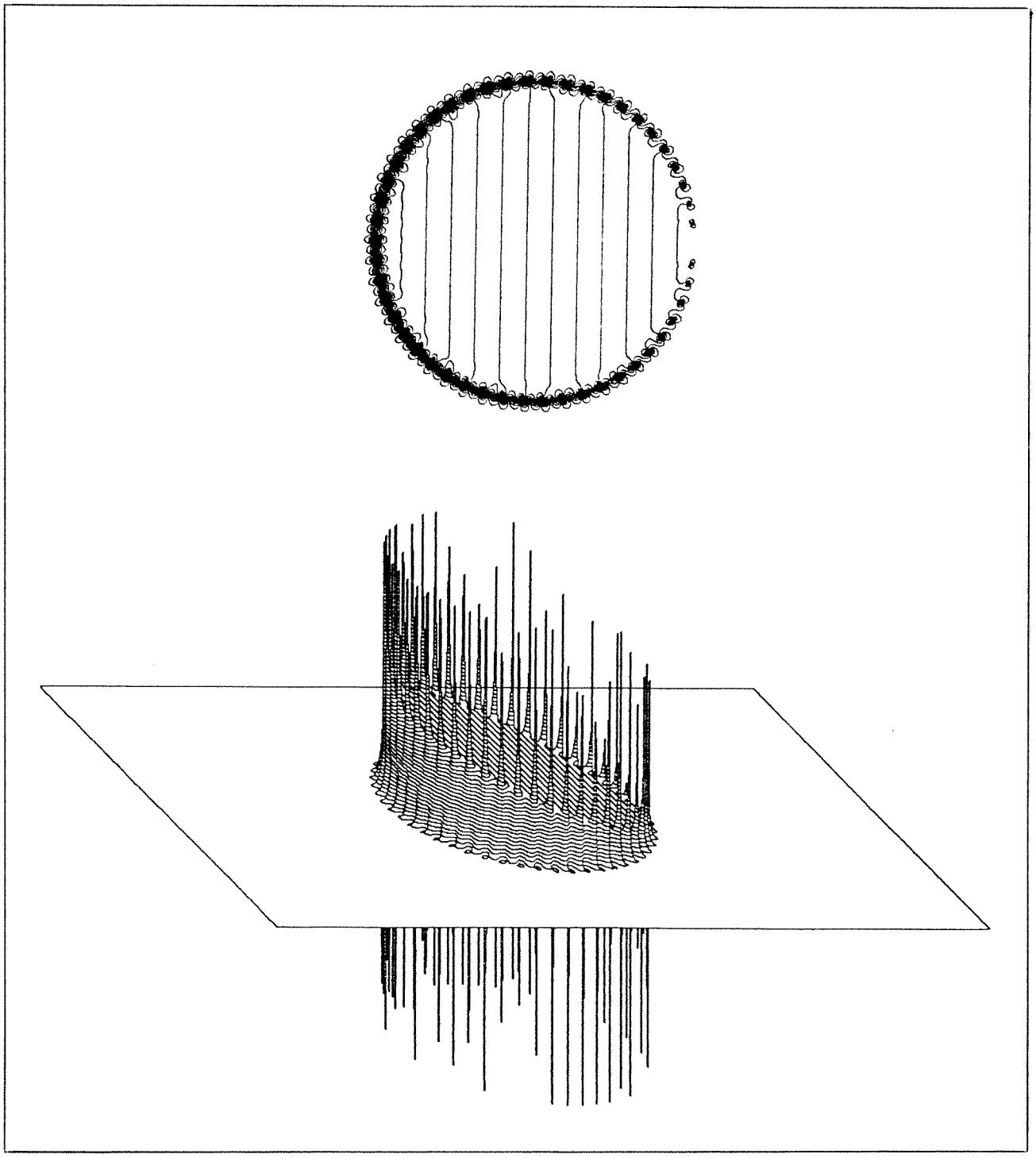
# L'OUVERT

JOURNAL DE L'A.P.M.E.P. D'ALSACE ET DE L'I.R.E.M. DE STRASBOURG
n° 75 – JUIN 1994 I.S.S.N. 0290 - 0068



NOTRE COUVERTURE :

COURBES DE NIVEAU

Courbes de niveau de la partie réelle de $\frac{1}{P_{50}(z)}$ avec $P_n(z) = \Sigma_{k=0}^{n} z^k$ en vue de dessus et en perspective cavalière.

$$-3 < Re(z) < 3\ ;\ -2 < Im(z) < 2\ ;\ -5 < Re\Big(\frac{1}{P_{50}(z)}\Big) < 5.$$

On constate qu'à l'intérieur du disque de rayon 1, $P_n$ est proche de la somme infinie $\Sigma_{k=0}^{\infty} z^k = \frac{1}{1-z}$ alors qu'en-dehors du disque ce polynôme prend des valeurs infiniment grandes. La transition se fait de façon particulièrement mouvementée. Cela illustre la propriété des fonctions analytiques non standard d'avoir deux comportements bien marqués : dans certaines régions elles sont bien régulières, dans d'autres (ici sur le cercle de convergence) elles sont très irrégulières.

# NOS ÉLÈVES SORTANT DE CLASSE TERMINALE SONT-ILS PRÊTS POUR L'UNIVERSITÉ?

De toutes époques, il y a eu, pour l'élève passant du lycée à l'université, un certain nombre de difficultés. Aujourd'hui, dans le Deug sciences filière mathématiques, nous constatons qu'il y a plus que jamais un fossé entre ce que les enseignants exigent et ce que les nombreux étudiants arrivent à faire. Il ne s'agit pas ici de se plaindre que les "forts en math" aient préféré aller en classes préparatoires, mais d'examiner quelques causes de difficultés pour nos étudiants.

Un premier aspect tient à l'organisation de l'enseignement universitaire :

– Le cours magistral : prendre convenablement des notes dans un amphi rempli et parfois bruyant n'est pas simple, surtout lorsqu'on n'en a jamais fait l'expérience. La phase qui consiste, après le cours à reprendre, mettre en ordre et compléter ses notes, est toute nouvelle et n'est pas toujours effectuée.

– Les travaux dirigés : contrairement à la classe de terminale, où l'élève avait un professeur consciencieux qui faisait le cours, le commentait, proposait une batterie d'exercices et insistait jusqu'à ce que tout le monde ait compris, la séance de T.D. a pour vocation de faire des **applications** du cours. Cela suppose que le cours soit compris de l'étudiant. Or ce dernier ne prend pas conscience que c'est maintenant à lui de fournir un travail personnel pour comprendre par lui-même ce cours qu'on lui expliquait en long et en large l'année précédente.

– L'absence de moyens incitatifs. Malgré les incitations de l'assistant chargé des T.D., l'étudiant ne se sent pas obligé de chercher à l'avance les exercices proposés. Le T.D. consistera donc, selon le tempérament de l'assistant, à une solution rapide fournie par les quelques rares travailleurs du groupe, soit par une demi-heure de silence – parsemée de quelques indications de temps en temps – pour que chacun fasse effectivement l'effort de chercher la solution. Dans le premier cas, l'étudiant dispose d'une belle solution, mais il n'a en réalité rien compris aux difficultés de l'exercice, et dans l'autre cas on avance à la vitesse $v$ voisine de zéro, et les quelques consciencieux se tournent les pouces, au point d'être découragés, la fois suivante, de chercher à l'avance.

Un autre aspect relève de la culture et de la formation générale, et est fortement lié à la maîtrise de la langue française.

– La compréhension d'un énoncé : les erreurs de lecture et de compréhension ne sont pas rares, même dans une épreuve d'examen : séparer les hypothèses d'un paragraphe de celles du suivant, ou savoir distinguer une simple phrase de l'énoncé d'une question posée.

– La structuration d'un raisonnement : peu d'étudiants sont capables de construire ou structurer un raisonnement. D'ailleurs les problèmes (style bac) étaient tout découpés en tranches, il suffisait de se laisser conduire question par question. Comment arriver à construire soi-même sa démarche déductive?

– La rédaction : il y a des étudiants qui savent bien rédiger, c'est certain. Mais pour la majorité, une démonstration consiste en une suite de lignes liées par un signe $\Longleftrightarrow$ dont on ne se soucie pas de savoir la signification. Il est inquiétant de constater que trop d'étudiants ignorent que le raisonnement mathématique est déductif et qu'au mieux un signe $\Longrightarrow$ suffirait. Les seuls mots de français sont parfois *donc* ou *alors*. Pourtant, ces mêmes élèves ont fait des dissertations, où l'on avance des arguments, explique, justifie. Pourquoi cette indigence dès qu'il s'agit des mathématiques? Quant à énoncer un théorème et vérifier que les hypothèses sont satisfaites, n'en parlons pas.

Il y a les hyperconsciencieux (qui ne rédigent d'ailleurs pas mieux) pour qui plus on met d'étapes intermédiaires, plus ce sont des mathématiques : chaque suppression de parenthèse donnera lieu à une ligne complète de calcul. Ces mêmes consciencieux, après avoir fait une démonstration dans le cas $x < y$, referont tous les calculs dans le cas $y < x$, malgré la symétrie évidente du problème, faute d'avoir compris que faire des mathématiques consiste à remplacer un calcul par un raisonnement.

Il y a deux autres points qui sont tout aussi importants pour faire des études scientifiques :

– L'observation : devant une formule à démontrer, une expression compliquée, l'attitude la plus fréquente est de se lancer dans un calcul sans avoir pris le temps de réfléchir ou même de regarder. Un minimum d'observation permet souvent de comprendre la signification d'une formule, de voir d'où elle est issue, de constater qu'elle ressemble à telle autre. C'est en observant qu'on découvre les termes d'une identité remarquable, etc...

– L'imagination : même dans un domaine rigoureux comme les mathématiques, l'imagination est indispensable. Or il suffit de lire un problème de bac (montrer que, démontrer que, en déduire que) pour se rendre compte que non seulement l'imagination n'est pas sollicitée, mais qu'elle est bannie, et l'élève qui en aurait est prié de la mettre de côté et de faire comme c'est indiqué. On se retrouve avec des étudiants incapables de démontrer quoi que ce soit si le chemin à suivre ne leur est pas explicitement donné. Or faire des mathématiques, c'est *aussi* (j'allais écrire c'est *d'abord*) savoir aborder un problème. Que de fois ai-je entendu des étudiants dire : "*je ne sais pas faire telle question, on ne me l'a jamais appris*" et, la conscience tranquille, poser leur crayon. Ces étudiants sauraient-ils disserter sur les notions d'invention et de progrès?

Tous ces points passés en revue devraient ne pas poser de difficultés insurmontables à un bachelier (de quelque section que ce soit). Et si les étudiants qui viennent en Deug mathématique les avaient acquis, il leur suffirait d'un niveau convenable en mathématiques et une motivation pour des études, pour qu'ils réussissent des études honorables.

La réalité est malheureusement décevante, et même préoccupante. Voici les résultats du premier trimestre octobre/décembre 1993 du Deug mathématiques à Strasbourg :

Sur 185 étudiants inscrits pour la première fois en Deug et présents à l'examen de décembre :
- 32 ont eu la moyenne générale,
- 37 ont eu entre 8 et 10,
- 116 ont eu moins que 8 sur 20 et n'ont pas été admis à poursuivre au second semestre.

En filière physique, c'est sensiblement la même chose. Et si on regarde les notes de mathématiques au lieu de la moyenne générale, les chiffres ne changent guère.

Vous pouvez réagir à ce texte. Ecrivez à '*L'Ouvert*'.

M. Krier,
Directeur pédagogique
Filière mathématique du Deug.

# SOMMAIRE

N° 75 – 1994




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 (suite)

Paul GIRAULT

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

*2.2 La géométrie finie et les formules de J.v. Szökefalvi-Nagy.* — Nous venons de voir les formules de Plücker pour les courbes algébriques *complexes* du plan. Mais nos courbes sont en fait des variétés holomorphes compactes de dimension *complexe* 1, c'est-à-dire que ce sont topologiquement des surfaces compactes, alias des surfaces de Riemann, dans le cas non singulier. La figure 6 illustre le cas d'une courbe de genre 1.

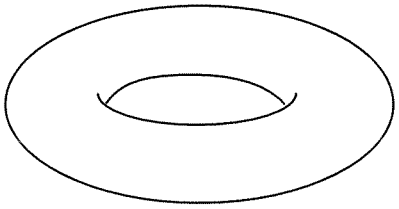


*Figure 6. La courbe* $X_3X_2^2 = X_1(X_1^2 - X_3^2)$ *de genre* $g = 1$.

Ce n'est pas la représentation que l'on se fait usuellement d'une courbe! Par conséquent, les parties réelles des courbes tracées précédemment n'étaient qu'une petite partie des figures complètes! Il est néanmoins tentant de savoir si l'on peut avoir des formules à la Plücker pour les courbes algébriques réelles et — pourquoi pas — pour les courbes ordinaires. En fait, la fin du XIX$^{e}$ siècle a vu peu de travaux consacrés à la forme des courbes : citons les noms de Mœbius (1848), Perrin (1877), Brunn (1889), Kneser (1893), sans oublier — comme toujours — Gauss.

Les seuls résultats intéressants ont été obtenus pour les courbes algébriques réelles par Harnack et Klein : nous y reviendrons. Les immenses perspectives offertes par les idées de Riemann, sont certainement à l'origine de l'apparent désintérêt pour ce genre de questions car c'est à ce moment que se bâtissent la géométrie algébrique et la géométrie différentielle modernes... Vastes programmes.

Au début de ce siècle, tout change avec ce qu'on appelle — assez plaisamment d'ailleurs — la *géométrie finie* ou *géométrie de Juel*, en l'honneur du chercheur qui a le plus contribué au sujet. De quoi s'agit-il ?

*a) La géométrie finie.* — Soit $\mathbb{P}^2(\mathbb{R})$ le *plan projectif réel* ou tout simplement *le plan* : sa définition est analogue à celle de $\mathbb{P}^2(\mathbb{C})$, il suffit de changer le corps des complexes par celui des réels. Dans ce plan, on a des points et des droites...

Définissons l'élément simple qui va nous servir à construire les courbes planes. Cet élément est l'*arc élémentaire* : c'est un arc de courbe coupée en au plus deux points par toute droite du plan et qui possède une tangente variant continûment avec le point de contact. Un tel arc sera aussi appelé *arc convexe.*

Assemblons deux arcs élémentaires $AB$ et $AC$ par une extrémité commune $A$ de telle sorte que les tangentes coïncident : nous obtenons ainsi les quatre possibilités représentées par la figure 7.

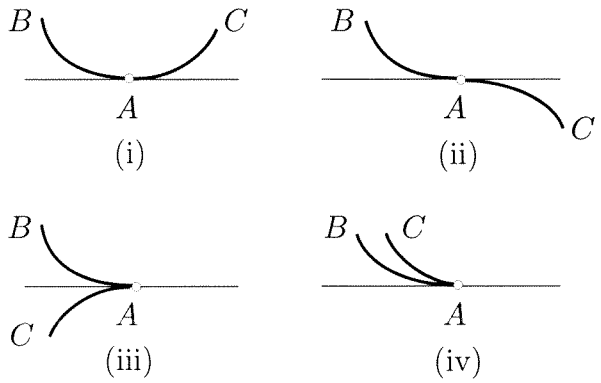



*Figure 7. Point intérieur, point d'inflexion, épine et bec.*

(i) $A$ devient un point intérieur à un arc élémentaire.

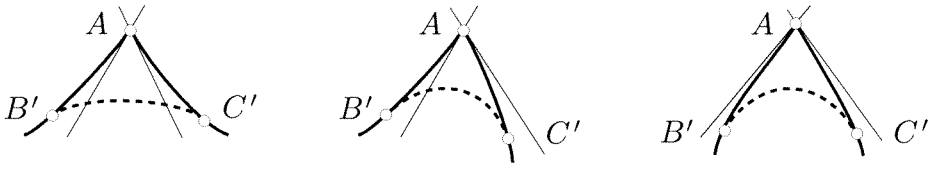
(ii) $A$ est *point d'inflexion* et la tangente en $A$ est *tangente inflexionnelle.*

(iii) $A$ est une *épine* ou *point de rebroussement*[1] *de première espèce* : la tangente en $A$ est de type ordinaire car elle tourne toujours dans le même sens lorsque le point de contact se déplace de $B$ vers $A$, puis de $A$ vers $C$.

(iv) $A$ est un *bec* ou *point de rebroussement*[1] *de deuxième espèce* : la tangente en $A$ est de type inflexionnelle car la tangente tourne d'abord dans un sens lorsque le point de contact se déplace de $B$ vers $A$, puis revient en sens contraire lorsque le point de contact se déplace de $A$ vers $C$.

[1] Les points de rebroussement sont encore appelés *pointes.*

Observons maintenant les différentes situations lorsque les tangentes sont distinctes au point $A$ :




(i) (ii) (iii)

*Figure 8. Épine, bec et chapeau.*

Nous obtenons ainsi un *point anguleux* :

- dans le cas (i), on a une *épine*;
- dans le cas (ii), on a un *bec*;
- dans le cas (iii), on a un *chapeau.*

On peut faire disparaître la discontinuité de la tangente en $A$ à l'aide d'un *raccordement* (Fig. 8). Suivant l'espèce du point anguleux, le raccordement fait apparaître deux, un ou zéro points d'inflexion. On peut évidemment appliquer l'opération du raccordement au bec et à l'épine ordinaires. C'est une opération importante en géométrie finie.

Après ces préambules, il est alors possible de définir *une courbe élémentaire* : c'est une courbe fermée du plan projectif réel formé par la réunion d'un nombre fini d'arcs élémentaires.

Une courbe élémentaire possède un nombre fini de points d'inflexions ou de pointes. Il en est de même du nombre de points de rencontre avec une droite du plan. Toujours dans les généralités, indiquons qu'elles peuvent présenter des *points doubles* (ou points à croisements normaux) et des *tangentes doubles* (ou bitangentes) : pour la définition, le mieux est de se reporter à la figure 4.

Il nous reste à introduire deux notions importantes pour l'étude des courbes élémentaires inspirées de l'étude des courbes algébriques complexes. Soit $\mathcal{C}$ une courbe élémentaire.

- L'*ordre de réalité* ou, tout simplement, l'*ordre* de $\mathcal{C}$ est le nombre maximum de ses points de rencontre avec une droite du plan. Remarquons en passant que, lorsque la droite varie, le nombre des points de rencontre change, mais sa *parité* est invariable puisqu'il augmente ou diminue de deux unités à chacune de ses variations.

- La *classe de réalité* ou simplement la *classe* de $\mathcal{C}$ (Fig. 2) est le nombre maximum de tangentes à la courbe que l'on peut mener par un point du plan : le nombre de ces tangentes a une parité invariable quand le point se déplace.

EXEMPLE. — Soit $\mathcal{C} = \{x \in \mathbb{P}^2(\mathbb{R}),\ F(x) = 0\}$ où $F$ est un *polynôme homogène* non constant de $\mathbb{R}[x_0, x_1, x_2]$. Désignons par $n$ le degré de $F$. Si l'ensemble $\mathcal{C}$ n'est pas vide, c'est une courbe élémentaire mais aussi une courbe algébrique projective réelle. L'ordre de $\mathcal{C}$ est inférieur au degré $n$ de $F$, la classe de $\mathcal{C}$ est inférieure à la classe complexe de $\mathcal{C}$. Par exemple, la quartique de Fermat, $x_1^4 + x_2^4 = x_0^4$ est d'ordre 2 et de classe 2.

La géométrie finie est donc une généralisation naturelle de la géométrie algébrique réelle. Mais il y a une différence considérable entre les deux : en effet, la géométrie algébrique réelle — ayant à son service une puissante machinerie mathématique — est bien plus élaborée. Ce sera l'objet d'un chapitre ultérieur.

De ces définitions, on déduit facilement les résultats suivants :

- Le nombre de tangentes d'inflexion et l'ordre d'une courbe élémentaire ont la même parité.
- Le nombre de pointes et la classe ont la même parité.
- Le nombre de points de rencontre de deux courbes élémentaires dont l'une est d'ordre pair est un nombre pair ; le nombre de points de rencontre de deux courbes élémentaires d'ordre impair est un nombre impair (ces deux résultats remontent à Möbius).
- Un raccordement ne peut pas augmenter l'ordre d'une courbe.

A partir des résultats précédents, on peut esquisser une classification des courbes de petit ordre :

*Ordre 1.* — Une courbe élémentaire d'ordre 1 est une droite.

*Ordre 2.* — Une courbe du second ordre n'a aucune singularité : pas de point double, pas de pointe, pas de tangente double, pas de tangente inflexionnelle.

Une courbe d'ordre deux n'a qu'une composante connexe et on peut la transformer en un ovale par projection. Réciproquement, Möbius et Juel ont montré que :

— toute courbe plane sans singularités est d'ordre 2 et de classe 2 ;

— toute courbe plane qui possède au plus des points doubles et des tangentes doubles mais pas d'autres singularités ponctuelles et tangentielles est d'ordre 2 et de classe 2.

Plus curieux est le fait suivant : pour tout entier positif pair $k$, il existe deux courbes d'ordre deux qui ont $k$ points communs : elles ont alors $k$ tangentes communes. Un tel résultat est impossible pour les courbes algébriques planes du second degré un vertu du théorème de Bézout.

