: En effet, chaque point distinct de A contient une unique droite, et chaque droite contient q points distincts de A. Or, on a $N = (q^3-1)/(q-1) = 1+q+q^2$.

Lemme : Soit Q une forme quadratique non dégénérée sur K^3, de forme bilinéaire φ. Soit F un plan de K^3 intersectant le cône $\mathcal{C}$ de Q en une droite Δ. Si F n'est pas l'orthogonal de Δ pour φ, alors $\mathcal{C} \cap F$ est la réunion de deux droites distinctes. Si F est l'orthogonal à Δ, $\mathcal{C} \cap F$ est la droite Δ.

Dem (lemme) : Posons $\Delta = K\overrightarrow{x}$, et $F = \mathrm{Vect}(\overrightarrow{x}, \overrightarrow{y})$. On a $Q(u\overrightarrow{x} + v\overrightarrow{y}) = 2uv\varphi(\overrightarrow{x}, \overrightarrow{y}) + v^2 Q(\overrightarrow{y})$. Comme Q est non dégénérée, on ne peut avoir à la fois $\varphi(\overrightarrow{x}, \overrightarrow{y}) = Q(\overrightarrow{y}) = 0$. En effet, dans ce cas, on aurait $F \subset \mathcal{C}$, ce qui est absurde, car $\dim F^\perp = 1 < \dim F$. Donc $\mathcal{C} \cap F$ est la réunion des droites correspondant à $v = 0$ et à $2u\varphi(\overrightarrow{x}, \overrightarrow{y}) + vQ(\overrightarrow{y}) = 0$. La première droite est Δ. La seconde est distincte de la première ssi $\varphi(\overrightarrow{x}, \overrightarrow{y}) \neq 0$. Or l'orthogonal de $\overrightarrow{x}$ pour φ est un plan contenant x, donc il correspond au seul choix possible de F pour lequel les deux droites sont confondues.

Dem (théorème 2). Considérons $A \in \mathcal{C}$. On choisit A comme le point $[0,1,0]$, et la tangente à $\mathcal{C}$ en A comme la droite de l'infini passant par A (c'est-à-dire la droite passant par A et $B = [1,0,0]$). On a $b = 0$. Comme la tangente en A admet pour équation $ux + wz = 0$, alors $u = 0$. L'équation de la conique s'écrit donc

$$ax^2 + z(vx + wy + cz) = 0$$

Comme $\mathcal{C}$ n'est pas dégénérée, alors a et w sont non nuls (en effet, le déterminant de la matrice associée à la forme quadratique vaut $-\frac{1}{4}aw^2$). Le changement de base $(X = x, Y = (vx+wy+cz)/a,\ Z = z)$, valide puisque le déterminant de la transformation associée est non nul (et égal à ω/a), conduit à l'équation $X^2 + YZ = 0$.

ANNEXES.

Annexe 1 : Quelques cardinaux classiques en algèbre sur les corps finis.

Annexe 2 : Paramétrisation rationnelle d'une conique. Soit K un corps commutatif. On se propose de prouver que toute conique $\mathcal{E}$ du plan $\mathbb{P}_2(K)$ est unicursale, c'est-à-dire admet une paramétrisation rationnelle. A propos des courbes unicursales, on pourra étudier le théorème de Liouville (thème 3) et le théorème de Lurŏth (thème ???).On suppose que la conique est non vide. Le principe est de considérer un point A de la conique, de paramétrer l'ensemble $\mathcal{F}_A$ des droites D_t passant par A par un unique paramètre t, et de déterminer le point d'intersection de $\mathcal{E}$ et de D_t.

Pour bien comprendre la structure de $\mathcal{F}_A$ et la possibilité d'un tel paramétrage, il convient d'utiliser la dualité. Considérons en effet l'application φ qui à tout point de $\mathbb{P}_2(K)$ de coordonnées homogènes $[a,b,c]$ associe la droite projective définie par l'équation homogène $ax + by + cz = 0$. On munit ainsi naturellement l'ensemble $\mathcal{F}$ des droites projectives d'une structure de plan projectif. On vérifie alors aisément que l'image par φ de $\mathcal{F}_A$ est une droite projective de $\mathcal{F}$. En effet, si $A = [x_0, y_0, z_0]$, alors $\mathcal{F}_A$ est la droite composée des points $[a,b,c]$ tels que $ax_0 + by_0 + cz_0 = 0$.

