



### NOTRE COUVERTURE :

L'Arithmétique, une science difficile. . .

Cela reste vrai aujourd'hui, à voir les difficultés rencontrées pour la vérification des travaux d'Andrew Wiles autour de la conjecture de Fermat. Ces difficultés nous amènent à différer la suite de l'article de Norbert Schappacher.

La profusion des rubriques de l'ancienne arithmétique, suggérée par la couverture (extraite de l'ouvrage de Jean Vial : "Les instituteurs - Douze siècles d'histoire", Paris, éd. Jean-Pierre Delarge, 1980), a été remplacée aujourd'hui par la diversité des nombres étudiés : réels, complexes, hypercomplexes, algébriques, transcendants, idéaux,  $p$ -adiques . . . et la diversité des branches mathématiques impliquées dans l'actuelle théorie des nombres.

## EDITORIAL

Lors d'une conférence à un colloque d'Histoire des Mathématiques, qui se déroulait à Besançon en 1989, Nicolas Rouche (\*) utilisa l'expression "*le mieux serait d'avoir une tête à la fois bien faite et bien pleine*". J'ai eu un certain plaisir à entendre sa formulation car, tout en essayant de former le raisonnement des élèves, j'avais à me battre pour qu'ils apprennent des théorèmes, afin qu'ils en connaissent les conditions d'utilisation en plus de la conclusion, ou qu'ils sachent quelques formules de trigonométrie sans pianoter sur leur calculatrice à mémoires; mais j'attribuais aussi au qualificatif de "*bien pleine*" une certaine culture mathématique. Et voilà que cette formulation me revient à l'esprit alors que je médite sur les modifications de programmes auxquelles nous sommes confrontés au lycée ces temps-ci. Il en vient qui ne tiennent pas compte des réflexions d'un Groupe de Travail Disciplinaire (G.T.D.) et qui ne sont sûrement pas le fruit de mûres réflexions. Les projets pour Terminales scientifiques, tels qu'ils se présentent encore à la fin janvier 94, demandent de traiter – pour des élèves ayant choisi la spécialité mathématique – en deux heures par semaine les parties les plus ardues du programme actuel qu'on traitait en quatre heures pour atteindre le stade de la compréhension, de l'assimilation et de l'outil utilisable par l'élève. Utilisable où ça, me direz-vous : au bac? Oh, c'est déjà une chose d'avoir son bac, et c'est même indispensable pour accéder au post-bac. Mais y a-t-il des élèves de Terminales scientifiques qui choisissent de s'arrêter là? Et pour ceux qui prennent une orientation scientifique il est bon qu'ils aient été initiés aux fonctions (d'une variable pour commencer), aux calculs différentiel et intégral, aux suites, aux probabilités, au calcul vectoriel, à quelques éléments de géométrie et **au raisonnement**. D'aucuns souhaiteraient qu'il y ait un peu d'Algèbre linéaire et de l'Arithmétique (en fait, est-ce que tous les universitaires – en mathématiques – savent qu'il n'y a plus du tout d'arithmétique au Collège et au Lycée?).

Revenons au raisonnement. Il est possible de mettre en place de petits raisonnements en Sixième, mais les programmes parlent tellement de constructions, de tracés, de reproduction de figures, de description et d'observations que la ligne qui suggère "*la mise en place de brèves séquences déductives*" fait pâle figure. Le langage est un peu le même dans le programme de Cinquième. Pourtant il ne faudrait pas installer chez les élèves le défaut de confondre mathématiques et observation. Que de temps perdu ensuite pour gommer ce défaut quand on en vient à étudier des situations où on ne peut plus se fier à l'observation, car ce n'est pas au premier argument que l'élève se laisse convaincre quand il s'est installé dans cette habitude. Et en classe de Seconde la différence se fait nettement sentir entre ceux qui ont été exercés à la démonstration et les autres. Car le raisonnement n'est pas une simple question de bon sens, à moins que le bon sens ne s'apprenne

---

(\*) G.E.M. (Groupe d'Enseignement Mathématique) de Louvain-la-Neuve.

aussi. Et là je pense à un professeur de taupe qui disait, lors d'une réunion, que les élèves arrivaient "*sans savoir mettre en place un raisonnement par récurrence, et pourtant c'est une question de bon sens*". Eh bien non, tant que vous n'avez pas rédigé au moins cinq raisonnements de ce nom avec les élèves, l'espoir qu'une majorité de la classe sache mettre en place le cadre du raisonnement ne vous est pas permis. Tout raisonnement s'apprend. Les raisonnements par l'absurde ou par contraposition aussi. Pour cela il faut du temps, et un contrôle oral autant qu'écrit pour guider la pensée. Mais voilà qu'après avoir conduit certains programmes à la baisse on voudrait que des élèves moins bien préparés que leurs prédécesseurs intègrent plus rapidement qu'eux les notions délicates ou difficiles.

Alors allons-nous réussir à former des têtes bien faites? Et sachant que les choses trop vite vues sont très vite oubliées seront-elles même bien pleines?

O. SCHLADENHAUFEN.

---

#### ATTENTION :

La brochure "Enseigner les probabilités en classe de Première" est provisoirement épuisée (prix 55 F). Sa réédition est prévue vers le mois d'avril 1994.

Au même moment devrait paraître "Enseigner les probabilités en classe de Terminale".

#### A NOTER :

Tél. :	Direction :	88 41 63 09
Tél. :	Secrétariat :	88 41 63 07
Tél. :	Bibliothèque :	88 41 64 40
Fax :		88 41 64 49

## SOMMAIRE

N° 74 – 1994

◇ Notre couverture : <i>L'arithmétique, une science difficile</i> ...	i
◇ Editorial : <i>Avoir la tête à la fois bien faite et bien pleine</i> ...	ii
◇ Quelques résultats sur les courbes planes, par P. GIRAULT ...	1
◇ La factorisation complète du neuvième nombre de Fermat, par J.-P. FRIEDELMEYER ...	13
◇ Sur les coniques à centre tangentes aux trois côtés d'un triangle, par J. DAUTREVAUX ...	21
◇ Géométrie projective, un nouveau livre de J.-C. SIDLER ...	37
◇ Mathématiques dans nos classes ...	39
◇ Problèmes pour nos élèves (... et leurs professeurs) ...	44
◇ A vos stylos, par 'L'Ouvert' ...	48

### L'OUVERT

ISSN 0290 – 0068

- ◇ Responsable de la publication : Odile SCHLADENHAUFEN
- ◇ Rédacteur en chef : Jean-Pierre FRIEDELMEYER
- ◇ Correspondance à adresser à :  
Université Louis Pasteur  
Bibliothèque de l'I.R.E.M.  
10, rue du Général Zimmer  
67084 STRASBOURG CEDEX  
Tél : 88-41-64-40  
Fax : 88-41-64-49
- ◇ Abonnement (pour 4 numéros annuels)  
80 F (130 F/2 ans) pour les membres A.P.M. d'Alsace,  
120 F (200 F/2 ans) dans les autres cas.  
Chèque à l'ordre de Monsieur l'Agent  
Comptable de l'U.L.P. (IREM)
- ◇ Prix du numéro : 30.- F

# QUELQUES RÉSULTATS SUR LES COURBES PLANES

Paul GIRAULT

Strasbourg, U.F.R de Mathématiques et d'Informatique

*En hommage au Professeur Marcel Berger*

L'objet de cet exposé est de promener le lecteur dans le merveilleux jardin des propriétés globales des courbes planes. Pour cela, j'ai choisi parmi les résultats les plus récents ceux qui m'ont paru les plus séduisants, les plus élégants, bref, ceux dont la beauté étonne. C'est pourquoi je ne lésinerai pas sur les nombreuses illustrations nécessaires à l'intelligence de l'exposé. L'apparente simplicité des résultats obtenus a été aussi un mobile puissant de sélection.

Je donnerai quelques démonstrations lorsqu'elles me paraissent originales, me bornant — la plupart du temps — à indiquer les outils modernes utilisés pour atteindre l'alléluia de la solution. Bien sûr — et ceci afin de maintenir le lecteur en haleine — je n'hésiterai pas à replacer ces résultats (quand c'est possible) dans un cadre plus général.

**1. Introduction.** — Le tracé des courbes fermées planes est toujours une activité fascinante à cause de la variété des formes obtenues. Mais comment caractériser la *forme* d'une courbe ?

La théorie *globale* des courbes va nous aider à préciser ce point qui paraît — a priori — fort vague. Pour cela, on part de la connaissance de propriétés locales : une courbe peut avoir des points doubles, des points d'inflexion, des points de rebroussement, des sommets, etc. Dans les bons cas, ces quantités sont en nombre fini, ce qui permet de passer du local au global en montrant qu'on a une relation, alias une formule, entre certaines de ces quantités pour toute courbe fermée. C'est tout le secret de la géométrie moderne ! La suite sera en grande partie une illustration massive de cette démarche.

**2. La formule de Fabricius-Bjerre.** — A cause des allusions qui seront faites ultérieurement, et par souci d'autonomie, nous allons commencer par un bref

rappel des formules de Plücker, qui furent les premiers résultats globaux obtenus sur les courbes algébriques planes.

2.1. *Les formules de Plücker (1834–1836).* — Commençons par rappeler quelques définitions classiques.

a) *Le plan projectif complexe.* — Nous désignerons par  $\mathbb{P}^2(\mathbb{C})$  le plan projectif complexe. Un élément de  $\mathbb{P}^2(\mathbb{C})$  s'appelle un *point* et se représente à l'aide des triplets  $(\lambda x_0, \lambda x_1, \lambda x_2)$  avec  $\lambda \in \mathbb{C} \setminus \{0\}$ . Nous dirons encore que le triplet  $\underline{x} = (x_0, x_1, x_2)$  est un ensemble de *coordonnées* du point  $P$ .

L'application  $(x_1, x_2) \mapsto (1, x_1, x_2)$  définit un plongement canonique de  $\mathbb{C}^2$  dans  $\mathbb{P}^2(\mathbb{C})$ .

Un *automorphisme linéaire* de  $\mathbb{P}^2(\mathbb{C})$  est une application de  $\mathbb{P}^2(\mathbb{C})$  dans lui-même induite par un automorphisme linéaire de  $\mathbb{C}^3$ . Une propriété est *projective* si elle est invariante par tout automorphisme linéaire de  $\mathbb{P}^2(\mathbb{C})$ .

b) *Courbes algébriques*

- Une courbe *algébrique affine*  $\mathcal{C}_0$  est un sous-ensemble de  $\mathbb{C}^2$  de la forme

$$(1) \quad \mathcal{C}_0 = \{x \in \mathbb{C}^2 ; f(x) = 0, f \in \mathbb{C}[x_1, x_2]\}.$$

Le *degré* de  $\mathcal{C}_0$  est le degré de  $f$ .

- Une *courbe algébrique projective* (ou plus simplement une courbe algébrique) est un sous-ensemble de  $\mathbb{P}^2(\mathbb{C})$  de la forme

$$(2) \quad \mathcal{C} = \{\underline{x} \in \mathbb{P}^2(\mathbb{C}) ; F(x) = 0\},$$

où  $F$  est un polynôme *homogène* non constant de  $\mathbb{C}[x_0, x_1, x_2]$ . Le *degré* de la courbe  $\mathcal{C}$  est celui du polynôme  $F$ .

Du plongement canonique de  $\mathbb{C}^2$  dans  $\mathbb{P}^2(\mathbb{C})$ , il résulte qu'il existe une relation entre courbes algébriques affines et courbes algébriques projectives. Plus précisément, soit  $\mathcal{C}_0$  la courbe affine (1) et posons

$$F(\xi) = F(\xi_0, \xi_1, \xi_2) = (\xi_0)^{\deg f} f\left(\frac{\xi_1}{\xi_0}, \frac{\xi_2}{\xi_0}\right).$$

La courbe algébrique  $\mathcal{C}$  définie par l'équation  $F(\xi) = 0$  vérifie

$$(3) \quad \mathcal{C} \cap \mathbb{C}^2 = \mathcal{C}_0.$$

Réciproquement, considérons une courbe projective et posons :

$$f(x_1, x_2) = F(1, x_1, x_2).$$

La courbe affine  $\mathcal{C}_0$  définie par (1) vérifie alors (3).

## COURBES PLANES

Considérons maintenant la courbe algébrique  $\mathcal{C}$ . Nous pouvons décomposer  $F$  en un produit de *facteurs homogènes irréductibles*

$$F = F_1^{m_1} \cdots F_k^{m_k}.$$

Comme cette factorisation est unique à des constantes multiplicatives près, ceci nous autorise à écrire

$$\mathcal{C} = m_1\mathcal{C}_1 + \cdots + m_k\mathcal{C}_k,$$

où les  $\mathcal{C}_i$  sont les courbes algébriques

$$\mathcal{C}_i = \{x \in \mathbb{P}^2(\mathbb{C}) ; F_i(x) = 0.\}$$

Ces courbes sont appelées les *composantes irréductibles* de la courbe algébrique  $\mathcal{C}$  ; l'entier  $m_i$  est la *multiplicité* de  $\mathcal{C}_i$  dans  $\mathcal{C}$ .

On dit que  $\mathcal{C}$  est une courbe *irréductible* lorsque le polynôme  $F$  est irréductible.

*Exemples.* — Soit  $n$  le degré de l'équation  $F$  de  $\mathcal{C}$ .

- Si  $n = 1$ , on dit que  $\mathcal{C}$  est une *droite projective* (ou plus simplement une droite). Une droite est bien évidemment une courbe irréductible.

- Si  $n = 2$ , nous devons distinguer deux sous-cas. Si  $F$  est irréductible, la courbe  $\mathcal{C}$  s'appelle une *conique* (irréductible). Si  $F = F_1F_2$  avec  $\deg F_1 = \deg F_2 = 1$ , la courbe  $\mathcal{C}$  est une droite *comptée deux fois* lorsque  $F_2 = \lambda F_1$  et la *réunion de deux droites concourantes* sinon.

Terminons par deux remarques importantes :

- Le degré d'une courbe est un invariant projectif.
- Soient  $\mathcal{C}$  une courbe de degré  $n$  et  $\mathcal{D}$  une droite qui n'est pas une composante de  $\mathcal{C}$ . Si on convient de compter les points multiples de  $\mathcal{D} \cap \mathcal{C}$  avec leur multiplicité, on a :

$$\text{card}(\mathcal{C} \cap \mathcal{D}) = n,$$

c) *Tangentes et points singuliers*

- Soit  $\mathcal{C}_0$  une courbe affine. Un point  $P = (p_1, p_2)$  de cette courbe est appelé un *point simple* (ou encore un *point ordinaire*) s'il existe un indice  $j$  pour lequel on ait

$$\frac{\partial f}{\partial x_j}(P) \neq 0.$$

En un tel point, la droite affine

$$T_P(\mathcal{C}_0) = \left\{ y \in \mathbb{C}^2 ; (y_1 - p_1) \frac{\partial f}{\partial x_1}(P) + (y_2 - p_2) \frac{\partial f}{\partial x_2}(P) = 0 \right\}$$

s'appelle la *tangente* au point  $P$  à  $\mathcal{C}_0$ . Concrètement, on peut interpréter la tangente en  $P$  comme la position limite des sécantes  $PQ$  lorsque le point  $Q$  tend vers  $P$  tout en restant sur  $\mathcal{C}_0$  (Fig. 1). Les points de  $\mathcal{C}_0$  qui ne sont pas des points simples sont appelés des *points singuliers*. On dit encore que  $\mathcal{C}_0$  est *lisse* (ou encore *non singulière*) lorsque tous ses points sont simples.

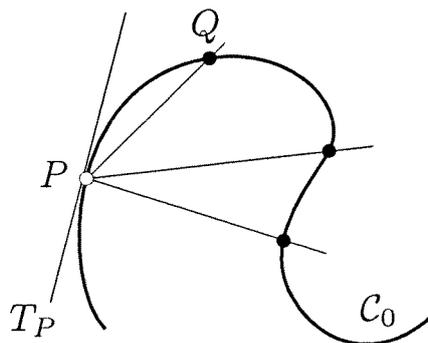


Figure 1

- Considérons maintenant une courbe algébrique  $\mathcal{C}$ . Un point  $P$  de cette courbe est appelé un *point simple* (ou encore un *point ordinaire*) s'il existe un indice  $j$  pour lequel on ait

$$\frac{\partial F}{\partial x_j}(P) \neq 0.$$

En un tel point, la droite projective

$$T_P(\mathcal{C}) = \left\{ \underline{y} \in \mathbb{P}(\mathbb{C}^2) ; y_1 \frac{\partial f}{\partial x_1}(P) + y_2 \frac{\partial f}{\partial x_2}(P) = 0 \right\}$$

s'appelle la *tangente* au point  $P$  à  $\mathcal{C}$ . On peut faire la même remarque que précédemment (Fig. 1).

Les points de  $\mathcal{C}$  qui ne sont pas des points simples sont appelés des *points singuliers*. On dit encore que  $\mathcal{C}$  est *lisse* (ou encore *non singulière*) lorsque tous ses points sont simples.

- Il résulte assez facilement du plongement canonique de  $\mathbb{C}^2$  dans  $\mathbb{P}^2(\mathbb{C})$  que l'on a :

$$T_P(\mathcal{C}_0 \cap \mathbb{C}^2) = T_{(1,P)}(\mathcal{C}) \cap \mathbb{C}^2.$$

Ces généralités étant dites, considérons une courbe algébrique  $\mathcal{C}$  et soit  $P$  un point simple de cette courbe. En vertu du théorème des fonctions implicites, nous voyons que — dans un voisinage du point  $P$  — la courbe  $\mathcal{C}$  est homéomorphe à un

## COURBES PLANES

ouvert de  $\mathbb{C}$ . Il en résulte qu'il faut s'attendre à des complications au voisinage des points singuliers. C'est ce que nous allons examiner avec plus de précision.

Soit  $P$  un point *quelconque* de  $\mathcal{C}$  et choisissons un système de coordonnées de telle sorte que  $P = (1, 0, 0)$ . Posons alors :

$$f(x_1, x_2) = F(1, x_1, x_2).$$

La courbe d'équation  $f(x_1, x_2) = 0$  correspond donc à  $\mathcal{C} \cap \mathbb{C}^2$ . Nous pouvons écrire  $f \in \mathbb{C}[x_1, x_2]$  sous la forme

$$f = f_k + f_{k+1} + \cdots + f_n,$$

où  $f_j$  est un polynôme homogène de degré  $j$  et  $f_k \neq 0$ . Puisque  $f(0, 0) \neq 0$ , nous avons certainement  $k \geq 1$ .

- Si  $k = 1$ , nous pouvons écrire

$$f(x_1, x_2) = ax_1 + bx_2$$

avec  $a \neq 0$  ou  $b \neq 0$ . Comme  $a = \partial f / \partial x_1(P)$  et  $b = \partial f / \partial x_2(P)$ , nous voyons ainsi que  $P$  est un point simple et que la tangente en  $P$  est la droite

$$f_1(x_1, x_2) = ax_1 + bx_2.$$

Il peut arriver que  $f_1$  divise  $f_2, \dots, f_{\ell-1}$  mais pas  $f_\ell$ . Si  $\ell = 3$ , on dit que  $P$  est un *point d'inflexion ordinaire*. Si  $\ell > 3$ , on dit que l'on a un *point d'inflexion d'ordre élevé* (on a par exemple un *point d'ondulation* pour  $\ell = 4$ , ce que Maupertuis appelait très joliment un *point de serpentement* en 1729).

- Si  $k \geq 2$ , on voit facilement que le point  $P$  est un point singulier (condition nécessaire et suffisante). On dit alors que le point  $P$  est un *point multiple* d'ordre  $k$  et que les  $k$  droites  $f_k = 0$  sont les *tangentes* en  $P$  à la courbe. Si ces tangentes sont distinctes, on dit que  $P$  est un *point multiple ordinaire* d'ordre  $k$ .

Si  $k = 2$ , on dit encore que le point  $P$  est un *point double ordinaire* ou un *point de rebroussement* (alias une *pointe*) selon que les deux tangentes sont distinctes ou confondues. Si les tangentes sont confondues, on a donc

$$f(x_1, x_2) = (u_1(x_1, x_2))^2,$$

le polynôme  $u_1$  étant homogène de degré 1. On dit alors que  $P$  est un point de rebroussement de *première espèce* si  $u_1$  ne divise pas  $f_3$ .

Nous n'irons pas plus loin dans l'étude des points singuliers. Nous nous contenterons d'énoncer le résultat suivant.

THEORÈME (MacLaurin, 1720). — Une courbe algébrique irréductible de degré  $n$  possède au plus

$$\frac{1}{2}(n-1)(n-2)$$

points doubles, un point multiple d'ordre  $k$  comptant pour  $\frac{1}{2}k(k-1)$  points doubles.

d) *Le théorème de Bézout.* — Ce résultat, démontré vers 1765, s'énonce comme suit :

THEORÈME. — Soient  $\mathcal{C}$  et  $\mathcal{C}'$  deux courbes algébriques irréductibles, distinctes et de degrés  $n$  et  $n'$ . La somme des multiplicités d'intersection des points communs à ces deux courbes est égale à  $nn'$ .

Nous avons déjà vu un cas particulier de ce théorème lorsque  $\mathcal{C}'$  est une droite. Mais cet énoncé n'est pas une généralisation banale. Examinons en effet la figure 2. Les courbes  $\mathcal{C}$  et  $\mathcal{C}'$  peuvent se couper transversalement comme en  $P$  ; elles peuvent aussi présenter des contacts comme en  $R$  ou — pire encore — se couper en des points singuliers comme  $S$  et  $Q$  ! Si nous nous rappelons la petite incursion faite dans le zoo des singularités, nous voyons que nous sommes loin d'avoir épuisé les situations les plus affreuses. C'est pourquoi on associe à chaque point de  $\mathcal{C} \cap \mathcal{C}'$  une « multiplicité » de manière à se débarrasser des cas d'espèces afin d'obtenir exactement l'égalité du théorème.