*Ordre 3.* — Une courbe du troisième ordre sans point double et sans pointe a trois points d'inflexion qui partagent la courbe en trois arcs convexes. Une courbe d'ordre trois a au plus un point singulier, à savoir un point double ou une pointe.

Une courbe singulière d'ordre trois a exactement une tangente inflexionnelle.

Une courbe d'ordre trois a au plus deux composantes connexes comme dans le cas algébrique.

Les courbes d'ordre trois sans point singulier sont de classe 6 ou 4. Par une perspective, on peut les ramener à présenter l'une des dispositions de la figure 9, où l'on a tracé d'un trait plein les courbes d'ordre trois formées d'une seule composante connexe.

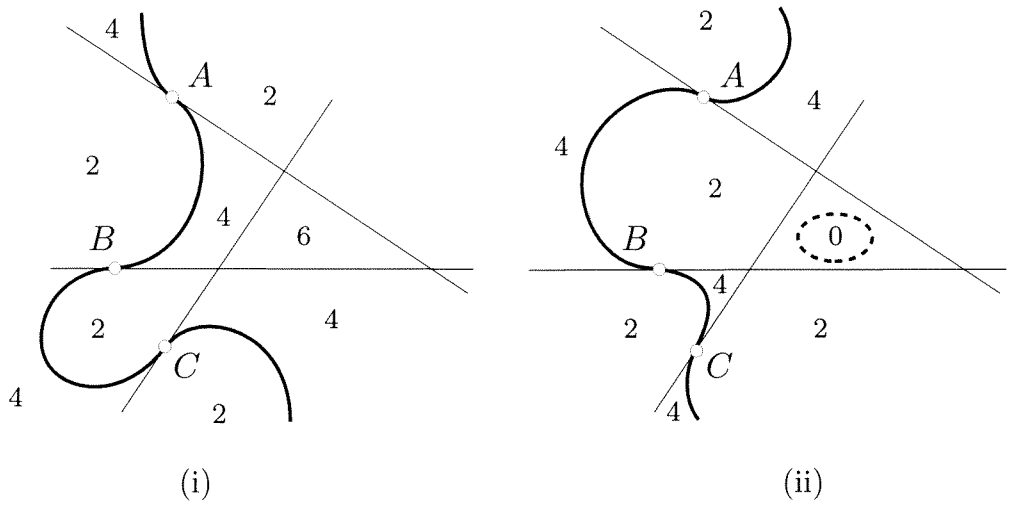



*Figure 9. Présentation canonique d'une courbe d'ordre* 3.

Les nombres placés sur la figure indiquent le nombre de tangentes que l'on peut mener à la courbe par un point de la région correspondante. A la courbe donnée par la figure 9 (ii), on peut ajouter un ovale situé à l'intérieur du triangle délimité par les tangentes inflexionnelles, la classe augmentant alors de deux unités : la courbe reste du troisième ordre, mais est de classe 6 avec deux composantes connexes.

*Ordre 4.* — Nous ne donnerons pas la classification des courbes de cet ordre car elle est beaucoup plus compliquée (Fig. 10). Indiquons toutefois que si $k$ est un entier positif, il existe toujours une courbe d'ordre 4 qui admet $k$ composantes connexes. Le contraste est alors saisissant avec les courbes algébriques réelles de degré 4 : d'après un résultat de Zeuthen (1874), elles ont au plus quatre composantes connexes. Le lecteur amusé pourra construire autant de courbes du quatrième ordre qu'il voudra en s'inspirant de la figure 10.

Pour terminer, rappelons qu'une courbe du quatrième ordre peut avoir un nombre de points doubles $d$, de tangentes doubles $t$, de points d'inflexion $w$, tout à fait quelconque. Si la courbe n'a qu'une composantes connexe et si elle est sans pointe, alors on a $w = 2(t - d)$ d'après Juel.

*Ordres supérieurs à 5.* — A ma connaissance, rien n'a été tenté pour ces ordres. Avis aux amateurs !

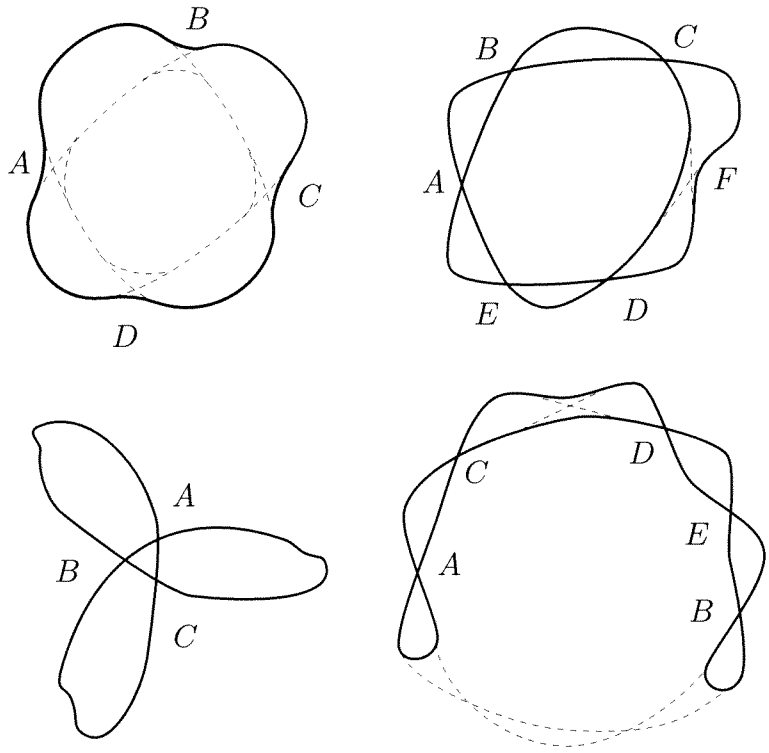



*Figure 10.*

*b) Les formules de J.v. Szökefalvi-Nagy.* — D'après ce qui précède, il paraît donc difficile, voire aventureux, de tenter une classification générale des courbes élémentaires en utilisant l'ordre pour seul outil. Il est certainement plus judicieux d'établir d'abord une relation entre un certain nombre de paramètres qui caractérisent la forme d'une courbe. Pour cela, on peut choisir comme paramètres ceux qui apparaissent dans les formules de Plücker, quitte à en introduire de nouveaux si cela s'avère insuffisant. Nous allons donc exposer quelques résultats de J.v. Szökefalvi-Nagy dont les travaux — quoique assez oubliés aujourd'hui (comme d'ailleurs tout ce qui ressortit à la géométrie finie) — ont porté essentiellement sur les courbes et les surfaces en géométrie finie.

Soit $\mathcal{C}$ une courbe élémentaire. On a défini son *ordre* et sa *classe*. Il reste à définir son *index* (linéaire) et son *index de classe* ou *index tangentiel*.

- L'*index* est le nombre *minimum* de ses points de rencontre avec une droite du plan.

- L'*index de classe* est le nombre *minimum* de tangentes à $\mathcal{C}$ que l'on peut mener par un point du plan.

Rappelons que le genre $p(D)$ d'un domaine $D$ du plan est le nombre des sections transverses que l'on peut pratiquer sans morceler le domaine. Plus vulgairement c'est le nombre de « trous » (Fig. 12).

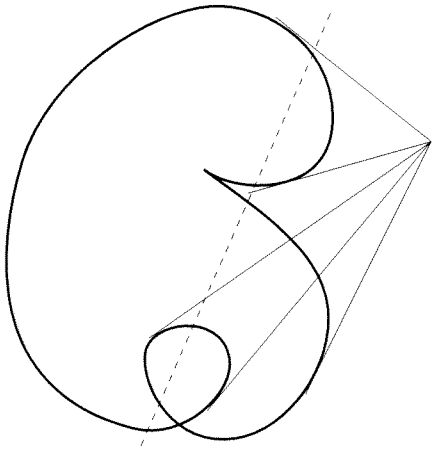


*Figure 11. Une courbe d'ordre* 6, *d'index* 0, *de classe* 5 *et d'index de classe* 1.

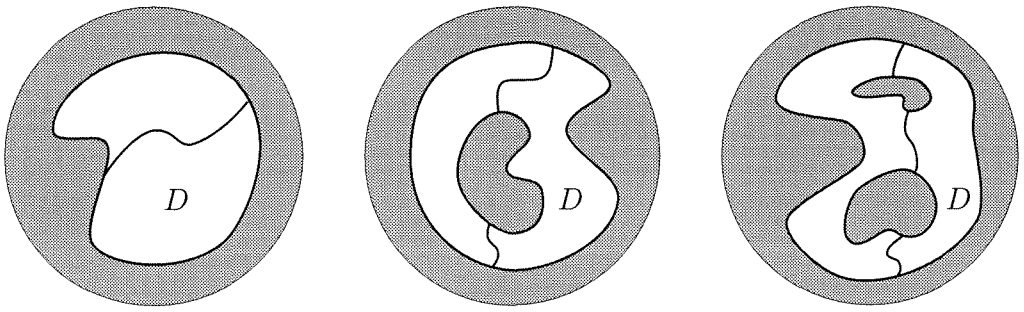



*Figure 12. Pas de trou, un trou, deux trous, etc.*

On a alors le théorème suivant.

THEORÈME (Szökefalvi-Nagy, 1923). — *Soit $\mathcal{C}$ une courbe élémentaire de classe $n$, d' index de classe $(n-2)$. Désignons*

— *le nombre de points doubles par $d$,*

— *le nombre de pointes par $r$,*

— *le nombre de tangentes inflexionnelles par $w$,*

— *le nombre de tangentes doubles par $t$.*

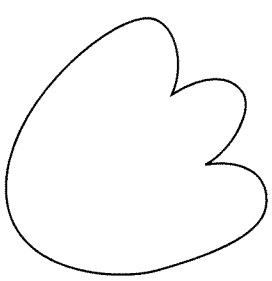
*Avec ces notations, on a $d = 0$ et $w = 0$ ou 1. En outre, si $p$ est le genre du domaine d'où l'on peut mener exactement $n-2$ tangentes à $\mathcal{C}$, on a*

$$r = n - 2 + 2p, \quad p = \tfrac{1}{2}(n-1)(n-2) - t - w,$$

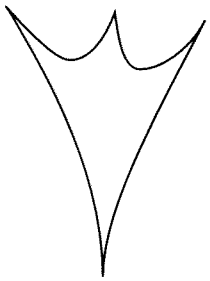
*et si $m$ est l'ordre de $\mathcal{C}$,*

$$m \leq n(n-1) - 2t - 3w = n + r - w = 2n - 2 + 2p - w.$$

REMARQUE. — La dernière inégalité est la meilleure possible (Fig. 13).



$n = 4,\ w = 0,\ r = 2,$
$p = 0,\ t = 3$



$n = 4,\ w = 0,\ r = 3,$
$p = 1,\ t = 2$

*Figure 13.*

Par dualité, il est facile d'obtenir une série de relations pour les courbes d'ordre $m$ et d'index $(m-2)$.

Indiquons pour terminer que les formules de Szökefalvi-Nagy ont été obtenues *sans calculs*, par voie géométrique. Il en est de même des principaux résultats de la géométrie finie. Il s'agit d'une démarche intellectuelle particulièrement élégante, mais tout de même limitée comme le montre l'étude des surfaces dans cette discipline.

*2.3 La formule de Fabricius-Bjerre.* — Soit $\mathcal{C}$ une courbe fermée du plan affine réel. On permet à cette courbe d'avoir des pointes et des croisements normaux (ou points doubles ordinaires). Désignons

— l'ensemble des becs par $B$ et posons $b = \mathrm{Card}(B)$ ;
— l'ensemble des épines par $C$ et posons $c = \mathrm{Card}(C)$ ;
— l'ensemble des points d'inflexion par $F$ et posons $b = \mathrm{Card}(F)$ ;
— l'ensemble des points doubles par $N$ et posons $n = \mathrm{Card}(N)$ ;
— l'ensemble des tangentes doubles par $D$, (Fig. 14 (i)) ;
— l'ensemble des droites joignant deux éléments de $B \cup C$ par $D_S$ (ce qui est illustré Fig. 14 (iii)) ;
— l'ensemble des tangentes à la courbe au point régulier $x$ passant par un point $y \in B \cup C$ par $D_*$, (Fig. 14 (ii)) ;

Maintenant, considérons une droite $s$ de $\Delta = D \cup D_S \cup D_*$. Désignons par $p_1$ et $p_2$

— les deux points de contact entre $s$ et $\mathcal{C}$ (Fig. 14 (i)) ;
— ou les deux points singuliers, (Fig. 14 (iii)) ;
— ou le point singulier et le point de contact avec $\mathcal{C}$, (Fig. 14 (i)).

Prenons deux voisinages suffisamment petits $D_1, D_2$ de $p_1, p_2$ et posons $\sigma_i = \mathcal{C} \cap D_i$. Le complémentaire de $s$ dans $\mathbb{R}^2$ a *deux composantes connexes* : si $\sigma_1 \setminus \{p_1\}, \sigma_2 \setminus \{p_2\}$ appartiennent à la même composante, on dit que $s$ est un élément *positif* de $\Delta$, sinon $s$ est un élément *négatif.*

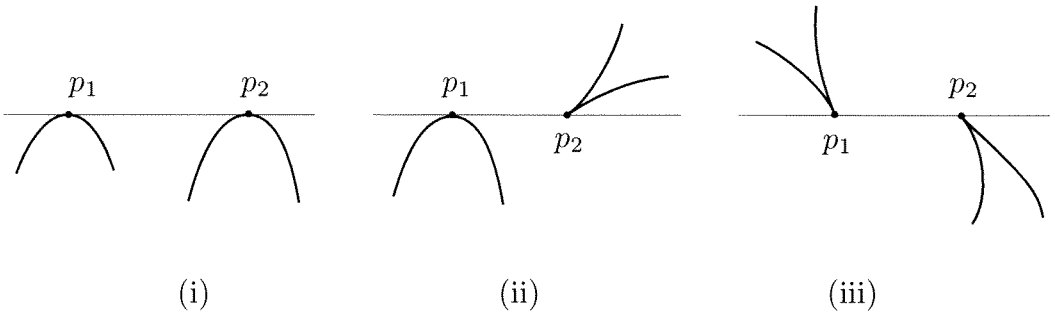



*Figure 14.*

Désignons :

— par $d^+$ le nombre de *tangentes doubles positives* et par $d^-$ le nombre de *tangentes doubles négatives* ;

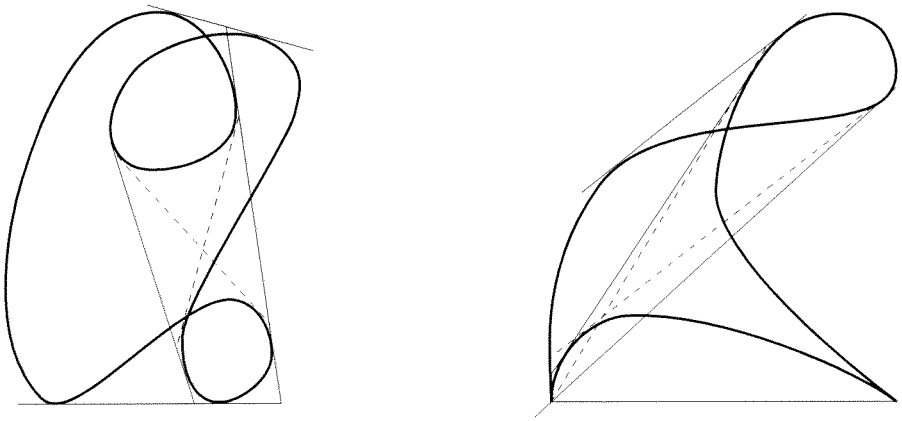
— par $d_S^+$ le nombre d'*éléments positifs* de $D_S$ et par $d_S^-$ le nombre *d'éléments négatifs*) ;

— par $d_*^+$ le nombre d'*éléments positifs* de $D_*$ et par $d_*^-$ le nombre d'*éléments négatifs.*

On a alors le petit joyau suivant.

THEORÈME (Fabricius-Bjerre). — *Sous des conditions raisonnables, de telle sorte que chacun des ensembles $B$, $C$, $D$, $F$ et $N$ soit de cardinal fini, on a l'égalité :*

$$b + f + 2(n + c) = 2(d^+ - d^- + d_S^+ - d_S^- + d_*^+ - d_*^-).$$



$d^+ = 5,\ d^- = 2,$
$d_S^+ = d_S^- = d_*^+ = d_*^- = 0,$
$b = 0,\ f = 2,\ n = 2,\ c = 0$

$d^+ = 2,\ d^- = 1,$
$d_S^+ = 1,\ d_S^- = 0,\ d_*^+ = 2,\ d_*^- = 1,$
$b = 1,\ f = 1,\ n = 1,\ c = 1$

*Figure 15. Deux exemples de la formule de Fabricius-Bjerre.*

COROLLAIRE. — *(Juel, voir plus haut) Soit $C$ une courbe du plan affine, non singulière et d'ordre 4. Alors, on a l'égalité :*

$$f = 2(d^+ - n), \quad d^- = 0.$$

REMARQUE. — La formule de Fabricius-Bjerre est loin d'être banale comme le montre la figure 16 sur laquelle pourra s'exercer le lecteur peu convaincu.

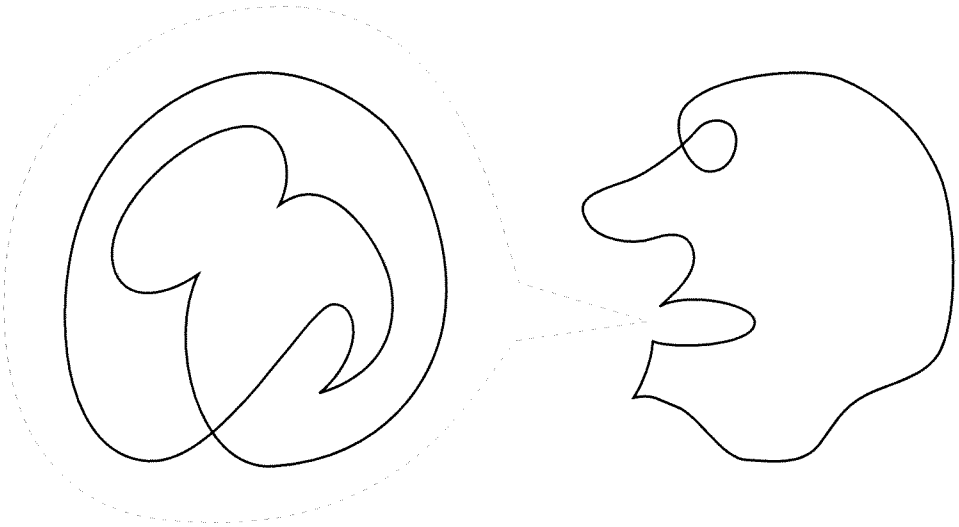


*Figure 16. Fabricius-Bjerre exposant ses travaux.*

Cette formule a d'abord été prouvée par Fabricius-Bjerre en 1962, dans le cas non singulier, en utilisant les méthodes de la géométrie finie, puis par Halpern (1969) à l'aide de la théorie des zéros des champs de vecteurs. Mais c'est en 1977 que Fabricius-Bjerre — le diable d'homme — obtint la formule générale énoncée plus haut par voie géométrique. C'est grâce à l'expérience acquise sur les formules de Plücker que celui-ci a pu obtenir l'extension désirée. A ma connaissance, il n'existe pas de démonstration analytique de son théorème, mais est-ce bien utile ?

*2.4 Résultats épars.* — Dans son travail de 1969, Halpern a prouvé l'énoncé suivant.

THEORÈME. — *Soient $C$ et $C'$ deux courbes fermées du plan $\mathbb{R}^2$ non singulières. Désignons*

— *le nombre de tangentes doubles positives par $d^+$,*

— *le nombre de tangentes doubles négatives par $d^-$,*

— *le nombre de points d'intersection (transversale) de $C$ avec $C'$ par $n$.*

*Dans ces conditions, on a l'égalité $d^+ = n + d^-$ (Fig. 17).*

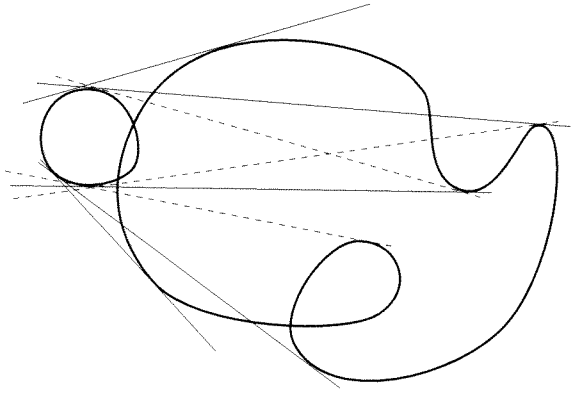


*Figure 17. Un cas particulier de la formule d'Halpern : $d^+ = 5$, $d^- = 3$ et $n = 2$.*

La contemplation du théorème de Fabricius-Bjerre suggère le problème suivant : construire *effectivement* des courbes vérifiant l'égalité de ce théorème.