Supposons par exemple que $A = [0,0,1]$, c'est-à-dire que A est l'origine du plan $\mathbb{P}_2(K)$. On peut toujours se ramener à ce cas par un changement de repère projectif. L'ensemble $\varphi(\mathcal{F}_A)$ est la droite composée des points $[a,b,0]$, c'est-à-dire des points $[t,1,0]$, où $t \in K$ et du point $[0,1,0]$ (correspondant à $t = \infty$). Autrement dit, on considère dans le plan K^2 la droite D_t passant par A et de vecteur directeur $\overrightarrow{w} = (t,1)$, et la droite D_∞ de vecteur directeur $\overrightarrow{w} = (1,0)$. La conique $\mathcal{E}$ admet une équation de la forme $ax^2 + bxy + cy^2 + ux + vy = 0$. Les points d'intersection de $\mathcal{E}$ et de D_t sont de la forme $A + \lambda\overrightarrow{w}$. On obtient alors une équation du second degré en λ, dont $\lambda = 0$ est solution. On en conclut que la droite D_t rencontre la conique $\mathcal{E}$ en A et en $M(t) = (\lambda t, \lambda)$, avec $\lambda = -(ut+v)(at^2+bt+c)^{-1}$, c'est-à-dire plus précisement $M(t) = [-(ut+v)\,t, -(ut+v), (at^2+bt+c)]$. On a aussi $M(\infty) = [-u, 0, a]$. Notons au passage que $(a,u) \neq (0,0)$, car la forme quadratique $Q(x,y,z) = ax^2 + bxy + cy^2 + uxz + vyz$ n'est pas dégénérée. On obtient ainsi le paramétrage rationnel de $\mathcal{E}$:

$$M(t) = (x(t), y(t)) \text{ avec } x(t) = \frac{-(ut+v)\,t}{(at^2+bt+c)} \text{ et } y(t) = \frac{-(ut+v)}{(at^2+bt+c)} \text{ pour tout } t \in K \cup \{\infty\}$$

Les paramétrages rationnels des coniques servent en particulier dans le calcul des intégrales abéliennes, c'est-à-dire des intégrales de la forme $\int R(x, \sqrt{ax^2+bx+c}\,dx$, où R est une fraction rationnelle à deux variables. On se ramène au calcul d'une primitive d'une fraction rationnelle en considérant un paramétrage unicursal de la conique d'équation $y^2 = ax^2 + bx + c$. Dans le cas d'une hyperbole, on choisit souvent A comme étant un des deux points à l'infini. Dans ce cas, les droites D_t sont les droites dont la direction est la direction asymptotique correspondante. Par exemple, dans le cas de l'hyperbole d'équation $y^2 = x^2+x+1$, on choisit $D_t : y = x+t$, et on obtient le paramétrage rationnel $M(t) = (x(t), y(t))$ avec $x(t) = (1-t^2)(2t-1)^{-1}$ et $y(t) = x(t) + t$.

11 Loi de réciprocité quadratique

ENONCÉ DES PROPRIÉTÉS.

On rappelle en annexe 1 la définition et la notation du symbole de Legendre.

Loi de réciprocité quadratique : Soient p et q deux nombres premiers *impairs distincts.*

On pose $m = (p-1)/2$ et $n = (q-1)/2$. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{mn}$.

Soit p un nombre premier. Il existe de nombreuses preuves de la loi de réciprocité quadratique (cf annexe 3). Dans le démosntration proposée, l'idée est d'évaluer de deux façons le nombre de solutions dans $(\mathbb{F}_p)^q$ de $x_1^2 + ... + x_q^2 = a$,où $a \in (\mathbb{F}_p)^*$.

Ce nombre est inchangé si on multiplie a par un carré non nul. En effet, les solutions sont alors multipliées par b. Dans $\mathbb{F}_p$, le quotient de deux carrés est un carré, mais il en est de même du quotient de deux éléments non nuls de $\mathbb{F}_p$ qui ne sont pas des carrés (cf remarque en annexe 1). On en déduit que le nombre de solutions de $x_1^2 + ... + x_q^2 = a$, avec a non nul, ne peut prendre (au plus) que deux valeurs, selon que a est un carré ou non. En réalité, il n'est pas nécessaire de calculer explicitement ces deux valeurs, mais seulement leur différence (modulo q).