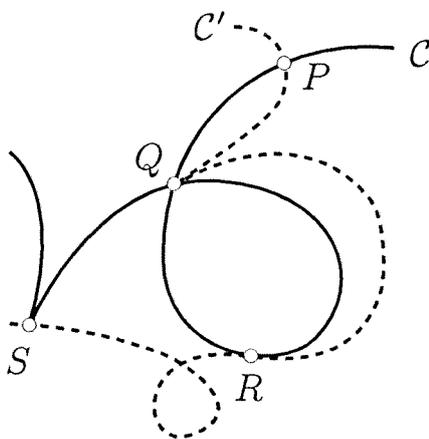


Figure 2

Nous invoquerons plusieurs fois le théorème de Bézout par la suite. Nous ne donnerons cependant pas la définition exacte de la multiplicité de l'intersection pour la bonne raison que cela nous entraînerait beaucoup trop loin.

e) *Polaires et duale d'une courbe.* — Soient  $\mathcal{C}$  une courbe algébrique de degré  $n$  et  $P$  un point de coordonnées  $(y_0, y_1, y_2)$  n'appartenant pas à cette courbe.

La courbe  $\mathcal{P}$  définie par

$$\mathcal{P} = \left\{ (\underline{x} \in \mathbb{P}^2(\mathbb{C}) ; y_0 \frac{\partial F}{\partial x_0} + y_1 \frac{\partial F}{\partial x_1} + y_2 \frac{\partial F}{\partial x_2} = 0 \right\}$$

s'appelle la *polaire* de  $P$  relativement à  $\mathcal{C}$ . Cette courbe est de degré  $(n - 1)$  si  $\mathcal{C}$  est de degré  $n$ .

Observons que la polaire passe par les points singuliers de la courbe. . .

*Exercice.* — Quelle est la polaire d'un point relativement à une droite, à une conique ?

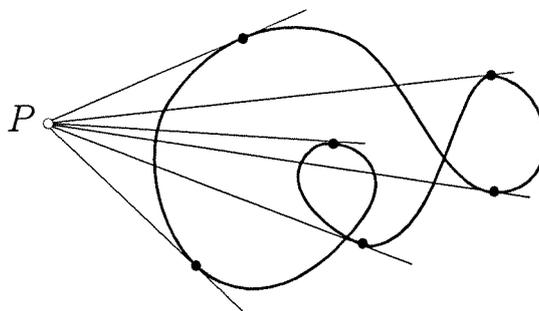


Figure 3

Selon Gergonne (vers 1827), désignons par  $\nu$  la *classe* de  $\mathcal{C}$ , c'est-à-dire le nombre de tangentes à  $\mathcal{C}$  que l'on peut mener d'un point non situé sur la courbe (Fig. 3). Les points de contacts avec  $\mathcal{C}$  des tangentes issues de  $P$  sont donc les solutions du système

$$\begin{cases} F(x_0, x_1, x_2) = 0, \\ y_0 \partial F / \partial x_0 + y_1 \partial F / \partial x_1 + y_2 \partial F / \partial x_2 = 0. \end{cases}$$

On se convainc ainsi que la classe ne dépend pas du point  $P$  choisi ; c'est donc une quantité parfaitement définie qui est manifestement un invariant projectif. Si  $\mathcal{C}$  est une courbe non singulière, le théorème de Bézout montre que nous avons

$$\nu = n(n - 1).$$

Il ne nous reste plus qu'à introduire la compagne favorite d'une courbe algébrique, à savoir sa *duale*. Pour cela, commençons par interpréter l'ensemble des droites de  $\mathbb{P}^2(\mathbb{C})$  comme un autre plan projectif  $(\mathbb{P}^2(\mathbb{C}))^*$  en considérant le triplet  $(a_0, a_1, a_2)$  comme un ensemble de coordonnées de la droite  $a_0 x_0 + a_1 x_1 + a_2 x_2 = 0$ . Soient maintenant  $\mathcal{C}$  une courbe algébrique et  $P$  un point

simple de cette courbe et  $T_P$  la tangente à  $\mathcal{C}$  en  $P$ . Désignons enfin par  $\text{sing}(\mathcal{C})$  l'ensemble des points singuliers de  $\mathcal{C}$ . L'application

$$\psi : P \longmapsto T_P$$

définit une application de  $\mathcal{C} \setminus \text{sing}(\mathcal{C})$  dans  $(\mathbb{P}^2(\mathbb{C}))^*$ . La *duale*  $\mathcal{C}^*$  de  $\mathcal{C}$  est par définition la courbe algébrique

$$\mathcal{C}^* = \overline{\psi(\mathcal{C} \setminus \text{sing}(\mathcal{C}))}.$$

Il est remarquable que l'on retrouve la courbe de départ en dualisant sa duale, i.e.

$$\mathcal{C}^{**} = \mathcal{C}.$$

La détermination explicite de la duale d'une courbe est une activité périlleuse car il s'agit d'éliminer  $x_0, x_1, x_2$  et  $\lambda$  dans le système

$$\begin{cases} F(x_0, x_1, x_2) = 0, \\ \lambda \xi_i = \partial F / \partial x_i, \quad i = 0, 1, 2. \end{cases}$$

(Ce système montre en passant que la duale d'une courbe algébrique est encore une courbe algébrique.) S'il est facile de prouver que la duale d'une conique est une conique, il est déjà beaucoup plus difficile de déterminer la duale d'une courbe d'ordre 3. Le lecteur intéressé pourra s'exercer avec la courbe  $x_0^3 + x_1^3 + x_2^3 = 0$ . . .

Il serait pourtant plaisant de déterminer l'ordre  $n^*$  de la duale  $\mathcal{C}^*$  d'une courbe  $\mathcal{C}$  d'ordre  $n$ . Heureusement, l'équation de  $\mathcal{C}^*$  est inutile. En effet, nous avons vu qu'il suffit de compter le nombre d'intersections d'une droite générique avec  $\mathcal{C}^*$ . Par dualité, on s'aperçoit qu'il s'agit tout bonnement du nombre de tangentes que l'on peut mener à  $\mathcal{C}$  d'un point générique du plan, ce qui nous donne

$$n^* = \nu.$$

Si  $\mathcal{C}$  n'est pas singulière, nous avons donc

$$n^* = \nu = n(n-1).$$

Mais nous avons encore  $n = n^*(n^* - 1)$  par dualité puisque  $\mathcal{C}^{**} = \mathcal{C}$ . Lorsque  $n > 2$ , on aboutit à un joli enchevêtrement ! C'est en levant cette *aporie* que Plücker obtint ses formules célèbres.

*Question.* — Pourquoi le raisonnement précédent est-il incorrect ?

f) *Les formules de Plücker.* — Nous dirons qu'une courbe  $\mathcal{C}$  n'a que des *singularités traditionnelles* si chaque point  $P$  de  $\mathcal{C}$  satisfait l'une des assertions suivantes :

COURBES PLANES

- $P$  est un point simple.
- $P$  est un point d'inflexion ordinaire.

*Remarque.* — On peut montrer que sous cette hypothèse, le point  $P$  appartient aussi à la Hessienne  $\mathcal{H}$  de  $\mathcal{C}$ , c'est-à-dire la courbe

$$\mathcal{H} = \left\{ \underline{x} \in \mathbb{P}^2(\mathbb{C}) ; \det \left( \frac{\partial F}{\partial x_i \partial x_j} \right) = 0 \right\}.$$

- $P$  est un point de rebroussement de première espèce.
- $P$  est un point double ordinaire.
- On a une bitangente en  $P$ , ce qui signifie que la tangente en  $P$  (que l'on suppose ne pas être un point d'inflexion) est tangente en  $\mathcal{C}$  à un autre point  $Q \neq P$ .

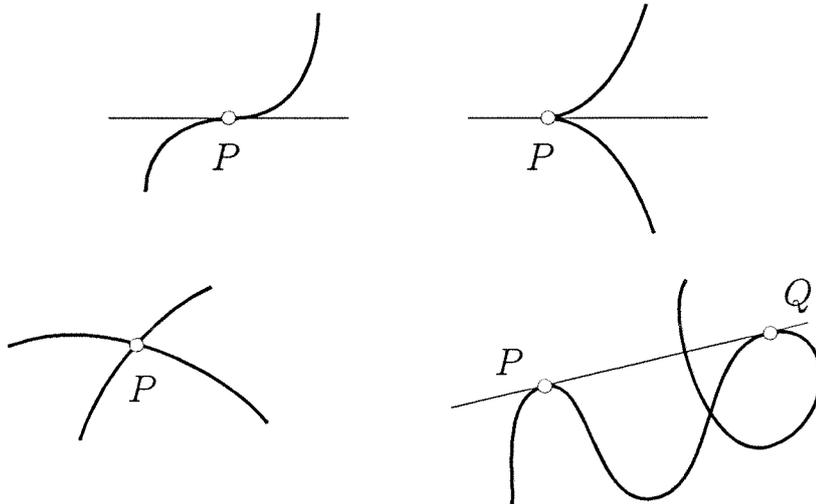


Figure 4

La figure 4 illustre les différentes situations.

Lorsque la courbe  $\mathcal{C}$  n'a que des singularités traditionnelles, désignons par :

- $n$  l'ordre de  $\mathcal{C}$ ;
- $\nu$  la classe de  $\mathcal{C}$ ;
- $d$  le nombre de points doubles de  $\mathcal{C}$ ;
- $\delta$  le nombre de bitangentes de  $\mathcal{C}$ ;
- $r$  le nombre de points de rebroussement de  $\mathcal{C}$ ;
- $\rho$  le nombre de points d'inflexion de  $\mathcal{C}$ .

Les formules de Plücker sont alors les suivantes :

$$\begin{aligned}
 (P_1) \quad & \nu = n(n-1) - 2d - 3r, \\
 (P_2) \quad & n = \nu(\nu-1) - 2\delta - 3\rho, \\
 (P_3) \quad & \rho = 3n(n-2) - 6d - 8r, \\
 (P_4) \quad & r = 3\nu(\nu-2) - 6\delta - 8\rho, \\
 (P_5) \quad & \delta = \frac{1}{2}n(n-2)(n^2-9) - (n^2-n-6)(2d+3r) \\
 & \quad \quad \quad + 2d(d-1) + 6dr + \frac{9}{2}r(r-1), \\
 (P_6) \quad & d = \frac{1}{2}\nu(\nu-2)(\nu^2-9) - (\nu^2-\nu-6)(2\delta+3\rho) \\
 & \quad \quad \quad + 2\delta(\delta-1) + 6\delta\rho + \frac{9}{2}\rho(\rho-1).
 \end{aligned}$$

*Exemples*

- Si la courbe  $\mathcal{C}$  est de degré 4 et non singulière, nous avons :

$$n = 4, \quad \nu = 12, \quad \rho = 24, \quad \delta = 28, \quad d = r = 0.$$

- Si la courbe  $\mathcal{C}$  est l'astroïde complexe  $x_1^{2/3} + x_2^{2/3} + \lambda^{2/3}x_0^{2/3}$ , nous avons :

$$n = 6, \quad \nu = 4, \quad \rho = 0, \quad \delta = 3, \quad d = 4, \quad r = 6.$$

Évidemment, énoncées sans démonstration, ces formules ne sont pas très parlantes. Une preuve élémentaire consiste à étudier l'effet des singularités sur la première polaire et la Hessienne. On obtient alors les formules  $(P_1)$  et  $(P_3)$  à l'aide du théorème de Bézout, puis  $(P_2)$  et  $(P_4)$  par dualité. Les formules  $(P_5)$  et  $(P_6)$  sont plus difficiles à obtenir. Indiquons une démarche heuristique afin de bien faire comprendre comment la présence de singularités modifie les formules.

Remarquons tout d'abord que si  $\mathcal{C}$  est non singulière, en patouillant un peu, on peut déduire des formules  $(P_1)$ ,  $(P_2)$  et  $(P_3)$  l'égalité  $2\delta = n(n-2)(n^2-9)$ . Maintenant, si  $\mathcal{C}$  n'a que des singularités traditionnelles, ce nombre diminue compte tenu des remarques suivantes :

- de tout point double, on peut mener  $(\nu-4)$  tangentes à la courbe et chacune de ces tangentes compte pour 2 bitangentes ;
- de tout point de rebroussement, on peut mener  $(\nu-3)$  tangentes et chacune d'elles compte pour 3 bitangentes ;
- toute droite qui joint deux points doubles compte pour 4 bitangentes ;
- toute droite qui joint un point double et un point de rebroussement compte pour 6 bitangentes ;
- toute droite qui joint deux points de rebroussement compte pour 9 bitangentes.

Cela donne  $2\delta = n(n-2)(n^2-9) - 4d(\nu-4) - 6r(\nu-3) - 4d(d-1) - 12dr - 9r(r-1)$ . La formule  $(P_5)$  s'en déduit par un petit calcul et  $(P_6)$  par dualité. Avec un peu d'imagination, la figure 5 justifie ce qui vient d'être dit !

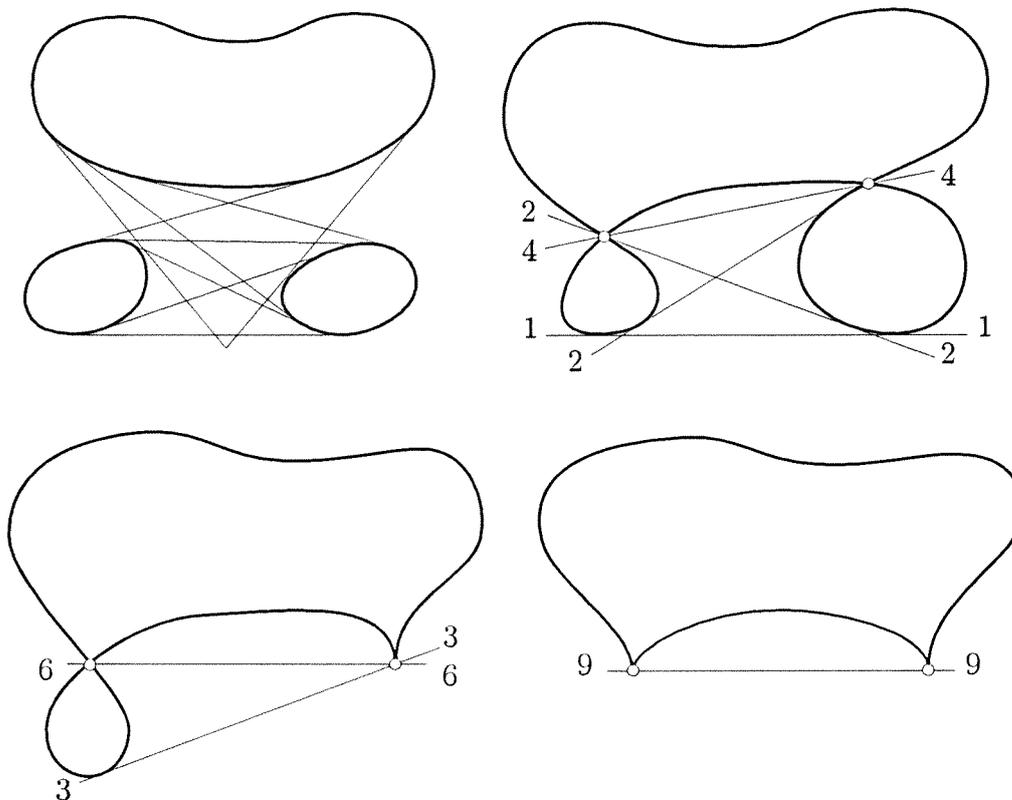


Figure 5

On pourrait bien sûr trouver la formule  $(P_5)$  en calculant  $(8n - 3r)$  et en utilisant la formule  $(P_1)$ , mais une telle démonstration — irréprochable quant à la rigueur — ne nous apprend rien géométriquement !

En combinant ces relations, nous pouvons en obtenir bien d'autres :

$$(P_7) \quad r - \rho = 3(n - \nu)$$

$$(P_8) \quad 2(\delta - d) = (\nu - n)(\nu + n - 9)$$

$$(P_9) \quad \frac{1}{2}n(n + 3) - d - 2r = \frac{1}{2}\nu(\nu + 3) - \delta - 2\rho,$$

$$(P_{10}) \quad \frac{1}{2}(n - 1)(n - 2) - d - r = \frac{1}{2}(\nu - 1)(\nu - 2) - \delta - \rho.$$

Arrêtons-nous un instant sur la dernière formule et posons :

$$g(\mathcal{C}) = \frac{1}{2}(n - 1)(n - 2) - d - r.$$

L'entier  $g(\mathcal{C})$  s'appelle le *genre* de la courbe  $\mathcal{C}$  (nom introduit par Clebsch en 1864). La formule  $(P_{10})$  montre alors qu'une courbe et sa duale ont même genre.

Dans son mémoire de 1857 — riche en idées nouvelles — Riemann a montré que le genre est un invariant *birationnel*, inaugurant ainsi l'étude de la *géométrie birationnelle* qui a dominé presque toute la géométrie algébrique par la suite.

La formule ( $P_{10}$ ) établit donc une relation entre l'invariant « intrinsèque »  $g$  et les quantités « extrinsèques »  $n, d, r$  et  $\nu, \delta, \rho$ .

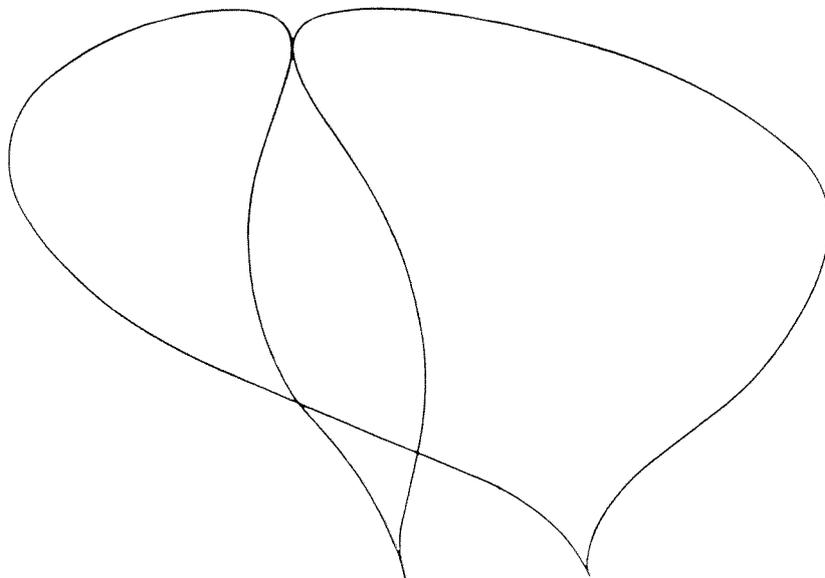
Notons encore que des formules « à la Plücker » ont été obtenues pour les courbes et les surfaces de  $\mathbb{P}^3(\mathbb{C})$  par Cayley, Salmon et bien d'autres auteurs du milieu du siècle dernier. Admirons au passage le *flair* de ces mathématiciens en nous rappelant l'état de l'étude des singularités des surfaces à cette époque. Salmon, pour ne citer que lui, avait annoncé dès 1854 — après quelques considérations heuristiques — que le nombre  $t$  des plans tritangents à une surface est donné par la formule

$$6t = n(n-2)(n^7 - 4n^6 + 7n^5 - 45n^4 + 114n^3 - 111n^2 + 548n - 960).$$

Les surfaces de degré 4 ont donc 3 200 plans tritangents, celles de degré 5 en ont 56 575 et celles de degré 6 en ont 449 520 ! Il revint à Ronga en 1984 de donner la démonstration de cette formule, ainsi que son domaine de validité.

Nous avons donc atteint notre but, qui était d'exposer succinctement les formules de Plücker. Cette première incursion dans l'univers de la géométrie algébrique ne donne qu'une très faible idée de l'immense domaine qu'elle recouvre ainsi que la diversité et le renouvellement des idées qu'elle met en œuvre.

à suivre ...



$$216 x = (36 \pm y \sqrt{3y}) (3 \pm \sqrt{48 - 2y})^2$$

**ACTUALITÉ MATHÉMATIQUE :**  
**LA FACTORISATION COMPLÈTE**  
**DU NEUVIÈME NOMBRE DE FERMAT**

Jean-Pierre FRIEDELMEYER

La récente médiatisation qu'a connue la démonstration par A. Wiles du dernier théorème de Fermat (1) est plutôt rare pour un résultat mathématique. Cette démonstration, si elle s'avère définitivement correcte, ne clôt pourtant pas les travaux suscités par ce grand mathématicien, dont certains continuent à stimuler diverses activités de recherche certes moins éclatantes mais parfois plus utiles. Parmi celles-ci, certaines ont des retombées directement utilisables dans des domaines non mathématiques, par exemple pour les problèmes de cryptographie, c'est-à-dire de messages codés. Les milieux financiers, politiques ou militaires ont besoin de codes secrets qui résistent à la puissance de calcul des ordinateurs actuels. Or une nouvelle méthode dite à "clef publique" a été inventée en 1975 par un groupe de trois personnes : Rivest, Shamir et Adleman qui satisfait parfaitement à cette exigence (2). Cette performance tient au fait que l'on connaît aujourd'hui de très grands nombres premiers, mais qu'il est pratiquement impossible (c'est-à-dire dans un délai raisonnable) de trouver les facteurs premiers  $p$  et  $q$  d'un nombre  $N = p \times q$  lorsque  $N$  est très grand (plus d'une centaine de chiffres décimaux). Une excellente illustration de cette difficulté nous est fournie par la toute récente décomposition en facteurs premiers du nombre dit de Fermat  $F_9 = 2^{2^9} + 1$ , qui a 155 chiffres décimaux.