En 1972, Halpern a montré que si $a_1, a_2, a_3 \geq 0$ et $a_4 > 0$ sont des entiers quelconques, il existe toujours une courbe $\mathcal{C}$ non singulière qui vérifie $d^+ = a_1$, $d^- = a_2$, $n = a_3$ et $f = 2a_4$. En revanche, il avait conjecturé $f = 0$ implique $d^- \leq n(n-1)$, résultat qui fut prouvé par Ozawa en 1984. Ceci montre que nos courbes, dans le cas non singulier, ne satisfont pas d'autres conditions nécessaires.

A-t-on épuisé le sujet ? Loin de là ! La formule de Fabricius-Bjerre — formule plückerienne, ne l'oublions pas — admet bien des généralisations.

Une première généralisation, déjà suggérée en 1969 par Halpern, démontrée par Girault (1984, non publié), Weiner (1987) concerne le cas des courbes sphériques. Une généralisation plus naturelle et plus intéressante à la fois est le cas des courbes élémentaires du plan projectif $\mathbb{P}^2(\mathbb{R})$.

Contemplons encore une fois la formule de Fabricius-Bjerre : il saute aux yeux qu'elle n'est pas projective. En effet, si $d$ est une droite de $\mathbb{P}^2(\mathbb{R})$, alors $\mathbb{P}^2(\mathbb{R}) \setminus d$ est *connexe* ! Par conséquent, la notion d'élément positif (resp. négatif) est inadéquate (on se reportera aux préliminaires à la formule de Fabricius-Bjerre). En surmontant cette difficulté, Pignoni a réalisé en 1992 le tour de force de prouver la généralisation souhaitée. Malheureusement, la grande technicité de la formule de Pignoni ne permet pas son exposé succinct.

Prenons maintenant un peu de hauteur et abordons le cas des courbes dans l'espace dont l'étude est beaucoup plus difficile ! Dans le plan, on s'est intéressé aux bitangentes d'une courbe ; dans l'espace il est naturel d'examiner les plans tritangents d'une courbe. C'est ce que nous allons faire en guise de conclusion en exposant essentiellement les résultats d'Ozawa (1985).

Débutons par quelques rappels et notations. Soient $\mathcal{C}$ une courbe fermée et $f : S^1 \to \mathbb{R}^3$ une paramétrisation de classe $C^\infty$ de cette courbe. On suppose que le vecteur tangent unitaire, le vecteur normal principal et le vecteur binormal sont définis en chaque point de $\mathcal{C}$. Si la courbe est paramétrée par l'abscisse curviligne,

les vecteurs précédents notés $e_1, e_2$ et $e_3$ vérifient les formules de Serret-Frenet :

$$\frac{\mathrm{d}}{\mathrm{ds}}\begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix} = \begin{pmatrix} 0 & \kappa & 0 \\ -\kappa & 0 & \tau \\ 0 & \tau & 0 \end{pmatrix}\begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix},$$

où $\kappa$ et $\tau$ sont *la courbure* et *la torsion* de $\mathcal{C}$.

Dans la suite, nous supposerons que *la courbure est non nulle* en chaque point de $\mathcal{C}$. Désignons encore par $w(s)$ le plan osculateur[2] au point d'abscisse $s$.

Soient $A(2,3)$ l'ensemble des plans affines de $\mathbb{R}^3$ et $P$ un plan affine de $\mathbb{R}^3$ tangent à $\mathcal{C}$ au point d'abscisse $s$. On définit l'*ordre du contact* $n$ de $P$ avec $\mathcal{C}$ en ce point comme suit :

$$n = \begin{cases} 0 & \text{si } e_1(s) \text{ n'est pas parallèle à } P, \\ 1 & \text{si } e_1(s) \text{ est parallèle à } P \text{ et } e_2(s) \text{ n'est pas parallèle à } P \\ 2 & \text{si } e_1(s) \text{ et } e_2(s) \text{ sont parallèles à } P \text{ et } \tau(s) \neq 0, \\ 3 & \text{si } e_1(s) \text{ et } e_2(s) \text{ sont parallèles à } P \text{ et } \tau(s) = 0,\ \tau'(s) \neq 0. \end{cases}$$

Definition 1. — L'ordre total du contact de $P$ avec $\mathcal{C}$ est la somme des ordres de contact en chaque point de $P$ avec $\mathcal{C}$.

Definition 2. — Une courbe $\mathcal{C}$ de $\mathbb{R}^3$ est dite en *position générale* si elle vérifie les conditions suivantes :

(i) $f : S^1 \longrightarrow \mathbb{R}^3$ est un plongement, ce qui se traduit géométriquement en disant que $\mathcal{C}$ est sans points doubles et sans pointes.

(ii) La courbure $\kappa$ n'est jamais nulle.

(iii) Si $\tau(s) = 0$, alors $\tau'(s) \neq 0$.

(iv) Les ordres totaux de contact de tout plan avec $\mathcal{C}$ sont $\leq 4$.

(v) Si $P \in A(2,3)$ est tangent à $\mathcal{C}$ en trois points, ces trois points ne sont pas alignés.

(vi) Si un plan osculateur $w(s_1)$ de $\mathcal{C}$ au point d'abscisse $s_1$ est tangent à $\mathcal{C}$ au point d'abscisse $s_2$, avec $s_1 \neq s_2$, alors le point d'abscisse $s_2$ n'est pas sur la tangente à $\mathcal{C}$ au point d'abscisse $s_1$.

Cette longue liste de conditions vérifiées par une courbe en position générale est inquiétante, mais le théorème suivant nous apporte un soulagement très vif.

Theorème (Banchoff, Gaffney, McCrory, 1985). — *L'ensemble des courbes qui sont en position générale est un ouvert partout dense de* $C^\infty(S^1, \mathbb{R}^3)$.

Dans la suite, nous supposerons que $\mathcal{C}$ est en position générale.

[2] Le mot osculateur provient du latin *osculari* qui veut dire embrasser. Cette terminologie remonte à Lagrange.

DEFINITION 3. — Soit $P \in A(2,3)$. On dit que $P$ est un *plan tritangent* de la courbe $\mathcal{C}$ si l'ordre total du contact est égal à 3.

Nous dirons encore qu'un plan tritangent est un *T-plan* (Fig. 18 (i)), un *C-plan* (Fig. 18, (ii)) ou un *I-plan* (Fig. 18, (iii)), selon que le nombre de points de contact est 3, 2 ou 1.

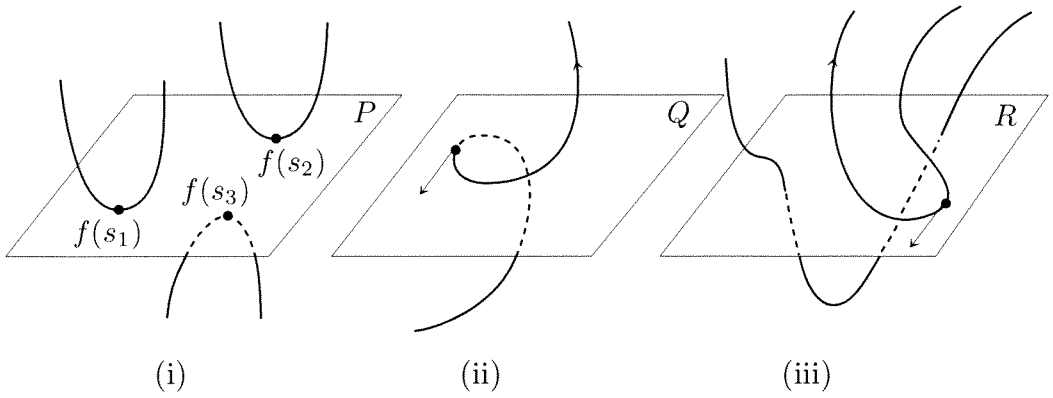



*Figure 18.*

Passons aux ultimes définitions. Munissons $\mathbb{R}^3$ de son produit scalaire usuel noté $\langle\ ,\ \rangle$.

Soient $P$ un T-plan de $\mathcal{C}$ et $s_1, s_2$ et $s_3$ les abscisses des points de contacts avec $s_1 < s_2 < s_3$. Posons :

$$v = \big(f(s_2) - f(s_1)\big) \times \big(f(s_3) - f(s_1)\big).$$

Puisque $\mathcal{C}$ est en position générale, $v$ n'est pas nul et orthogonal à $P$. Posons encore :

$$H_v = \big\{x \in \mathbb{R}^3\ ;\ \langle x - f(s), v\rangle \geq 0\big\}.$$

DEFINITION 4. — L'index $\mathrm{Ind}(P)$ du $T$-plan $P$ est défini par :

$$\mathrm{Ind}(P) = \begin{cases} 1 & \text{si le nombre de branches locales de } \mathcal{C} \\ & \qquad \text{qui se trouvent dans } H_v \text{ est impair,} \\ -1 & \text{si ce nombre est pair.} \end{cases}$$

Sur la figure 18 (i) (orientée conformément à la règle de la main gauche), le vecteur $v$ est dirigé vers le haut, d'où $\mathrm{Ind}(P) = -1$.

Soient $Q$ un $C$-plan de $\mathcal{C}$, $s_1$ et $s_2$ les abscisses des points de contact avec pour ordres de contact 1 et 2 respectivement. Le vecteur tangent unitaire $e_1(s_2)$ et le vecteur normal principal $e_2(s_2)$ sont parallèles à $Q$, tandis que $e_1(s_1)$ est parallèle à $Q$ et $e_2(s_1)$ n'est pas parallèle à $Q$.

DEFINITION 5. — L'index $\mathrm{Ind}(Q)$ du $C$-plan $Q$ est défini par :

$$\mathrm{Ind}(Q) = \begin{cases} 1 & \text{si } \langle e_1(s_2) \cdot (f(s_1) - f(s_2)), e_2(s_1) \rangle > 0, \\ -1 & \text{si } \langle e_1(s_2) \cdot (f(s_1) - f(s_2), e_2(s_1) \rangle < 0. \end{cases}$$

Sur la figure 18 (ii), le $C$-plan $Q$ a pour index $\mathrm{Ind}(Q) = -1$.

Soit $R = w(s_0)$ le plan osculateur au point d'abscisse $s_0$. C'est un $I$-plan, i.e. $\tau(s_0) = 0$ (d'où $\tau'(s_0) \neq 0$).

DEFINITION 6. — L'index $\mathrm{Ind}(R)$ du $I$-plan $R$ est défini par

$$\mathrm{Ind}(R) = \varepsilon(\text{le nombre d'intersection transverse de } C \text{ avec } R),$$

où $\varepsilon = \begin{cases} 1 & \text{si } \tau'(s_0) < 0 \\ -1 & \text{si } \tau'(s_0) > 0. \end{cases}$

Sur la figure 18 (iii), le $I$-plan $R$ a pour index $\mathrm{Ind}(R) = -2$.

Remarquons pour finir que si l'on renverse l'orientation de la courbe, tous les indices changent de signe.

Il ne nous reste plus qu'à énoncer le résultat suivant.

THEORÈME (Ozawa, 1985). — *Soit $C$ une courbe de $\mathbb{R}^3$ en position générale. Posons*

$$T = \sum_{\text{T- plans}} \mathrm{Ind}(P), \quad C = \sum_{\text{C-plans}} \mathrm{Ind}(Q), \quad I = \sum_{\text{I-plans}} \mathrm{Ind}(R).$$

*Alors on a :*

$$C = I, \quad 6T = 2C + I.$$

Le principal ingrédient pour la démonstration de ce théorème est la théorie de Morse et... beaucoup de sueur !

Comme le suggère la haute technicité des préliminaires, le théorème d'Ozawa n'a pas évidemment clos le sujet. Des résultats intéressants de la sorte ont été obtenus par Banchhoff, Gaggney et McCrory (1985) d'une part, et Fuster (1988) d'autre part, mais il reste beaucoup de chemin à parcourir avant que la situation soit complètement maîtrisée.

## BIBLIOGRAPHIE

BERGER (M.) et GOSTIAUX (B), *Géométrie différentielle : variétés, courbes et surfaces*, P.U.F., 1986.

# ROTATIONS, NOMBRES COMPLEXES ET QUATERNIONS

Constantin TZANAKIS
DEPARTEMENT D' ÉDUCATION
UNIVERSITÉ DE CRÈTE
74100 RETHYMNON, CRÈTE, GRÈCE

## 1. INTRODUCTION

L'approche habituelle de l'enseignement des Mathématiques, est essentiellement déductive. Mais cette approche a l'inconvénient de cacher la motivation de l'introduction de nouveaux concepts, théorèmes et théories, et empêche par conséquent la compréhension profonde du sujet. Il est difficile de discerner la relation entre concepts ou domaines mathématiques qui de prime abord sont tout à fait differents.

D'autre part, en suivant les étapes fondamentales du développement historique d'un problème mathématique et en présentant les questions et problèmes qui ont servi comme prototypes à ce développement, le problème peut être enseigné, en mettant au clair les motivations qui ont permis d'introduire les nouveaux concepts ou axiomes. Ainsi la relation entre différents concepts mathématiques ou théories peut être présentée avec clarté et l'étudiant peut se servir de ces notions pour une étude plus approfondie de résultats plus avancés qui sont assez souvent hors du contexte du cours enseigné.

Comme exemple de cette approche, nous allons considérer la relation entre les concepts suivants : (i) nombres complexes (ii) groupe de rotations (iii) isomorphisme et homomorphisme de structures algébriques abstraites, comme elles peuvent être enseignées à un niveau élémentaire au lycée, ou au niveau plus élevé d'un cours universitaire. Plus spécialement, nous présenterons des aspects d'importants développements de l'algèbre du $19^{e}$ siècle, qui ont été motivés par l'interprétation géométrique des nombres complexes. La présentation n'est pas strictement historique mais elle est inspirée par les étapes décisives de cette évolution.

Il est bien connu que pendant une longue période, après leur première introduction au $16^{e}$ siècle, comme moyen de résolution d'équations algébriques, les nombres complexes ont été considérés comme un concept, logiquement non satisfaisant, d'où le nom d'unité imaginaire pour $i = \sqrt{-1}$. Leur présentation géométrique comme points du plan euclidien (Wessel 1797, Argand 1806, Gauss 1831 et autres) et la formulation ultérieure de Hamilton, comme couples de nombres réels (1833–1837), jouèrent un rôle crucial pour leur acceptation comme un concept mathématique admissible (voir [6] p. 7–11, 23–26). En plus, cette présentation géométrique suivie par une présentation trigonométrique qui lui est associée, était étroitement liée

aux rotations du plan (voir les citations du travail de Wessel dans [19] p. XIV). Mais ce qui est moins connu est que ce fait joua un rôle important dans l'évolution de l'algèbre du 19$^{e}$ siècle, en soulevant naturellement la question :
**"Est-il possible de généraliser les nombres complexes, en établissant d'une manière ou d'une autre, une relation avec les rotations de l'espace?"**

A cette question, formulée précisement en langage moderne dans la section 2, beaucoup de mathématiciens ont essayé de donner une réponse; entre autres, Wessel, Argand, Français, Servois, Gauss et Rodrigues ([19] p.XV–XVI, [12] p. 172–173, [6] p. 10–11 et références incluses). Certains ont approché la solution du problème (en particulier Gauss (1819), Rodrigues (1840) et Servois, comme le reconnaît Hamilton, voir [12] p. 173, [6] p. 10 et références citées). Cependant, Hamilton était le premier à donner une réponse explicite en 1843 en introduisant les quaternions. Même s' il faut admettre que l'approche originale de Hamilton était algébrique, il avait certainement à l'esprit que la généralisation demandée des nombres complexes, (ou triplets comme il les a originellement appelés, voir le commentaire historique en section 4) devait être liée aux rotations de l'espace, dans le sens que nous avons déjà esquissé (voir l'abstract de sa procédure dans [6] p. 28). Ceci est confirmé par les remarques suivantes : (a) Dans la première moitié du 19$^{e}$ siècle, les mathématiciens ont essayé de généraliser le concept de nombre (réel) en respectant les lois usuelles d'opérations algébriques et en les interprétant géométriquement. Il paraît que Gauss était convaincu qu'il n' y avait qu'une seule possibilité, en l'occurence les nombres complexes, dont il a établi l'interprétation géométrique bien connue ([3] p. 84–85 et p. 151). Bien sûr ce fait n' a pas arrêté la recherche pour la généralisation des systèmes de nombres. (b) Dans sa formulation abstraite de nombres complexes comme couples de nombres réels, Hamilton interprétait leur produit en termes de rotations du plan et il a cherché une généralisation de nombres complexes permettant d'établir une interprétation analogue des rotations de l'espace ([4] p.625). Ceci est explicitement exprimé dans la préface de son fameux livre "lectures on quaternions" achevé en 1848 et publié en 1853 ([10] p. 117–155, particulièrement §§36, 43, [3] p. 85). En plus, dans ses "Elements of quaternions" publié pour la première fois en 1866, il introduisit les quaternions et interpréta leurs propriétés algébriques – en particulier la non commutativité de leur produit – par le moyen des rotations de l'espace (voir la citation de ce travail, dans [16] p. 677–683, particulièrement p. 679–680, 683).

Même si Peacock et De Morgan avaient déjà étudié des algèbres différentes de l'algèbre des nombres réels, leurs travaux n' étaient pas largement reconnus comme importants. "C'est l'application géométrique des quaternions de Hamilton qui conduisit à une appréciation générale de nouvelles algèbres qui étaient essentiellement non-commutatives ou associatives dans le sens classique" ([16] p. 678). Ainsi l'invention des quaternions était en fait la première structure non commutative étudiée, influençant énormément l'évolution de l'algèbre, la signification des lois [commutative, associative et distributive des opérations algébriques] seulement

après le développement des systèmes de nombres (particulièrement, les quaternions) qui ne leur obéissent pas" ([6] p. 26).

Au moins implicitement, la question mentionnée ci-dessus a joué un rôle dans le travail de Grassman "Ausdehnungslehre" (1844, 1862) ancêtre du calcul différentiel extérieur ([6] ch. 3). En plus il est possible que ce même problème ait influencé indirectement[1] le travail de Cayley sur la formulation et l'étude de la théorie des matrices et des transformations linéaires. Ceci est d'autant plus plausible que Cayley s'intéressait profondément aux quaternions et publia, le premier après Hamilton, un travail sur le sujet en 1845 ([6], p. 35) où il examine explicitement la correspondance entre rotations de l'espace et quaternions (voir section 4, fin de section 3 et [5] vol. 1, p. 123, [9] p. 74–75). Finalement en 1848 il suivit les fameux exposés donnés par Hamilton sur les quaternions où Hamilton présentait la liaison entre quaternions et autres concepts mathématiques, et particulièrement ceux de déterminant ([6] p. 35–36).

Comme nous l'avons déjà mentionné, dans ce travail nous inversons l'approche habituelle du problème précité. Inspirés par le processus historique, nous allons être amenés à définir d'importantes notions mathématiques, comme le groupe de rotations, les quaternions, les homomorphismes de groupes etc, au lieu de les utiliser comme point de départ, comme il est fait habituellement.

Dans la section 2 la relation de $\mathbb{C}$ au groupe de rotations du plan est présentée brièvement et le problème de généralisation de $\mathbb{C}$ sera précisément formulé. Dans la section 3 les rotations de l'espace tridimensionel sont étudiées et leur représentation matricielle est donnée. Ainsi en section 4, nous sommes amenés à la découverte des quaternions et à la résolution de notre problème. Afin d'éviter l'utilisation de quaternions pour la représentation de rotations de l'espace nous expliquons en section 5, comment on est amené naturellement à l'étude de matrices unitaires $2 \times 2$. En plus nous présentons leur relation aux quaternions et à la fondation de la cinématique des corps solides réalisée par Cayley et Klein. Il doit être remarqué que les travaux originaux ne sont pas explicitement mentionnés. Nous avons préféré donner une bibliographie plus accessible, où l'intéressé trouvera les références des papiers originaux.