Prop 1. Notons X et Y respectivement le nombre de solutions dans $(\mathbb{F}_p)^q$ de $x_1^2 + ... + x_q^2 = a$, où a est un carré non nul dans $\mathbb{F}_p$ et de $x_1^2 + ... + x_q^2 = a$, où a n'est pas un carré. Si q est un carré dans $\mathbb{F}_p$, alors $X \equiv 2\ [q]$ et $Y \equiv 0\ [q]$. Si q n'est pas un carré, alors $X \equiv 0\ [q]$ et $Y \equiv 2\ [q]$. Autrement dit, on a $X - Y \equiv 2\left(\frac{q}{p}\right)\ [q]$.

On évalue alors $X - Y$ d'une autre façon, à partir des propriétés des cardinaux des coniques sur un corps fini. En effet, le nombre de solutions de $x^2 + y^2 = a$ ne dépend pas du choix de a non nul dans $\mathbb{F}_p$. On note alors Δ la différence du nombre de solutions entre les cas $a = 0$ et $a \neq 0$. En posant $p = 2m + 1$, on a $\Delta = (-1)^m p$ par le lemme 1 ci-dessous. Le lemme 2 permet (par récurrence sur n) de traiter le cas de l'équation $x_1^2 + ... + x_{2n}^2 = a$. En effet, en l'écrivant sous la forme

$$(x_1^2 + x_2^2) + (x_3^2 + x_4^2) + ... + (x_{2n-1}^2 + x_{2n}^2) = a$$

on montre que la différence entre le cas $a = 0$ et $a \neq 0$ est égale à Δ^n. Pour évaluer $X - Y$, il suffit d'écrire l'équation $x_1^2 + ... + x_q^2 = a$ sous la forme $(x_1^2 + ... + x_{2n}^2) + x_q^2 = a$, et de distinguer deux cas, selon que a est un carré non nul ou n'est pas un carré. La différence provient du fait que si a est un carré non nul, alors il existe des solutions telles que $x_1^2 + ... + x_{2n}^2 = 0$. La prop 2 donne $X - Y = 2(-1)^{mn}p^n$. Comme p^n est congru à $\left(\frac{p}{q}\right)$ modulo q, les prop 1 et 2 permettent de conclure que $2\left(\frac{q}{p}\right)$ et $2(-1)^{mn}\left(\frac{p}{q}\right)$ sont congrus modulo q. Comme les symboles de Legendre appartiennent à $\{-1, 1\}$ et que q est impair, on obtient bien $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{mn}$.

Lemme 1. On pose $p = 2m + 1$. Soit $a \in \mathbb{F}_p$.

Si $a \neq 0$, Le nombre de solutions de l'équation $x^2 + y^2 = a$ dans $(\mathbb{F}_p)^2$ est $\begin{cases} p-1 \text{ si } m \text{ est pair} \\ p+1 \text{ si } m \text{ est impair} \end{cases}$

Le nombre de solutions de l'équation $x^2 + y^2 = 0$ dans $(\mathbb{F}_p)^2$ est $\begin{cases} 2p-1 \text{ si } m \text{ est pair} \\ 1 \text{ si } m \text{ est impair} \end{cases}$

Ainsi, le nombre de solutions dans $(\mathbb{F}_p)^2$ de l'équation $x^2 + y^2 = a$ ne dépend pas de a, sauf pour $a = 0$ où il y a $\Delta = (-1)^m p$ solutions en plus.

Lemme 2. Soit $n \geq 1$. Le nombre N_n de solutions dans $(\mathbb{F}_p)^{2n}$ de l'équation $a = x_1^2 + ... + x_{2n}^2$ ne dépend pas de a, sauf pour $a = 0$, où il y a avec $\Delta_n = (-1)^{mn}p^n$ solutions en plus pour $a = 0$.

Prop 2. On pose $q = 2n + 1$. Avec les notations de la prop 1 et du lemme 1, on a $X - Y = 2(-1)^{mn}p^n$.

