $y = a'x + b'$ avec $a \neq a'$. Leurs points communs sont les points d'abscisse x satisfaisant $ax + b = a'x + b'$. Cette équation s'écrit :

$$(a - a')x = b' - b. \tag{2}$$

Puisque $a - a'$ est un élément non nul de $\mathbb{F}_p$, par la proposition 3, il admet un unique inverse $1/(a - a')$ et en multipliant les deux termes de (2) par cet inverse on voit que cette équation implique $x = (b' - b) \cdot 1/(a - a')$. Et, réciproquement, cette égalité, en la multipliant par $(a - a')$ implique (2). Donc D et D' n'ont qu'un point commun, le point d'abscisse $(b' - b)/(a - a')$.

— Si D', par exemple, est verticale, définie par $x = x_0$, alors D n'est pas verticale, d'équation $y = ax + b$ et l'unique point commun à D et D' est le point de D d'abscisse x_0, c'est à dire $(x_0, ax_0 + b)$.

□

Proposition 5. *Le nombre de droites du plan affine sur $\mathbb{F}_p$ est $p^2 + p$.*

Démonstration: L'application qui associe au couple (a, b) la droite d'équation $y = ax + b$ est une bijection de $\mathbb{F}_p \times \mathbb{F}_p$ sur l'ensemble des droites non verticales, qui sont donc au nombre de $p \times p = p^2$. L'application qui associe à l'élément x_0 de $\mathbb{F}_p$ la droite d'équation $x = x_0$ est une bijection de $\mathbb{F}_p$ sur l'ensemble des droites verticales qui sont donc au nombre de p. Le nombre total de droites est donc $p^2 + p$. □

3.2 Le plan projectif $P_2(\mathbb{F}_p)$.

Dans le §1.2, nous avons construit le plan projectif réel à partir du plan affine réel. Dans cette section nous construisons, de la même manière, le plan projectif sur $\mathbb{F}_p$ à partir du plan affine sur $\mathbb{F}_p$, en rajoutant un point à l'infini pour chaque direction de droite du plan affine. Dans le plan réel il y a une infinité de directions, car il y a une infinité de pentes, donc une infinité de points à l'infini. Dans le plan affine sur $\mathbb{F}_p$, il n'y a que p pentes possibles, les pentes $0, 1, 2, \ldots, p - 1$. Pour chacune de ces pentes a on crée un point à l'infini qui sera le point commun à toutes les droites de pente a, que l'on note (a, ∞). Ceci nous donne les p points à l'infini $(0, \infty), (1, \infty), \ldots, (p-1, \infty)$. Il reste une dernière direction de droite, la direction verticale, qui nous donne un dernier point à l'infini, le point à l'infini dans la direction verticale que l'on notera (∞, ∞).

L'ensemble des points à l'infini est donc l'ensemble à $p + 1$ éléments :

$$(0, \infty), (1, \infty), (2, \infty), \ldots (p - 1, \infty), (\infty, \infty).$$

Cet ensemble est, par définition, la droite à l'infini du plan projectif. Les autres droites du plan projectif sont constituées d'une droite du plan affine, à laquelle on ajoute le point à l'infini associé à sa direction. On les appelle les droites ordinaires.

Proposition 6. *Si D, D' sont deux droites distinctes du plan projectif sur $\mathbb{F}_p$ elles ont exactement un point commun.*

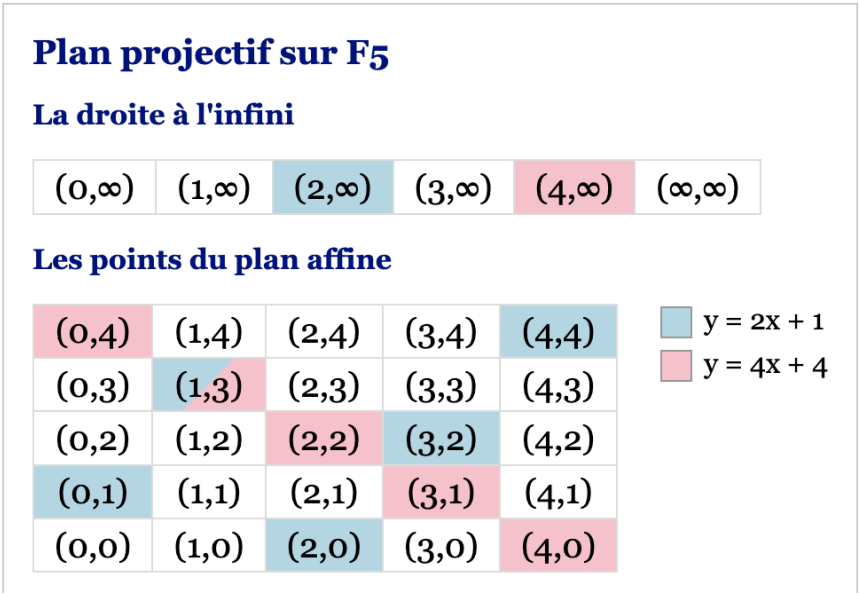


FIGURE 7 – Deux droites du plan projectif sur $\mathbb{F}_5$. En rose $D_1 : y = 4x + 4$, et, en bleu $D_2 : y = 2x + 1$.