### 1. Les nombres de Fermat

Les nombres de Fermat sont les nombres de la forme  $F_n = 2^{2^n} + 1$  où  $n$  est un entier naturel. Fermat les croyait tous premiers :

*"Je suis quasi persuadé que tous les nombres progressifs augmentés de l'unité, desquels les exposants sont des nombres de la progression double, sont des nombres premiers comme 3, 5, 17, 257, 65537, 4294967297 et le suivant de 20 lettres 18446744073709551617; etc..."*

*Je n'en ai pas la démonstration exacte, mais j'ai exclu si grande quantité de diviseurs par démonstrations infaillibles, et j'ai de si grandes lumières qui établissent ma pensée, que j'aurais peine à me dédire" (3).*

---

(1) Voir l'article de N. Schappacher dans 'L'Ouvert' n° 73 : "Les 350 ans du grand théorème de Fermat".

(2) Voir l'article de M. Mignotte dans 'L'Ouvert' n° 18 : "Transmission des messages secrets grâce à l'arithmétique".

(3) Lettre de Fermat à Frénicle (août 1640) dans P. Fermat, Oeuvres X LIII, p. 205-206.

effectivement  $F_n$  est premier pour  $n \leq 4$  mais en 1732 Euler a démontré que  $F_5$  est composé :

$$F_5 = 4.294967297 = 641 \times 6700417.$$

En 1801 Gauss a mis en évidence l'intérêt des nombres de Fermat en géométrie : un polygone régulier de  $N$  côtés peut être construit à la règle et au compas si et seulement si  $N$  est une puissance de 2 ou le produit d'une puissance de 2 et de nombres de Fermat premiers distincts. Il en est ainsi pour  $N = 17 = F_2$  ou  $N = 340 = 2^2 \times 5 \times 17 = 2^2 \times F_1 \times F_2$ , mais pas pour  $N = 7$  ou  $N = 13$ .

Comme le montre l'écriture décimale de  $F_5$  ou  $F_6$  ci-dessus, les nombres de Fermat deviennent vite très grands. Comment savoir s'ils sont premiers ou non ?

## 2. Les connaissances actuelles sur les facteurs premiers composant $F_n$ .

Il faut attendre 1877 pour obtenir deux résultats importants concernant les diviseurs éventuels de  $F_n$ . Le premier est publié par E. Lucas qui démontre que pour  $n > 1$ , tout diviseur de  $F_n$  est de la forme  $2^{n+2} \times k + 1$  ( $k \in \mathbb{N}$ ). Ainsi pour  $n = 5$ ,  $641 = 2^7 \times 5 + 1$  divise  $F_5$ , de même que l'autre facteur  $6700417 = 2^7 \times 52347 + 1$ . Ce sont probablement des diviseurs de ce type qu'Euler a essayé, puisque dans une publication datée en 1747 nous trouvons énoncé le résultat suivant :

*“Tout diviseur de  $F_n$  est de la forme  $2^{n+1} \times k + 1$ ”*

Le second résultat est un test remarquable, le test de Pépin, qui permet de savoir si  $F_n$  est premier ou composé :

*“ $F_n$  est premier si et seulement si il divise  $3^{\frac{F_n-1}{2}} + 1$ ”*

Ce test demande néanmoins du temps pour être appliqué, car déjà  $F_n$  est grand, combien plus grand encore est  $3^{\frac{F_n-1}{2}} + 1$  ! Par exemple  $F_{1945}$  est un nombre si grand qu'il faut plus de 580 chiffres pour écrire le nombre de ses chiffres. Et pourtant le test de Pépin lui fut appliqué avec succès, et en 1957, R.-M. Robinson découvrit que  $5 \times 2^{1947} + 1$  divise  $F_{1945}$ . Aujourd'hui, le plus grand nombre de Fermat connu comme composé est  $F_{23471}$ . En 1984, Keller en avait trouvé un diviseur premier, le nombre  $5 \times 2^{23473} + 1$ . L'on conjecture qu'il n'existe pas de nombre de Fermat premier au-delà de l'indice  $n = 4$ .

Mais savoir que  $F_n$  est composé ne signifie pas pour autant qu'on connaisse des diviseurs, encore moins **tous ses diviseurs premiers**. Ainsi nous ne connaissons l'ensemble des diviseurs de  $F_7$  que depuis 1970 (Morrison et Brillhart). Pour  $F_9$ , Western avait déterminé en 1903 le diviseur  $37 \times 2^{16} + 1 = 2424833$ , mais on ne savait rien du quotient. Il faudra attendre 1967 pour que Brillhart démontre que ce quotient était lui-même composé, ce que l'on peut considérer comme un exploit, compte tenu du fait que  $F_9/2424833$  s'écrit avec 148 chiffres.

Voici l'état actuel des connaissances sur cette question :

- la décomposition complète de  $F_n$  en facteurs premiers est connue pour  $n \leq 9$  et  $n = 11$ ;
- un ou plusieurs facteurs de  $F_n$  sont connus pour les entiers  $n$  inférieurs ou égaux

à 32 sauf 14, 20, 22, 24, 28, 31 ainsi que pour 76 valeurs plus grandes de  $n$ , la plus grande, comme nous l'avons signalé plus haut étant  $n = 23471$ ;

- pour  $n = 10, 12, 13, 15, 16, 17, 18$  on sait que le cofacteur est composé;
- aucun facteur de  $F_{14}$  et  $F_{20}$  n'est connu, mais on sait que ces nombres sont composés;
- pour  $n = 22, 24, 28, 31$  et les valeurs supérieures à 32 exceptées les 76 évoquées plus haut, on ne sait pas si  $F_n$  est premier ou composé.

Le plus petit nombre de Fermat non encore complètement décomposé est  $F_{10}$ . Deux de ses facteurs premiers sont connus :  $11131 \times 2^{12} + 1 = 45592577$  et  $395937 \times 2^{14} + 1 = 6487031809$ .

La décomposition de  $F_9$  est récente. Elle a été réalisée en 1990 par une équipe américaine du Mathematical Science Research Institute de Berkeley.  $F_9$  a 155 chiffres :

$$\begin{aligned}
 F_9 = & 134\ 078\ 079\ 299\ 425\ 970\ 995\ 740\ 249\ 982\ 058\ 461\ 274 \\
 & 793\ 658\ 205\ 923\ 933\ 777\ 235\ 614\ 437\ 217\ 640\ 300\ 735 \\
 & 469\ 768\ 018\ 742\ 981\ 669\ 034\ 276\ 900\ 318\ 581\ 864\ 860 \\
 & 508\ 537\ 538\ 828\ 119\ 465\ 699\ 464\ 336\ 490\ 060\ 840\ 97.
 \end{aligned}$$

Il est le produit de trois nombres premiers, ayant respectivement 7, 49 et 99 chiffres :

$$\begin{aligned}
 P_7 = & 242\ 483\ 3 \text{ déjà connu} \\
 P_{49} = & 745\ 560\ 282\ 564\ 788\ 420\ 833\ 739\ 573\ 620\ 045\ 491\ 878\ 336\ 634\ 265\ 7 \\
 P_{99} = & 741\ 640\ 062\ 627\ 530\ 801\ 524\ 787\ 141\ 901\ 937\ 474\ 059\ 940\ 781\ 097\ 519 \\
 & 023\ 905\ 821\ 316\ 144\ 415\ 759\ 504\ 705\ 008\ 092\ 818\ 711\ 693\ 940\ 737.
 \end{aligned}$$

Il ne nous est pas possible, dans le cadre de cet article, de rendre compte en détail des techniques utilisées pour cette décomposition (4). Celle-ci a mis à contribution environ 700 centres de calcul dispersés à travers le monde entier et dans l'une des dernières étapes un super ordinateur. La factorisation complète a duré quatre mois. Nous voudrions seulement montrer ici combien la mise en œuvre de cette décomposition a eu recours à toutes les ressources de l'algèbre moderne : algèbre linéaire, corps finis, anneaux d'entiers algébriques. En voici quelques aperçus.

### 3. Le sous groupe des racines carrées de l'unité, dans $\mathbb{Z}/n\mathbb{Z}$

Dans la suite,  $n$  est un entier impair supérieur à 1. Ce sera en fait l'entier que nous souhaitons décomposer en facteurs premiers. Selon les notations habituelles  $\mathbb{Z}$  désigne l'anneau des entiers relatifs,  $\mathbb{Z}/n\mathbb{Z}$  l'anneau des entiers modulo  $n$ , et  $(\mathbb{Z}/n\mathbb{Z})^*$  le groupe des éléments inversibles de  $\mathbb{Z}/n\mathbb{Z}$ . Alors l'ensemble

$$E = \{x \in \mathbb{Z}/n\mathbb{Z}; x^2 = 1\}$$

---

(4) Celles-ci sont développées dans un article paru dans la revue "Mathematics of computation" vol. 61, n° 203, July 1993, pp. 319-349 : "The factorization of the ninth Fermat number" A.K. Lenstra, H.-W. Lenstra, J.-R. M.-S. Manasse and J.-M. Pollard.

est un sous-groupe de  $(\mathbb{Z}/n\mathbb{Z})^*$  et peut être considéré comme un espace vectoriel sur le corps fini à deux éléments  $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ , l'addition vectorielle étant définie par la multiplication. Par exemple, pour  $n = 3 \times 5 \times 7 = 105$ , l'ensemble  $E$  est constitué des éléments :  $E = \{1, 29, 34, 41, 64, 71, 76, 104\}$  dont une base est définie par  $e_1 = 29; e_2 = 34; e_3 = 64$  engendrant  $41 = e_1 + e_2 \equiv 29 \times 34; 104 = e_1 + e_2 + e_3 \equiv 29 \times 34 \times 64$  (modulo 105) etc...

Cette base de  $E$  contient trois éléments parce que 105 comprend trois facteurs premiers distincts : 3, 5 et 7. Ce fait est général et se trouve à l'origine de nombre d'algorithmes de décomposition des entiers en facteurs premiers : la dimension de l'espace vectoriel  $E$  sur  $\mathbb{F}_2$  est égale au nombre de facteurs premiers distincts de  $n$ .

Si  $n$  n'est pas une puissance de nombre premier, on montre qu'il existe alors un élément  $x$  de  $\mathbb{Z}/n\mathbb{Z}; x \neq \pm 1$ , tel que  $x^2 = 1$ . De plus, la connaissance explicite d'un tel élément  $x$ , disons  $x \equiv y \pmod{n}$  conduit à une factorisation non triviale de  $n$ . En effet :  $y^2 \equiv 1; y \not\equiv \pm 1 \pmod{n}$  entraîne que  $n$  divise le produit  $(y-1)(y+1)$  sans diviser aucun des facteurs  $(y-1)$  ou  $(y+1)$ , de sorte que les pgcd de  $(y-1, n)$  et  $(y+1, n)$  sont des diviseurs non triviaux de  $n$ . En fait, il y a des facteurs complémentaires, de sorte qu'un seul des deux pgcd suffit, qu'on peut déterminer par l'algorithme d'Euclide. Nous pouvons donc conclure que pour factoriser  $n$ , il suffit de trouver un  $x$  de  $\mathbb{Z}/n\mathbb{Z}$  vérifiant  $x^2 = 1$  sans que  $x = 1$  ou  $x = -1$ .

Cette méthode, cependant, est en défaut si  $n$  est une puissance de nombre premier. Il faudrait donc s'assurer d'abord que l'entier  $n$  que l'on veut décomposer ne rentre pas dans cette catégorie. On peut d'abord soumettre  $n$  à un test de primalité. Si  $n$  est premier, la factorisation est terminée. S'il ne l'est pas, la vérification qu'il n'est pas une puissance de nombre premier reste à faire. Des test existent là aussi, mais cette vérification est souvent omise, car il est hautement improbable que  $n$  soit une puissance de nombre premier lorsqu'il n'est pas premier. Les auteurs de la décomposition de  $F_9$  avouent avoir tout simplement oublié de penser à cette vérification :

*“Si (le nombre  $F_9/2424833$ ) avait été une puissance de nombre premier, notre méthode aurait échoué complètement, et nous aurions été extrêmement embarrassés envers les nombreuses personnes qui nous ont aidé dans ce projet. On peut penser que le risque que nous avons pris inconsciemment était extrêmement faible, mais jusqu'à ce que le nombre ait été factorisé, ce n'était là rien de plus qu'une conviction.”*

Voici, en trois étapes, le schéma général utilisé par l'équipe américaine pour la décomposition de  $n = F_9/2424833$  qui, rappelons le, est un nombre d'environ 150 chiffres.

#### 4. Schéma général de recherche d'un système de générateurs du $\mathbb{F}_2$ espace vectoriel $E$ .

La recherche d'un élément  $x$  de  $\mathbb{Z}/n\mathbb{Z}$  vérifiant  $x^2 = 1$  et  $x \neq \pm 1$  qui permette d'aboutir à un facteur non trivial de  $n$ , peut se faire par la détermination d'un système de générateurs de l'espace vectoriel  $E$  sur  $\mathbb{F}_2$ . Comment obtenir un tel

système?

### Première étape : sélection d'une base de facteurs

Il s'agit de choisir un ensemble d'éléments  $a_p$  de  $\mathbb{Z}/n\mathbb{Z}$  où  $p$  parcourt un ensemble fini  $P$  d'indices. Le choix de cet ensemble est fait de façon à rendre efficace la prochaine étape décrite ci-dessous. L'ensemble des  $(a_p)_{p \in P}$  est appelé **base de facteurs**. Nous supposons que tous les  $(a_p)$  appartiennent à  $(\mathbb{Z}/n\mathbb{Z})^*$  ce qui en pratique est vraisemblable, puisque  $n$  étant difficile à factoriser, on ne peut guère espérer que l'un de ses facteurs soit l'un des  $a_p$ . Soit alors  $\mathbb{Z}^P$  le groupe abélien additif formé des vecteurs  $(v_p)_{p \in P}$  avec  $v_p \in \mathbb{Z}$ , et  $f$  l'homomorphisme de groupe :  $\mathbb{Z}^P \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$  qui à  $(v_p)_{p \in P}$  associe  $\prod_{p \in P} a_p^{v_p}$ . Cette application est surjective si et seulement si les  $(a_p)_{p \in P}$  engendrent  $(\mathbb{Z}/n\mathbb{Z})^*$ . Pour le choix des  $a_p$  fait en pratique (5), c'est généralement le cas, mais, avouent encore les auteurs : “*nous sommes en général incapables de le prouver*”, et d'ajouter : “*D'ailleurs peu de chose a été prouvé rigoureusement au sujet des algorithmes pratiques de factorisation!*”.

### Seconde étape : rassembler des relations entre les $a_p$

Chaque élément  $v = (v_p)_{p \in P}$  du noyau de  $f$  donne une relation entre les  $a_p$ , en ce sens que  $\prod_{p \in P} a_p^{v_p} = 1$ . La seconde étape va consister à collecter de telles relations, jusqu'à ce que leur nombre soit grossièrement supérieur au cardinal de  $P$ .

### Troisième étape : recherche de dépendances

Soit  $V$  l'ensemble des  $v$  déterminés dans la seconde étape, et  $\bar{v} \in (\mathbb{Z}/2\mathbb{Z})^P = \mathbb{F}_2^P$  le vecteur obtenu à partir de  $v$  en réduisant ses composantes modulo 2. Comme le cardinal de  $V$  est supérieur à celui de  $P$ , les vecteurs  $\bar{v}$  sont linéairement dépendants sur  $\mathbb{F}_2$ . La troisième étape va consister à chercher des dépendances explicites en résolvant un système linéaire. La matrice de ce système tend à être énorme mais avec beaucoup de 0 et des 1 éparpillés par ci par là, et il existe des méthodes spéciales pour résoudre ce type de système. Néanmoins ici, les auteurs ont utilisé la méthode classique de Gauss. Les matrices les plus importantes présentaient approximativement 80000 colonnes et un peu moins de lignes!

Chaque dépendance trouvée peut s'écrire  $\sum_{v \in W} \bar{v} = 0$  pour un certain ensemble  $W$  inclus dans  $V$ , et chaque  $W$  donne naissance à un vecteur  $w = \frac{1}{2}(\sum_{v \in W} v) \in \mathbb{Z}^P$  pour lequel  $2.w$  appartient à  $\ker f$ . Chaque  $w$  de ce type, à son tour, donne naissance à un élément  $x = f(w)$  qui appartient à  $(\mathbb{Z}/n\mathbb{Z})^*$  et qui vérifie  $x^2 = f(2.w) = 1$  et donc donne naissance à une décomposition de  $n$  en facteurs non triviaux.

## 5. Mise en place d'une base de facteurs

Pour la décomposition de  $n = F_9/2424833$  la sélection d'une base de facteurs a été construite sur l'utilisation de l'anneau des entiers algébriques  $\mathbb{Z}[\sqrt[5]{2}]$ . Rappelons-en les principales caractéristiques.

L'ensemble  $\mathbb{Z}[\sqrt[5]{2}]$  est formé des réels  $\alpha = \sum_{i=0}^{i=4} \alpha_i \sqrt[5]{2}^i$  où les  $\alpha_i$  sont des entiers

(5) Voir § 5 du présent article.

relatifs. Multiplier un élément  $x = \sum_{i=0}^{i=4} x_i \sqrt[5]{2}^i$  par  $\alpha$  revient à multiplier le vecteur colonne  $(x_i)_{0 \leq i \leq 4}$  par la matrice

$$\begin{pmatrix} \alpha_0 & 2\alpha_4 & 2\alpha_3 & 2\alpha_2 & 2\alpha_1 \\ \alpha_1 & \alpha_0 & 2\alpha_4 & 2\alpha_3 & 2\alpha_2 \\ \alpha_2 & \alpha_1 & \alpha_0 & 2\alpha_4 & 2\alpha_3 \\ \alpha_3 & \alpha_2 & \alpha_1 & \alpha_0 & 2\alpha_4 \\ \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 & \alpha_0 \end{pmatrix}$$

La norme  $N(\alpha)$  est définie comme étant le déterminant de cette matrice, qui est un entier. Elle vérifie :

$$N(\alpha\beta) = N(\alpha).N(\beta) \text{ pour } \alpha \text{ et } \beta \text{ appartenant à } \mathbb{Z}[\sqrt[5]{2}].$$

En particulier la norme  $N(a - b\sqrt[5]{2}^i) = a^5 - 2^i b^5$  pour  $(a, b) \in \mathbb{Z}^2; 0 \leq i \leq 4$ , joue un rôle important dans la décomposition de  $n$ .

### Homomorphisme d'anneaux

Si  $\mathcal{A}$  est un anneau commutatif unitaire, et  $\Psi : \mathbb{Z}[\sqrt[5]{2}] \longrightarrow \mathcal{A}$  un homomorphisme d'anneau, alors l'élément  $c = \Psi(\sqrt[5]{2})$  de  $\mathcal{A}$  vérifie  $c^5 = 2$  où 2 est l'élément  $1 + 1$  de l'anneau unitaire  $\mathcal{A}$ . Réciproquement, si  $c$  appartenant à  $\mathcal{A}$  vérifie  $c^5 = 2$ , il existe un unique homomorphisme d'anneau  $\Psi : \mathbb{Z}[\sqrt[5]{2}] \longrightarrow \mathcal{A}$ , tel que  $\Psi(\sqrt[5]{2}) = c$ , à savoir l'application définie par :

$$\Psi\left(\sum_{i=0}^{i=4} \alpha_i \sqrt[5]{2}^i\right) = \sum_{i=0}^{i=4} \alpha_i c^i \quad (\alpha_i \in \mathbb{Z})$$

où les  $\alpha_i$  à droite sont interprétés comme éléments de  $\mathcal{A}$ , de la même manière que nous avons définis  $2 = 1 + 1$ . Ainsi, se donner un homomorphisme d'anneau de  $\mathbb{Z}[\sqrt[5]{2}]$  dans  $\mathcal{A}$  est équivalent à se donner un élément  $c$  de  $\mathcal{A}$  vérifiant  $c^5 = 2$ . L'exemple suivant va jouer le rôle essentiel dans la décomposition de  $n = F_9/2424833$ .

Prenons  $\mathcal{A} = \mathbb{Z}/n\mathbb{Z}$  et  $c \equiv 2^{205} \pmod{n}$ .

En nous rappelant que  $F_9 = 2^{512} + 1$ , alors  $2^{512} \equiv -1 \pmod{n}$  et donc  $c^5 \equiv 2^{1025} \equiv 2 \times (2^{512})^2 \equiv 2 \pmod{n}$ .

Il existe donc un homomorphisme  $\Psi : \mathbb{Z}[\sqrt[5]{2}] \longrightarrow \mathbb{Z}/n\mathbb{Z}$  avec  $\Psi(\sqrt[5]{2}) \equiv 2^{205} \pmod{n}$ .

Cet homomorphisme a l'avantage suivant que l'image de  $\alpha = -\sqrt[5]{2}^3$  étant  $\Psi(\alpha) \equiv (-2^{615}) \equiv 2^{103} \pmod{n}$ ,  $2^{103}$  est relativement petit par rapport à  $n$  (une trentaine de chiffres seulement, contre 150 pour  $n$ ).

### Anneau principal

L'anneau  $\mathbb{Z}[\sqrt[5]{2}]$  se trouve avoir cette propriété remarquable d'être un anneau principal, ce qui signifie que tout idéal  $\mathbf{b}$  de cet anneau est principal, c'est-à-dire engendré par un unique élément  $\beta$ , ou encore qu'il est de la forme  $\beta\mathbb{Z}[\sqrt[5]{2}]$  avec  $\beta$  appartenant à  $\mathbb{Z}[\sqrt[5]{2}]$ . ( $\beta$  est appelé générateur de l'idéal  $\mathbf{b}$ ).