## 2. NOMBRES COMPLEXES ET ROTATIONS DU PLAN

Dans un système de coordonnées donné, chaque nombre complexe a une représentation trigonométrique qui correspond à un point du plan euclidien

$$z \in \mathbb{C}, z = a + ib = \rho(\cos\theta + i\sin\theta) = \rho e^{i\theta},\ \theta \in ]-\pi, \pi] \tag{2.1}$$

où la dernière relation, suggérée par le théorème de de Moivre définit la fonction exponentielle complexe, de telle manière que les principales propriétés algébriques de la fonction exponentielle réelle restent valables sur $\mathbb{C}$. En plus, elle implique

[1] Il doit être souligné que Cayley en 1894 a explicitement nié avoir introduit la notion de matrice à partir des quaternions.

une interprétation géométrique de la multiplication de $z$ par $e^{i\phi}$, c'est à dire une rotation de $z$ autour de 0 d'angle $\phi$. D'autre part, si une telle rotation applique le point $A = (x, y)$ au point $A' = (x', y')$ alors :

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \tag{2.2}$$

Donc une rotation plane d'angle $\phi$, definit une matrice $2 \times 2$

$$A_\phi = \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} \tag{2.3}$$

L'équation (2.3) donne une forme générale pour les matrices orthogonales $2 \times 2$ de déterminant 1 c.a.d une matrice satisfaisant

$$A^{-1} = A^t \tag{2.3'i}$$

$$\det A = 1 \tag{2.3'ii}$$

En général les matrices $n \times n$ satisfaisant (2.3') forment un groupe multiplicatif qui s' appelle groupe orthogonal spécial $SO(n)$. Le nom vient du fait que pour chaque $\vec{x} \in \mathbb{R}^n$ et $\vec{x'} = A\vec{x}$, $A$ satisfait (2.3'$i$), si et seulement si

$$|\vec{x'}| = |A\vec{x}| = |\vec{x}| \tag{2.4}$$

où $|\vec{x}|$ est la norme euclidienne de $\vec{x} \in \mathbb{R}^n$. Notez que $SO(2)$ est un groupe Abélien, et il est facile de vérifier que la matrice $A_{\phi_1} A_{\phi_2}$ provenant de la composition de deux rotations d' angles $\phi_1$ et $\phi_2$ est égale à $A_{\phi_1+\phi_2}$. Donc nous sommes amenés à la

Proposition 2.1 : $SO(2)$ muni de la multiplication des matrices est un groupe Abélien, isomorphe au groupe de rotations du plan, muni de l'opération de composition, (l'angle de rotation appartenant à $]-\pi, \pi](2\pi)$)

Par le théorème de de Moivre, nous pouvons obtenir le corollaire suivant :

Corollaire : Le groupe $(SO(2), .)$ est isomorphe au sous-groupe multiplicatif $S^1 = \{z \in \mathbb{C},\ |z| = 1\}$ de $\mathbb{C}$, l'isomorphisme étant établi par :

$$e^{i\theta} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \tag{2.5}$$

Les égalités (2.1) et (2.5) suggérent la définition de l'application :

$$a + bi = \rho e^{i\theta} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \rho \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \tag{2.5'}$$

et exactement de la même façon nous pouvons démontrer :

Proposition 2.2 : Si

$G = \left\{ A : A \text{ est une matrice réelle } 2 \times 2 \text{ de la forme } \begin{pmatrix} a & -b \\ b & a \end{pmatrix},\ |a| + |b| \neq 0 \right\}$

et $G_0 = G \cup \{0\}$ alors : (a) $G_0$ est un espace vectoriel réel de dimension 2, pour les opérations habituelles sur les matrices. (b) L'équation (2.5′) définit un isomorphisme entre les espaces vectoriels $G_0$ et $\mathbb{C}$, $\mathbb{C}$ étant identifié avec l'espace vectoriel $\mathbb{R}^2$. (c) $G$ et $\mathbb{C}^* = \mathbb{C} - \{0\}$ sont des groupes multiplicatifs, isomorphes, abéliens, et la relation (2.5′) définit leur isomorphisme.

La proposition 2.2(b,c), montre que $G_0$ est un corps isomorphe à $\mathbb{C}$. D'autre part chaque $A \in G$ définit la composition d'une rotation d'angle $\theta = \arccos\left(\frac{a}{(a^2+b^2)^{1/2}}\right) = \arcsin\left(\frac{b}{(a^2+b^2)^{1/2}}\right)$ et d'une homothétie $\vec{x} \mapsto \rho\vec{x}$ où $\rho = \sqrt{\det A} = \sqrt{a^2+b^2}$. Ainsi "la question se pose maintenant : comment les transformations correspondantes dans l'espace de dimension 3 peuvent-elles être représentées par calculs de nombres complexes d'un ordre supérieur" ([12] p. 172). Cette question est identique a celle soulevée en section 1 et la proposition 2.2 permet d'établir une formulation précise :

Question : **Est-il possible de trouver un corps, extension de $\mathbb{C}$ (c'est-à-dire qui contient un sous-corps isomorphe à $\mathbb{C}$), dont le groupe de multiplication est isomorphe au groupe généré par les rotations et les homothéties de l'espace euclidien tridimensionel?**

Il est évident que ce que nous cherchons est une généralisation de la Proposition 2.2(c) dans l'espace, pour une sorte de nombres "complexes généralisés".

Remarques (a) : Contrairement à ce qui se passe en deux dimensions, rotations et similitudes dans l'espace tridimensionel, ne génèrent pas un ensemble de matrices qui soit un espace vectoriel réel. En section 5 nous généralisons la Proposition 2.2(b,c) pour les matrices complexes $2 \times 2$.

(b) : En 1833 Peacock introduisit le "Principle of Permanence" selon lequel, chaque généralisation d'une notion algébrique doit obéir à des règles de calcul, ayant les mêmes propriétés que celles de la notion d'origine ([7], vol. II p.360–361 et vol I p. 92–93 et 106. Voir aussi remarques sur quaternions en section 1). Ce principe apparaît alors en langage mathématique moderne dans la formulation de la question mentionnée plus haut.

(c) : Chaque $a + ib$ définit biunivoquement un opérateur linéaire sur $\mathbb{C}$ :

$$x + iy \mapsto x' + iy' = (a + ib)(x + iy) \tag{2.6}$$

qui, d'un point de vue géométrique, est la composition d'une rotation et d'une homothétie dans le plan (cf (2.5′), (2.2)). C'est un point essentiel qui révèle la relation entre $\mathbb{C}$ et les rotations du plan, contenue dans la Proposition 2.2. Cependant, une deuxième interprétation, mathématiquement équivalente mais conceptuellement différente, est de regarder (2.6) comme une relation qui permet

la multiplication des vecteurs du plan. Et c'est un fait historique qu'au début tous les mathématiciens (y compris Hamilton) pensaient que les vecteurs dans l'espace étaient une sorte de généralisation de nombres complexes, pour lesquels une règle de multiplication devait être inventée ayant une interprétation analogue à celle impliquée par (2.6) pour les vecteurs du plan ([10] Préface au "Lectures on Quaternions" §§36, 43). Mais de ce point de vue, la question posée plus haut ne pourrait pas être formulée si précisement, étant donné que la deuxième interprétation de la multiplication de $\mathbb{C}$ est essentiellement due à la Proposition 2.2(a,b) pour laquelle il n' existe pas d'analogue dans l'espace tridimensionel (voir remarque (a) et les commentaires historiques en Section 4).

D'autre part, cette seconde interprétation, était plus évidente en ce temps là (c'est-à-dire avant 1843) parce que la notion de matrice (si bien adaptée pour l'étude des rotations et des transformations linéaires en général) n' était pas encore disponible : en fait, comme il était affirmé plus tard par Gibbs ([6] p. 76, [19] p. XXIII), l'idée décisive permettant de l'établir ne peut pas être recherchée avant le travail de Grassmann, en 1844. En 1850 Sylvester introduisit la notion—et le nom— de matrice et il montra comment former son déterminant ([7] vol. I p. 96, [3] p. 85, [14] vol. 3 ch. XLII, §704). Cependant, c'est Cayley qui en 1855 définit la multiplication de matrices et ultérieurement en 1858 et 1866, présenta la théorie algébrique adéquate et leur relation aux transformations linéaires ([5] vol. 2 p. 475, [7] vol. I p. 96, [11] p. 204–205). En fait "la réponse est venue directement de la simple observation de la méthode par laquelle les transformations (linéaires) de la théorie des invariants algébriques [dans laquelle Cayley et Sylvester ont été impliqués à la fois] sont combinées.

## 3. LES ROTATIONS DE L'ESPACE

Nous allons étudier maintenant les rotations de l'espace. Sans perdre en généralité, nous considérons seulement des rotations autour d'un axe passant par l'origine $O$ d'un système de coordonnées $Oxyz$ arbitrairement choisi. Une rotation est complètement déterminée si (a) : on connait l' axe de rotation, disons la ligne droite $(\epsilon)$ et l'angle de rotation $\omega$ ou si (b) : on sait que le système $Oxyz$ est amené, par rotation à coincider avec le système $Ox'y'z'$.
Cas (a) : Soit $(\epsilon)$ dans la direction du vecteur unitaire $\vec{n}$, et $\alpha$, $\beta$, $\gamma$ les angles de direction : en général nous pouvons supposer $\alpha$, $\beta$, $\gamma \in [0, \pi]$ (figure 1).

Alors,

$$\vec{n} = (\cos\alpha, \cos\beta, \cos\gamma), \quad \cos^2\alpha + \cos^2\beta + \cos^2\gamma = 1 \tag{3.1}$$

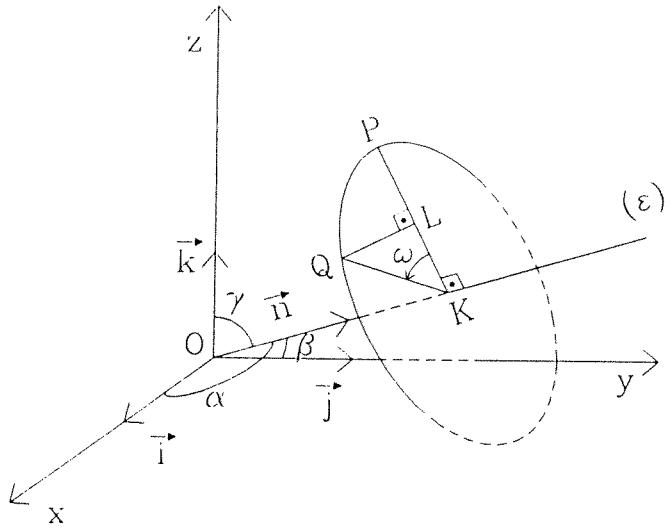



*Figure 1*

Soit le point $P = (x, y, z)$ transformé en $Q = (x', y', z')$ sous l'effet de la rotation. Nous voulons exprimer $x', y', z'$ comme fonctions de $x, y, z$. Si $\Pi$ est le plan de $P, K, Q$ où $K$ est la projection de $P$ sur $(\epsilon)$ et si $L$ est la projection de $Q$ sur $PK$, alors par les figures 1 et 2 et grâce à la relation $|\overrightarrow{KQ}| = |\overrightarrow{KP}|$ nous pouvons trouver facilement :

$$\overrightarrow{OQ} = \overrightarrow{OP} + \overrightarrow{PL} + \overrightarrow{LQ} \tag{3.2}$$

$$\overrightarrow{PL} = (1 - \cos\omega)\overrightarrow{PK} = (1 - \cos\omega)(\overrightarrow{OK} - \overrightarrow{OP}) = -(1 - \cos\omega)(\overrightarrow{OP} - (\overrightarrow{OP} \cdot \vec{n})\vec{n}) \tag{3.3i}$$

$$\overrightarrow{LQ} = \frac{|\overrightarrow{LQ}|\vec{n} \times \overrightarrow{KP}}{|\vec{n} \times \overrightarrow{KP}|} = \frac{|\overrightarrow{KQ}| \sin\omega\vec{n} \times \overrightarrow{OP}}{|\overrightarrow{KP}|} = \sin\omega\vec{n} \times \overrightarrow{OP} \tag{3.3ii}$$

où nous avons utilisé la notation habituelle pour le produit scalaire et le produit vectoriel de vecteurs. La substitution de (3.3) dans (3.2) nous permet d'obtenir finalement :

$$\overrightarrow{OQ} = \overrightarrow{OP} - (1 - \cos\omega)(\overrightarrow{OP} - (\overrightarrow{OP} \cdot \vec{n})\vec{n}) + \sin\omega\ \vec{n} \times \overrightarrow{OP} \tag{3.4}$$

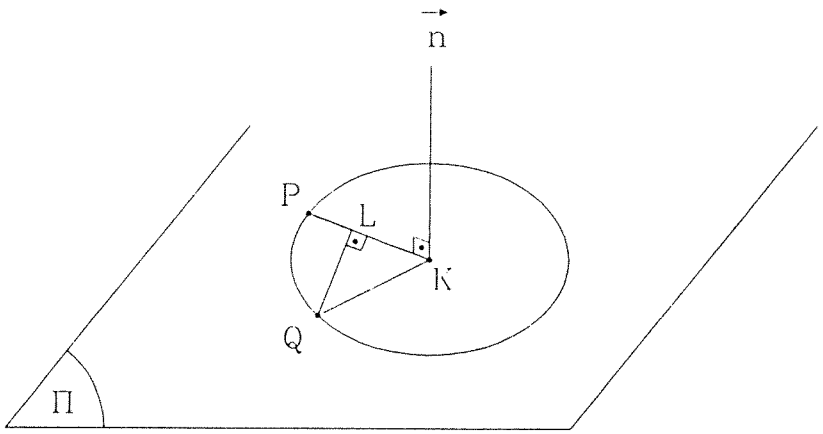



*Figure 2*

L'équation (3.4) écrite sous forme de composantes algébriques, nous suggère l'introduction des paramètres d'Euler (voir notice historique à la fin de cette section) définis par

$$\left.\begin{aligned} e_0 &= \cos(\omega/2), \qquad e_1 = \cos\alpha \sin(\omega/2) \\ e_2 &= \cos\beta \sin(\omega/2), \; e_3 = \cos\gamma \sin(\omega/2) \end{aligned}\right\} \text{ ou } \begin{cases} e_0 = \cos(\omega/2) \\ \vec{e} \equiv (e_1, e_2, e_3) = \vec{n}\sin(\omega/2) \end{cases} \tag{3.5}$$

Remarquez que (3.4) peut être mise sous la forme suivante :

$$\overrightarrow{OQ} = (2e_0^2 - 1)\overrightarrow{OP} + 2(\overrightarrow{OP} \cdot \vec{e})\vec{e} + 2e_0\vec{e} \times \overrightarrow{OP}$$

ou sous forme matricielle, en utilisant la relation

$$e_0^2 + e_1^2 + e_2^2 + e_3^2 = 1 \tag{3.6}$$

qui est déduite de (3.5), comme

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} e_0^2 + e_1^2 - e_2^2 - e_3^2 & 2(e_1e_2 - e_0e_3) & 2(e_1e_3 + e_0e_2) \\ 2(e_1e_2 + e_0e_3) & e_0^2 - e_1^2 + e_2^2 - e_3^2 & 2(e_2e_3 - e_0e_1) \\ 2(e_1e_3 - e_0e_2) & 2(e_2e_3 + e_0e_1) & e_0^2 - e_1^2 - e_2^2 + e_3^2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} \tag{3.4'}$$

Le sens de (3.6) sera étudié en section 4. Ici nous remarquons seulement que si $A$ est la matrice définie en (3.4'), alors après quelques calculs algébriques nous trouvons que $A \in SO(3)$. Des démonstrations plus simples qui évitent des calculs, peuvent être obtenues à partir de (3.7) ou par l'équation de conservation de la norme du vecteur, (2.4). Inversement pour chaque $A \in SO(3)$, il est évident que la transformation $\vec{x'} = A\vec{x}$ de $\mathbb{R}^3$ définit une rotation autour de l'origine du système de coordonnées. Ainsi $SO(3)$ est en correspondance biunivoque avec les rotations de l'espace.

Cas (b) : Supposons que le système $Oxyz$ soit transformé en $Ox'y'z'$. Soit $O\xi$ l'intersection des plans $Oxy$ et $Ox'y'$. Alors les angles d'Euler (Euler 1776) $\phi$, $\theta$, $\psi$ sont déterminés de façon unique par (Figure 3c)

$$\phi, \psi \in [0, \pi],\ \theta \in [0, 2\pi]$$

$$\phi = \angle(Ox, O\xi),\ \psi = \angle(O\xi, Ox'),\ \theta = \angle(Oz, Oz')$$

où la notation indique qu'ils sont mesurés dans le sens inverse des aiguilles d'une montre. Maintenant, il est évident que la rotation de $Oxyz$ à $Ox'y'z'$ est la composition des rotations suivantes, dans le sens inverse des aiguilles d'une montre.
— une rotation d'un angle $\phi$ autour de l'axe $Oz$ (système $O\xi\eta\zeta$)
— une rotation d'un angle $\theta$ autour de l'axe $O\xi$ (système $O\xi'\eta'\zeta'$)
— une rotation d'un angle $\psi$ autour de l'axe $O\zeta'$ (système $Ox'y'z'$)
Remarque : Dans la littérature concernant les angles d'Euler, la définition n'est pas unique. Ici nous suivons [8] ch. 4

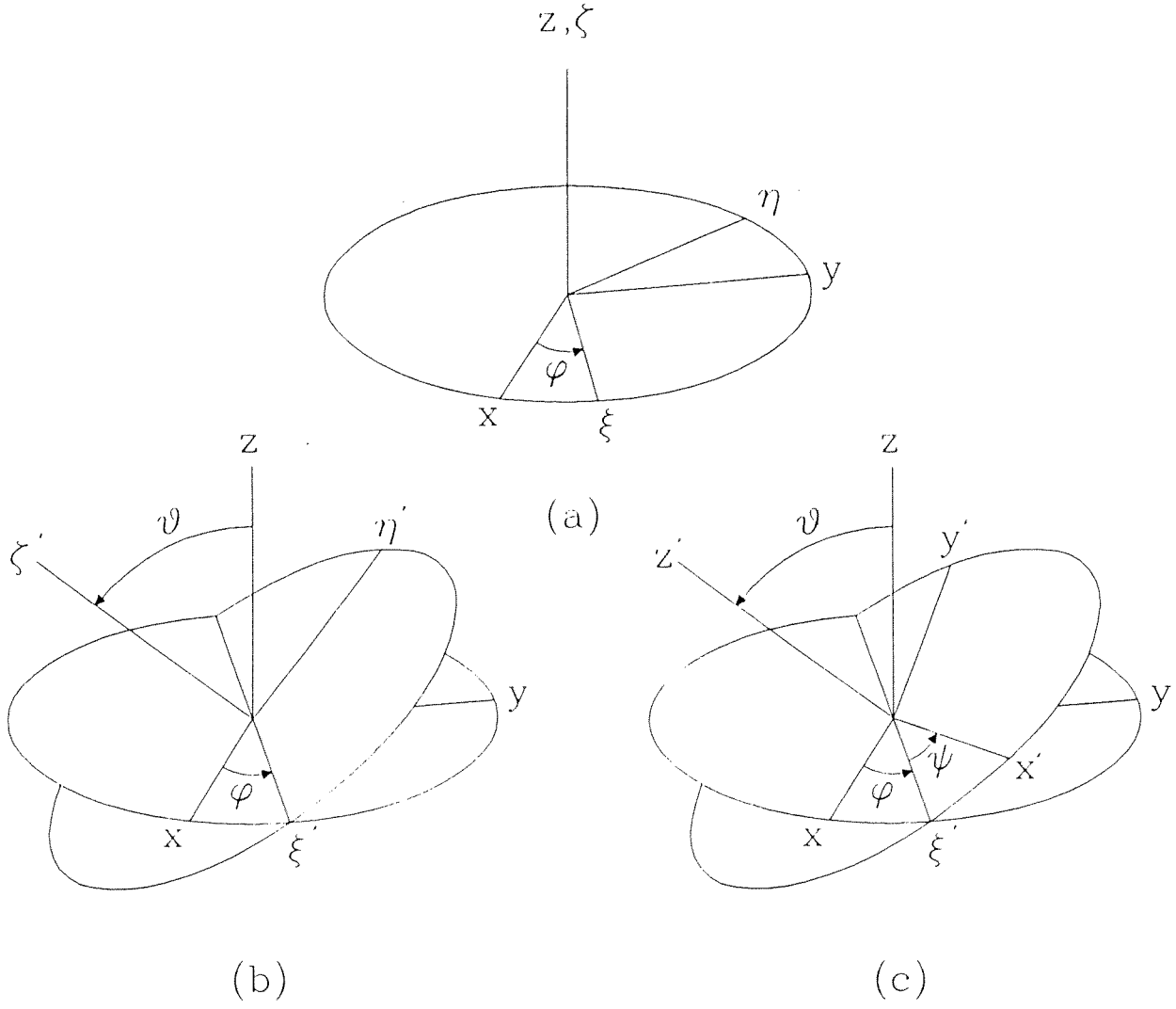



*Figure 3*

Une expression explicite des rotations définies plus haut peut être obtenue en remarquant que chacune d'entre elles est une rotation autour d'un des axes du système de coordonnées correspondant. Par exemple pour la rotation $\phi$, il est clair que $z$ n'est pas changé et en conséquence l'équation matricielle correspondante est [cf (2.2)]

$$\begin{pmatrix} \xi \\ \eta \\ \zeta \end{pmatrix} = \begin{pmatrix} \cos\phi & -\sin\phi & 0 \\ \sin\phi & \cos\phi & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = A_\phi \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

De la même façon :

$$\begin{pmatrix} \xi' \\ \eta' \\ \zeta' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \xi \\ \eta \\ \zeta \end{pmatrix} = A_\theta \begin{pmatrix} \xi \\ \eta \\ \zeta \end{pmatrix}$$

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} \cos\psi & -\sin\psi & 0 \\ \sin\psi & \cos\psi & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \xi' \\ \eta' \\ \zeta' \end{pmatrix} = A_\psi \begin{pmatrix} \xi' \\ \eta' \\ \zeta' \end{pmatrix}$$

Alors,

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = A_\psi A_\theta A_\phi \begin{pmatrix} x \\ y \\ z \end{pmatrix} \tag{3.7}$$

Les descriptions des rotations de l'espace (a) et (b) données par (3.4′) et (3.7) sont évidemment équivalentes, et par conséquent la relation entre les angles d'Euler et les paramètres d'Euler est donnée par l' identification des matrices correspondantes. Ainsi après quelques calculs élémentaires nous obtenons :

$$\begin{aligned} e_0 &= \pm\cos\left(\tfrac{\psi+\phi}{2}\right)\cos\tfrac{\theta}{2} \quad & e_2 &= \pm\sin\left(\tfrac{\psi-\phi}{2}\right)\sin\tfrac{\theta}{2} \\ e_1 &= \pm\cos\left(\tfrac{\psi-\phi}{2}\right)\sin\tfrac{\theta}{2} \quad & e_3 &= \pm\sin\left(\tfrac{\psi+\phi}{2}\right)\cos\tfrac{\theta}{2} \end{aligned} \tag{3.8}$$

L'équation (3.5) nous permet facilement de déduire que chaque ensemble $\{e_i\}$ définit exactement une rotation dans l'espace. L'inverse n' est pas vrai, parce que $\{-e_i\}$ définit la même rotation à cause de (3.5). Nous y reviendrons dans les sections suivantes. D'après (3.4′), (3.7) il est clair que la représentation des rotations par les angles d'Euler est plus compliquée et moins symétrique que celle basée sur les paramètres d'Euler ou $(\omega, \alpha, \beta, \gamma)$. Bien sûr l'avantage de leur utilisation est la factorisation de la rotation (3.7) et le fait qu'elles sont indépendantes, contrairement à ce qui se passe avec $\{e_i\}$ ou $\{\omega, \alpha, \beta, \gamma\}$ (cf (3.1), (3.6)). Dans une terminologie plus rigoureuse, elles forment un ensemble de coordonnées pour $SO(3)$ considéré comme groupe de Lie.