Démonstration:

- Si D est la droite à l'infini tous ses points sont à l'infini, et D' qui est une droite ordinaire, n'a qu'un point à l'infini, qui est l'unique point qu'elle partage avec D.
- Sinon ces deux droites sont deux droites ordinaires.
  - Si elles ont même pente a elles sont parallèles, elles n'ont pas de point commun à distance finie, mais, puisqu'elles sont de même pente a elles ont le même point à l'infini, le point (a, ∞).
  - Si leurs pentes a_1, a_2 ne sont pas égales, leurs points à l'infini (a_1, ∞) et (a_2, ∞) sont distincts, et leurs points à distance finie sont ceux de deux droites affines non parallèles, qui ont un unique point commun par la proposition 4

□

Proposition 7. *Le nombre de points et le nombre de droites du plan projectif $P_2(\mathbb{F}_p)$ sont tous les deux égaux à $p^2 + p + 1$.*

Démonstration: Chaque droite ordinaire du plan projectif est définie à partir de l'une des droites du plan affine ; par la proposition 5 celles-ci sont au nombre de $p^2 + p$. En rajoutant la droite à l'infini on obtient $p^2 + p + 1$ droites projectives.

Quant au nombre de points du plan projectif c'est le nombre des points du plan affine, p^2 plus le nombre $p + 1$ de points à l'infini ce qui donne le

nombre total de points : $p^2 + p + 1$. □

4 Une application, le jeu de Dobble

Dobble est un jeu de société, édité par Asmodée. Ce jeu est constitué de 55 cartes, sur chacune desquelles sont dessinées 8 images. La propriété remarquable de ces cartes est la suivante : *pour toute paire de cartes, il existe une image et une seule qui figure sur ces deux cartes.* La figure 8 représente une paire de cartes. On peut jouer de plusieurs manières, mais dans tous les cas, il s'agit, pour chacun des joueurs, de trouver le plus rapidement possible l'image commune aux deux cartes situées devant lui.

La propriété *pour toute paire de cartes, il existe une image et une seule qui figure sur ces deux cartes* nous fait penser à la propriété fondamentale des droites d'un plan projectif : *Étant données deux droites du plan projectif, il existe un seul point appartenant à ces deux droites.*

Construire un jeu de Dobble. Pour construire un jeu dont chaque carte contient $p + 1$ images, il suffit de numéroter de 1 à $p^2 + p + 1$ les points du plan projectif $P_2(\mathbb{F}_p)$ et de disposer de $p^2 + p + 1$ images numérotées elles aussi de 1 à $p^2 + p + 1$. À chaque droite D de $P_2(\mathbb{F}_p)$ on associe une carte sur laquelle figurent les images dont les numéros sont les numéros des points de D. Pour $p = 7$ on obtient ainsi un jeu de 57 cartes portant chacune 8 images. Curieusement le jeu de Dobble n'a que 55 cartes : deux des droites du plan projectif ont été oubliées. Pour $p = 11$, $p^2 + p + 1 = 133$, on obtient un jeu de 133 cartes de 12 images.

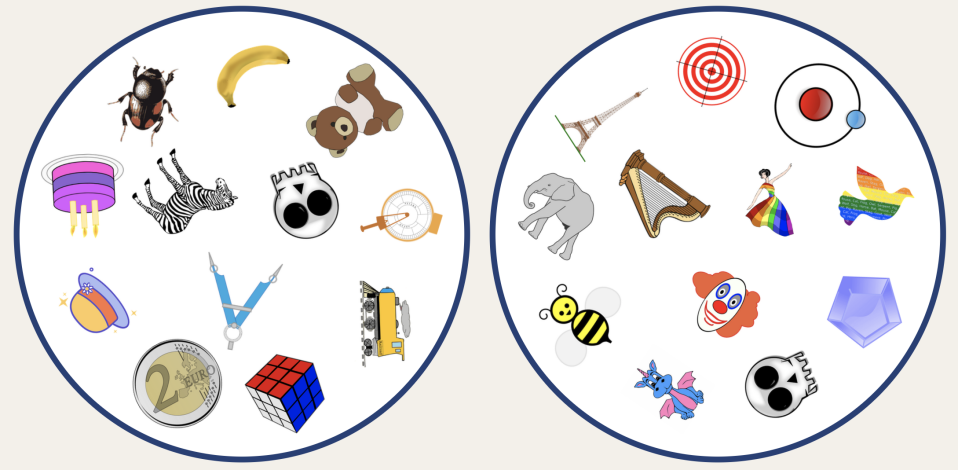


FIGURE 8 – Deux cartes d'un jeu de 133 cartes de 12 images (p = 11) : l'unique image figurant sur ces deux cartes est la tête de mort.