Un ensemble de  $\mathbb{Z}[\sqrt[5]{2}]$  en est un idéal si et seulement si il est le noyau d'un homomorphisme d'anneau défini sur  $\mathbb{Z}[\sqrt[5]{2}]$ . On appelle **idéal premier** de  $\mathbb{Z}[\sqrt[5]{2}]$  tout idéal qui est le noyau d'un homomorphisme d'anneau de  $\mathbb{Z}[\sqrt[5]{2}]$  sur un corps fini  $\mathbb{F}_p$ . En particulier, si  $p$  est un entier premier, l'idéal est appelé idéal premier du premier ordre (first-degree prime). Ces idéaux là jouent le même rôle dans  $\mathbb{Z}[\sqrt[5]{2}]$  que les nombres premiers dans  $\mathbb{Z}$ . Précisément, tout élément non nul  $x$  de  $\mathbb{Z}[\sqrt[5]{2}]$  peut se décomposer de façon unique sous la forme :

$$x = \varepsilon \prod_p \pi_p^{m(p)}$$

où  $\varepsilon$  appartient au groupe  $(\mathbb{Z}[\sqrt[5]{2}])^*$  des éléments inversibles de  $\mathbb{Z}[\sqrt[5]{2}]$  (ses unités).  $p$  désigne un idéal premier et  $\pi_p$  un générateur de cet idéal;  $m(p)$  désigne un entier naturel.

Par exemple  $5 = \varepsilon_3(1 + \sqrt[5]{2}^2)^5$  avec  $\varepsilon_3 = \varepsilon_1^2 \varepsilon_2^{-2}$  où  $\varepsilon_1 = -1 + \sqrt[5]{2}^2$  et  $\varepsilon_2 = -1 + \sqrt[5]{2}^2 - \sqrt[5]{2}^3 + \sqrt[5]{2}^4$ .

La base de facteurs  $(a_p)_{p \in P}$  utilisée pour la décomposition de  $n$  sera finalement construite à partir de l'ensemble  $P$  des éléments suivants :

- 1) Les 99700 nombres premiers  $p$  inférieurs à  $B_1 = 1295377$ .
- 2) Les trois entiers algébriques  $\varepsilon_0, \varepsilon_1, \varepsilon_2$  où  $\varepsilon_0 = -1$  et  $\varepsilon_1$  et  $\varepsilon_2$  sont les nombres définis ci-dessus. Ces trois entiers sont des générateurs du sous anneau  $(\mathbb{Z}[\sqrt[5]{2}])^*$  des éléments inversibles de  $\mathbb{Z}[\sqrt[5]{2}]$ , c'est-à-dire que chaque élément  $\varepsilon$  de ce sous anneau peut s'écrire sous la forme  $\varepsilon = \varepsilon_0^{v(0)} \varepsilon_1^{v(1)} \varepsilon_2^{v(2)}$  avec  $v(0), v(1), v(2)$  éléments de  $\mathbb{Z}$ .
- 3) Les générateurs  $\pi_p$  des 99500 entiers algébriques du premier ordre de  $\mathbb{Z}[\sqrt[5]{2}]$  dont la norme est inférieure à  $B_2 = 1294973$ .

Les contraintes  $B_1$  et  $B_2$  sont des contraintes empiriques imposées par la réalisation effective des divers calculs.

La base de facteurs  $(a_p)_{p \in P}$  est alors définie pour chaque indice  $p \in P$  par  $a_p = \Psi(p)$  où  $\Psi$  est l'homomorphisme défini ci-dessus. Elle était donc composée de  $3 + 99700 + 99500 = 199203$  éléments, pour lesquels ont été déterminés un ensemble  $V$  de 226688 relations. La recherche de celles-ci avait été répartie entre environ 700 "workstations" reliées à un centre général de calcul DEC SRC à Palo Alto. Voici comment les auteurs décrivent les dernières minutes de cette prodigieuse réalisation.

*"Le 15 juin 1990, tôt dans la matinée, les relations de dépendance furent envoyées électroniquement à DEC SRC où elles furent converties en dépendances sur la 200000 matrice originale (6).*

*Du moins, nous espérions que les choses se passeraient bien ainsi. A 9 h 15 PDT (7) nous démarrions notre programme final, la tentative de factoriser  $n$*

---

(6) La matrice  $226688 \times 199203$  regroupant les relations, réduites modulo 2.

(7) heure locale soit heure GMT - 7h.

*en parcourant les relations de dépendance séquentiellement jusqu'à ce que la factorisation soit trouvée. Ce fut le moment le plus excitant de toute la factorisation de  $F_9$  : à 9 h 45 PDT le programme concluait que la première relation trouvée entre les colonnes de la 200000 matrice était une relation exacte. Ce moment de grande émotion ne put être gâté par le message décevant émis à 10 h 15 PDT, que la première relation de dépendance n'a donné naissance qu'à la factorisation triviale de  $n$ . Une heure plus tard, à 11 h 15 PDT (18 h 15 GMT) la seconde dépendance s'avéra plus chanceuse en détectant un facteur de 49 chiffres. Ce facteur ainsi que le cofacteur de 99 chiffres furent tous deux annoncés comme premiers, parce qu'aucun témoignage de leur éventuel caractère composé ne put être découvert parmi cinq entiers choisis de façon aléatoire (8).*

*Cinq minutes après, le processus d'élimination gaussien, ne fonctionnant pourtant plus que dans un seul poste de calcul était terminé, cinq jours avant le délai fixé. Le même jour encore, ce 15 juin, Andrew Odlyzk utilisait un test de primalité pour prouver que chacun des deux facteurs était vraiment premier".*

### TROIS GRANDS THÉORICIENS DES APPRENTISSAGES SCOLAIRES

par Jean-Paul FISCHER  
(IUFM de Lorraine)

Cette nouvelle brochure de l'IREM de Strasbourg présente et discute les élaborations de trois grands théoriciens – **Case** (Canada), **Bruner** (Etats-Unis) et **Brousseau** (France) – des apprentissages scolaires.

En se limitant à trois théoriciens, l'auteur réussit la gageure, en moins d'une centaine de pages, d'approfondir leurs théories, de développer des exemples ou applications précises, et de mener des discussions critiques s'appuyant sur la littérature internationale.

Ecrit à partir d'un cours destiné à des étudiants (de maîtrise) en psychologie cognitive et en didactique des mathématiques, il devrait aussi intéresser les étudiants en IUFM et tous les pédagogues (instituteurs, professeurs, ...) ou formateurs confrontés à l'enseignement des mathématiques, de la didactique ou de la psychologie.

---

Prix : 50 F (port compris si envoi à un établissement scolaire en France – Autrement 68 F – Commande à envoyer à la Bibliothèque de l'IREM de Strasbourg – Paiement à l'ordre de M. l'Agent Comptable de l'ULP - IREM.

---

(8) pour lesquels  $a^n \equiv a \pmod{n}$ .

# SUR LES CONIQUES À CENTRE TANGENTES AUX TROIS CÔTÉS D'UN TRIANGLE

Jacques DAUTREVAUX

Comme nous l'annonçons dans le n° 73, M. Dautrevaux nous a fourni, à propos du problème 25 de "À vos stylos", une étude très détaillée sur les centres des coniques tangentes à trois droites données; il utilise deux méthodes (équations affines ponctuelles ou tangentielles).

Voici la partie de ce travail traitée par la méthode tangentielle. (Nous laissons aux lecteurs l'étude ponctuelle analogue, nous contentant de l'indication suivante : écrire l'équation de la conique sous la forme

$$a(x - \lambda)^2 + 2b(x - \lambda)(y - \mu) + c(y - \mu)^2 + d = 0,$$

où  $\lambda$  et  $\mu$  sont les coordonnées du centre.)

---

## 1. GÉNÉRALITÉS

Soient dans le plan trois droites déterminant un vrai triangle  $ABC$ ,  $O$  un point quelconque du plan. S'il existe une conique de centre  $O$  tangente à ces trois droites elle l'est aussi à leurs symétriques par rapport à  $O$ , soit au total à six droites deux à deux parallèles, formant une figure ayant un centre de symétrie  $O$ .

Inversement, si on se contente de cinq de ces droites, il est clair que  $O$  est déterminé comme centre de symétrie de l'ensemble des quatre droites deux à deux parallèles; sous réserve que la cinquième droite ne soit pas parallèle à l'une des quatre autres et qu'elle ne passe pas par l'un des points communs à deux quelconques des quatre autres, il existe une conique unique tangente à ces cinq droites; cette conique a naturellement pour centre  $O$  et elle est aussi tangente à une sixième droite, la symétrique de la cinquième par rapport à  $O$ . Ainsi qu'il a été dit, le problème n'a pas de solution si trois de ces six droites sont parallèles ou passent par un même point. D'après le mode de construction de cet ensemble de droites à partir du triangle  $ABC$ , le premier cas d'exception ne saurait se produire, mais en ce qui concerne le second on voit aisément que les points par où sont susceptibles de passer trois droites sont les sommets  $A, B, C$  du triangle et que par suite les points du plan à exclure pour le choix de la position de  $O$  sont ceux des droites joignant les milieux des côtés du triangle  $ABC$ .

On en retiendra le résultat suivant :

Tout point  $O$  du plan non situé sur l'une quelconque des droites passant par les milieux des côtés du triangle  $ABC$  est le centre d'une, et d'une seule conique tangente aux trois côtés de ce triangle.

Le problème posé se résume donc en un problème de régionnement du plan.

## 2. ÉTUDE ANALYTIQUE

Le problème posé étant d'essence typiquement affine, on rapportera le plan au repère  $[A; \frac{1}{2}\overrightarrow{AB}, \frac{1}{2}\overrightarrow{AC}]$ , ce qui se traduit par un système d'axes de coordonnées  $(Ax, Ay)$  dans lequel les coordonnées de  $B$  sont  $(2, 0)$  et celles de  $C$   $(0, 2)$ . On se donne en outre le point  $O(\lambda, \mu)$ .

Dans ce repère les cinq droites auxquelles doit être tangente la conique cherchée sont les droites d'équations :

$$x = 0, \quad x = 2\lambda, \quad y = 0, \quad y = 2\mu \quad \text{et} \quad x + y = 2$$

et leurs coordonnées tangentielles respectives  $[(u, v, w)$ , triplet de réels non tous nuls tel que l'équation ponctuelle de la droite s'écrive  $ux + vy + w = 0$  — la droite de coordonnées  $(0, 0, 1)$  est la droite de l'infini ] sont :

$$(1, 0, 0), \quad (1, 0, -2\lambda), \quad (0, 1, 0), \quad (0, 1, -2\mu) \quad \text{et} \quad (1, 1, -2).$$

L'équation tangentielle de la conique cherchée s'en déduit, car ces cinq conditions permettent le calcul facile des six coefficients homogènes non tous nuls de la forme générale  $\varphi(u, v, w) = Au^2 + 2Buv + Cv^2 + 2Duw + 2Evw + Fw^2 = 0$ .

On trouve alors aisément :

$$4(\lambda + \mu - 1)uv + 2\lambda uw + 2\mu vw + w^2 = 0,$$

soit  $\varphi(u, v, w) = 0$ , qui est l'équation tangentielle de l'unique conique de centre  $O$  tangente aux trois côtés du triangle  $ABC$ .

On vérifie sans peine que la symétrique par rapport à  $O$  de la droite  $BC$  (d'équation  $x + y = 2$ ) est tangente à cette conique car ses coordonnées tangentielles sont  $(1, 1, -2(\lambda + \mu - 1))$  [obtenues à partir de l'équation ponctuelle  $x + y = 2(\lambda + \mu - 1)$  de cette droite].

Si  $(u, v, w)$  est une droite tangente à la conique,  $u, v$  et  $w$  vérifient  $\varphi(u, v, w) = 0$  et les coordonnées du point de contact, rendues homogènes sont  $\bar{x} = \frac{\partial \varphi}{\partial u}(u, v, w)$ ,  $\bar{y} = \frac{\partial \varphi}{\partial v}(u, v, w)$  et  $\bar{z} = \frac{\partial \varphi}{\partial w}(u, v, w)$ . Si  $\bar{z} = 0$  le point de contact est à l'infini dans la direction de vecteur directeur le vecteur de composantes  $(\bar{x}, \bar{y})$ , tandis que si  $\bar{z} \neq 0$  les coordonnées ponctuelles du point de contact sont  $x = \frac{\bar{x}}{\bar{z}}, y = \frac{\bar{y}}{\bar{z}}$ .

Ici,  $\frac{\partial \varphi}{\partial u} = 4(\lambda + \mu - 1)v + 2\lambda w$ ,  $\frac{\partial \varphi}{\partial v} = 4(\lambda + \mu - 1)u + 2\mu w$ , et  $\frac{\partial \varphi}{\partial w} = 2(\lambda u + \mu v + w)$ .

Ce point de contact est à l'infini lorsque  $\frac{\partial \varphi}{\partial w}(u, v, w) = 0$  soit lorsque  $\lambda u + \mu v + w = 0$ , c'est-à-dire lorsque la droite  $ux + vy + w = 0$  passe par le centre  $O$  de la conique. En effet, les seules tangentes à une conique dont le point de contact est à l'infini sont les asymptotes d'une hyperbole.

SUR LES CONIQUES À CENTRE TANGENTES AUX TROIS CÔTÉS D'UN TRIANGLE

Dans les autres cas le point de contact de la droite  $(u, v, w)$  avec la conique a pour coordonnées ponctuelles :

$$x = \frac{2(\lambda + \mu - 1)v + \lambda w}{\lambda u + \mu v + w}, \quad y = \frac{2(\lambda + \mu - 1)u + \mu w}{\lambda u + \mu v + w}.$$

Ainsi par exemple les points de contact de la conique avec les trois côtés du triangle sont :

$$\begin{array}{lll} \text{droite } AC : & x = 0 & (u = 1, v = 0, w = 0) \quad B_0 : x = 0, y = \frac{2(\lambda + \mu - 1)}{\lambda} \\ \text{droite } AB : & y = 0 & (u = 0, v = 1, w = 0) \quad C_0 : x = \frac{2(\lambda + \mu - 1)}{\mu}, y = 0 \\ \text{droite } BC : & x + y = 2 & (u = 1, v = 1, w = -2) \quad A_0 : x = \frac{2(\mu - 1)}{\lambda + \mu - 2}, y = \frac{2(\lambda - 1)}{\lambda + \mu - 2} \end{array}$$

et on voit apparaître des singularités lorsque  $\lambda = 0$ , ou  $\mu = 0$  ou  $\lambda + \mu = 2$ , c'est-à-dire lorsque le centre  $O$  de la conique a été choisi sur l'une des trois droites portant les côtés du triangle : cette droite est alors une asymptote de la conique obtenue, qui est nécessairement dans ce cas une hyperbole.

### Nature de la conique

Elle est conditionnée par l'existence de tangentes passant par  $O$ . S'il en existe deux, ce sont des asymptotes et on a affaire à une **hyperbole**; s'il n'en existe pas, la conique est une **ellipse**.

L'équation tangentielle de la conique peut aussi s'écrire :

$$4(\lambda + \mu - 1)uv + (\lambda u + \mu v + w)^2 - (\lambda u + \mu v)^2 = 0$$

soit, après transformation :

$$\lambda^2 u^2 - 2[2(\lambda + \mu - 1) - \lambda\mu]uv + \mu^2 v^2 - (\lambda u + \mu v + w)^2 = 0.$$

Le triplet  $(u, v, w)$  représentant une tangente passant par  $O$  (de coordonnées ponctuelles  $(\lambda, \mu)$ ) satisfait aux deux équations homogènes :

$$\begin{cases} \lambda u + \mu v + w = 0 \\ \lambda^2 u^2 - 2[2(\lambda + \mu - 1) - \lambda\mu]uv + \mu^2 v^2 = 0 \end{cases}$$

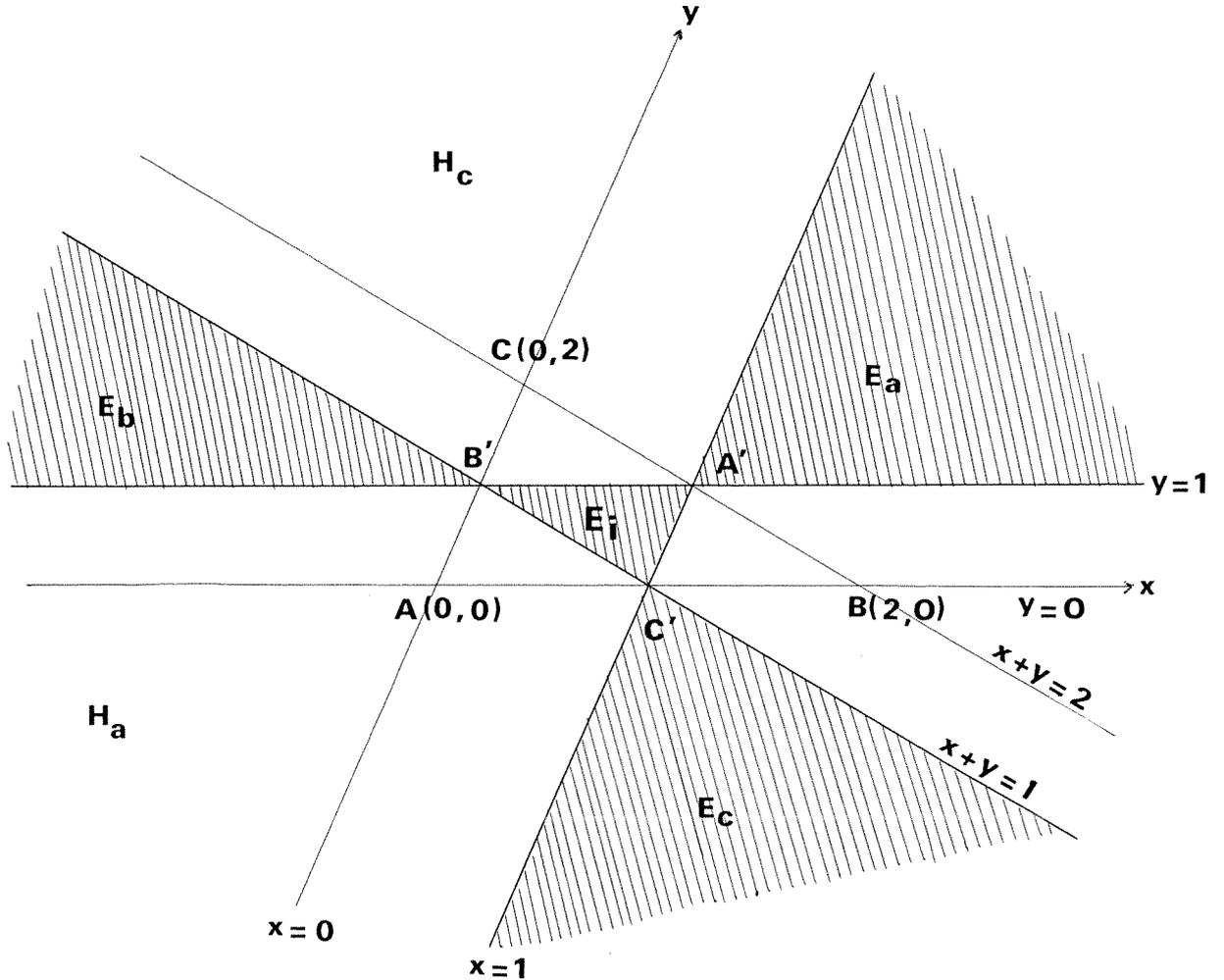
Le discriminant de la deuxième équation est :

$$\begin{aligned} [2(\lambda + \mu - 1) - \lambda\mu]^2 - \lambda^2 \mu^2 &= 4(\lambda + \mu - 1)^2 - 4\lambda\mu(\lambda + \mu - 1) = \\ &= -4(\lambda + \mu - 1)(\lambda\mu - (\lambda + \mu - 1)) = -4(\lambda + \mu - 1)(\lambda - 1)(\mu - 1) \end{aligned}$$

soit

$$\Delta = -4(\lambda - 1)(\mu - 1)(\lambda + \mu - 1)$$

Selon le signe de  $\Delta$  on obtient un régionnement du plan par les droites  $x = 1$ ,  $y = 1$ ,  $x + y = 1$  qui sont les droites passant par les milieux des côtés du triangle  $ABC$ .



- Si  $\Delta < 0$ , il n'existe pas de tangentes issues de  $O$ . La conique est une **ellipse**.  $O$  se trouve dans l'une des zones  $E$  du diagramme ci-dessus.
- Si  $\Delta = 0$ , c'est-à-dire si  $O$  se trouve sur l'une des trois droites  $(A'B')$ ,  $(B'C')$ ,  $(A'C')$  formant la frontière des zones précédentes, on est en présence de singularités.
- Si  $\Delta > 0$ , il existe deux tangentes distinctes issues de  $O$  (ce sont des asymptotes) et la conique est une **hyperbole**.  $O$  se trouve dans l'une des zones marquées  $H$ .

L'équation tangentielle  $\lambda^2 u^2 - 2[2(\lambda + \mu - 1) - \lambda\mu]uv + \mu^2 v^2 = 0$  représente deux droites d'équation ponctuelle  $u(x - \lambda) + v(y - \mu) = 0$  où  $u$  et  $v$ , satisfont la relation précédente. L'élimination de  $u$  et  $v$ , par :  $u = k(y - \mu)$ ,  $v = -k(x - \lambda)$  où  $k \neq 0$ , donne alors par substitution :

$$\mu^2(x - \lambda)^2 + 2[2(\lambda + \mu - 1) - \lambda\mu](x - \lambda)(y - \mu) + \lambda^2(y - \mu)^2 = 0$$

qui est l'équation ponctuelle de l'ensemble des deux asymptotes de l'hyperbole obtenue lorsque  $\Delta > 0$ .

**Remarque :** Lorsque  $\Delta < 0$ , l'expression trouvée à la suite du calcul précédent représente l'ensemble des asymptotes (droites imaginaires) de l'ellipse.

Dans tous les cas, on vérifie que l'équation ponctuelle de la conique cherchée s'écrit :

$$\mu^2(x - \lambda)^2 + 2[2(\lambda + \mu - 1) - \lambda\mu](x - \lambda)(y - \mu) + \lambda^2(y - \mu)^2 + \Delta = 0,$$

ce qui met en évidence le centre et les asymptotes (éventuelles).