Remarque : Les démonstrations des lemmes 1 et 2, et de la prop 2 proposées ici s'adaptent aisément au problème plus général du dénombrement des solutions de l'équation $q(x) = a$, où q est une forme quadratique sur $\mathbb{F}_p$ et $a \in \mathbb{F}_p$ (cf annexe 2).

DÉMONSTRATIONS.

Dem (prop 1) : On considère l'action de $(\mathbb{Z}/q\mathbb{Z}, +)$ sur les q-uplets solutions par :

$$1_{\mathbb{Z}/q\mathbb{Z}} \cdot (x_1, x_2, ..., x_q) \longmapsto (x_q, x_1, ..., x_{q-1})$$

Les seuls points fixes sont les solutions vérifiant $x_1 = x_2 = ... = x_q$. Les autres orbites sont de cardinal q. Si q est un carré dans $(\mathbb{Z}/p\mathbb{Z})^*$, l'équation $qx^2 = 1$ admet deux solutions et $qx^2 = a$ n'en admet aucune. Donc $X \equiv 2\ [q]$ et $Y \equiv 0\ [q]$. Si q n'est pas un carré dans $(\mathbb{Z}/p\mathbb{Z})^*$, l'équation $qx^2 = a$ admet deux solutions et $qx^2 = 1$ n'en admet aucune. Donc $X \equiv 0\ [q]$ et $Y \equiv 2\ [q]$.

Remarque : Le principe de cette démonstration est souvent utilisé. Citons par exemple la preuve du lemme de Cauchy proposée dans [aG] page 27.

Dem (lemme 1). Si m est pair, c'est-à-dire si $p \equiv 1[4]$, alors -1 est un carré dans $\mathbb{F}_p$ Considérons $i \in \mathbb{F}_p$ tel que $i^2 = -1$. L'équation $x^2 + y^2 = a$ s'écrit $(x + iy)(x - iy) = a$. Le couple $(x + iy, x - iy)$ décrit $(\mathbb{F}_p)^2$ lorsque (x, y) décrit $(\mathbb{F}_p)^2$ car 2 est inversible dans $\mathbb{F}_p$. Donc le nombre de solution est égal au nombre de solutions de $xy = a$, c'est-à-dire $p - 1$ si a est non nul, et $2p - 1$ si a est nul.

Si m est impair, c'est-à-dire si $p \equiv 3[4]$, alors -1 n'est pas un carré dans $\mathbb{F}_p$. Donc $x^2 + y^2 = 0$ implique $x = y = 0$. Supposons que a est un carré non nul. Par homogénéïté, le nombre N de solutions ne dépend pas de a carré. Le nombre de solutions $(x, y, z) \in (\mathbb{F}_p)^3$ de $x^2 + y^2 = z^2$ est $1 + N(p - 1)$. Mais l'équation s'écrit $x^2 = (z - y)(z + y)$. Cette équation admet $(2p - 1) + (p - 1)^2$ solutions (x, y, z) (on distingue les cas $x \neq 0$ et $x = 0$). On en déduit $N = p + 1$. Le nombre de solutions M pour a non carré ne dépend pas de a. De plus, $mN + mM + 1 = p^2$, donc $M = p + 1$.

Remarque : La démonstration est immédiate si on suppose connus les résultats sur les coniques projectives non dégénérées sur un corps fini (cf thème 10). On en déduit que, pour tout a non nul, la conique non dégénérée d'équation $x^2 + y^2 = a$ admet $p + 1$ points, en comptant les points à l'infini $[x, y, 0]$ où $x^2 + y^2 = 0$ et $(x, y) \neq (0, 0)$. Il y a donc 2 points à l'infini si -1 est un carré, et aucun sinon. Le cas de la conique dégénérée $x^2 + y^2 = 0$ se traite directement : Si -1 est un carré, la

conqie est réunion de deux droites sécantes en $(0,0)$, donc $2p-1$ solutions. Si -1 n'est pas un carré, la conique admet $(0,0)$ comme unique point.