Commentaire historique : En 1770, Euler introduisit les $e_i$ dans l'expression paramétrique d'une isométrie de la métrique euclidienne de $\mathbb{R}^3$ (il obtint aussi le résultat correspondant pour $\mathbb{R}^4$). Ils apparaissent aussi en 1776 dans son étude

de la mécanique des corps rigides. En 1841 ils sont introduits par Rodrigues dans la description de rotations infinitésimales dans $\mathbb{R}^3$. En 1845, c'est en utilisant les quaternions, que Cayley obtient les expressions d'Euler dans la toute première publication sur les quaternions après celle de Hamilton (voir Sections 1 et 4) et en 1846 il réussit à les généraliser dans $\mathbb{R}^n$. Un peu plus tard, Hermite donna la forme paramétrique des isométries de toute forme quadratique dans $\mathbb{R}^3$. Finalement, en 1855 Cayley exprima les résulats de Hermite comme produit de matrices. Il parait que ce fait joua un rôle essentiel dans sa formulation du calcul matriciel en 1858 (pour des détails supplémentaires voir [7] vol. I p. 66–67, 95–96, [5] vol. 1 p. 123 et 2 p. 475, [9] p. 71, [20] §9 et références ci mentionnées).

## 4. "LE PROBLÈME DE HAMILTON" ET LES QUATERNIONS

Maintenant nous sommes preparés à étudier en détail la question posée à la fin de la Section 2. Appelons ce problème "problème de Hamilton" non pour cause de précision historique mais dans le but de mettre en évidence le fait que ce problème dans sa vague formulation présentée en section 1, était une des motivations principales de Hamilton, dans son effort vers une de ses plus grandes découvertes qui était la définition des quaternions. Dans cette section cette notion sera décrite en langage moderne . Comme point de départ nous prenons (3.6) qui nous suggère de considérer $\{e_i\}$ comme coordonnées d'un point de $\mathbb{R}^4$. Par conséquent si nous écrivons :

$$\vec{p} \in \mathbb{R}^4, \vec{p} = e_0\vec{1} + e_1\vec{\imath} + e_2\vec{\jmath} + e_3\vec{k} \tag{4.1}$$

où

$$\vec{1} = (1,0,0,0),\ \vec{\imath} = (0,1,0,0),\ \vec{\jmath} = (0,0,1,0),\ \vec{k} = (0,0,0,1) \tag{4.2}$$

est le repère canonique de $\mathbb{R}^4$, alors (3.7) représente la sphère tridimensionelle de rayon 1, $S^3$, dont chaque point définit exactement une rotation. L'inverse n'est pas vrai, voir dernier paragraphe de la Section 3.

Le pas crucial vers la découverte des quaternions, relié au problème de Hamilton, est l'étude de la composition (produit) de deux rotations de l' espace et des paramètres d'Euler correspondants. Plus spécialement, si pour deux rotations de matrices $A$, $A'$ et de paramètres d'Euler respectifs $\{e_i\}$, $\{e'_i\}$ , leur composition de matrice $A'' = AA'$ a comme paramètres d'Euler $\{e''_i\}$, alors en utilisant (3.4) et (3.6) nous obtenons (après quelques calculs algébriques, fastidieux mais élémentaires) que :

$$\begin{aligned} e''_0 &= e_0e'_0 - e_1e'_1 - e_2e'_2 - e_3e'_3 \\ e''_1 &= e_1e'_0 + e_2e'_3 - e_3e'_2 + e_0e'_1 \\ e''_2 &= e_2e'_0 + e_3e'_1 - e_1e'_3 + e_0e'_2 \\ e''_3 &= e_3e'_0 + e_1e'_2 - e_2e'_1 + e_0e'_3 \end{aligned} \tag{4.3}$$

L'interprétation la plus intéressante de (4.3) est qu'elle nous définit une règle de multiplication pour les éléments de $\mathbb{R}^4$. Plus précisément si $\vec{p}$, $\vec{p'} \in \mathbb{R}^4$ avec

$$\vec{p} = e_0\vec{1} + e_1\vec{\imath} + e_2\vec{\jmath} + e_3\vec{k}, \quad \vec{p'} = e'_0\vec{1} + e'_1\vec{\imath} + e'_2\vec{\jmath} + e'_3\vec{k} \tag{4.3'}$$

et si nous définissons le produit

$$\vec{p}\vec{p'} = \vec{p''} = e_0''\vec{1} + e_1''\vec{\imath} + e_2''\vec{\jmath} + e_3''\vec{k} \tag{4.3''}$$

où $\{e_i''\}$ sont donnés par (4.3), alors en prenant successivement $\vec{p}$, $\vec{p'}$ comme éléments du repère canonique (4.2) nous obtenons que $\vec{1}$ est l'élément neutre et que

$$\vec{\imath}^2 = \vec{\jmath}^2 = \vec{k}^2 = -\vec{1} \tag{4.4$i$}$$

$$\vec{\imath}\vec{\jmath} = -\vec{\jmath}\vec{\imath} = \vec{k}, \qquad \vec{\jmath}\vec{k} = -\vec{k}\vec{\jmath} = \vec{\imath}, \qquad \vec{k}\vec{\imath} = -\vec{\imath}\vec{k} = \vec{\jmath} \tag{4.4$ii$}$$

qui sont les relations réputées de Hamilton définissant le produit des éléments du repère de quaternions. Il est clair maintenant que à cause de (4.4) les équations (4.3) et (4.3'') sont équivalentes. Alors de (4.4) nous concluons que cette multiplication est non communative, dotant ainsi $\mathbb{R}^4$ de la structure d'un corps non abélien. Donc nous pouvons donner la

Définition 4.1 : $(\mathbb{R}^4, +, \cdot)$ avec l'addition habituelle et le produit défini par (4.4) (et étendu linéairement à tous les éléments) est le corps (non abélien) $H$ des quaternions.

Remarques : Si pour $\vec{p}$ dans (4.1), $|\vec{p}|$ est la norme euclidienne et si nous définissons son conjugué $\vec{p^*}$ par :

$$\vec{p^*} = e_0\vec{1} - e_1\vec{\imath} - e_2\vec{\jmath} - e_3\vec{k} \tag{4.5}$$

nous pouvons démontrer facilement :

$$(\vec{p}\vec{q})^* = \vec{q^*}\vec{p^*}, \quad |\vec{p}\vec{q}| = |\vec{p}||\vec{q}|, \quad \vec{p}^{-1} = \frac{\vec{p^*}}{|\vec{p}|^2} \tag{4.6}$$

et par conséquent que

(a) : l'ensemble $H_1 = \{\vec{p} \in H : |\vec{p}| = 1\}$ est un sous groupe multiplicatif de $H$

(b) : le sous ensemble de $H$, $\{\vec{p} = e_0\vec{1} + e_1\vec{\imath},\ e_0, e_1 \in \mathbb{R}\}$ est un corps isomorphe à $\mathbb{C}$.

Ceci explique la notation inhabituelle dans (4.2).

(c) : L'application

$$H_1 \to SO(3) : e_0\vec{1} + e_1\vec{\imath} + e_2\vec{\jmath} + e_3\vec{k} \mapsto \{e_0, e_1, e_2, e_3\} \tag{4.7}$$

est un homomorphisme injectif de groupes, son expression explicite étant (3.4'). En fait, un calcul direct montre qu'en utilisant les quaternions, (3.4') peut être présentée dans une forme plus élégante :

$$\vec{x'} = \vec{p}\vec{x}\vec{p}^{-1} \tag{4.8}$$

Ici $\vec{p}$ est donné par (4.1) en termes d'angles d'Euler et :

$$\vec{x} = x\vec{\imath} + y\vec{\jmath} + z\vec{k}, \quad \vec{x'} = x'\vec{\imath} + y'\vec{\jmath} + z'\vec{k}$$

Cette relation des quaternions aux rotations de l'espace fut découverte par Cayley dès 1845 dans sa publication déjà mentionnée en section 1. En plus, celle-ci montre clairement que $\vec{p}$ et $-\vec{p}$ définissent la même rotation comme nous l'avons mentionné déjà au dernier paragraphe de la Section 3.

Finalement si la contrainte (3.6) ne s' impose plus, alors (4.7) est un homomorphisme injectif de $H - \{0\}$ dans le groupe généré par les rotations et les similitudes de l'espace. Il est clair maintenant que (b) et (c) impliquent une réponse négative au problème de Hamilton pour deux raisons : (i) La multiplication dans $H$ est non commutative, (ii) (4.7) n'est pas un isomorphisme (voir (4.8)). Dans la section suivante nous verrons comment nous pouvons surmonter (ii) pour obtenir une compréhension plus profonde des rotations de l'espace et généraliser ainsi la proposition (2.2). D'autre part, la raison (i) qui constitue l'innovation majeure de Hamilton dans son travail sur les quaternions vue dans un contexte moderne, est insurmontable à cause du fait que $SO(3)$ est un groupe non abélien et l'isomorphisme entre groupes conserve la (non) commutativité du produit.
Commentaires historiques : Comme nous l'avons déjà mentionné en Section 1, l'approche originale de Hamilton était de caractère algébrique. Exprimée en langage moderne, elle consiste à munir $\mathbb{R}^4$ d'un produit de telle façon qu'avec l'addition habituelle il devienne un corps commutatif satisfaisant (4.6*ii*) ([7] ch. III p. 106 ff). Hamilton dépensa bien du temps en essayant d'obtenir un résultat semblable dans $\mathbb{R}^3$. En fait il essaya de définir le produit de deux vecteurs de l'espace en respectant les propriétés principales du produit de deux vecteurs du plan (particulièrement (4.6ii)), imposée par la représentation géométrique des nombres complexes (voir remarque (c) en Section 2). Bien sûr il s'avéra que c'était impossible. En fait il lui a fallu presque 14 ans pour se rendre compte que la réponse à son problème pouvait être obtenue en considérant $\mathbb{R}^4$ et en rejetant la commutativité du produit ([6] §2 IV, [18]). Plus tard, Cayley (en 1881) et Hurwitz (en 1898) montrèrent que si un produit est défini dans $\mathbb{R}^n$, et induit une structure d'algèbre (en général non associative) réelle, alors (4.6*ii*) peut être valable pour la norme euclidienne seulement si $n = 1, 2, 4, 8$. D'autre part, Frobenius en 1878 et C.S Pierce en 1881 avaient déjà montré que chacune de ces algèbres qui en même temps est un corps (non nécessairement commutatif) c'est-à-dire avec une division non ambigüe, est (isomorphe à) $\mathbb{R}$, $\mathbb{C}$ ou $H$ ou à une somme directe de ces corps ([2] p. 159, [7] vol I p. 108, [3] p. 151 et références là-dedans).

## 5. LES PARAMÈTRES DE CAYLEY–KLEIN ET LE GROUPE $SU(2)$

Dans la section précédente nous avons vu qu'avec la notion des quaternions une réponse négative fut donnée au problème de Hamilton, suggérée par les deux raisons (i) et (ii) données à la fin de la Section 4. Ici nous verrons qu'il est possible (i) de formuler la proposition 2.2 pour $H$ en utilisant des "rotations" dans l'espace complexe $\mathbb{C}^2$, (ii) de donner une réponse au problème de Hamilton en terme de ces "rotations".

Nous avions constaté qu'à cause de (3.6), les paramètres d'Euler peuvent être

interprétés comme coordonnées d'un point sur la sphère $S^3$ dans $\mathbb{R}^4$. Ceci nous amène aux quaternions dont le calcul correspondant ne nous est pas très familier.

C'est pourquoi si nous voulons éviter cette interprétation évidente des paramètres d'Euler, alors (3.8) suggère naturellement l'introduction des paramètres de Cayley–Klein (CK) (Cayley 1879, Klein 1896)[2]

$$a = \cos(\theta/2)e^{i(\phi+\psi)/2}, \qquad b = \sin(\theta/2)e^{i(\psi-\phi)/2} \tag{5.1$i$}$$

$$d = a^*, \qquad c = -b^* \tag{5.1$ii$}$$

En choisissant le signe + dans (3.8) nous avons

$$\left.\begin{aligned} a &= e_0 + ie_3 \\ b &= e_1 + ie_2 \end{aligned}\right\} \Leftrightarrow \left\{\begin{aligned} e_0 &= \tfrac{a+d}{2} \quad e_1 = \tfrac{b-c}{2} \\ e_3 &= \tfrac{a-d}{2i} \quad e_2 = \tfrac{b+c}{2i} \end{aligned}\right. \tag{5.1$'$}$$

$$ad - bc = 1 \tag{5.2}$$

C'est une question d'algèbre élémentaire de montrer qu'avec l'aide de (5.1′) l'égalité (3.4) s' écrit :

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} \frac{(a^2+b^2+c^2+d^2)}{2} & \frac{i(a^2-b^2+c^2-d^2)}{2} & -i(ab+cd) \\ \frac{i(-a^2-b^2+c^2+d^2)}{2} & \frac{(a^2-b^2-c^2+d^2)}{2} & dc-ab \\ i(ac+bd) & db-ac & ad+bc \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} \tag{5.3}$$

Maintenant si, comme en Section 4, nous considérons des rotations de matrices $A, A'$ et de paramètres CK correspondants $(a,b,c,d)$, $(a',b',c',d')$ et si leur composition ayant comme matrice $A'' = AA'$, a pour paramètres CK $\{a'', b'', c'', d''\}$ alors par (5.3) nous obtenons après des calculs fastidieux mais élémentaires que :

$$\begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \tag{5.4}$$

Ainsi nous sommes amenés naturellement à considérer des matrices complexes de la forme suivante

$$T = \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix} \tag{5.5}$$

L'égalité (5.5) donne la forme la plus générale d'une matrice complexe $2 \times 2$ qui satisfait

$$TT^+ = I \tag{5.6}$$

et ayant comme déterminant $+1$, où $T^+$ est la matrice adjointe de $T$. Des matrices $n \times n$ ayant cette propriété sont appelées unitaires. Elles ont un déterminant $\pm 1$ et forment le groupe multiplicatif $U(n)$. Celles qui ont un déterminant $+1$ forment le groupe $SU(n)$ qui est un sous-groupe de $U(n)$. Il est clair que $U(1) = S^1$. En plus pour $T \in U(n)$ et $\vec{x} \in \mathbb{C}^n$

$$|T\vec{x}| = |\vec{x}| \tag{5.7}$$

[2] Dans son travail original, Cayley utilisa $a^*, ib$ au lieu de $a$, $b$ ([5], vol 10 p. 153)

où $|\vec{x}|$ est la norme habituelle de $\mathbb{C}^n$. Ainsi (5.7) est l'analogue de (2.4) justifiant l'image présentant les matrices unitaires, comme "rotations" dans $\mathbb{C}^n$. Nous pouvons donc conclure que par (4.1) (5.1′) et (5.5) il existe une correspondance biunivoque entre $H$ et $SU(2)$. De ce qui a été dit plus haut, et en se rappelant de (5.4), (4.3″) il est maintenant facile de compléter les détails dans la démonstration de la proposition :

Proposition 5.1 : Si

$$F = \left\{ T : T \text{ est une matrice } 2 \times 2 \text{ complexe, de forme } \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix},\ |a|+|b| \neq 0 \right\}$$

alors (a) : $F \cup \{0\} \equiv F_0$ est un espace vectoriel réel de dimension 4.
(b) : L'application (voir (5.1′))

$$\vec{p} = e_0\vec{1} + e_1\vec{i} + e_2\vec{j} + e_3\vec{k} \rightarrow T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{5.8}$$

de $H$ à $F_0$ est un isomorphisme entre espaces vectoriels.
(c) : L'égalité (5.8) définit un isomorphisme entre les groupes $H^*$ et $F$, et $H_1$ et $SU(2)$. Celle-ci est la généralisation de la proposition 2.2 mentionnée au début de cette Section et elle nous donne une réponse positive au problème de Hamilton si au lieu de "rotations" dans $\mathbb{R}^3$, elle est formulée pour les "rotations" dans $\mathbb{C}^2$ et si nous ne demandons pas un produit commutatif. Pour exprimer son contenu explicitement nous notons que avec l'aide de (5.1′) l'égalité (5.8) prend la forme :

$$\vec{p} = e_0\vec{1} + e_1\vec{i} + e_2\vec{j} + e_3\vec{k} \rightarrow T = e_0 I + e_1\tau_1 + e_2\tau_2 + e_3\tau_3 \tag{5.8′}$$

où

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \tau_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$
$$\tau_2 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad \tau_3 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \tag{5.9}$$

Ici les $\tau_n$ $(n = 1, 2, 3)$ sont les matrices de Pauli. Pauli les introduisit en 1927 pour réussir à formuler mathématiquement le concept du spin de l'électron, introduit peu de temps avant (1925) par Goudsmidt et Uhlenbeck ([11] §3.4, [15] §13 b). Les $\{\tau_n\}$ ont un tableau de multiplication identique à celui de la base de quaternions. Ceci entraine la démonstration de la proposition 5.1(c).

Finalement, puisque les groupes $H_1$, $SU(2)$ sont isomorphes et (4.7) définit un 2-1 homomorphisme de $H_1$ sur $SO(3)$, la même chose est valable pour $SU(2)$ (les quaternions $\vec{p}, -\vec{p}$ et les matrices $T, -T$ dans (5.8′) définissent la même rotation dans $\mathbb{R}^3$).

Néanmoins il est intéressant d'écrire explicitement cet homomorphisme, puisque ceci est possible dans une forme compacte et élégante, ce qui n'est pas le cas pour (4.7). Plus spécifiquement, de (5.1) et (5.5) nous obtenons immédiatement :

$$T = \begin{pmatrix} e^{i\psi/2} & 0 \\ 0 & e^{-i\psi/2} \end{pmatrix} \begin{pmatrix} \cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & \cos(\theta/2) \end{pmatrix} \begin{pmatrix} e^{i\phi/2} & 0 \\ 0 & e^{-i\phi/2} \end{pmatrix} = T_\psi T_\theta T_\phi \tag{5.10}$$

Par conséquent l'expression explicite de l'homomorphisme cité plus haut est :

$$SU(2) \to SO(3) : A \mapsto T \tag{5.11}$$

où $A$ est donnée par (3.7). La factorisation (5.10) de $T \in SU(2)$ correspond exactement à (3.7) pour $SO(3)$. Une comparaison entre (3.7) et (5.11) nous amène à quelques remarques très intéressantes :

(i) Les matrices $T_\psi$, $T_\theta$, $T_\phi$ correspondent à $A_\psi$, $A_\theta$, $A_\phi$ respectivement, définissant en même temps des sous-groupes à un paramètre de $SU(2)$ et $SO(3)$.

(ii) Le fait que (5.11) n'est pas un isomorphisme est dû à l'apparition de demi-angles dans (5.10) en contraste avec (3.7).

(iii) L'équation (5.11) montre que l'homomorphisme $SU(2) \to SO(3)$ est plus explicite en termes d'angles d'Euler qu'en termes de paramètres d'Euler ou de paramètres CK. Ceci est lié directement au fait que les deux groupes sont étroitement reliés comme groupes de Lie et les angles d'Euler peuvent êtres utilisés comme coordonnées (locales) pour tous les deux. En effet $SU(2)$ est ce qu'on appelle le revêtement universel de $SO(3)$. Mais cela nous amène directement dans les domaines de la Topologie et de la Géométrie Differentielle.