### Examen des différents cas

#### 1) Cas singulier : $\Delta = 0$

Ce cas se produit lorsque  $\lambda = 1$  ou  $\mu = 1$  ou  $\lambda + \mu = 1$ , c'est-à-dire lorsque  $O$  est choisi sur l'une des trois droites passant par les milieux des côtés du triangle  $ABC$ .

- $\lambda + \mu = 1$ .  $O$  est un point de la droite  $(B'C')$

L'équation tangentielle de la conique devient :

$$w(2\lambda u + 2\mu v + w) = 0.$$

La conique est dégénérée en deux points :

$w = 0$ , équation tangentielle du point  $A(0, 0)$

$2\lambda u + 2\mu v + w = 0$ , équation tangentielle du point  $A_1(2\lambda, 2\mu)$  situé sur la droite d'équation  $x + y = 2$  (car  $\lambda + \mu = 1$ ) et il est clair que  $O$  est le milieu de  $AA_1$ .

- $\lambda = 1$  ou  $\mu = 1$  ces cas se traitent de façon analogue. Donc :

Lorsque  $O$  est choisi sur l'une des droites  $(B'C')$ ,  $(A'C')$  ou  $(A'B')$  contenant les milieux des côtés du triangle  $ABC$ , la conique est dégénérée en deux points, respectivement  $A, B$  ou  $C$  et son symétrique par rapport à  $O$ .

#### 2) Ellipse : $\Delta < 0$

a) Domaine  $E_i$  intérieur au triangle  $A'B'C'$ .

Alors,  $0 < \lambda < 1$ ,  $0 < \mu < 1$  et  $1 < \lambda + \mu < 2$ .

Il s'ensuit que les coordonnées des points de contact  $A_0, B_0$  et  $C_0$  vérifient, comme on s'en assure aisément :

– pour  $A_0$  :  $0 < x < 2$  et  $0 < y < 2$

– pour  $B_0$  :  $0 < y < 2$

– pour  $C_0$  :  $0 < x < 2$ .

Ces points de contact sont donc situés respectivement sur les segments  $BC, AC$  et  $AB$ . Dès lors, en vertu de la convexité de l'ellipse, courbe fermée, celle-ci est intérieure au triangle  $ABC$ , aux côtés duquel elle est tangente en  $A_0, B_0, C_0$ . Il s'agit donc d'une **ellipse inscrite** dans le triangle.

b) Domaine  $E_a$ , angle extérieur de sommet  $A'$ .

Alors,  $\lambda > 1$  et  $\mu > 1$ .

On s'assure comme précédemment que les coordonnées des points de contact  $A_0, B_0, C_0$  vérifient :

= pour  $A_0$  :  $0 < x < 2$  et  $0 < y < 2$

= pour  $B_0$  :  $y > 2$

= pour  $C_0 : x > 2$ .

Ces points de contact sont situés respectivement sur le segment  $BC$  et sur les prolongements du côté opposé à  $A$  des côtés  $AC$  et  $AB$ . Une ellipse de ce type est donc **exinscrite** dans l'angle  $A$  du triangle.

De même pour les domaines  $E_b$  et  $E_c$  définis de façon analogue.

Puisque les centres des ellipses forment les quatre domaines  $E_i, E_a, E_b$  et  $E_c$ , ceci montre que **l'ensemble des centres des ellipses inscrites dans un triangle  $ABC$  est le domaine  $E_i$  intérieur au triangle ayant pour sommets les milieux des côtés du triangle  $ABC$ ; l'ensemble des centres des ellipses exinscrites dans l'angle  $A$ , (respectivement  $B, C$ ) du triangle  $ABC$  est le domaine  $E_a$  (respectivement  $E_b, E_c$ ) intérieur au secteur angulaire extérieur au triangle  $A'B'C'$ , de sommet  $A'$  (respectivement  $B', C'$ ).**

### 3) Hyperbole : $\Delta > 0$

On obtient dans le plan trois domaines  $Ha, Hb, Hc$  contenant respectivement les points  $A, B, C$ . Par raison de symétrie, il suffit d'étudier l'un de ces domaines,  $Hb$  par exemple, dans lequel on a :

$$\lambda > 1, \mu < 1 \text{ et } \lambda + \mu > 1.$$

Comme une hyperbole comporte deux branches, deux configurations sont possibles : ou bien les trois points de contact  $A_0, B_0, C_0$  se situent sur la même branche, ou bien on a deux des points sur une branche, le troisième sur l'autre.

Nous savons caractériser deux points situés sur une même branche d'hyperbole par le fait que les tangentes en ces points se coupent dans la région du plan limitée par les asymptotes contenant la courbe.

Par suite la disposition des trois points de contact  $A_0, B_0, C_0$  sur une seule ou bien sur les deux branches de l'hyperbole dépend de la position des points de concours des tangentes en ces points par rapport aux asymptotes.

$$\left\{ \begin{array}{l} \text{Les tangentes en } B_0 \text{ et } C_0 \text{ sont les droites } AC \text{ et } AB \text{ qui se coupent en } A, \\ \text{les tangentes en } A_0 \text{ et } C_0 \text{ sont les droites } BC \text{ et } AB \text{ qui se coupent en } B, \\ \text{les tangentes en } A_0 \text{ et } B_0 \text{ sont les droites } BC \text{ et } AC \text{ qui se coupent en } C. \end{array} \right.$$

- Les trois points de contact sont sur la même branche d'hyperbole si, et seulement si,  $A, B, C$  sont tous trois dans la région limitée par les asymptotes et contenant la courbe;
- Deux des points de contact sont sur une branche d'hyperbole et le troisième sur l'autre si, et seulement si, **un seul** des trois points  $A, B, C$  se trouve dans la région limitée par les asymptotes et contenant la courbe, les deux autres se trouvant dans l'autre.

Pour un point  $M(x, y)$  du plan on pose :

$$f(M) = \mu^2(x - \lambda)^2 + 2[2(\lambda + \mu - 1) - \lambda\mu](x - \lambda)(y - \mu) + \lambda^2(y - \mu)^2.$$

La quantité  $f(M)$  s'annule sur les asymptotes de l'hyperbole. Elle prend la valeur  $-\Delta$  sur l'hyperbole puisqu'ainsi qu'il a été vu précédemment l'équation de l'hyperbole s'écrit :

$$f(M) + \Delta = 0.$$

Par suite  $f(M) < 0$  dans toute la région limitée par les asymptotes et contenant la courbe.

**Remarque :** Ce résultat pouvait être trouvé en l'absence des propriétés évoquées ci-dessous, puisqu'on connaît trois points situés sur l'hyperbole, les points  $A_0, B_0$  et  $C_0$ .

Choisissant  $B_0$ , puisque nous sommes assurés que  $\lambda \neq 0$  (car  $\lambda > 1$ ) dans le domaine étudié on a :

\* coordonnées de  $B_0$  :  $x = 0, y = \frac{2(\lambda + \mu - 1)}{\lambda}$ .

$$\begin{aligned} * \quad f(B_0) &= \lambda^2 \mu^2 - 2[2(\lambda + \mu - 1) - \lambda\mu]^2 + [2(\lambda + \mu - 1) - \lambda\mu]^2 \\ &= \lambda^2 \mu^2 - [2(\lambda + \mu - 1) - \lambda\mu]^2 \\ &= [\lambda\mu + 2(\lambda + \mu - 1) - \lambda\mu][2\lambda\mu - 2(\lambda + \mu - 1)] \\ &= 4(\lambda + \mu - 1)(\lambda\mu - \lambda - \mu + 1) \end{aligned}$$

$$\text{soit } f(B_0) = 4(\lambda - 1)(\mu - 1)(\lambda + \mu - 1) = -\Delta < 0.$$

\* Il en résulte bien que  $f(M) < 0$  dans toute la région limitée par les asymptotes et contenant la courbe.

**Discussion :** Deux configurations sont possibles.

I.- Ou bien  $A_0, B_0, C_0$  sont sur une même branche d'hyperbole. Alors  $A, B, C$  sont tous trois situés dans la région limitée par les asymptotes et contenant la courbe. Cette configuration est caractérisée par :

$$f(A), f(B), f(C) \text{ sont tous trois négatifs.}$$

II.- Ou bien  $A_0, B_0$  et  $C_0$  sont, deux d'entre eux sur une branche et le troisième sur une autre. Alors, des trois points  $A, B, C$ , l'un seulement est situé dans la région limitée par les asymptotes et contenant la courbe. Cette configuration est caractérisée par :

Seul l'un des trois nombres  $f(A), f(B), f(C)$  est négatif.

On calculera donc  $f(A), f(B)$  et  $f(C)$ . La caractérisation des configurations I et II se réduit alors à :

- On a la configuration II, si et seulement si un et un seul, des trois nombres  $f(A), f(B)$  et  $f(C)$  est **négatif**.
- On a la configuration I si, et seulement si les trois nombres  $f(A), f(B)$  et  $f(C)$  sont **négatifs**.

1) Coordonnées de  $A : x = 0, y = 0$ .

$$\begin{aligned} f(A) &= \lambda^2 \mu^2 + 2\lambda\mu[2(\lambda + \mu - 1) - \lambda\mu] + \lambda^2 \mu^2 = 2\lambda\mu[\lambda\mu + 2(\lambda + \mu - 1) - \lambda\mu] \\ f(A) &= 4\lambda\mu(\lambda + \mu - 1). \end{aligned}$$

2) Coordonnées de  $B : x = 2, y = 0$ .

$$\begin{aligned} f(B) &= \mu^2(2 - \lambda)^2 - 2\mu(2 - \lambda)[2(\lambda + \mu - 1) - \lambda\mu] + \lambda^2 \mu^2 \\ &= \mu^2(\lambda - 2)^2 + 4\mu(\lambda - 2)(\lambda + \mu - 1) - 2\lambda(\lambda - 2)\mu^2 + \lambda^2 \mu^2 \\ &= 4\mu^2 + 4\mu(\lambda - 2)(\lambda + \mu - 1) \end{aligned}$$

soit par un calcul simple :

$$f(B) = 4\mu(\lambda - 1)(\lambda + \mu - 2).$$

3) Coordonnées de  $C : x = 0, y = 2$

$$f(C) = \lambda^2 \mu^2 - 2\lambda(2 - \mu)[2(\lambda + \mu - 1) - \lambda\mu] + \lambda^2(2 - \mu)^2$$

Un calcul analogue donne :

$$f(C) = 4\lambda(\mu - 1)(\lambda + \mu - 2)$$

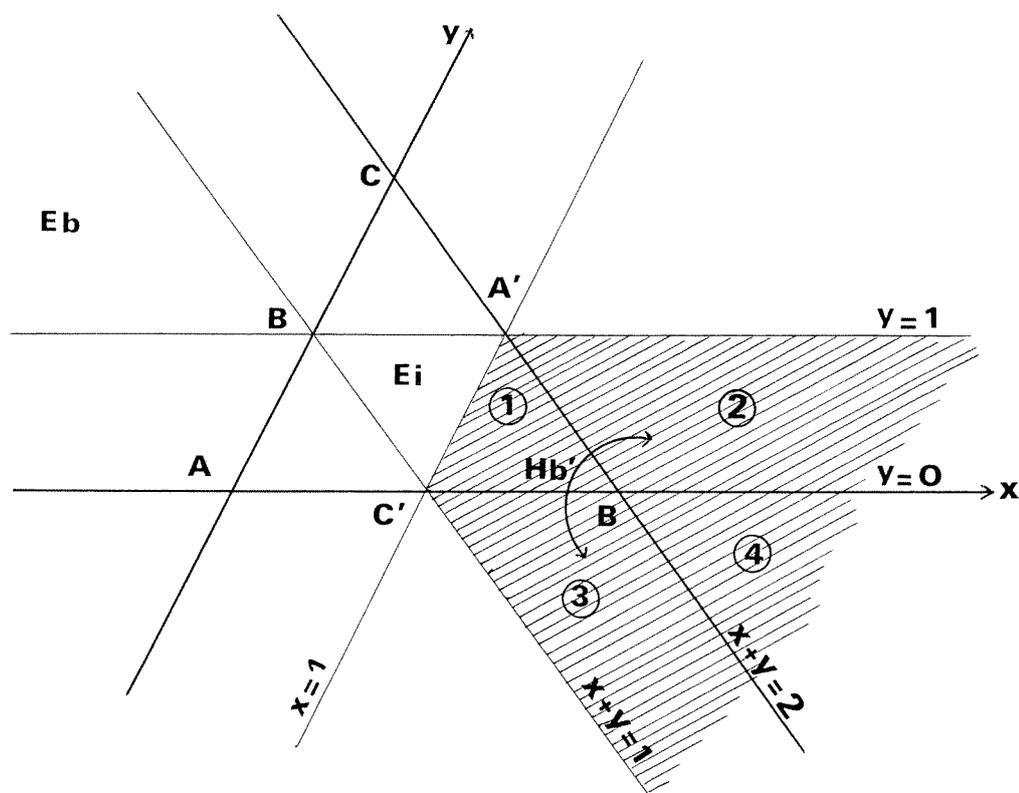
On note que :

$$\begin{aligned} f(A)f(B)f(C) &= 64\lambda^2 \mu^2 (\lambda + \mu - 2)^2 (\lambda - 1)(\mu - 1)(\lambda + \mu - 1) \\ &= -(4\lambda\mu(\lambda + \mu - 2))^2 \Delta < 0 \text{ comme il était à prévoir} \end{aligned}$$

Le domaine  $H_b$  étudié satisfait à :  $\lambda > 1, \mu < 1, \lambda + \mu > 1$ . Il est partagé (voir figure) par les droites  $y = 0$  et  $x + y = 2$  en quatre parties notées ① , ② , ③ , ④ .

Dans les domaines ① et ② on a  $\mu > 0$  d'où  $f(A) > 0$ . On a donc alors la configuration II.

SUR LES CONIQUES À CENTRE TANGENTES AUX TROIS CÔTÉS D'UN TRIANGLE



Dans les domaines ① et ③ on a :  $\lambda + \mu < 2$  d'où  $f(C) > 0$ .

On a aussi la configuration II.

Dans le domaine ④ on a  $\mu < 0$  et  $\lambda + \mu > 2$ . D'où  $f(A) < 0$  et  $f(B) < 0$  : c'est la configuration I.

On subdivise donc le domaine  $H_b$  en deux parties :  $H_b$  (limitée à la région ④) correspondant aux trois points de contact sur la même branche, et  $H_{b'}$  (réunion des régions ①, ② et ③) correspondant à deux points de contact sur une branche et un sur l'autre.

**Remarque :** Dans la région ①, on a  $f(B) < 0$  : ce sont les points  $A_0$  et  $C_0$  qui sont sur une branche d'hyperbole,  $B_0$  sur l'autre.

Dans la région ②, on a  $f(C) < 0$  : ce sont les points  $A_0$  et  $B_0$  qui sont sur la même branche,  $C_0$  sur l'autre.

Dans la région ③, on a  $f(A) < 0$  : les points  $B_0$  et  $C_0$  sont sur la même branche,  $A_0$  est sur l'autre.

Une étude plus poussée permet en outre de préciser la position des points de contact sur les côtés du triangle  $ABC$ , en utilisant leurs coordonnées déjà déterminées.

On raisonnera, ce qui n'est pas compliqué, dans la totalité de la zone  $(\lambda + \mu - 1)(\mu - 1) < 0$  (qui englobe aussi les régions  $E_b$  et  $E_i$ ).

1) Le point de contact  $B_0$  a pour coordonnées  $x = 0, y = 2 \frac{\lambda + \mu - 1}{\lambda}$  d'où  $y - 2 = 2 \frac{\mu - 1}{\lambda}$ .

Si  $\lambda + \mu - 1 < 0$  alors  $\mu - 1 > 0$  et donc  $\lambda < 0$ .

Si  $\lambda + \mu - 1 > 0$  alors  $\mu - 1 < 0$  et donc  $\lambda > 0$ .

Il en résulte  $y > 0$  et  $y - 2 < 0$  donc  $0 < y < 2$ .

Dans tous les cas  $B_0$  est situé sur le segment  $AC$ .

2) Le point de contact  $C_0$  a pour coordonnées  $x = 2\frac{\lambda+\mu-1}{\mu}$ ,  $y = 0$  d'où  $x - 2 = 2\frac{\lambda-1}{\mu}$ .

• Si  $\lambda + \mu - 1 < 0$  alors  $\mu - 1 > 0$  et on se trouve dans  $Eb$ . Il en résulte  $x < 0$  et  $C_0$  se trouve sur la demi-droite  $Ax'$ .

• Si  $\lambda + \mu - 1 > 0$  alors  $\mu - 1 < 0$  d'où aussi  $\lambda > 0$ .

- Si  $0 < \lambda < 1$ , on se trouve dans  $E_i$ . On voit que  $\lambda - 1 < 0$ , d'où  $\mu > 0$  et on voit que  $x > 0$  et  $x - 2 < 0$ , soit  $0 < x < 2$  :  $C_0$  se trouve sur le segment  $AB$ .

- Si  $\lambda > 1$  on a  $\lambda - 1 > 0$

Ou bien  $0 < \mu < 1$  et on se trouve dans  $Hb'_1$  ou  $Hb'_2$ ;

comme  $x - 2 > 0$ ,  $C_0$  est situé sur la demi-droite  $Bx$ .

Ou bien  $\mu < 0$  et on se trouve dans  $Hb'_3$  ou  $Hb$ ;

comme  $x < 0$ ,  $C_0$  est situé sur la demi-droite  $Ax'$ .

3) Le point de contact  $A_0$  a pour coordonnées  $x = 2\frac{\mu-1}{\lambda+\mu-2}$ ,  $y = 2\frac{\lambda-1}{\lambda+\mu-2}$  et, puisque  $x + y = 2$  on a  $x - 2 = -y$ .

• Si  $\lambda + \mu - 1 < 0$  alors  $\mu - 1 > 0$  et par suite  $\lambda < 0$ . On se trouve dans  $Eb$  et, comme  $\lambda + \mu - 2 < 0$  on a  $x < 0$  et  $A_0$  est située sur la demi-droite  $Cz'$ .

• Si  $\lambda + \mu - 1 > 0$  alors  $\mu - 1 < 0$  et donc  $\lambda > 0$ .

- Si  $0 < \lambda < 1$  on se trouve dans  $E_i$ .  $\lambda - 1 < 0$  entraîne  $\mu > 0$ , et  $\lambda + \mu - 2 = (\lambda - 1) + (\mu - 1) < 0$  donne  $x > 0$  et  $y > 0$ , soit  $x < 2$ . On a donc  $0 < x < 2$  et  $A_0$  se trouve sur le segment  $BC$ .

- Si  $\lambda > 1$  on a  $\lambda - 1 > 0$

Ou bien  $\lambda + \mu - 2 < 0$  et on se trouve dans  $Hb'_1$  ou  $Hb'_3$ ;

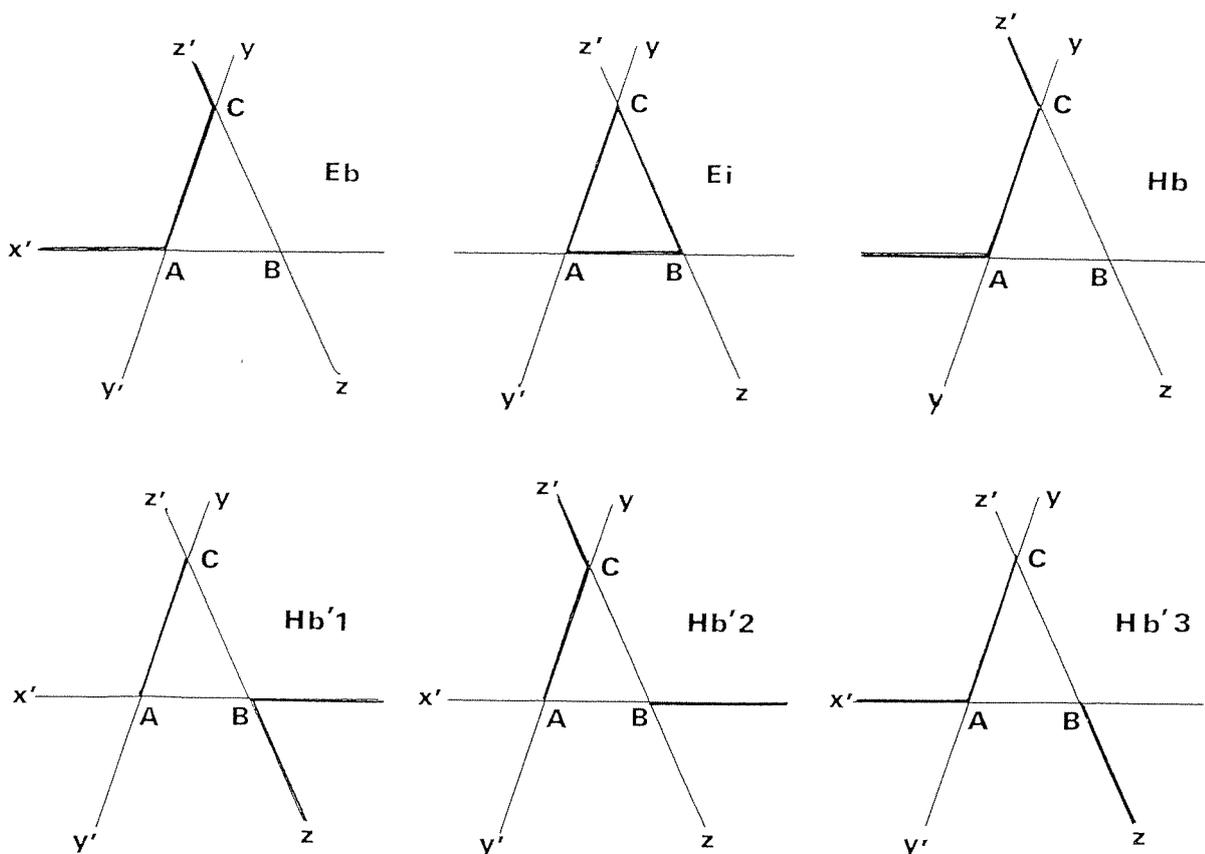
on a  $y < 0$  donc  $x > 2$  :  $A_0$  est sur la demi-droite  $Bz$

Ou bien  $\lambda + \mu - 2 > 0$  et on se trouve dans  $Hb'_2$  ou  $Hb$ ;

on a  $x < 0$ , et  $A_0$  est situé sur la demi-droite  $Cz'$ .