Dem (lemme 2). Notons $N_n(a)$ le nombre de solutions dans $(\mathbb{F}_p)^{2n}$ de l'équation

$$x_1^2 + ... + x_{2n}^2 = a$$

On raisonne par récurrence sur $n \geq 1$. On suppose par récurrence que $N_n(a)$ ne dépend pas du choix de a, sauf si $a = 0$. Par le lemme 1, la propriété est vraie pour $n = 1$. Pour simplifier, on note N_n ce nombre, et on définit Δ_n comme la différence $N_n(0) - N_n(a)$. Sachant que $x_1^2 + ... + x_{2n+2}^2 = (x_1^2 + ... + x_{2n}^2) + (x_{2n+1}^2 + x_{2n+2}^2)$, on a

$$N_{n+1}(a) = \sum_{b \in \mathbf{F}_p} N_n(a-b)N_1(b)$$

Supposons $a \neq 0$. Parmi les couples $(a-b, b)$, seuls les deux couples $(0,a)$ et $(a,0)$ contiennent un élément nul. Donc N_{n+1} ne dépend pas de a, et $N_{n+1} = (p-2)N_nN_1 + N_n(N_1 + \Delta_1) + (N_n + \Delta_n)N_1$. Si $a = 0$, seul le couple $(0,0)$ admet un élément nul. Donc $N_{n+1} + \Delta_{n+1} = (p-1)N_nN_1 + (N_n + \Delta_n)(N_1 + \Delta_1)$. On en déduit $\Delta_{n+1} = \Delta_n\Delta_1$. On obtient ainsi $\Delta_n = (\Delta_1)^n$.

Dem (prop 2) : On écrit l'équation $x_1^2 + ... + x_q^2 = a$ sous la forme $(x_1^2 + ... + x_{2n}^2) + x_q^2 = a$.
Pour chaque choix de x_q dans $\mathbb{F}_p$, le nombre de solutions $(x_1, ..., x_q)$ est égal à N_n, sauf si $x_q^2 = a$, c'est-à-dire $x_1^2 + ... + x_{2n}^2 = 0$, où il y a un surplus de solutions égal à Δ_n. Si a est un carré non nul, il existe exactement deux valeurs de q pour lesquelles $x_q^2 = a$, et aucune si a n'est pas un carré. Donc $X - Y = 2\Delta_n$.

ANNEXES.

Annexe 1. Symbole de Legendre. Si p est un nombre premier et si $a \in \mathbb{Z}$ est premier avec p, on note $\left(\frac{a}{p}\right)$ le symbole de Legendre. Il vaut 1 si a est un carré dans $\mathbb{F}_p$ et -1 sinon. On a donc $\left(\frac{a}{p}\right) = a^{(p-1)/2}$ dans $\mathbb{F}_p$. On a alors $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ pour tous a et $b \in \mathbb{Z}$. Autrement dit, le symbole de Legendre est un caractère sur $(\mathbb{F}_p)^*$. Comme $(\mathbb{F}_p)^*$ est cyclique, les seuls caractères réels sur $(\mathbb{F}_p)^*$ sont le caractère trivial 1 et le symbole de Legendre.

Remarque : On obtient en particulier que le quotient de deux éléments qui ne sont pas des carrés, est un carré. Une démonstration directe consiste à considérer les ab, où a est fixé et n'est pas un carré, et où b décrit l'ensemble des $\frac{1}{2}(p-1)$ carrés non nuls. Comme ab appartient à l'ensemble des éléments qui ne sont pas des carrés, dont le cardinal est aussi égal à $\frac{1}{2}(p-1)$, alors il le décrit.

On peut prolonger le symbole $x \longmapsto \left(\frac{x}{p}\right)$ en un caractère sur $\mathbb{Z}$, en posant $\left(\frac{a}{p}\right) = 0$ si p divise a. La loi de réciprocité quadratique permet de calculer les symboles de Legendre par réductions successives. En effet, on se ramène aux cas connus de $\left(\frac{a}{p}\right)$ et de $\left(\frac{2}{p}\right) = (-1)^{(n^2-1)/8}$. Par exemple,

$$\left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{7}{29}\right) = -\left(\frac{7}{29}\right) = -\left(\frac{1}{7}\right) = -1$$