Nous concluons ce travail avec quelques commentaires historiques sur les équations (5.11) et (5.8) : Historiquement la relation entre $SU(2)$ et $SO(3)$ contenue dans (5.11), ne fût pas trouvée comme nous venons de le présenter. Cayley et Klein procédèrent d'une manière différente mais équivalente; nous donnons ici un bref aperçu : (voir [5] Vol. 10, p. 153, "Princeton Lectures" de 1896 de Klein sur "The mathematical theory of the top" réédité en [13] ch. LXXV et [20] §12 et références là-dedans. Pour un traitement plus détaillé consultez le travail assez accessible de Synge dans [17]) : Klein dans son travail sur les solides réguliers (1875) et spécialement sur l'icosaèdre (1875), considéra la relation entre les rotations d'une sphère et les transformations homographiques ([13] chs. LI, LIV). Plus spécifiquement il considéra la projection stéréographique d'une sphère centrée à l'origine des coordonnées, du pôle nord défini lui même comme le point d'intersection avec l' axe des $z$, sur le plan complexe. Par conséquent chaque rotation de la sphère induit une transformation (conforme) sur le plan. Puisque les cercles sont projetés stéréographiquement sur des cercles, nous concluons facilement que la transformation induite sur le plan, applique disques circulaires sur disques circulaires. Alors en tenant compte d'un résultat de la théorie des fonctions, c'est une transformation homographique $z \mapsto z = (az+b)/(cz+d)$, où $a$, $b$, $c$, $d$ sont par démonstration les paramètres CK (Cayley (1879), Klein (1896)). Maintenant il suffit de quelques calculs directs pour montrer que la composition de deux rotations, induit la composition des transformations homographiques correspondantes, c'est-à-dire l'équation (5.4) sur laquelle est basée la démonstration de la proposition 5.1 ([20], §12).

Remerciements : L'auteur est reconnaissant au professeur M. Lambrou des nombreuses discussions fructueuses et des remarques critiques ainsi qu'aux Docteurs A. Dimakis et J. Stratis qui lui ont rendu accessible une partie de la littérature originale.

## RÉFÉRENCES

1. E.T. Bell, "Men of Mathematics", Penguin books 1953.
2. E.T. Bell, "Mathematics : Queen and Servant of Science", McGraw-Hill, New York 1951.
3. N.Bourbaki, "Éléments d'histoire des Mathématiques", Hermann, Paris 1969.
4. C.B. Boyer, "A history of mathematics", J. Wiley, New York 1968.
5. A. Cayley, "Collected Mathematical Papers", Cambridge University Press, Cambridge 1889-1898.
6. M.J. Crowe, "A history of vector analysis", Dover Publications Inc., New York 1985.
7. J. Dieudonné (editeur), "Abrégé d'histoire des Mathématiques 1700–1900", Hermann, Paris 1978.
8. H. Goldstein, "Classical Mechanics", Addison-Wesley, Reading Massachussets 1980.
9. G. Greenhill, "Gyroscopic theory", Chelsea Publishing Co., New York 1966.
10. W.R. Hamilton, "The mathematical papers of Sir William Rowan Hamilton", Vol. III, Cambridge University Press, Cambridge 1967.
11. M. Jammer, "The conceptual development of Quantum Mechanics", McGraw-Hill, New York 1966.
12. F. Klein, "Development of Mathematics in the 19th century", Mathematical Science Press, Brookline Massachussets 1979.
13. F. Klein, "Gessamelte Mathematische Abhandlungen" Vol. 2, Springer, Berlin 1973.
14. G. Loria, "Storia delle Matematiche", U. Hoepli, Milan 1950.
15. W. Pauli, "General Principles of Quantum Mechanics", Springer Verlag, Berlin 1980.
16. D.E. Smith, "A source book in Mathematics", Dover, New York 1959.
17. J.L. Synge, dans le "Handbuch der Physik", édité par S. Flügge, Springer, Berlin 1960, Vol III/1, Section 13.
18. B.L. van der Waerden, Mathematics Magazine, vol. 49 No 4, 1976.
19. A.P. Wills, "Vector analysis with an introduction to tensor analysis", Dover, New York 1958.
20. E.T. Whittaker, "Analytical Dynamics of particles and rigid bodies", Cambridge University Press, Cambridge (1937, 1970).

# LES 350 ANS DU "GRAND THÉORÈME DE FERMAT"

# (SUITE)

Norbert SCHAPPACHER

Dans une série de trois conférences à l'Institut Isaac Newton (Cambridge) en juin 1993, Andrew Wiles de l'Université de Princeton annonçait une preuve du "Grand théorème de Fermat". Au moment d'écrire cette introduction à la suite du précédent article (*'L'Ouvert'* n° 73) en ce mois d'avril 1994, il n'y a pas encore de manuscrit de Wiles disponible. En fait, Wiles a rencontré quelques difficultés inattendues en rédigeant les détails techniques du noyau central de son argumentation. Il semble difficile de dire si oui, et quand, la preuve complète éventuelle sera achevée et acceptée par la communauté mathématique. Toutefois, la partie de la preuve de Wiles qui fonctionne avec certitude, représente déjà des progrès considérables dans l'histoire du problème. Cela justifie, nous l'espérons, la publication de la suite de cet article.

## 2.– Kummer et la création de la théorie des nombres algébriques (1844-1855)

Ernst Eduard Kummer (1810-1893) était un scientifique, plus précisément un professeur de l'Université de Berlin, plus ou moins tel que nous imaginons un professeur aujourd'hui : il était payé autant pour enseigner que pour faire de la recherche en mathématiques. Il a publié dans des journaux scientifiques réputés, notamment le Journal de Crelle. La théorie des nombres n'était pas son seul domaine de recherche active, mais faisait officiellement partie de son travail de professeur. Tout cela montre combien la situation de la science pure et particulièrement celle de la théorie des nombres avait évolué depuis Fermat, lorsque Kummer a commencé à produire son immense contribution au Grand théorème de Fermat et à l'histoire des mathématiques (12). Au moment où la situation sociologique des mathématiques était très proche de ce à quoi nous sommes habitués aujourd'hui, ses mathématiques ne sont déjà plus aussi faciles à expliquer que celles de Fermat, bien que les résultats principaux que nous allons étudier maintenant ont environ 150 ans. La théorie que Kummer a commencé à créer est enseignée dans les cours universitaires de niveau licence. Et quelques unes de ses découvertes sont encore réservées à des cours plus avancés.

Le point de départ est facile à expliquer. Nous avons déjà réduit l'étude des équations de Fermat aux exposants $n = p$ qui sont des nombres premiers impairs,

(12) Voir C. Goldstein "Le métier des nombres aux XVII$^{e}$ et XIX$^{e}$ siècles", in : Eléments d'Histoire des Sciences (M. Serres, éd.), Paris (Bordas) 1989, 275-295.

au moins égaux à 5. Réécrivons l'égalité en question sous la forme

$$a^p = c^p - b^p = \prod_{i=0}^{p-1}(c - \zeta_p^i b)$$

où $\zeta_p$ est une racine p$^{\text{ième}}$ de l'unité avec $\zeta_p = 1$ et $\zeta_p \neq 1$. En considérant que $\zeta_p$ est complexe on peut prendre $\zeta_p = e^{2i\pi/p}$ pour fixer les idées.

Le gain stratégique de cette décomposition est que nous pouvons espérer jouer avec les propriétés arithmétiques des produits $p$-uples qui apparaissent maintenant des deux côtés de l'équation. La difficulté est que l'arithmétique de ce nouvel anneau que nous étudions maintenant, l'anneau

$$\mathbb{Z}[\zeta_p] = \{\sum_{i=0}^{p-1} a_i \zeta_p^i | a_i \in \mathbb{Z}\}$$

des entiers algébriques en les racines $p^{\text{ième}}$ de l'unité, par opposition à l'anneau usuel $\mathbb{Z}$ des entiers relatifs, est moins facilement accessible parce que la factorisation unique en nombres premiers n'est pas vraie en général dans $\mathbb{Z}[\zeta_p]$. Pour expliquer aussi simplement que possible ce qui arrive, observons un exemple d'anneau où la factorisation unique est mise en défaut, qui n'est pas de la forme $\mathbb{Z}[\zeta_p]$ mais plutôt $\mathbb{Z}[\alpha]$, où $\alpha$ est un complexe racine carrée de -5, $\alpha^2 = -5$. Dans cet anneau nous avons les trois façons suivantes, essentiellement différentes, pour factoriser 21 en éléments de l'anneau qui ne peuvent être factorisés davantage :

$$21 = 3 \times 7 = (1 + 2\alpha)(1 - 2\alpha) = (4 + \alpha)(4 - \alpha).$$

L'idée de Kummer pour traiter cet imbroglio de factorisations différentes est de supposer seulement quatre "nombres premiers idéaux" déterminés de façon **unique**, non nécessairement éléments de l'anneau lui-même, qui opèrent comme le plus grand commun diviseur de différents éléments irréductibles; par exemple:

$$\wp_1 = (3, 1 + \alpha); \wp_2 = (3, 1 - \alpha); \wp_3 = (7, \alpha + 3); \wp_4 = (7, \alpha - 3).$$

Alors les trois différentes décompositions de 21 sont expliquées par l'unique factorisation du même nombre en "premiers idéaux" :

$$21 = \wp_1\wp_2\wp_3\wp_4; 3 = \wp_1\wp_2; 7 = \wp_3\wp_4; 1 + 2\alpha = \wp_2\wp_4;$$
$$1 - 2\alpha = \wp_1\wp_3; 4 + \alpha = \wp_1\wp_4; 4 - \alpha = \wp_2\wp_3.$$

Il est bien sûr aisé de postuler l'existence d'une telle décomposition "idéale", mais cela ne crée pas une théorie mathématique effective. Cependant Kummer pouvait utiliser la structure spécifique des anneaux $\mathbb{Z}[\zeta_p]$ qu'il étudiait afin de donner un critère entièrement rigoureux et aussi efficace pour qu'un élément de $\mathbb{Z}[\zeta_p]$ soit

divisible par un nombre premier idéal $\wp$, spécifique. (En termes actuels, le point fondamental est qu'on peut "voir" le corps fini qui sera la réduction de $\mathbb{Z}[\zeta_p]$ modulo un quelconque $\wp$, parce que les corps finis sont formés à partir de racines de l'unité...) Nous ne donnons pas les formules ici, mais nous recommandons la lecture des articles de Kummer écrits durant la période indiquée dans le titre de ce paragraphe (13).

Afin d'établir les résultats en lien avec le Grand théorème de Fermat, nous allons introduire le nombre de classes $h_p$ de l'anneau $\mathbb{Z}[\zeta_p]$. Cet invariant compte les nombres idéaux que nous devons ajouter aux éléments actuels de l'anneau, afin d'obtenir un domaine idéal où la factorisation unique est valable. Il est calibré de telle façon que si, comme c'est le cas pour $p = 3$, il arrive que $\mathbb{Z}[\zeta_p]$ soit factoriel, alors $h_p = 1$ et nous n'avons besoin que de la classe des éléments de l'anneau actuel pour obtenir une factorisation unique.

D'autre part, en ajoutant un nombre idéal premier $\wp$, nous ajoutons la classe de tous les éléments de l'anneau multipliés par $\wp$ à notre domaine d'opération. Kummer savait dans tous les cas que la factorisation unique idéale peut être réalisée dans un domaine formé d'un nombre fini de telles classes, précisément $h_p$ classes.

**Le théorème de Kummer.** *Si $p$ ne divise pas le nombre de classes $h_p$, alors l'assertion du Grand Théorème de Fermat est vraie pour l'exposant $n = p$.*

En fait, Kummer n'a pas seulement prouvé ce résultat, mais il a donné en même temps un critère efficace pour qu'un nombre premier $p$ satisfasse à l'hypothèse $p \not| \ h_p$ c'est-à-dire, comme il l'exprimait, un critère pour vérifier que $p$ est un nombre premier régulier.

**Le critère de Kummer.** *Le nombre premier $p$ est régulier si et seulement si pour tout $k = 2, 4, 6, \ldots p-3$, le nombre premier $p$ ne divise pas le numérateur du nombre de Bernoulli $B_k$.*

Rappelons que les nombres de Bernoulli peuvent être définis par la série entière

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}$$

de telle façon que $B_0 = 1, B_1 = -1/2, B_2 = 1, B_3 = 0$ et en général $B_{2n+1} = 0$ pour tout $n \geq 1$ ; alors que $B_4 = 1/30; B_6 = 1/42; B_8 = -1/39; B_{10} = 5/66; B_{12} = -691/2730$.

D'après le critère de Kummer, la dernière valeur signifie que $p = 691$ n'est pas un nombre premier régulier. Incidemment, la liste des nombres premiers irréguliers commence avec 37, 59, 67, 101, 103, 131, 149, 157.

(13) Voir Kummer's Collected Papers (Springer Verlag) avec la préface instructive d'A. Weil. Il existe également un livre très détaillé sur la théorie de Kummer : H.E. Edwards, "Fermat's last Theorem". A Genetic Introduction to Algebraic Number Theory, GTM 50 (Springer Verlag) 1977.

Nous n'entrerons pas dans des détails techniques ici. Mais il sera évident que la théorie de Kummer a représenté un grand pas en avant dans l'histoire du Grand théorème de Fermat. D'un autre côté, on peut également penser que ce n'était pas le début d'une preuve complète de la conjecture de Fermat. En fait, nous savons aujourd'hui qu'il y a une infinité de nombres premiers irréguliers, mais nous ne pouvons pas encore prouver qu'il y a une infinité de nombres premiers réguliers. Kummer lui-même, et beaucoup de mathématiciens après lui ont bien entendu affiné ces résultats. En conséquence, aujourd'hui, pour chaque nombre premier à l'intérieur d'un intervalle confortable de calcul et même s'il est irrégulier, il y aura quelque critère raffiné permettant de conclure (essentiellement à la façon de Kummer) que le Grand théorème de Fermat est valable pour ce nombre premier. Mais en même temps, il semble assez désespéré de développer cette approche en une véritable théorie générale qui fournirait éventuellement une chance d'établir la conjecture pour **chaque** nombre premier.

Néanmoins cet état de la situation, non seulement ne diminue en rien l'exploit de Kummer, mais il nous en fait voir plus clairement l'impact le plus important que la recherche de Kummer a eu dans l'histoire de l'arithmétique. Cet impact est double.

D'abord les générations qui ont suivi immédiatement Kummer ont généralisé son travail aux anneaux d'entiers de toute extension algébrique finie du corps $\mathbb{Q}$ des rationnels, et pas seulement les corps cyclotomiques $\mathbb{Q}[\zeta_p]$ (et leurs extensions obtenues par adjonction des racines $p^{\text{ième}}$ des éléments de $\mathbb{Q}[\zeta_p]$, que Kummer avait aussi étudiées). Cette théorie générale est connue aujourd'hui comme **la théorie des entiers algébriques**. Elle a été établie dans ses bases de manière indépendante par Richard Dedekind (1831-1916) qui n'a pas seulement traduit les "nombres idéaux" de Kummer en idéaux de l'anneau en question (comme nous faisons encore aujourd'hui : au lieu de travailler avec la quantité $\wp$ de Kummer, d'une manière quelque peu incertaine, nous étudions le sous ensemble de tous les éléments de l'anneau divisibles par $\wp$) il a introduit également beaucoup de concepts et de méthodes d'algèbre moderne (14) caractérisée par sa perspective structurelle. Ainsi, pratiquement toute l'algèbre moderne, autant que les développements profonds de la théorie des nombres algébriques de la première moitié du 20$^{\text{e}}$ siècle tels la théorie du corps de classes, se situent dans la continuité historique évidente du travail de Kummer.

Mais il y a un autre aspect qui est presque comme la face cachée de la même pièce. Inévitablement, quand on généralise une théorie profonde, comme le fit Dedekind si fructueusement avec la théorie arithmétique des corps cyclotomiques de Kummer, alors il faut aussi sacrifier certains caractères spéciaux – ceux en rapport avec le cas cyclotomique, et qui tout simplement n'existent pas pour un corps de nombres arbitraire.

(14) Cette utilisation particulière du mot "moderne" date des années 1920 ou 1930.

En 1897 David Hilbert publia son œuvre capitale le **Zahlbericht** (15) qui représente pour l'époque un compte rendu d'ensemble de l'état de la théorie des nombres algébriques, utilisant le point de vue de Dedekind (16) et incorporant aussi la propre recherche de Hilbert sur l'arithmétique des extensions de Galois des corps de nombres, dans la partie III. Suivant cette partie III (qui traite de la théorie des corps quadratiques et dont une grande partie renvoie aux travaux de Gauss et Dirichlet, avant Kummer) le **Zahlbericht** s'attaque spécifiquement à la théorie cyclotomique de Kummer (parties IV et V) et en fait la seconde moitié de ce volumineux rapport. Eh bien, contrairement à la première partie, Hilbert est visiblement non satisfait avec le fait qu'il doive suivre de près les pas de Kummer. Les deux générations entre Kummer et Hilbert ont tout simplement échoué à produire des avancées conceptuelles dans la partie de la théorie où la virtuosité cyclotomique de Kummer avait atteint son sommet (17). Ne pouvant se contenter de répéter fondamentalement Kummer, mais aussi, incapable de produire une présentation véritablement nouvelle de la théorie, Hilbert signale du moins (dans le chapitre 35) la possibilité de prouver les théorèmes et les lemmes de Kummer dans un ordre différent : voir les remarques de Hilbert, en particulier les §166, 170 et 171.

Aujourd'hui nous sommes dans une meilleure situation grâce à la théorie commencée dans les années 1950 par Kenkichi Iwasawa qui fournit un nouveau cadre et en fait un prolongement très profond de la théorie cyclotomique la plus avancée de Kummer. C'est autant que nous puissions le dire aujourd'hui, l'autre ligne de développement qui avait démarré avec l'arithmétique de Kummer. Elle est toujours au premier rang des recherches courantes en théorie des nombres comme l'atteste par exemple le fait que deux des plus importants titres à la renommée d'Andrew Wiles avant l'annonce de sa preuve du Grand théorème de Fermat étaient des démonstrations (reconnues) de ce que l'on appelle la **conjecture principale de la théorie d'Iwasawa** (18).

## 3. La géométrie arithmétique des courbes de Fermat (1901-1983)

Les développements dont je veux traiter maintenant appartiennent à notre siècle. Ils ont été rendus possibles grâce aux progrès de la géométrie algébrique réalisés aux cours du 19$^{e}$ siècle, en particulier pendant sa seconde moitié. L'année 1901 mentionnée dans le titre de cette section renvoie à un écrit remarquable d'Henri

(15) Jahresbericht der D.M.V.4 175-546.

(16) La plus grande partie de I du Zahlbericht est écrite dans la veine de Dedekind. Pour une exception bien connue (Satz 7, le théorème fondamental de décomposition des idéaux) voir H.E. Edwards, "The Genesis of Ideal Theory", Archive Hist. Ex. Sc. 23 1980, 321-378, en particulier p. 349. Cf. la bibliographie sur cette question dans les références d'Edwards, Neumann, Purkert, Archive Hist. Ex. Sc. 27 1983, 49-85. Plus récemment, on trouve la thèse (Göttingen 1993) sur Dedekind, ainsi qu'une prépublication sur l'émergence de la théorie des nombres algébriques, par le jeune Ralph Haubrich.

(17) Pour citer un exemple, le calcul formel de Kummer des "dérivées logarithmiques" d'unités cyclotomiques.

(18) Travail conjoint avec Mazur en 1984 pour le cas abélien; et Wiles par lui-même en 1991 pour l'ensemble des extensions de $\mathbb{Q}$.

Poincaré (1854-1912) qui parut cette année là : *Sur les propriétés arithmétiques des courbes algébriques* (19).

Dans cet écrit, le but de Poincaré est d'appliquer les notions développées par la géométrie algébrique du 19$^e$ siècle – en particulier, l'idée d'invariance birationnelle – pour classer les problèmes diophantiens. Avant de décrire plus nettement ce que cela signifie, je vais essayer d'expliquer la motivation de Poincaré (incidemment, ceci est aussi en accord avec la remarque que je faisais au début, quant au fait que "le Grand théorème de Fermat" est lui-même sans intérêt...)

Ce qui rend le domaine de l'Analyse diophantienne (20) si peu attrayant pour un mathématicien (à l'esprit théorique) (21) c'est son caractère morcelé. En regardant par exemple dans l'**Histoire de la Théorie des nombres** de Dickson – dont je ne mets pas en doute la valeur comme source de références historiques détaillées pour des problèmes spécifiques! – le lecteur est frappé par le manque apparent d'organisation intrinsèque pour les différents problèmes diophantiens examinés. La forme extérieure des équations semble être le principal critère déterminant l'ordre des chapitres. Mais tout le monde sait que les équations peuvent être rendues tout à fait différentes par certaines substitutions, sans modification du problème. Ansi la compilation de Dickson illustre le manque traditionnel d'invariants théoriques dans l'Analyse diophantienne. C'est à ces desiderata fondamentaux que Poincaré souhaitait remédier.

Nous allons maintenant expliquer la disposition d'ensemble de l'article de Poincaré, en donnant les équations du "Grand théorème de Fermat" comme un exemple.