Les schémas ci-dessous résument les résultats obtenus sur la disposition des points de contact suivant la zone où se trouve  $O$  :

SUR LES CONIQUES À CENTRE TANGENTES AUX TROIS CÔTÉS D'UN TRIANGLE



On pourra remarquer, ce qui ne présentait aucune évidence a priori, que les points de contact situés sur une même branche d'hyperbole se trouvent sur des segments ou demi-droites contiguës.

**Cas particulier**

Il a déjà été noté que, si on choisissait  $O$  sur l'une des trois droites contenant les milieux des côtés du triangle, la conique correspondante était dégénérée en deux points dont l'un est toujours l'un des trois sommets  $A, B$  ou  $C$  du triangle.

Mais trois autres séparatrices interviennent, qui sont les trois droites portant les trois côtés du triangle  $ABC$ . Si par exemple on choisit  $O$  sur la droite  $AB$  on a  $\mu = 0$  et l'équation ponctuelle de l'ensemble des deux asymptotes devient :

$$4(\lambda - 1)(x - \lambda)y + \lambda^2 y^2 = 0$$

$$\text{soit } y[\lambda^2 y + 4(\lambda - 1)(x - \lambda)] = 0,$$

c'est-à-dire qu'on a effectivement une hyperbole dont l'une des asymptotes est la droite  $AB$ . Bien entendu, si on choisit  $O$  en  $B$ , la conique de centre  $O$  (c'est-à-dire  $B$ ), tangente aux trois côtés du triangle est une hyperbole dont les asymptotes sont les droites  $AB$  et  $BC$ , résultat au demeurant fort logique puisque dans une conique, les tangentes passant par le centre sont les asymptotes (qui ne sont réelles que si la conique est une hyperbole).

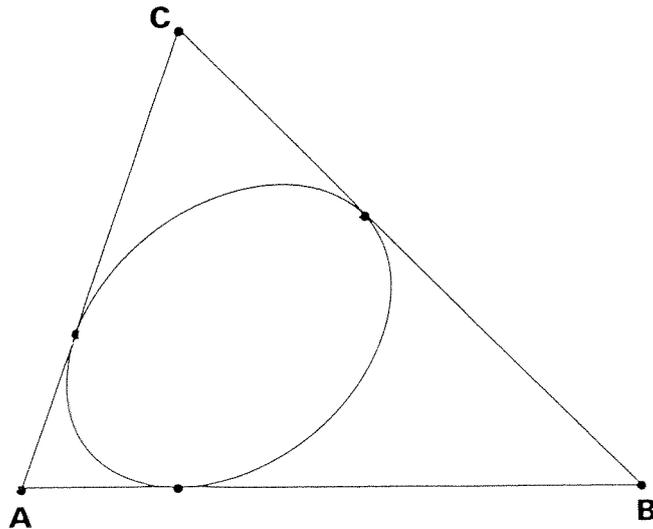
### Régionnement complet du plan

En permutant circulairement les sommets  $A, B, C$  aux deux autres secteurs angulaires, de sommets  $A'[(\lambda + \mu - 1)(\lambda - 1) > 0]$  et  $C'[(\lambda - 1)(\mu - 1) < 0]$  les zonages obtenus dans les secteurs de sommet  $B'[(\lambda + \mu - 1)(\mu - 1) < 0]$  et l'ensemble recouvre bien le plan avec une partie commune  $Ei$ .

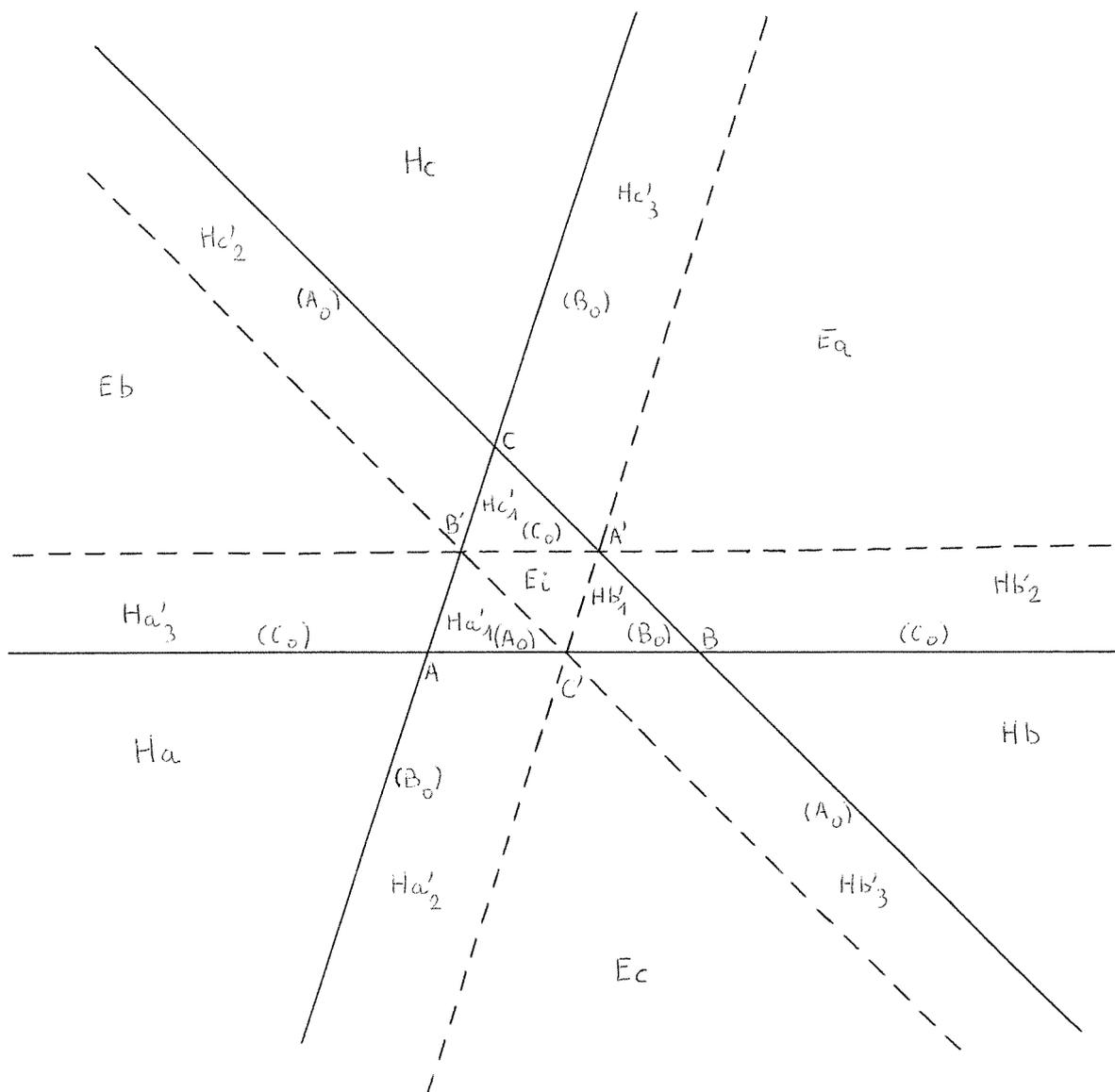
Le zonage est représenté page suivante et doit être lu de la façon suivante : si le centre  $O$  de la conique est choisi :

- sur l'une des droites joignant les milieux des côtés du triangle  $ABC$ , la conique est dégénérée en deux points dont l'un est  $A, B$  ou  $C$ ,
- dans  $Ei$  la conique est une ellipse inscrite dans le triangle;
- dans  $Ea, Eb$  ou  $Ec$  la conique est une ellipse exinscrite;
- dans  $Ha, Hb$  ou  $Hc$  la conique est une hyperbole telle que les trois côtés du triangle soient tangents à la même branche;
- dans  $Ha'_i, Hb'_i, Hc'_i$  ( $i \in \{1, 2, 3\}$ ) la conique est une hyperbole telle que deux côtés du triangle soient tangents à une branche, le troisième à l'autre. Pour  $i = 1$  les deux côtés du triangle tangents à la même branche sont issus du sommet du triangle intérieur à la zone;
- sur l'un des côtés du triangle, la conique est une hyperbole dont l'une des asymptotes est le côté considéré.

Dans les régions  $H'$  où deux points de contact sont sur une branche et le troisième sur l'autre, les considérations précédentes permettent de déterminer dans chacune des zones  $Hb'_i$  le point de contact isolé et par suite, par permutation circulaire, dans les autres zones. Ce point est indiqué sur le régionnement.



SUR LES CONIQUES À CENTRE TANGENTES AUX TROIS CÔTÉS D'UN TRIANGLE

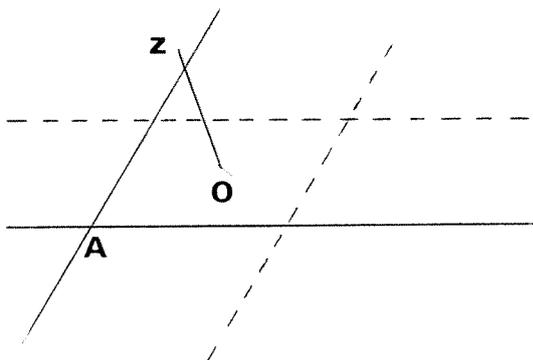


### 3. Approche géométrique

Une approche géométrique du problème proposé, déjà esquissée dans la partie ①, est certainement beaucoup plus intuitive, mais la rigueur mathématique n'est pas nécessairement au rendez-vous.

La conique cherchée doit être tangente à six droites deux à deux parallèles, dont trois quelconques d'entre elles ne sauraient être parallèles ni passer par un même point, cet ensemble de six droites ayant un centre de symétrie  $O$  (centre de la conique cherchée). La première exclusion ne saurait se produire, mais il est clair que la deuxième nécessite que  $O$  soit choisi en dehors des droites joignant les milieux des côtés du triangle  $ABC$ .

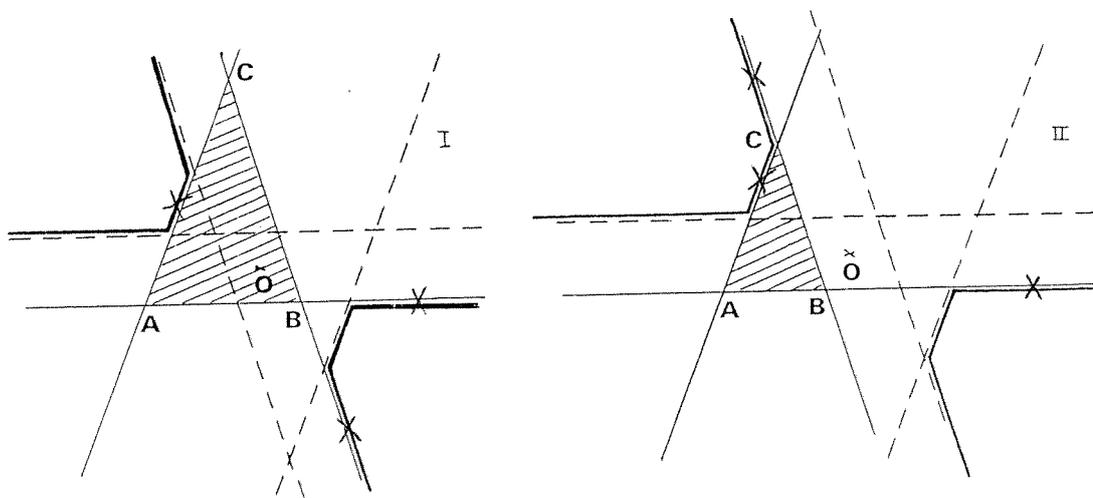
Les deux premières paires de droites parallèles se recoupent en définissant un parallélogramme de centre  $O$ , point imposé comme centre de la conique. On peut alors supposer, moyennant éventuellement des symétries affines adéquates, que la figure obtenue présente la disposition ci-contre par rapport à la direction  $Oz$  du troisième côté, les



droites en trait plein étant les supports de deux des côtés du triangle, se coupant en  $A$  et celles figurées en trait tireté étant leurs symétriques par rapport à  $O$ .

La troisième paire de droites parallèles est formée de deux droites parallèles à  $Oz$ , symétriques par rapport à  $O$ , dont l'une est le troisième côté du triangle et l'autre son symétrique par rapport à  $O$ . Ces droites ne doivent pas passer par un sommet du parallélogramme, et nonobstant cette restriction **six** configurations sont possibles, représentées ci-dessous :

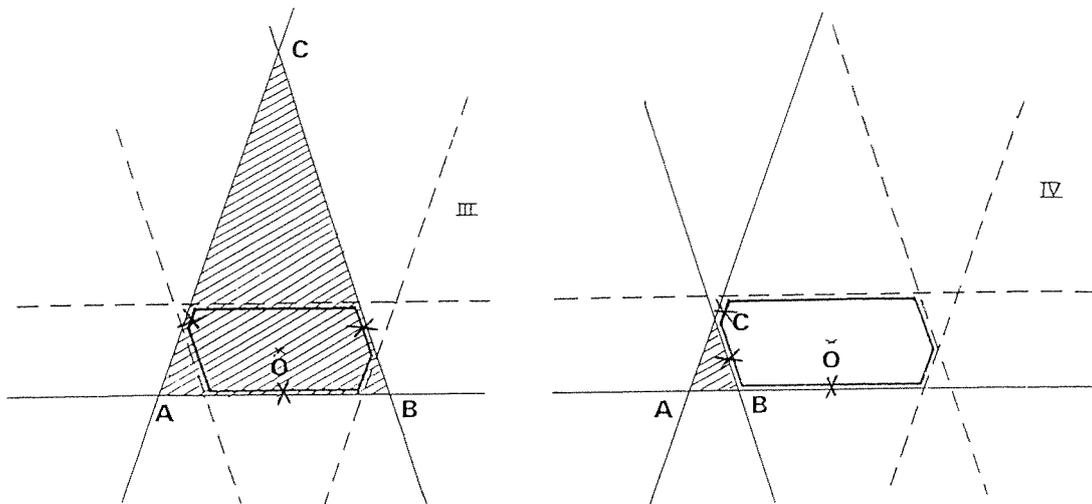
1)



Dans ces deux configurations, les six droites se divisent en deux groupes de trois, chacun délimitant une figure convexe, les deux étant symétriques par rapport à  $O$ . On se trouve là dans le cas de l'**hyperbole** dont une branche est tangente à deux côtés du triangle, l'autre au troisième côté.

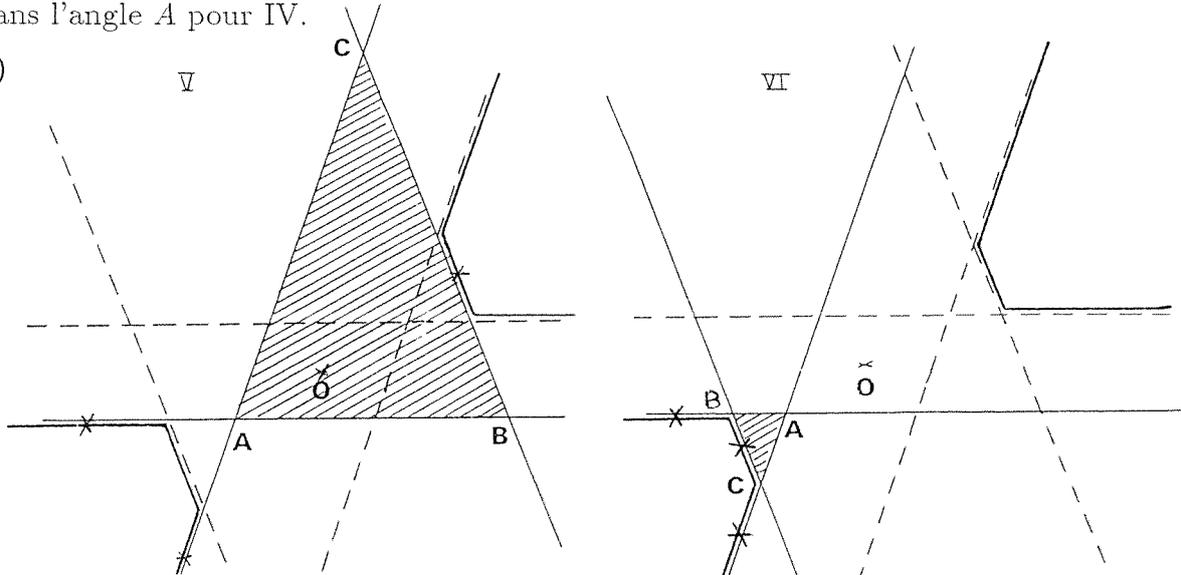
SUR LES CONIQUES À CENTRE TANGENTES AUX TROIS CÔTÉS D'UN TRIANGLE

2)



Dans les configurations III et IV, les six droites délimitent un hexagone convexe de centre  $O$ . On se trouve donc dans le cas de l'**ellipse**, inscrite pour III, exinscrite dans l'angle  $A$  pour IV.

3)

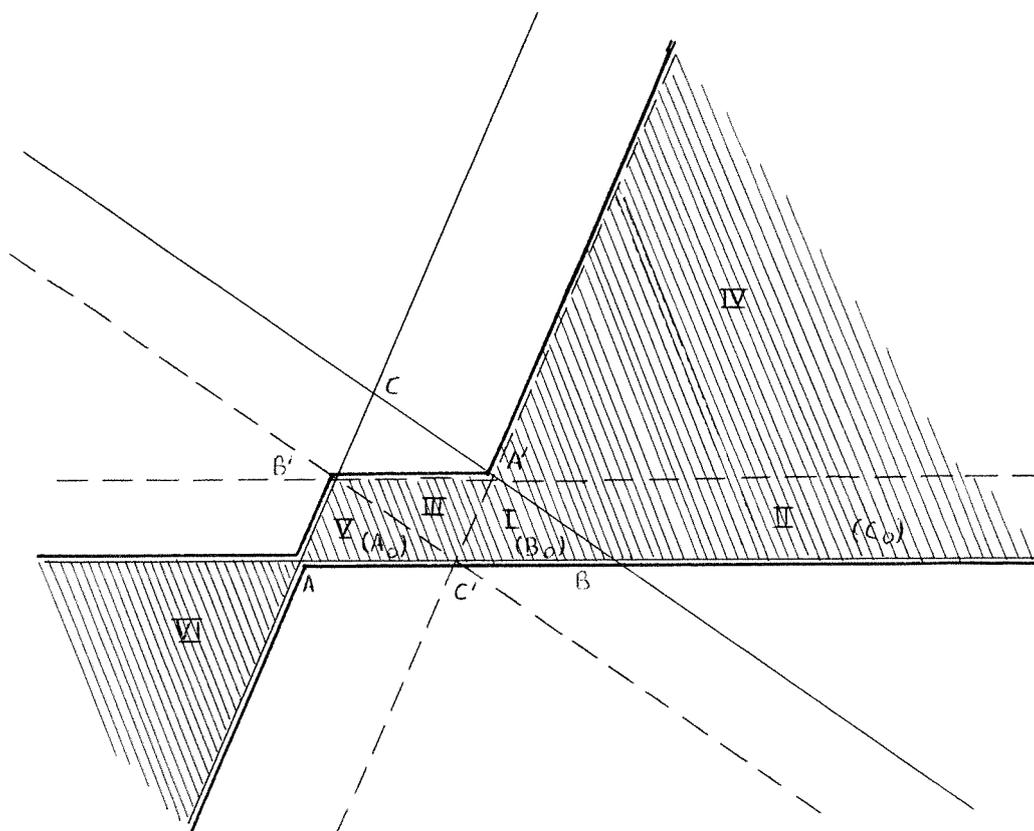


Ainsi qu'on le voit les configurations V et VI sont des cas d'**hyperboles** : hyperbole dont une branche est tangente à deux côtés et l'autre au troisième côté dans V, tandis qu'en VI les trois côtés sont tangents à la même branche.

Ces différentes configurations ont été établies, pour  $O$  donné, en fonction de la disposition du côté  $BC$  (on s'est limité ici au secteur délimité par les demi-droites  $AB$  et  $AC$  et à son opposé). Il faut les traduire par un régionnement du plan en fonction de la position du point  $O$  par rapport au triangle  $ABC$ .

On voit que les conditions d'intersection font intervenir les trois droites  $A'B'$ ,  $B'C'$  et  $C'A'$  joignant les milieux des côtés du triangle  $ABC$ . Ainsi, dans la configuration I,  $O$  est en dessous de  $A'B'$  et à droite de  $A'C'$ , donc intérieur au triangle  $BA'C'$ . Les autres cas se verront facilement de façon analogue. On obtient alors dans le plan un régionnement figuré ci-dessous, regroupant dans la

portion de plan limitée par un surlignage les zones précédemment dénommées (voir fin du (2)) :  $Ei, Ea, Ha, Ha'_1, Hb'_1, Hb'_2$ . En permutant  $A, B, C$  de toutes les façons possibles, on obtient (grâce aux zones communes à deux ou plusieurs découpages) un recouvrement complet du plan, reproduisant finalement le zonage exposé à la fin de la partie (2).



Par exemple, en laissant  $A$  fixe et en échangeant  $B$  et  $C$  on obtient les zones  $Ei, Ea, Ha, Ha'_1, Hc'_1, Hc'_2$  et ainsi de suite.