Rappel : Pour prouver $\left(\frac{2}{p}\right) = (-1)^{(n^2-1)/8}$, c'est-à-dire $\left(\frac{2}{p}\right)$ ssi $p \equiv \pm 1$ [8], on considère α une racine 8-ième de l'unité dans une extension de corps $\mathbb{K}$ de $\mathbb{Z}/p\mathbb{Z}$. On pose $y = \alpha + \alpha^{-1}$. On a alors $y^2 = 2 + \alpha^2 + \alpha^{-2} = 2$ dans $\mathbb{K}$, car $\alpha^4 = -1$. D'autre part, $y^p = \alpha^p + \alpha^{-p}$. Or, $\left(\frac{2}{p}\right) = 2^{(p-1)/2} = y^{(p-1)}$ dans $\mathbb{K}$. Si $p \equiv \pm 1$ [8], alors $y^p = \alpha + \alpha^{-1} = y$, donc $\left(\frac{2}{p}\right) = 1$. Si $p \equiv \pm 3$ [8], alors $y^p = \alpha^3 + \alpha^{-3} = -(\alpha^{-1} + \alpha) = -y$, donc $\left(\frac{2}{p}\right) = -1$.

Annexe 2. Soit p un nombre premier impair. On se propose de déterminer le nombre $N_n(a, B)$ de solutions de l'équation $b_1x_1^2 + ... + b_nx_n^2 = a$ sur un corps fini $\mathbb{F}_p$ d'inconnue $(x_1, ..., x_n)$, où $a \in \mathbb{F}_p$ et où $B = (b_1, ..., b_n)$ est un n-uplet d'éléments de $\mathbb{F}_p$ tous non nuls.

Remarque : Par la décomposition en carrés des formes quadratiques, valable en caractéristique distincte de 2, toute forme quadratique q sur $\mathbb{F}_p$ peut s'écrire (via un changement de bases) sous la forme $q(\overrightarrow{x}) = b_1x_1^2 + ... + b_nx_n^2$. si q est non dégénérée, les b_k sont tous non nuls, ce que l'on peut toujours supposer (quitte à modifier n). En fait, on peut montrer (cf [aP] chap V §6 th 2) qu'on peut prendre $B = (1, ..., 1., 1)$ ou $(1, ..., 1, \alpha)$, où α n'est pas un carré dans $\mathbb{F}_p$. Autrement dit, il existe deux classes d'équivalence de formes quadratiques non dégénérées sur $(\mathbb{F}_p)^n$. On pourra noter au passage que l'argument essentiel est l'existence d'un couple $(x_1, x_2) \in (\mathbb{F}_p)^2$ tels que $b_1x_1^2 + b_2x_2^2 = 1$.

Le calcul de $N_n(a, B)$ est effectué dans [aT1] page ???. Le cas $n = 1$ est aisé. Le cas fondamental $n = 2$ se déduit des propriétés des coniques projectives comme dans la preuve du lemme 1. La démonstration proposée dans [aT1] consiste à munir la conique d'une structure de groupe (en fait, il s'agit ???). Le point essentiel est que $N_2(a, B)$ ne dépend pas de B, ni de a si celui-ci est non nul. Ensuite, pour $n \geq 3$, on établit comme dans la preuve du lemme 2 une relation de récurrence entre N_n et N_{n-2}.

Annexe 3. Il y a bien d'autres démonstrations de la loi de réciprocité quadratique. On en trouvera deux dans [aSe1], et une dans [bFG1]. La démonstration la plus classique utilise la somme de Gauss, c'est-à-dire

$$\tau = \sum_{x \in \mathbf{F}_p} \left(\frac{x}{p}\right)\omega^x$$

où ω est une racine primitive q-ième de l'unité dans une extension convenable $\mathbb{K}$ de $\mathbb{F}_p$. On note que ω^x a un sens puisque $\omega^q = 1$. On montre par le calcul que $\tau^2 = (-1)^{(p-1)/2}p1_{\mathbb{K}}$ et que $\tau^q = \left(\frac{q}{p}\right)\tau$ dans $\mathbb{K}$. On en déduit que $\left(\frac{q}{p}\right)1_{\mathbb{K}} = \tau^{q-1} = (\tau^2)^{(q-1)/2}$, donc $\left(\frac{q}{p}\right)1_{\mathbb{K}} = (-1)^{(p-1)(q-1)/2}\left(\frac{p}{q}\right)1_{\mathbb{K}}$. D'où le résultat.