Chercher des solutions entières de l'équation $X^n + Y^n = Z^n$ équivaut à chercher les points rationnels de la courbe $x^n + y^n = 1$. Plus précisément, les solutions entières $(X, Y, Z)$ de la première équation, avec $Z \neq 0$, correspondent aux points rationnels $(x, y) = (\frac{X}{Z}, \frac{Y}{Z})$ sur la courbe d'équation $x^n + y^n = 1$. Maintenant, dans le cas des équations de Fermat, les solutions restantes : $(X, Y, Z)$ avec $Z = 0$, sont facilement identifiables (et n'apportent pas de contradiction à la validité du "Grand théorème de Fermat"). Cependant elles doivent être prises en compte géométriquement et la méthode commune pour les traiter est de considérer les trois variables $X, Y, Z$ symétriquement, c'est-à-dire de ne pas en particulariser une qui soit ou ne soit pas nulle. La courbe projective $x^n + y^n = 1$ a comme points rationnels tous les triplets d'entiers $(X, Y, Z)$ tels que $XYZ \neq 0$; mais deux tels triplets $(X_1, Y_1, Z_1), (X_2, Y_2, Z_2)$ définissent le même point dans le plan projectif sur le corps des rationnels, si et seulement si il existe un nombre rationnel non nul $\lambda$ tel que $X_2 = \lambda X_1, Y_2 = \lambda Y_1, Z_2 = \lambda Z_1$. La condition pour qu'un tel point

(19) Journal de Mathématiques, 5$^e$ série, t. 7 fasc. III 1991, 161-233 (= Oeuvres V, 483-550).
(20) C'est-à-dire la branche des mathématiques qui s'occupe de la résolution concrète d'équations la plupart du temps polynômes à plusieurs variables ayant des coefficients entiers, résolution en nombres entiers ou rationnels.
(21) Ce qui est décrit ici comme un défaut en Analyse diophantienne est **"défaut"** uniquement sous l'hypothèse qu'il faut avoir des objectifs théoriques. Des problèmes diophantiens non systématiques sont bien sûr totalement acceptables dans un autre contexte, tel les mathématiques récréatives...

projectif appartienne à la courbe $X^n + Y^n = Z^n$ est bien définie indépendamment du triplet choisi pour représenter le point puisque l'équation est homogène : $(\lambda X_1)^n + (\lambda Y_1)^n - (\lambda Z_1)^n = \lambda^n (X_1^n + Y_1^n - Z_1^n)$. Notons que de cette manière, pour $Z \neq 0$, nous devons retrouver les points rationnels de $x^n + y^n = 1$ traités ci-dessus car les fractions peuvent être simplifiées : $\frac{\lambda X}{\lambda Z} = \frac{X}{Z}$.

Cela étant dit, à partir de maintenant toutes les courbes seront considérées comme des courbes projectives mais seront notées sous la forme affine : $x^n + y^n = 1$. Cet abus de notation est habituel dans ce domaine des mathématiques.

Il est un premier invariant qui se présente de lui-même quand on étudie la famille des courbes de Fermat : le degré $n$ de la courbe $F_n : x^n + y^n = 1$. C'est plus ou moins l'invariant de base que Poincaré utilise dans sa discussion – exception faite que le degré peut bien sûr changer sous des transformations. Par exemple, si on substitue $x = u, y = uv$ dans la courbe $F_3$, l'équation devient $u^3 + u^3 v^3 = 1$, qui a un degré total égal à 6. La raison pour laquelle ceci "ne doit pas compter" est que la substitution introduit une singularité. Plus précisément, nous obtenons une singularité à l'infini. En effet : écrivons la courbe transformée projectivement en $F(U, V, W) = 0$, où

$$F = U^3 W^3 + U^3 V^3 - W^6.$$

Ainsi nous ajoutons la puissance minimale de $W$ à chaque monôme pour rendre toute l'équation homogène. Il y a alors sur cette courbe deux points projectifs qui sont de la forme $(U, V, 0)$; ils peuvent être représentés par les triplets d'entiers $(1, 0, 0)$ et $(0, 1, 0)$. Notons que ces points sont "à l'infini" dans le sens qu'ils ne peuvent être trouvés dans les termes de l'équation affine $u^3 + u^3 v^3 = 1$ de variables $u$ et $v$. En ces deux points, les dérivées partielles $\frac{\partial F}{\partial U}, \frac{\partial F}{\partial V}, \frac{\partial F}{\partial W}$ s'annulent toutes trois. Cela signifie, par définition, que ce sont des points singuliers. L'équation d'origine : $x^n + y^n = 1$ n'a pas de points singuliers ni dans le plan affine $(x, y)$, ni à l'infini.

Aujourd'hui, il est acquis que le degré est un invariant de toutes les équations non singulières définissant la même courbe. Pour démontrer ceci, on utilise un invariant fondamental des courbes algébriques qui fut introduit par Bernhard Riemann (1822-1866) : le genre. – Et c'est le genre que Poincaré emploie pour la première classification des problèmes diophantiens liés aux courbes algébriques.

Cet invariant peut être défini de plusieurs manières substantiellement distinctes. Topologiquement, par exemple, examinons sur l'ensemble des nombres complexes les points de notre courbe algébrique (qui forment une surface de Riemann car $\mathbb{C}$ est de dimension 2 sur $\mathbb{R}$), le genre compte le nombre de "trous" : la sphère est de genre 0, le tore de genre 1, la surface d'un bretzel de genre 2, etc ...

Dans notre contexte nous avons cette formule : si la courbe algébrique est donnée par une équation non singulière de degré $n$, alors son genre est égal à

$$g = \frac{(n-1)(n-2)}{2}.$$

Ainsi la classification des courbes de Fermat selon leur genre donne ceci :

*Premier cas : genre $g = 0$, degré $n = 2$.*

Il s'agit alors de la courbe de Fermat $F_2$ : $x^2 + y^2 = 1$, qui est le cas exclu de l'énoncé du "Grand théorème de Fermat". Nous pouvons donner maintenant la raison géométrique qui fait que la conjecture ne peut être retenue pour $n = 2$. La courbe est naturellement un cercle (si nous la considérons sur $\mathbb{R}$) ou une sphère (sur $\mathbb{C}$), et elle a au moins un point rationnel, disons (0,1). Puis nous pouvons utiliser la méthode de projection stéréographique (qui convient pour toutes les coniques, c'est-à-dire toutes les courbes données par une équation quadratique non singulière ayant au moins un point rationnel) en paramétrant **tous** les points rationnels qui lui appartiennent en traçant toutes les droites de pente rationnelle passant par le point fixe (0,1). Une droite (étant donnée par une équation de degré 1) rencontre la courbe (qui est donnée par une équation de degré 2) en deux points (en comptant avec les multiplicités et, en général, en admettant tous les points projectifs comme intersections) : l'un d'eux est le point fixe, l'autre variera et se positionnera sur tous les autres points de la courbe, comme cela peut être facilement prouvé par un examen des équations algébriques concernées.

Ainsi nous voyons qu'une conique non singulière qui admet un point rationnel a une infinité de points rationnels. Dans le cas particulier de $F_2$ cela explique la paramétrisation des triplets pythagoriciens utilisée dans l'appendice.

En fait, le point de vue de Poincaré avait déjà été appliqué dans les problèmes diophantiens liés aux courbes de genre 0 par Hilbert et Hurwitz (22).

*Deuxième cas : genre $g = 1$, degré $n = 3$.*

Les courbes algébriques non singulières de genre 1 qui admettent un point rationnel sont appelées courbes elliptiques. Cette terminologie est un peu malheureuse car l'ellipse – qui est bien sûr une conique et ainsi de genre 0 – n'est pas une courbe elliptique (23). La raison en est historique : l'intégrale mesurant la longueur d'un arc d'ellipse nécessite l'intégration d'une expression de la forme $\frac{dx}{y}$ avec $x$ et $y$ liés par une équation cubique non singulière, c'est-à-dire une équation de genre 1.

Le cas du "Grand théorème de Fermat" pour lequel on a $F_n$ de genre 1 est $n = 3$ qui a été démontré par Euler, comme nous l'avons mentionné (dans l'article précédent). Contrairement au cas de genre 0 cette courbe de Fermat a donc par conséquent seulement un nombre fini de points rationnels – à savoir les points triviaux, ayant au moins une coordonnée projective nulle.

Ceci n'est pas vrai de façon générale pour toutes les courbes elliptiques. En fait certaines courbes elliptiques ont un grand nombre fini de points rationnels, certaines en ont un nombre infini. Et la question de savoir quel cas s'applique à

(22) D. Hilbert et A. Hurwitz, Über die diophantischen Gleichungen vom Geschlecht Null, Acta Mathematica 14 (1890) 217-224 = Hilbert, "Gesammelte Abhandlungen " II, 258-263 = Hurwitz, "Math. Werke" II, 116-121.

(23) Dans le dictionnaire français "Le Petit Larousse", on trouve la magnifique erreur : 'ELLIPTIQUE' : adj. math. Qui est en ellipse : Courbe elliptique.

une courbe elliptique donnée est intimement liée à l'une des grandes conjectures des mathématiques contemporaines : la conjecture de Birch et Swinnerton-Dyer (24).

Mais ce qui distingue vraiment le cas elliptique de tous les autres n'est pas tant cette gamme du nombre possible des solutions. C'est plutôt la structure supplémentaire présente sur les courbes elliptiques qui permet une théorie arithmétique riche qui n'existe pas pour les courbes de genre 0 ou supérieur à 1. Pour comprendre au moins le début de cela, utilisons le fait qu'une courbe elliptique peut être donnée par une équation cubique. Alors une droite rencontrant la courbe $E$ en deux points rationnels (comptant toujours avec les multiplicités) la rencontrera de nouveau en un troisième. L'opération binaire résultante (appelée communément **processus de tangente et sécante**)

$$E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow E(\mathbb{Q})$$

n'est pas en général une loi de groupe (25), mais peut être transformée en loi de groupe abélien, essentiellement par le choix d'une origine (26).

Le premier grand résultat fondamental de l'arithmétique des courbes elliptiques – pour lequel il n'est pas tout à fait clair si Poincaré en fit la conjecture dans son article ou simplement ne réussit pas à prévoir la possibilité que celui-ci soit faux – est que **pour une courbe elliptique $E$ sur $\mathbb{Q}$, le groupe abélien $E(\mathbb{Q})$ a un nombre de générateurs fini**. Ceci fut prouvé par J.-L. Mordell (1888-1972) à Cambridge en 1922. La preuve peut être interprétée joliment comme une version généralisée et théorique de la descente de Fermat mais nous ne l'introduisons pas ici.

*Troisième cas : genre $g \geq 2$, degré $n > 3$.*

Tout à la fin de son écrit de 1922, Mordell conjectura que toutes les courbes de genre au moins égal à 2 n'avaient qu'un nombre fini de points rationnels. Cette conjecture fut démontrée par Gerd Faltings (alors à Wuppertal) en 1983, une réussite qui lui valut la médaille Fields. Ainsi on peut dire de façon imagée que, lorsque les courbes deviennent trop compliquées, il n'y a en général pas de structure naturelle sur l'ensemble des points rationnels ; mais cet ensemble est fini.

Quand j'essayai d'expliquer le théorème de Faltings à ma mère (qui n'est pas une mathématicienne) en 1983, je choisis, comme je le fais ici, la famille des courbes $F_n$ de Fermat pour illustrer le résultat, parlai et expliquai pendant près d'une

(24) cf. N. Schappacher, Neuere Forschungsergebnisse in der Arithmetik elliptischer Kurven, Didaktik der Mathematik 17 (1989), 149-158.

(25) Dans le cas spécifique de la 3$^e$ courbe de Fermat, il y a déjà une loi de groupe, simplement parce qu'il y a si peu de points rationnels. La structure obtenue ainsi sur l'ensemble des solutions triviales de $x^3 + y^3 = 1$ (y compris le point à l'infini) est celle de 4-groupe de Klein, i.e. le groupe non cyclique d'ordre 4.

(26) cf. N. Schappacher, Développement de la loi de groupe sur une cubique, Séminaire de Théorie des Nombres Paris 1988-89, Progress in Mathematics 91 (Birkhäuser) 1991, 159-184.

demi-heure, et puis j'entendis ma mère remarquer plutôt sèchement qu'après tout Fermat restait non démontré.

Ma mère avait bien sûr raison : le "Grand théorème de Fermat" ne permet pas de bien apprécier l'importance du théorème de Faltings. Même aujourd'hui il n'existe pas de variante efficace de la conjecture de Mordell qui puisse faire tomber la conjecture de Fermat. Les propriétés de la famille des courbes $F_n$ sont justement très particulières. D'un autre côté le théorème de Faltings couvre toutes les courbes de genre au moins égal à 2, et qui plus est, pendant qu'il prouvait la conjecture de Mordell, en réalité Faltings établissait deux autres conjectures techniques (de Tate et de Safarevic) qui à elles seules suffisent à expliquer la grande réputation de son travail parmi les experts.

## 4.– Le lien avec l'Arithmétique des courbes elliptiques (1984-1993)

Ce fut un an et demi après le théorème de Faltings, en décembre 1984, que Gerhard Frey (de Saarbrück, à ce moment là) envoya une note de deux pages et demi à ses amis intimes dans laquelle il indiquait une stratégie de démonstration pour le fait que la conjecture de Taniyama-Shimura (voir plus loin) impliquerait le "Grand théorème de Fermat". Puisque le document était confidentiel, la nouvelle se répandit rapidement – et on découvrit aussi vite que la démonstration de Frey sur cette implication n'était pas complète. Mais l'idée avait été lancée et en 1986/87 Ken Ribet arriva à résoudre la question par une démonstration (très compliquée mais maintenant entièrement acceptée).

Voici l'idée de Frey dans une coquille de noix : supposons que le "Grand théorème de Fermat" soit faux. Alors il existerait un nombre premier $p \geq 5$ (en fait, $p$ serait même beaucoup plus grand ...) et trois entiers non nuls $a, b, c$ tels que $a^p + b^p = c^p$. Appelons $\mathcal{L} = (a, b, c)$ cette hypothétique solution de l'équation de Fermat pour l'exposant $p$. S'il existe un facteur commun divisant les trois composantes $a, b, c$ nous pouvons l'enlever car l'équation est homogène. Ainsi nous supposons que $\text{pgcd}(a, b, c) = 1$. Ceci implique que parmi $a$ et $b$ l'un est pair, et l'autre impair.

Disons que $b$ est pair; alors $a$ et $c$ sont impairs et par conséquent $\equiv \pm 1 \pmod 4$. Comme $p$ est impair nous pouvons échanger $a$ et $c$ en les multipliant par -1. Alors nous pouvons supposer sans perte de généralité que $c$ a pour reste 3 (et non 1) lorsqu'on le divise par 4. Avec ces normalisations, étant donnée une solution hypothétique $\mathcal{L}$ de l'équation de Fermat pour l'exposant $p$, nous écrivons l'équation suivante d'une courbe elliptique sur $\mathbb{Q}$ :

$$E_{\mathcal{L}} : y^2 = x(x - b^p)(x - c^p).$$

Notons que nous avons bien là une courbe elliptique : l'équation est de degré 3, et elle n'est pas singulière car le polynôme en $x$ du membre de droite a trois racines distinctes.

La courbe elliptique $E_{\mathcal{L}}$ monte vraiment sur scène comme un *deus ex machina*. Une telle écriture amène comme par magie la conjecture de Fermat à portée de la

théorie arithmétique des courbes elliptiques relativement bien développée – plutôt que de la laisser dans le domaine des courbes de genre supérieur, comme dans le paragraphe précédent. La courbe $E_{\mathcal{L}}$ se rencontre dans la littérature avant Frey (voir les articles référencés dans la note 2 de bas de page). Mais Frey fut apparemment le premier à envisager de démontrer la non existence de la courbe $E_{\mathcal{L}}$ de la manière qui suit.

**Théorème de Ribet.** La courbe $E_{\mathcal{L}}$ n'est pas une courbe elliptique modulaire.

**Conjecture de Taniyama-Shimura.** Toute courbe elliptique sur $\mathbb{Q}$ est modulaire.

**Théorème annoncé par Wiles.** Toute courbe elliptique semi-stable sur $\mathbb{Q}$ est modulaire.

Maintenant afin d'arriver à comprendre ces énoncés nous devons définir les notions de courbe modulaire et de courbe elliptique semi-stable. La courbe $E_{\mathcal{L}}$ se revèle être toujours semi stable, de sorte que le résultat annoncé par Wiles suffirait à déduire le "Grand théorème de Fermat".

*Courbes elliptiques semi-stables*

Pour définir ce qu'est une courbe elliptique semi-stable nous devons étudier la réduction d'une courbe elliptique (qui est définie sur $\mathbb{Q}$) modulo un nombre premier $q$. A première vue ceci est simple. Prenons par exemple l'équation définissant notre courbe $E_{\mathcal{L}} : y^2 = x(x - b^p)(x - c^p)$. Elle a des coefficients entiers que l'on peut considérer comme entiers modulo $q$, pour n'importe quel nombre premier $q$ donné. La courbe algébrique projective résultante sur le corps fini $F_q = \mathbb{Z}/q\mathbb{Z}$ ayant $q$ éléments est habituellement non singulière, et en conséquence une courbe elliptique – sur $F_q$. Plus précisément c'est le cas lorsque les trois racines $0, b^p, c^p$ du polynôme en $x$ de droite sont (non seulement distinctes dans $\mathbb{Z}$, comme elles le sont, mais aussi) deux à deux non congrues modulo $q$.

Les mauvais premiers $q$, c'est-à-dire ceux pour lesquels l'équation réduite a une singularité, sont ceux qui divisent l'une des différences des trois racines $0, b^p, c^p$ – en d'autres termes ce sont les premiers $q$ qui divisent le produit $abc$. Pour ces nombres $q$, la condition de réduction semi-stable à $q$ signifie qu'il y a deux tangentes distinctes au point singulier de la courbe réduite. Pour notre équation particulière ceci équivaut à dire que les racines du polynôme en $x$ de droite ne se réduisent pas toutes trois en un même élément de $F_q$ – une condition qui est satisfaite car nous avons fait en sorte que $\mathrm{pgcd}(a, b, c) = 1$.

Jusqu'ici ça va, mais nous voulons vraiment une notion géométrique qui ne dépende pas de l'équation spécifique utilisée pour décrire notre courbe. Et en étudiant les réductions modulo les premiers $q = 2$ et $q = 3$, les équations de la forme $y^2 = P(x)$, où $P(x)$ est un polynôme de degré 3 en $x$, ne sont justement pas assez générales. Par exemple, une telle équation aura toujours une singularité avec une tangente unique (de multiplicité deux) quand elle est réduite modulo $q = 2$.

Un type d'équation qui convient pour tous les premiers $q$, appelé **modèle général de Weierstrass**, est une équation non singulière de la forme suivante :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Deux telles équations définissent la même courbe si et seulement si l'une peut être obtenue à partir de l'autre par un changement de coordonnées $x = A^2x' + B; y = A^3y' + Cx' + D$, avec $A, B, C, D \in \mathbb{Q}$, et une division ultérieure par $A^6$.

**Définition.** Une courbe elliptique $E$ définie sur le corps $\mathbb{Q}$ des nombres rationnels est appelée semi-stable, si pour tout nombre premier $q$, il existe une équation définissant $E$, qui, lorsqu'elle est réduite modulo $q$, soit est non singulière soit admet une singularité avec deux tangentes de directions distinctes.

**Exemples** (27).
1. La courbe elliptique $y^2 = x(x+9)(x-16)$ est aussi donnée par $y^2+xy+y = x^3+x^2-10x-10$, et par conséquent semi-stable. Mais la courbe $y^2 = x(x-9)(x+16)$ n'est pas semi-stable pour le nombre premier $q = 2$.

2. Les courbes $E_{\mathcal{L}}$ de Frey admettent l'équation suivante (28) qui montre qu'elles sont semi-stables

$$v^2 + uv = u^3 - \frac{1 + b^p + c^p}{4}u^2 + \frac{b^pc^p}{16}u.$$

*Courbes elliptiques modulaires*

Soit $\mathcal{H}$ le demi-plan supérieur $\mathcal{H} = \{z = x + iy \in \mathbb{C} | y > 0\}$. Muni de la métrique $ds^2 = \frac{dx^2+dy^2}{y^2}$, c'est un des modèles courants de la géométrie hyperbolique non euclidienne. La métrique est invariante en ce qui concerne l'"action" suivante des matrices réelles $2 \times 2$ $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ayant un déterminant positif :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \longmapsto \frac{az + b}{cz + d}.$$

Nous allons utiliser le quotient de $\mathcal{H}$ sous l'action du sous-groupe suivant de matrices entières de déterminant 1, où $N$ est un entier donné :

$$\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Z) | c \equiv 0 (mod N)\}.$$

Ce quotient $\Gamma_0(N) \setminus \mathcal{H}$ est une surface de Riemann qui peut être compactifiée en ajoutant un nombre fini de pointes à savoir un point $i\infty$ à distance infinie dans la

(27) Le premier exemple est pris chez K. Rubin et A. Silverberg, Wiles prof of Fermat's Last Theorem; manuscrit de présentation non publié, accessible electroniquement par le réseau mathématique.
(28) Via $x = 4u, y = 8v + 4u$.

direction imaginaire positive, et ses translatés sous l'action de $\Gamma_0(N) \setminus SL_2(\mathbb{Z})$. La surface de Riemann compacte résultante est appelée la courbe modulaire $X_0(N)$.