On ne reviendra pas sur ce qui se passe lorsque  $O$  est choisi sur l'un des côtés du triangle mais la géométrie ne nous dit rien sur la dégénérescence de la conique lorsque  $O$  est choisi sur l'une des droites joignant les milieux des côtés du triangle  $ABC$ .

A PROPOS D'UN LIVRE RÉCENT

# **Géométrie projective**

Jean-Claude Sidler

*Cours, problèmes classiques  
et exercices résolus*

**InterEditions**

Le petit livre de J.-C. Sidler, intitulé tout simplement “Géométrie projective” séduit rien qu’au premier coup d’œil : en effet, bien servi par une excellente mise en page, il abonde en illustrations de toutes sortes allant à l’encontre d’une pratique bizarre et triste des années 1960-70 où l’on bannissait les figures en géométrie. Evidemment ce n’est pas le seul mérite de ce livre. En fait, ce qui frappe le plus à la lecture de l’ouvrage c’est la clarté, l’aisance et surtout le souci constant de l’auteur à vouloir transmettre son savoir comme son savoir-faire acquis au cours d’une longue pratique sous forme de cours, T.D. etc... dans l’enseignement de la géométrie à l’Université comme à l’I.R.E.M. de Strasbourg.

Indiquons brièvement l’organisation du livre qui est divisé approximativement en deux parties de longueur équilibrée.

Dans une première partie théorique, l’auteur expose les fondements et les principaux résultats de la géométrie projective : nous y trouvons outre les généralités sur les espaces projectifs

- les homographies d’une droite projective,
- les groupes d’homographies d’une droite projective,
- les homographies du plan projectif,
- les homographies et les coniques,
- les faisceaux de coniques

ainsi que les grands théorèmes qui ont pour nom Pappus, Désargues, Pascal, Frégier etc...

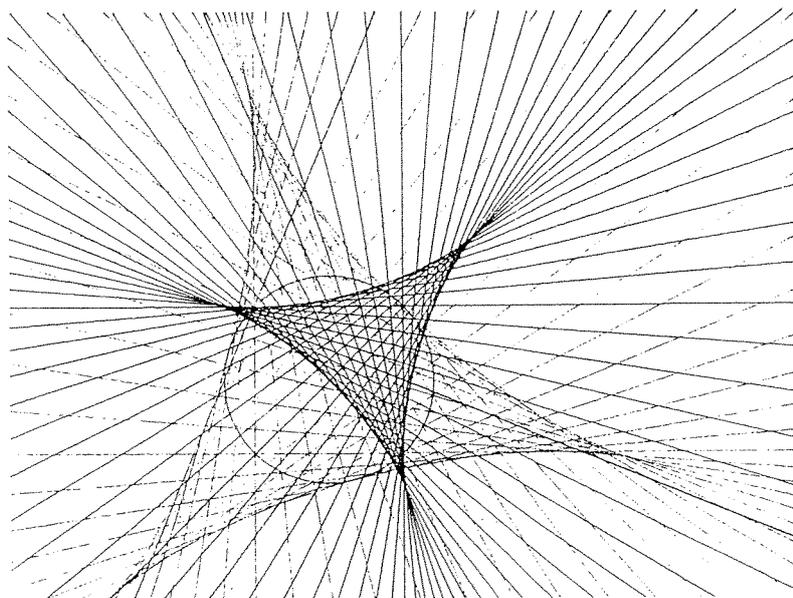
---

© L’OUVERT 74 (1994)

Dans cette partie rédigée avec élégance et naturel, d'une manière résolument moderne, louons l'auteur de nous avoir épargné les constructions absconses et les notations obscures si ennuyeuses pour les commençants. Mais ce n'est pas tout, car j'ai particulièrement aimé la résolution avec laquelle J.-C. Sidler introduit la **dualité** (ou comme dit très justement l'auteur le miracle de la dualité) si déroutante : tout simplement au début. C'est la façon la plus efficace pour s'imprégner de l'essence même de la géométrie projective et de ses méthodes. Rappelons que les géomètres qui vinrent à la suite de Gergonne furent particulièrement émerveillés face au principe de dualité, comme on disait alors, puisqu'il illumine bien des propriétés de la géométrie projective. Pour finir sur la présentation de la première partie, indiquons que chaque chapitre est accompagné d'une batterie d'exercices dont le corrigé se trouve en fin de livre afin de permettre au lecteur assidu de contrôler son savoir-faire.

Quant à la seconde partie, elle met en œuvre les acquis de la première partie : elle consiste en exercices de référence et problèmes classiques tous corrigés d'une manière courte et précise. On notera en passant que le classicisme n'a pas empêché la variété et l'intérêt des thèmes proposés. On reconnaît ici tout le talent de l'auteur soucieux du but qu'il s'est fixé, à savoir faire aimer la géométrie . . . Sur ce dernier point, la réussite est complète!

Concluons rapidement que cet ouvrage très utile permettra à tout lecteur d'acquérir une base et une pratique solide de la géométrie projective avant d'aborder des théories plus complexes situées hors du champ prévu par J.-C. Sidler. C'est pourquoi ce livre est particulièrement bien venu et devrait combler les étudiants (CAPES et Agrégation), les enseignants des lycées qui ont envie de se ressourcer, comme . . . les grosses bêtes de l'Université. Le mot de la fin, je le laisse à G. Reeb, préfacier du livre : "La beauté de l'art du géomètre n'occulte d'aucune manière l'utilité et l'actualité de cet art".



P. Girault

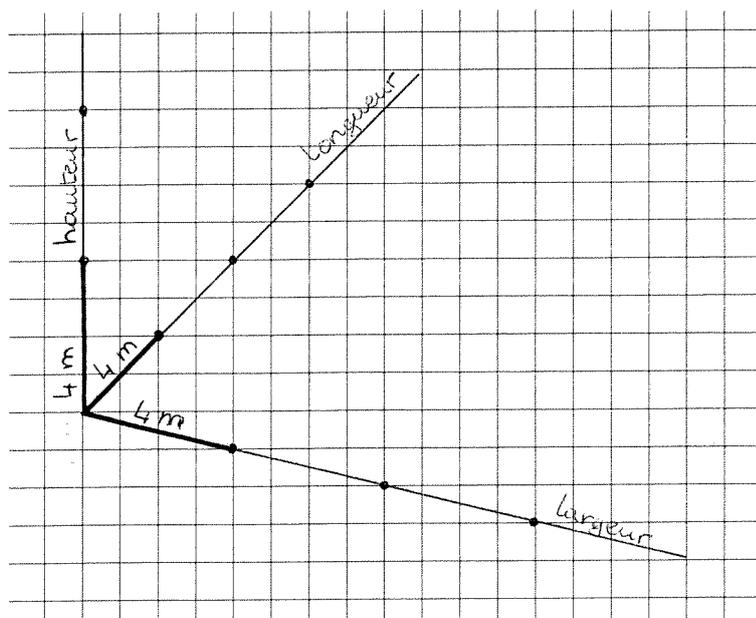
*Enveloppe des axes des paraboles inscrites dans un triangle*

## MATHÉMATIQUES DANS NOS CLASSES

Nous publions ici une activité que Monsieur André Martz, professeur au Lycée Jean Monnet de Strasbourg, a proposé à ses élèves de Seconde (en octobre et novembre) pendant des heures où la classe était séparée en groupes. Les instructions et explications fournies aux élèves ne sont pas détaillées dans ce document mais quelques remarques sont données, qui permettent de situer ce travail par rapport à une étude de la géométrie dans l'espace en Seconde. Cette activité se décompose en deux parties.

### Etude 1

Nous voulons construire une représentation d'une église et des instructions seront données au fur et à mesure de sa réalisation. Pour cela nous disposons de papier quadrillé, d'un crayon, d'une gomme et d'une règle. Les directions principales et unités sont indiquées sur la figure suivante :



Une première idée sur le repérage dans l'espace.

#### 1. Fondations : rectangle

- de largeur 12 m
- de longueur 16 m.

#### 2. Murs :

- hauteur 9 m.

3. Toit : à deux pans égaux, le faîte étant placé selon la longueur à 2,5 m au dessus du plafond.

Des commentaires relatifs aux règles

de la perspective cavalière

- conservation du parallélisme
- conservation du rapport des distances sur toute droite

...

On peut alors citer le "théorème du toit".

**4. Tour :** une tour à base carrée  $4\text{ m} \times 4\text{ m}$  est accolée à la façade avant en position centrale; elle a 18 m de hauteur.

La tour est surmontée d'un toit en forme de pyramide à quatre pans dont le sommet se trouve à 2 m du centre du plafond de la tour.

Ce toit est surmonté d'une croix dont la vue de face se présente comme suit :

**5. Ouvertures :**

- Porte : sur la façade avant de la tour dont la vue de face se présente comme suit :

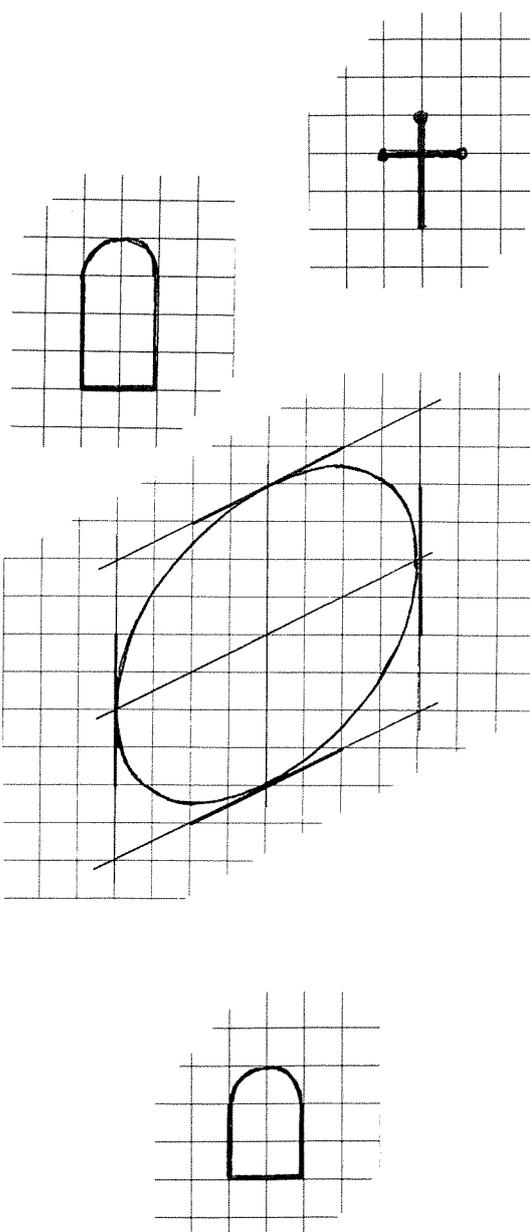
Pour dessiner un cercle en perspective nous pouvons "penser aux tangentes"

- Fenêtres : de manière harmonieuse, à 3 m du sol, deux fenêtres sur la façade avant de part et d'autre de la tour et quatre fenêtres sur la longueur, de même forme et de même dimension que la porte.

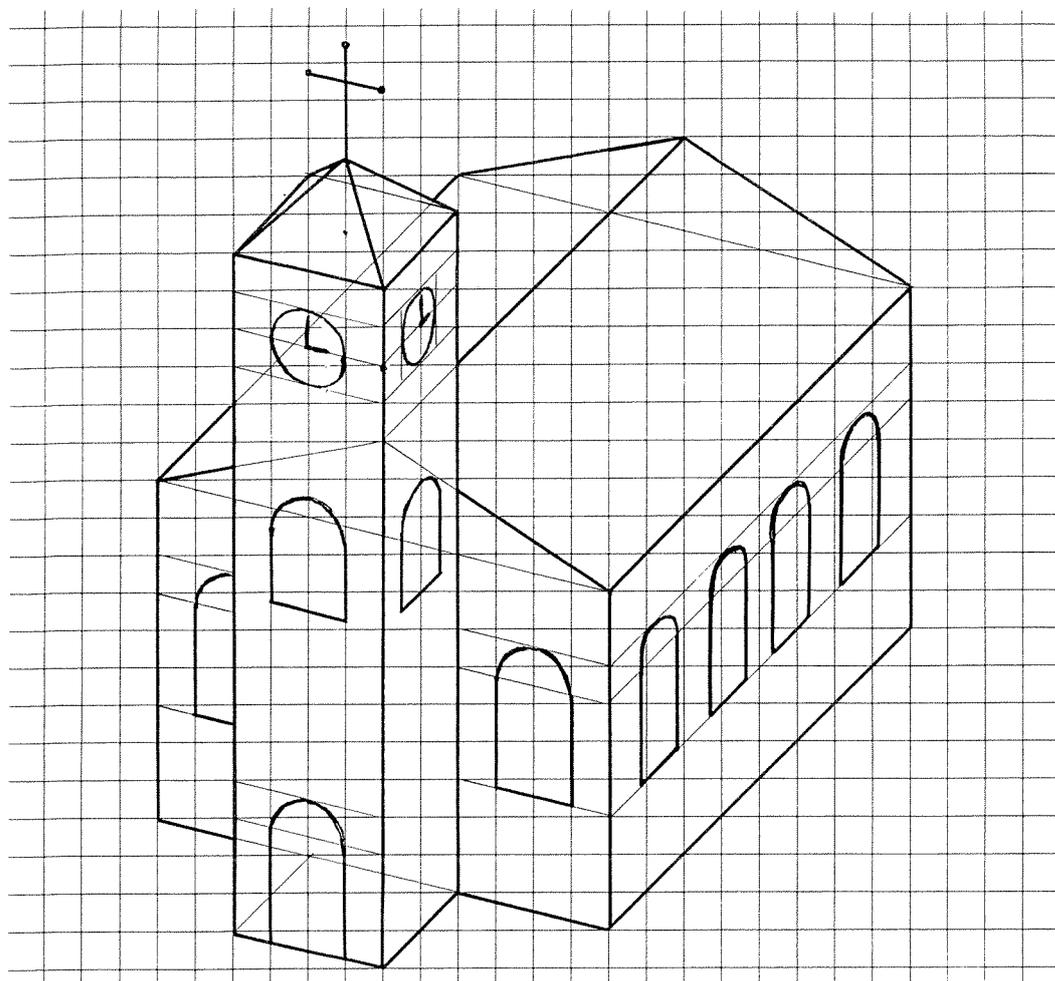
- Sur la tour deux ouvertures visibles de la forme ci-contre à 9 m du sol.

**6. Horloge :**

Sur chaque face de la tour, à 1 m sous son plafond, se trouve le cadran circulaire d'une horloge de 1 m de rayon. Il est 15 heures.

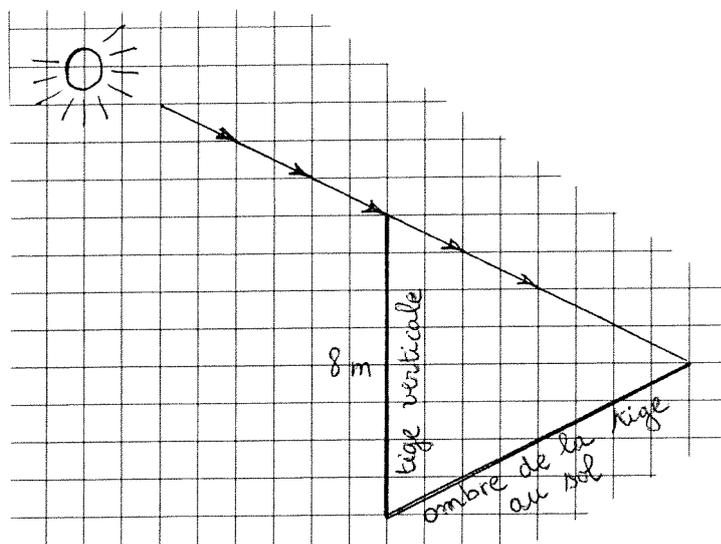


Voilà ce à quoi on devrait aboutir.



### Etude 2

**Ombres :** La direction des rayons de soleil et l'ombre projetée au sol d'une tige verticale sont données par la figure suivante :

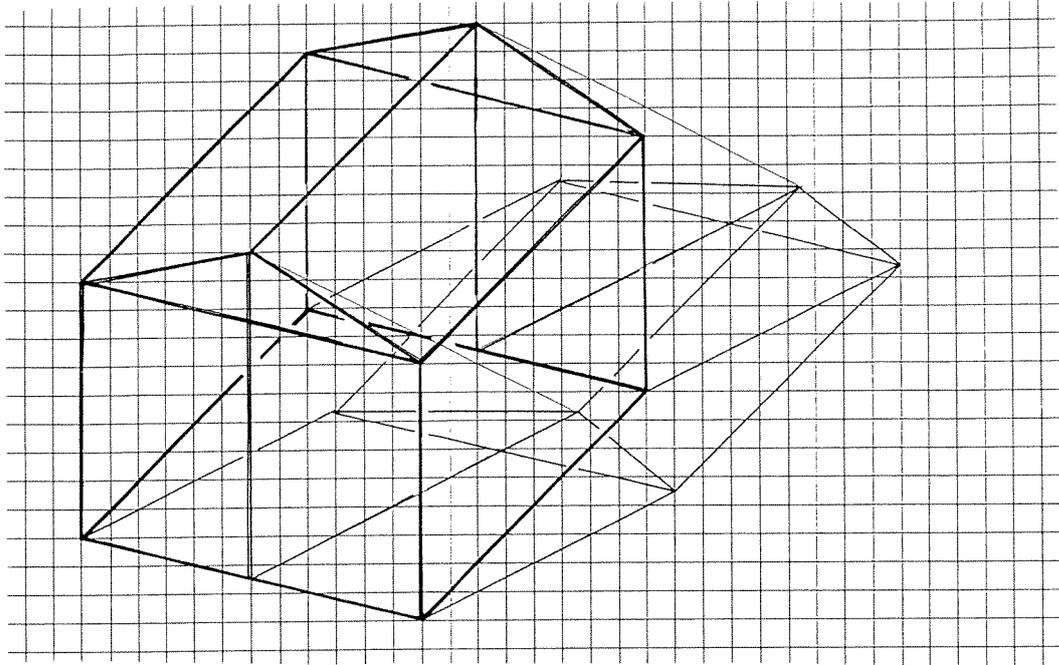


La construction de l'ombre permet d'introduire la notion de projection sur un plan suivant une direction de droite et de découvrir ses principales propriétés :

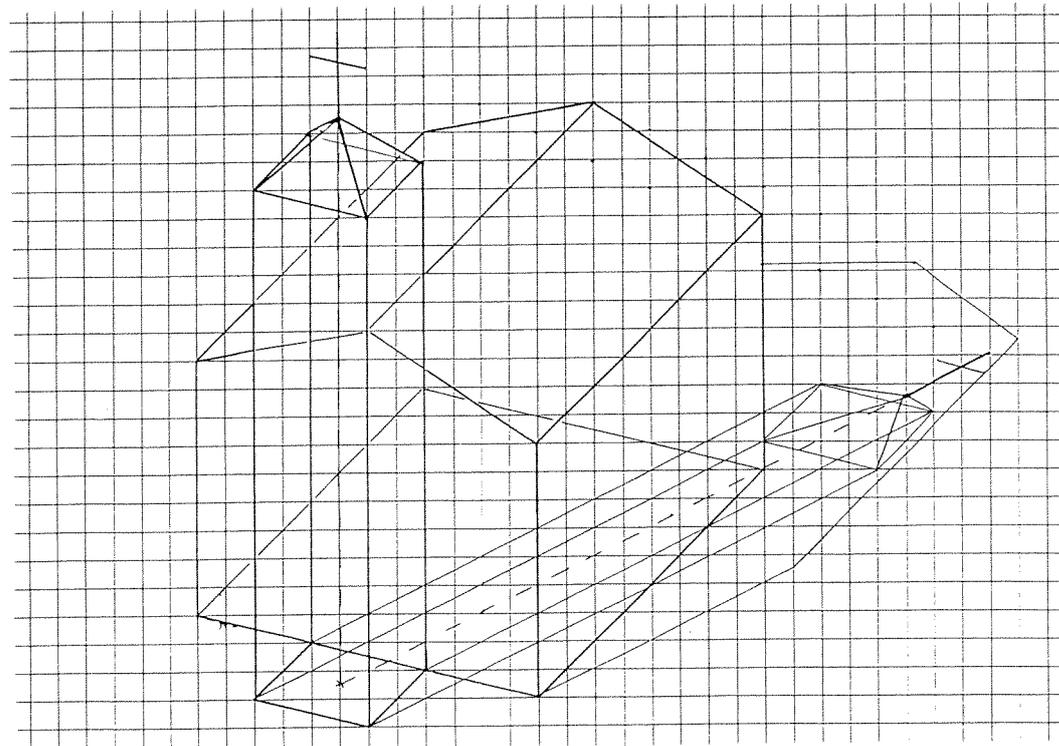
- conservation du parallélisme,
- conservation du rapport des distances.

MATHÉMATIQUES DANS NOS CLASSES

1. La construction de l'église est reprise sans ouvertures.  
Elle est supposée en "fil de fer".  
Dans une première étape on construit l'ombre au sol de la "carcasse en fil de fer".

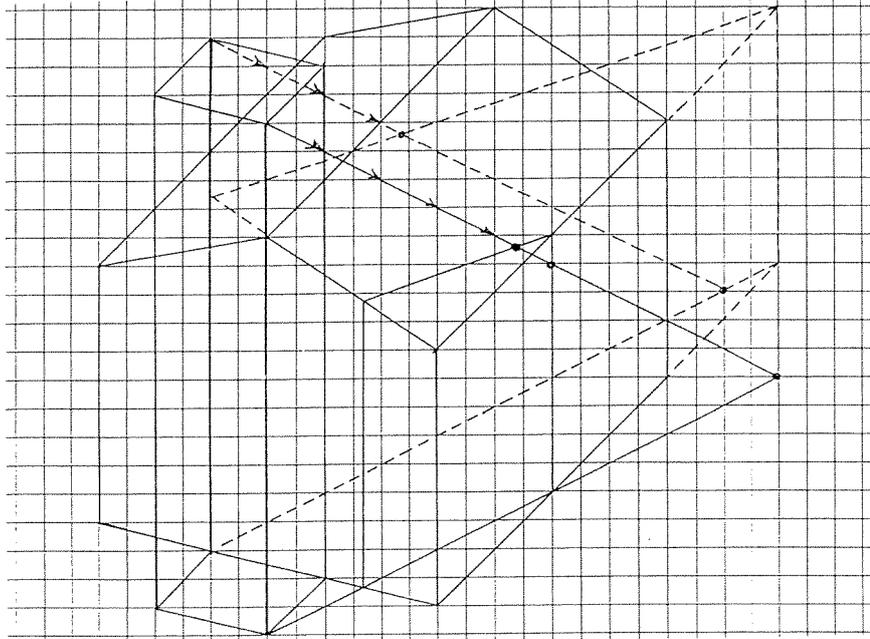


- La construction de l'ombre des tiges verticales suffit.  
On peut trouver "des raccourcis" liés aux propriétés des projections.  
On y ajoute l'ombre de la tour.



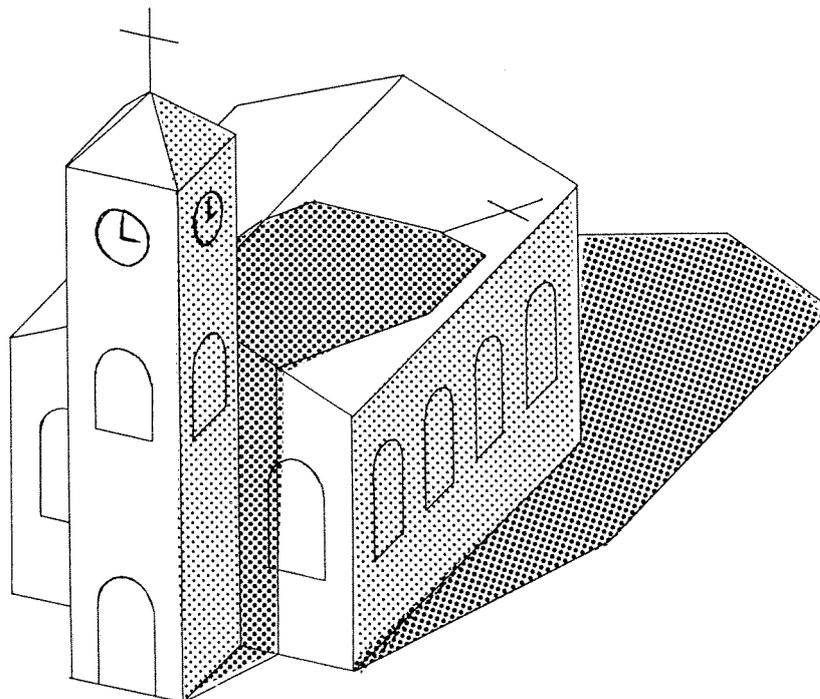
## MATHÉMATIQUES DANS NOS CLASSES

2. Après avoir construit l'ombre au sol de la tour on se rend compte qu'en fait cette ombre tombe sur la façade avant et pour la plus grande partie sur le pan droit du toit. Pour la construire on peut considérer les sections du bâtiment par des plans projetant les tiges verticales. Les rayons du soleil font le reste... C'est cette partie qui demande le plus d'explications quant aux règles d'incidence mais c'est aussi celle qui développe le plus la faculté de voir dans l'espace.



Pour la clarté de la figure, seules les ombres de deux tiges verticales de la tour ont été construites.

Et pour finir



## PROBLÈMES POUR NOS ÉLÈVES (...et leurs professeurs)

Il s'agit, dans cette rubrique, de présenter des problèmes historiques ou classiques, dont la solution ne requiert pas d'autres connaissances que celles enseignées au lycée (voire au collège) et qui par conséquent, peuvent faire l'objet de travaux dans nos classes.

Dans ce numéro nous proposons les énoncés de la compétition Georg Mohr proposée aux lycéens du Danemark de la série mathématique le 4 février 1993, de 9 h à 13 h.

### PROBLÈME 4

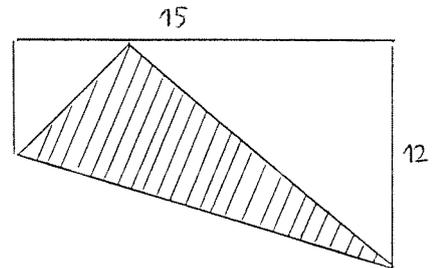
4.1) Trois amis A, B, C ont 120 couronnes ensemble.

A donne à B autant que B possède déjà. Puis B donne à C autant que C possède déjà. Enfin C donne à A autant que C possède déjà. Après ces échanges A, B et C ont autant d'argent.

Combien avaient-ils au début ?

4.2) Un coin est plié comme indiqué sur la figure ci-contre.

Déterminer l'aire de la zone hachurée.

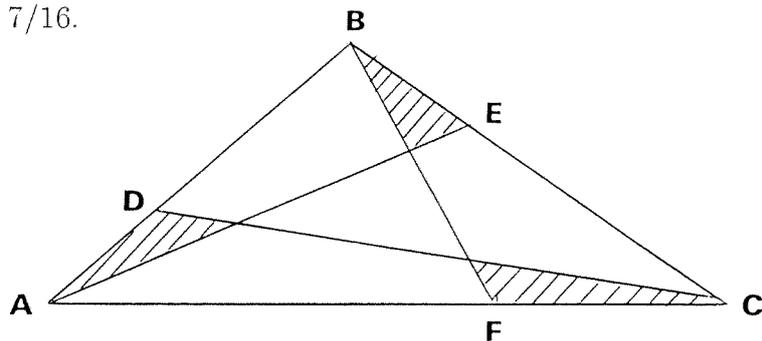


4.3) Résoudre dans  $\mathbb{R}^2$  le système :

$$\begin{cases} x^2 + y^2 = 1 \\ x^6 + y^6 = 7/16. \end{cases}$$

4.4) Dans le triangle  $ABC$ ,  $D$ ,  $E$  et  $F$  partagent les côtés respectifs au  $1/3$ .

Montrer que la somme des trois aires hachurées est égale à l'aire du triangle central.



4.5) Dans une boîte il y a des chaussettes. Certaines sont rouges; les autres sont bleues. Le nombre total de chaussettes est inférieur ou égal à 1993. La probabilité de tirer deux chaussettes de même couleur au hasard est  $1/2$ .

Quel est le plus grand nombre possible de chaussettes rouges dans la boîte ?

G. MOHR

# EUCLIDES DANICUS,

Bestaande udi To Deele.

Den Første Deel : Handler udaf de Sex  
Første / EUCLIDIS Bøger / de der udi begreffe  
Maalkunstige Werckstycker.

Den Anden Deel : Giffver anledning At=  
stillige Werckstycker at giøre / som Skæring / Røring / Deeling /  
Skinbar Legenkonst oc Soole-vijsere. Allerniste med  
en Cirkel (Foruden Linial at bruge) med Skæ-  
reller af Runder.

Forestillet.

Af

Georg Mohr.



Prentet i Amsterdam af Jacob van Velsen.  
For Authore, Aar 1672.

Ceci est un exemple rare pour l'époque d'ouvrage de géométrie en langue vernaculaire, où l'auteur prétend réaliser les constructions d'Euclide avec seulement un compas sans règle.

A l'automne 1927, un étudiant à l'université du nom de Victor Beck a trouvé chez un bouquiniste de Copenhague un livre "Euclides Danicus", écrit en hollandais par Georg Mohr, et imprimé à Amsterdam en 1672. Beck demanda à son professeur, Johannes Hjelmslev, son opinion sur son contenu, car Beck lui-même n'était pas capable de le lire. Hjelmslev s'aperçut immédiatement que c'était une découverte sensationnelle, pour l'auteur de l'époque, 125 ans avant Mascheroni, d'avoir prouvé de la façon la plus élégante que toutes les constructions d'Euclide pouvaient être réalisées avec un compas, sans utiliser de règle.

Il fut découvert que le livre se trouvait à la bibliothèque royale de Copenhague (en plusieurs exemplaires), à la bibliothèque universitaire, etc... Il existait dans une version danoise (l'originale) aussi bien qu'en hollandais. Bien qu'il fut mentionné dans de nombreuses bibliographies (par exemple celle de Nielsen Niels : "Matematiken i Danmark" 1528-1800, Copenhague 1912), il est évident que personne n'a réalisé son importance et il a été faussement décrit comme une traduction ou une compilation d'Euclide. C'était par conséquent une chance de redécouvrir ce livre. Un fac similé de l'édition était publié par la société royale danoise des sciences avec une traduction allemande de J. Pal. De nos jours la priorité de Mohr par rapport à ces constructions est généralement admise.

Le seul fait connu sur Georg Mohr tout d'abord était qu'il était né à Copenhague, le 1er avril 1640. En 1931 Hjelmslev, cependant, était capable de donner une biographie plus détaillée. La famille de Georg Mohr était originaire d'Ecosse. Son père était nommé Mohrendal et dans les dernières années, en Allemagne, Mohr écrit son nom sous la forme allemande Mohrenthal. Il montra tôt un intérêt pour les mathématiques. Nous ne savons pas s'il essaya ou non de cultiver son intérêt à l'université de Copenhague. Mais en 1662 il vint en Hollande pour étudier la philosophie et les mathématiques dans les cercles de Huyghens et de Spinoza à la fameuse université de Leiden où il évoluait. Il s'adapta bien, apprit la langue. Il prit une part active dans le conflit franco-hollandais de 1672-78 et fût fait prisonnier des troupes françaises – une période qui affecta sa santé. En Hollande, Mohr rencontra E. W. Tschirnhaus; ils devinrent amis et voyagèrent ensemble en Angleterre et en France où ils firent la connaissance de Leibniz. De ses correspondances (voir Hjelmslev, Arthur E : Beiträge zur Lebensbeschreibung von Georg Mohr. Mat. fys. Madd. Kgl. Danske Vid. Selsk, Vol. 2 : 4, 1931, pp. 1-21) on retire l'impression d'un solide mathématicien qui avait des contacts avec les plus importants collègues de sa génération.

Aux environs de 1681, Mohr retourna à Copenhague. Le roi, Christian V, lui offrit un poste de superviseur de la société royale de construction de bateaux mais Mohr ne voulait pas abandonner sa vie libre de mathématicien et de philosophe. Dans une lettre à Tschirnhaus il montre une grande surprise sur son mariage tardif. Cependant Mohr lui-même se maria en 1687, et vint avec sa femme en Hollande. En 1695 Mohr accepta, après de prudentes considérations, une offre de Tschirnhaus comme collaborateur à son Musée à Kieslingwalde, en Allemagne, et il y mourut le 26 janvier 1697.

En 1938 le mathématicien hollandais J. H. Schogt dans un article attira l'attention sur une petite publication anonyme "compendium Euclidis curiosis" qui est en possession de la librairie universitaire d'Amsterdam. Ce traité était imprimé à Amsterdam en 1673 et était relié avec la copie hollandaise de "Euclides Danicus". Il traite de constructions à l'aide d'un compas fixe (une fourche) et d'une règle, et l'auteur prouve que toutes les constructions d'Euclide peuvent être réalisées avec ces moyens réduits. Dans la préface l'auteur fait référence au "Euclides Danicus" de Georg Mohr. Ainsi ce travail n'a pas été immédiatement oublié. Maintenant nous savons que Mohr est l'auteur, grâce à une lettre de John Collins (1625-83) à James Gregory (1638-75) datée du 4 septembre 1675. Faisant référence à une visite chez Tschirnhaus, Collins écrit : "...là étaient présents avec lui un danois nommé Georg Mohr qui publia plus tard en hollandais deux petits livres dont l'un, intitulé "Euclides Danicus", prétendait réaliser les constructions de tous les problèmes d'Euclide avec seulement un compas sans règle, et l'autre intitulé "Euclides Curiosus", où avec une règle et une fourche compas à ouverture fixe, il réalisait la même chose..."

Dans le "Danicus" vous devez admirer les solutions élégantes de Mohr. Vous devez vous demander pourquoi le "Curiosus" apparut anonymement alors que le "Danicus" apparut sous le nom de Mohr, avec une dédicace soumise au roi danois, Christian V. Sans aucun doute Mohr savait que les constructions du "Curiosus" étaient réalisées par d'autres alors que les idées du "Danicus" étaient nouvelles. Ainsi considère-t-il, avec justesse, ce travail comme de plus grande valeur et plus original que le "Curiosus".

Un fils de Mohr a écrit une biographie de son père. Il nous dit que Georg Mohr avait écrit trois livres qui furent accueillis avec une satisfaction générale par les érudits. Maintenant nous en connaissons deux, mais une lettre de Collins à Gregory datée du 19 octobre 1675 nous révèle que le sujet de ce troisième livre était sans doute des solutions d'équations du 3ième degré etc... Il serait intéressant de découvrir ce traité de Georg Mohr...

#### **Oeuvres connues de Georg Mohr :**

- 1) Euclides Danicus, Amsterdam 1672. Fac simile, Kobenhavn 1928, 36 pp. + 3 plates (Preface by J. Hjelmolev).
- 2) Compendium Euclidis Curiosi, Amsterdam 1673, 24 pp. + 1 plate (english translation by Joseph Moscon, London 1677, 6 + 26 pp. + 1 plate).

Cet article est constitué d'extraits d'une introduction en anglais de Henrik Meyer, en novembre 1982, à une édition par la fondation Georg Mohr du "Compendium Euclidis Curiosi". La traduction a été assurée par Richard Cabassut.

## A VOS STYLOS

### PROBLÈME 26

#### Énoncé (proposé par R. Iss, d'Embrun)

Etant donnés  $n$  points distincts sur un cercle, on trace un polygone ayant ces points pour sommets. On suppose que  $p$  couples de côtés, et  $p$  seulement, ont un point commun autre qu'un sommet, et qu'aucun triplet de côtés n'a de point commun.

- 1) Ce polygone partage l'intérieur du cercle en  $r$  régions. Calculer  $r$  en fonction de  $n$  et de  $p$ .
- 2) Pour un nombre  $n$  donné de côtés, déterminer la valeur maximum du nombre  $p$  des points d'intersection des côtés.

**Solution** (adaptée de celle de l'auteur). Les deux questions sont indépendantes.

#### Première question

Le résultat est  $r = n + p + 1$ . Il peut se vérifier par récurrence sur  $n$  (en le démontrant non seulement pour des polygones, mais, plus généralement, pour des lignes polygonales non nécessairement fermées) ou directement, en appliquant la formule d'Euler.

#### Deuxième question

Le nombre de côtés qui coupent un côté donné est au maximum  $n - 3$  (les trois qui ne peuvent pas le couper étant lui-même et les deux côtés qui ont avec lui un sommet commun). Nous dirons qu'un côté est **maximal** s'il est coupé par  $n - 3$  autres côtés.

a) Cas où  $n$  est impair : posons  $n = 2k + 1$ . En joignant de  $k$  en  $k$  les  $n$  sommets placés sur le cercle, on obtient, puisque  $n$  et  $k$  sont premiers entre eux, un polygone étoilé dont chaque côté est maximal. Ceci donne pour  $p$  la plus grande valeur possible,  $p = \frac{1}{2}n(n - 3)$ .

b) Cas où  $n$  est pair. Remarquons d'abord que, si un côté  $AB$  est maximal, les deux côtés consécutifs à  $AB$  sont placés de part et d'autre de la droite  $AB$  et chacun des deux arcs limités par  $A$  et  $B$  porte la moitié des  $n - 2$  sommets autres que  $A$  et  $B$  (car ces  $n - 2$  sommets, pris successivement sur le polygone, doivent être alternativement de part et d'autre de  $AB$ ). Il en résulte que **si  $AB$  et  $CD$  sont deux côtés maximaux distincts, leurs extrémités  $A$  et  $C$  (ou  $A$  et  $D$ ) sont deux sommets consécutifs sur le cercle** (en d'autres termes, si les  $n$  sommets sont régulièrement espacés sur le cercle,  $AB$  et  $CD$  sont deux diamètres faisant entre eux un angle de  $2\pi/n$ ).

En effet, les points  $A, B, C$  et  $D$  divisent le cercle en quatre arcs  $\widehat{AC}, \widehat{CB}, \widehat{BD}$  et  $\widehat{DA}$ . Si un sommet  $E$  se trouve sur  $AC$  par exemple, les seuls trajets possibles à

partir de  $E$  pour le polygone sont  $EF, EBAF, EDCF, EBADCF$  ou  $EDCBAF$ ,  $F$  étant un point de  $\widehat{BD}$  (les autres trajets sont interdits par la double contrainte que chaque côté non consécutif à un côté maximal le rencontre et que les deux côtés consécutifs à un côté maximal soient de part et d'autre); donc le premier sommet après  $E$ , autre que  $A, B, C$  ou  $D$  est sur l'arc  $\widehat{BD}$ . De proche en proche, tous les sommets sont sur  $\widehat{AC}$  et  $\widehat{BD}$ , et les points  $A$  et  $D$  sont consécutifs sur le cercle.

En conséquence, le polygone a au plus deux côtés maximaux, puisque trois droites du plan ne peuvent faire deux à deux des angles de  $2\pi/n$  (cet argument est en défaut pour  $n = 6$ , mais le résultat subsiste : cela se vérifie par inspection directe). Tous les côtés, sauf peut-être deux, rencontrent au plus  $n - 4$  autres côtés. Ceci établit la majoration

$$p \leq \frac{1}{2}[2(n-3) + (n-2)(n-4)] = \frac{1}{2}(n^2 - 4n + 2).$$

Cette valeur est le maximum cherché, puisqu'elle est atteinte pour le polygone obtenu de la façon suivante : numérotions consécutivement les  $n$  sommets sur le cercle et joignons chaque sommet  $i$  à  $i + \frac{n}{2} + 1$  et  $i + \frac{n}{2} - 1$  (modulo  $n$ ). Ceci fournit un polygone étoilé si  $\frac{n}{2}$  est pair ou deux polygones étoilés si  $\frac{n}{2}$  est impair, chaque côté étant coupé par exactement  $n - 4$  autres. Effaçons les côtés joignant 1 à  $\frac{n}{2}$  et  $\frac{n}{2} + 1$  à  $n$ ; joignons 1 à  $\frac{n}{2} + 1$  et  $\frac{n}{2}$  à  $n$ . On obtient un polygone, dans lequel les deux nouveaux côtés sont maximaux, les  $n - 2$  autres continuant à être chacun coupé par  $n - 4$  côtés.

---

### PROBLÈME 27

#### Énoncé

Soient  $\alpha$  et  $x_0$  des nombres strictement positifs. On définit une suite  $(x_n)_{n \in \mathbb{N}}$  par

$$x_{n+1} = x_n + \frac{\alpha}{x_n}.$$

Donner un équivalent de  $x_n$  quand  $n$  tend vers l'infini.

#### Indication

$$x_n \sim \sqrt{2\alpha n}.$$

---

### PROBLÈME 28

#### Énoncé

Etant donné un ensemble fini  $S$  à  $n$  éléments (sommets) et l'ensemble  $A$  des parties de  $S$  à deux éléments (arêtes), trouver l'effectif maximal d'une partie  $G$  de  $A$  telle que, pour tous  $x, y$  et  $z$  de  $S$ ,

$$\{x, y\} \in G \text{ et } \{y, z\} \in G \implies \{x, z\} \notin G.$$

A VOS STYLOS

Autrement dit, exprimer, en fonction du nombre  $n$  de sommets, le nombre maximal d'arêtes d'un graphe sans triangle.

PROBLÈME 29

Vrai ou faux ? Toute suite de 100 nombres deux-à-deux distincts contient une sous-suite croissante de longueur 10 ou une sous-suite décroissante de longueur 12.

Vente au Numéro & Abonnements

Publiée par les Instituts universitaires de Recherche sur l'Enseignement des Mathématiques sous le patronage de l'ADIREM (Assemblée des Directeurs d'Irem), la revue « **Repères - IREM** » est un bulletin trimestriel s'adressant à tous les professeurs, et plus particulièrement aux enseignants des Collèges, des Lycées, des Lycées Professionnels, ou des Universités. Son but est de tenir chacun informé des questions actuelles, qu'elles aient trait aux grands débats du moment ou plus simplement aux applications concrètes, pour les classes, de la réflexion menée en commun entre praticiens et chercheurs. Elle est donc destinée à devenir un outil indispensable aussi bien aux professeurs de mathématiques qu'aux formateurs spécialisés ; ainsi qu'à tous ceux qui sont concernés par la pédagogie ou les Sciences de l'Education.

Elle se doit de figurer dans tout Centre de Documentation et d'Information ...

**prix du numéro** : 70 F ( + frais d'expédition si envoi par avion )

**abonnements** ( quatre numéros par an )

— Etablissements : 250 F — Particuliers : 200 F

Envoi par avion ( DOM - TOM ou Etranger )

— Etablissements : 330 F — Particuliers : 280 F



Bulletin d'abonnement à renvoyer à :

TŌPIQUES éditions, 24 rue du 26<sup>e</sup> B.C.P., 54700 PONT-À-MOUSSON  
accompagné du règlement par chèque ou d'un bon de commande officiel.

Nom : .....

en capitales svp

Adresse : .....

Code postal et Ville : .....

Ci-joint la somme de : .....

Mode de règlement :

- Chèque bancaire       Chèque postal  
 Virement administratif sur facture

Numéro souhaité pour  
débuter l'abonnement : .....

(en cas d'impossibilité, l'abonnement  
débuté au dernier numéro disponible)

**Repères - IREM**  
revue des Instituts de Recherche sur  
l'Enseignement des Mathématiques