*Définition.* Une courbe elliptique $E$ qui est définie sur le corps $\mathbb{Q}$ des nombres rationnels est appelée une courbe elliptique modulaire s'il existe $N \geq 1$ et une application holomorphe surjective

$$\varphi : X_0(N) \longrightarrow E(\mathbb{C}).$$

Cette définition (29) ne rend pas évident le contenu arithmétique de la notion. En fait, il existe un certaion nombre de conditions de nature différente, dont chacune caractérise des courbes elliptiques modulaires. Mais il est clair au moins à partir de la définition donnée, que nous entamons une autre source géométrique de classification des courbes et variétés algébriques, différente de celle discutée dans la section 3 (programme de Poincaré).

Plutôt que de continuer à introduire des concepts et des méthodes prérequises pour l'attaque par Wiles du "Grand théorème de Fermat", permettez-moi de revenir à mon point de départ : la question de l'intérêt du "Grand théorème de Fermat". Du théorème annoncé par Wiles on peut aussi déduire que l'équation plus générale que celle de Fermat:

$$Ax^p + y^p = z^p$$

n'a pas de solutions entières non nulles, pourvu que la constante $A$ soit de la forme $l^n$ avec $n \geq 1$ et $l$ l'un quelconque des nombres 3, 5, 7, 11, 13, 17, 19, 23, 29, 53 ou 59. (On pourrait pousser davantage la liste des $A$ admissibles.....)

Ceci peut donner une idée du degré de généralité de la méthode en question.

(29) Voir B. Mazur, Number Theory as Gadfly, Amer. Math. Monthly 98 (1991), 593-610.

# DANS NOS GROUPES I.R.E.M. : DEUX PROBLÈMES AMUSANTS DE PHYSIQUE

Jean-Luc GASSER

Au nom du GROUPE MATHS-PHYSIQUE

Le groupe Maths-Physique qui s'est formé à l'IREM de Strasbourg mène une réflexion depuis septembre 1992 sur les liaisons bilatérales que les professeurs de ces deux matières peuvent entretenir dans le cadre des programmes en vigueur, en tenant compte de la mise en place du nouveau programme de Physique (en seconde à la rentrée 1993).

Un des objectifs qu'il s'est fixé est de mettre à disposition des professeurs des activités qui peuvent être traitées dans l'une ou l'autre de ces matières, voire les deux conjointement, à un niveau de classe donné. Dans les manuels de mathématiques qui ont fait l'effort de proposer des activités mathématiques à support physique, on constate trop souvent un décalage, voire une totale inadéquation entre les notions de physique utilisées et les connaissances réelles de l'élève. On peut ainsi trouver des exercices de calcul en seconde portant sur les puissances de dix, les racines carrées et mettant en jeu des formules de la théorie de la relativité qui n'a jamais été au programme de la classe de seconde.

La lecture simultanée des programmes à un niveau donné a permis de mieux cerner les outils mathématiques dont ont besoin les élèves, et leur utilisation par le physicien. Il en résulte des pistes de progression annuelle possibles qui évitent l'utilisation précoce de notions mathématiques. Les habitudes de notation et de présentation des diverses notions sont échangées entre les membres du groupe, et il s'avère qu'il peut être facile d'en modifier quelques aspects pour une plus grande cohérence globale. De plus, il est apparu que certaines notions physiques peuvent être utilisées pour résoudre un problème mathématique, voire pour introduire ou motiver une nouvelle notion.

La terminologie utilisée dans ces deux matières est parfois commune, mais les contenus peuvent être différents! Ainsi, la notion de translation peut créer des difficultés de compréhension chez les élèves (et les professeurs!) car elle est bien différente dans chacune des disciplines. La notion de composant *linéaire* en physique, modélisée par une fonction *affine* en mathématiques est un autre exemple significatif de ces problèmes de vocabulaire ...

L'objectif de la série de deux articles qui débute avec celui-ci est de présenter deux problèmes intéressants, ayant un support physique concret, pouvant être traités pendant le cours de mathématiques. Ils sont présentés sous la forme d'un énoncé, dont une solution complète sera proposée dans le numéro suivant de *'L'Ouvert'*

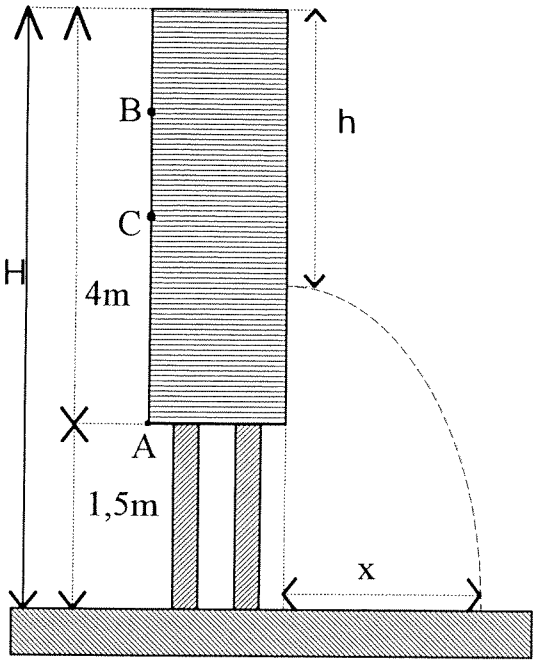
pour laisser au lecteur le plaisir de la recherche de leur résolution. La solution proposée mettra surtout en évidence l'intérêt physique ou mathématique de l'exercice proposé. Le lecteur qui est intéressé par le détail des calculs mathématiques ou physiques, ou qui aimerait mieux situer ces problèmes dans le cadre des programmes, est invité à se référer à la brochure dont ils sont extraits et que le groupe publiera en juin 1994.

Le premier problème présenté ci-dessous peut se traiter au niveau de la terminale scientifique. La notion de pression ne fait plus partie du programme du secondaire, et on propose donc une activité qui ne rentre pas strictement dans le cadre des programmes... Dans l'introduction, nous critiquions ce type d'exercice, mais nous l'avons conservé car cette notion n'est pas fondamentale pour résoudre l'exercice. On utilise d'une façon très intéressante la notion de travail d'une force pour aboutir à la formule qui donne la vitesse horizontale du jet d'eau, connue sous le nom de théorème de Toricelli par les Physiciens!

Un indice pour ne pas rester bloqué : ce problème donne l'occasion d'utiliser de façon motivante la fonction racine carrée.

Pour le deuxième problème, le lecteur est fortement invité à réaliser une petite maquette pour se rendre compte des phénomènes à observer, pour faire des conjectures, et éventuellement valider sa solution. Le niveau auquel il se situe est la première ou la terminale scientifique. Les notions mathématiques et physiques mises en œuvre ne sont pas difficiles, mais elles nécessitent une bonne vision dans l'espace!

## PREMIER PROBLÈME : LA COLONNE PERCÉE




Albert, Bertrand et Claude viennent de sortir du cours de Physique. Ils y ont déjà abordé les notions d'énergie cinétique, d'énergie potentielle, de travail d'une force et de pression. Ils marchent et longent un petit château d'eau qui est une colonne de quatre mètres de hauteur dont le niveau est maintenu constant grâce à un système de pompe. Cette colonne est à un mètre cinquante au dessus du sol. Si on perce convenablement un trou dans la colonne, et si l'on attend que le débit soit régulier, l'eau s'en échappera avec une vitesse horizontale constante.

Les trois amis parient, pour savoir où placer l'orifice de telle sorte que le jet d'eau touche le sol à la distance $x$ la plus grande possible de la colonne. Voici leurs remarques :

**Albert :** Plus la hauteur de la colonne d'eau au-dessus du trou est élevée, plus grande sera la vitesse initiale de l'eau, et donc plus loin ira le jet d'eau. Je perce le tonneau en $A$, à un mètre cinquante du sol.

**Bertrand :** Dans ce cas l'eau arrivera beaucoup trop rapidement au sol! Le jet d'eau n'ira pas loin! Une colonne d'eau d'un mètre de hauteur suffit amplement pour que l'eau acquière une vitesse initiale suffisante. Je percerais la colonne au point $B$, la hauteur de chute étant de quatre mètres cinquante, le jet d'eau ira beaucoup plus loin ...

**Claude :** Hum! Chacun des points de vue a son intérêt ... Je pense qu'une position intermédiaire me fera gagner le pari : je percerais le tonneau en un point $C$ tel que la hauteur de la colonne d'eau soit de deux mètres.

Qui gagnera le pari? Sauriez-vous proposer la position d'un point $D$, de telle sorte que le jet d'eau aille le plus loin possible?

## DEUXIÈME PROBLÈME : LE BICÔNE REMONTE LA PENTE

*Énoncé :* Fabriquer deux cônes à l'aide d'un transparent ou, à défaut, de carton souple, en coupant un demi cercle dont le rayon est le plus élevé possible (au moins vingt centimètres). Les assembler pour réaliser le solide dessiné sur la figure 2, que l'on appellera bicône. Réaliser en carton fort deux supports qui permettent de réaliser une déclivité dont on peut modifier l'angle $\gamma$, et dont on peut régler l'angle d'ouverture $\delta$ (voir fig. 1). Poser le solide sur cette pente, faire varier les angles $\gamma$ et $\delta$, observer ce qui se passe et faire des conjectures. Etablir une relation faisant intervenir les trois angles pour expliquer les phénomènes observés. On peut également changer la forme du solide si on le désire, en changeant l'angle $\beta$ au sommet du cône.

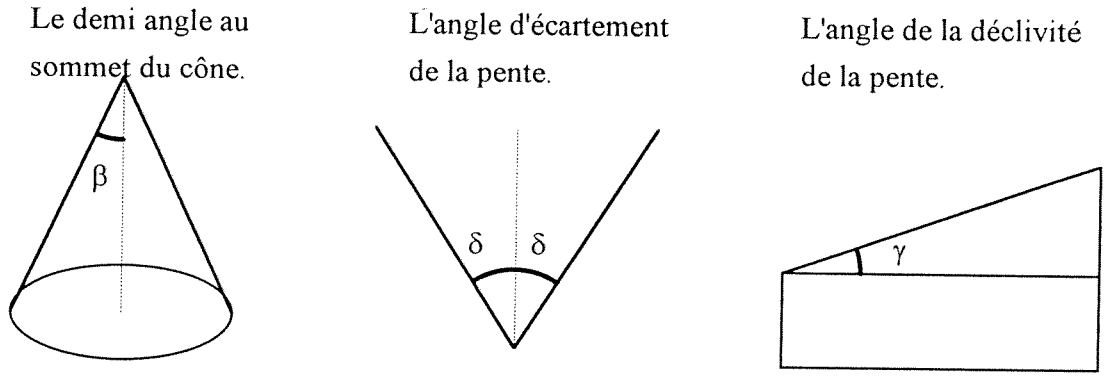



*Figure 1*

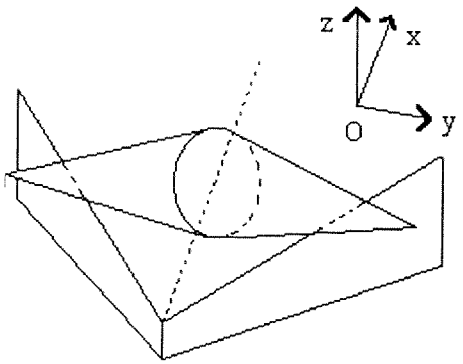



*Figure 2*

APMEP - 1994 **Journées nationales**
**les 13-14-15-16 octobre 1994**
**à Brest et Loctudy**
*MATHÉMATIQUES à la POINTE*
*Toniques, Naturelles, dans le Vent !*
BREST-LOCTUDY

Présentation complète et fiche d'inscription dans le "*Bulletin de l'A.P.M.E.P.*", n° 393 de juin 1994.

## Programme des journées :

**Jeudi 13 octobre 1994 : le Quartz à Brest**

| | |
|---|---|
| 8 h 30 - 09 h 30 | Accueil |
| 9 h 30 - 10 h 00 | Indications et renseignements |
| 10 h 00 - 11 h 15 | Conférence de Nicolas ROUCHE |
| 11 h 15 - 12 h 00 | Inauguration officielle |
| 14 h 00 - 17 h 00 | Visites-Ateliers et Exposés |
| 17 h 00 - 19 h 00 | Créneau Editeurs/Exposants |
| | Pot d'accueil |

**Vendredi 14 octobre 1994 : le Quartz**

| | |
|---|---|
| 9 h 00 - 10 h 15 | Conférence de Alain MENESGUEN |
| 10 h 45 - 12 h 00 | Conférence de Ivar EKELAND |
| 14 h 00 - | Départ vers Loctudy, en utilisant divers circuits touristiques |
| 18 h 00 - | Arrivée au Dourdy à Loctudy |
| | Repas - animation |

**Samedi 15 octobre 1994 : Le Dourdy à Loctudy**

| | |
|---|---|
| 8 h 30 - 10 h 45 | Ateliers "lourds" (2 h 1/4) |
| 9 h 30 - 10 h 30 | Ateliers |
| 11 h 00 - 12 h 15 | Conférence de Alain HILLION |
| 14 h 00 - 15 h 30 | Ateliers |
| 15 h 30 - 16 h 30 | Créneau Editeurs/Exposants |
| 16 h 30 - 17 h 30 | Réunion des régionales |
| 17 h 45 - 19 h 00 | Commissions APMEP |
| 20 h 30 - | Banquet - Animation |

**Dimanche 16 octobre 1994 :**

| | |
|---|---|
| 9 h 00 - 10 h 00 | Assemblée des Journées |
| | Présentation des Journées Nationales 95 |
| 10 h 15 - 12 h 00 | Conférence - Débat - Clôture |

*Exposants et éditeurs en permanence jeudi, vendredi matin et samedi toute la journée.*

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

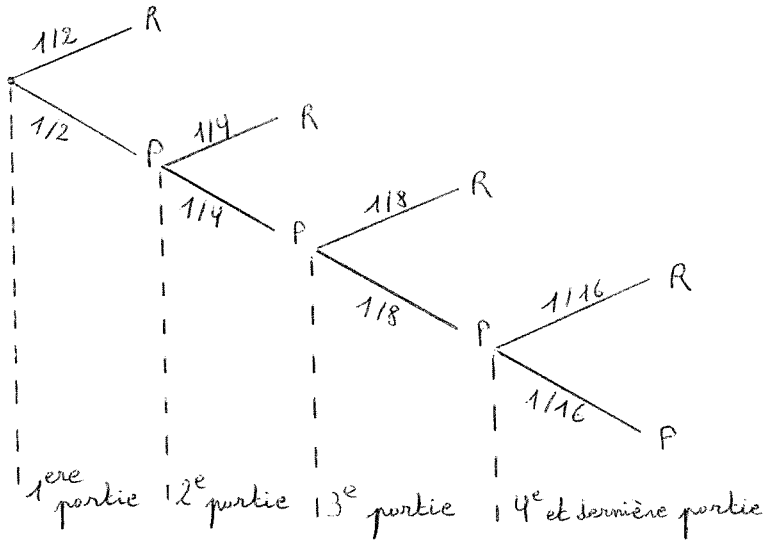
Il s'agit, dans cette rubrique, de présenter des problèmes historiques ou classiques, dont la solution ne requiert pas d'autres connaissances que celles enseignées au lycée (voire au collège) et qui par conséquent, peuvent faire l'objet de travaux dans nos classes.

Nous publions ici les réponses aux problèmes 1 et 3 envoyés respectivement par Bruno Muller et Estelle Schneider, tous deux élèves de Terminale C au Lycée Fustel de Coulanges de Strasbourg. Nous vous convions à envoyer des solutions des problèmes 2, 4 et 5 (de préférence d'élèves).

### SOLUTION DU PROBLÈME 1

Je vais tout d'abord représenter sur un schéma les probabilités de chaque joueur de gagner :

Appelons : R : l'événement où le riche gagne.
P : l'événement où le pauvre gagne.
1/2 représente la probabilité de chaque événement.



Lorsque le pauvre gagne, il accepte de rejouer. Le nombre de parties maximum par jour est de 4.

Donc pour que le pauvre gagne un jour, il doit gagner les 4 parties du jour. La probabilité pour que le pauvre gagne un jour est de

$$p_1 = \left(\frac{1}{2}\right)^4 = \frac{1}{16} \qquad \text{(voir schéma)}$$

Par contre, le riche arrête le jeu dès qu'il gagne, donc sa probabilité de gagner est de

$$p_2 = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} = 1 - \frac{1}{16} = \frac{15}{16}.$$

Pour la première partie, il y a 2 pièces d'or en jeu (une provenant du pauvre et une provenant du riche)

Pour la 2$^e$ partie, si elle a lieu, il y aura 4 pièces d'or en jeu (deux provenant du pauvre, les deux gagnées à la 1$^{ère}$ partie, et deux pièces supplémentaires du riche).

S'il y a une 3$^e$ partie, il y aura 8 pièces d'or en jeu (quatre provenant du pauvre, et quatre nouvelles pièces du riche)

Enfin la 4$^e$ partie, si elle a lieu, rassemblera 16 pièces d'or.

Donc si le pauvre gagne, il aura 16 pièces d'or (une provenant de lui, la première pièce jouée, et 15 autres pièces provenant du riche).

Par contre, quelque soit la partie, le riche ne gagne que la pièce d'or du pauvre jouée à la première partie, plus éventuellement les siennes qu'il récupère.

Donc, si on multiplie les probabilités de gagner par la somme gagnée, on obtient

pour le pauvre : $\frac{1}{16} \times 15 = \frac{15}{16}$

pour le riche : $\frac{15}{16} \times 1 = \frac{15}{16}$

Donc, même si le riche gagne souvent, les deux joueurs jouent dans les mêmes conditions; après plusieurs mois, le riche ne verra pas sa fortune s'accroître, tandis que le pauvre restera toujours pauvre.

## SOLUTION DU PROBLÈME 3

. $3°$ peut encore s'écrire $3° = 18° - 15°$

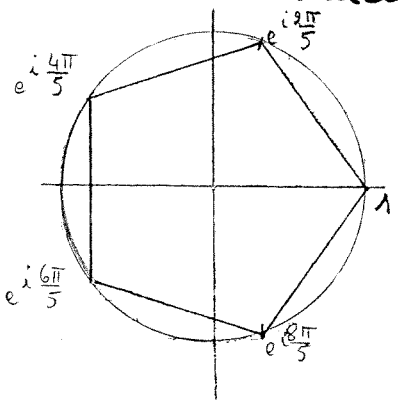
$= (90° - 72°) - (45° - 30°)$

Avec les formules de duplication on pourra trouver $\cos 3°$, $\sin 3°$ et $\tan 3°$.

Les cosinus et sinus de $90°$, $45°$ et $30°$ sont connus.

### 1) Calcul du cosinus et du sinus de $72° = \frac{2\pi}{5}$ rad

Déterminons les racines $5^e$ de 1




$z^5 - 1 = 0$

$(z-1)(z^4 + z^3 + z^2 + z + 1) = 0$

Si $z \neq 1$ $\quad z^4 + z^3 + z^2 + z + 1 = 0$

En divisant les 2 membres par $z^2$ :

$$z^2 + z + 1 + \frac{1}{z} + \frac{1}{z^2} = 0$$

$$\left(z^2 + \frac{1}{z^2}\right) + \left(z + \frac{1}{z}\right) + 1 = 0$$

or $\left(z+\frac{1}{z}\right)^2 = z^2 + \frac{1}{z^2} + 2$

d'où $\left(z+\frac{1}{z}\right)^2 + \left(z+\frac{1}{z}\right) - 1 = 0$

- Soit $u = z + \frac{1}{z}$

$$u^2 + u - 1 = 0$$

$\Delta = 1+4 = 5$ donc $u = \frac{-1 \pm \sqrt{5}}{2}$

Si $\varepsilon = \pm 1$ $\quad u = \frac{-1+\varepsilon\sqrt{5}}{2}$

- Si $u = z + \frac{1}{z}$ $\qquad uz = z^2 + 1$

$$z^2 - uz + 1 = 0$$

$$\Delta = u^2 - 4$$

$$= \left(\frac{-1 \pm \varepsilon\sqrt{5}}{2}\right)^2 - 4$$

$$= \frac{6 - 2\varepsilon\sqrt{5}}{4} - 4$$

$$= \frac{3 - \varepsilon\sqrt{5}}{2} - 4$$

$$= \frac{-5 - \varepsilon\sqrt{5}}{2}$$

$$z = \frac{u \pm i\sqrt{\frac{5+\varepsilon\sqrt{5}}{2}}}{2}$$

$$z = \frac{-1+\varepsilon\sqrt{5}}{4} \pm i \cdot \frac{1}{2}\sqrt{\frac{5+\varepsilon\sqrt{5}}{2}}$$

Sous cette forme, on peut déduire $\cos\frac{2\pi}{5}$ et $\sin\frac{2\pi}{5}$

* $\cos\frac{2\pi}{5} > 0$ donc $\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$

$*\sin\frac{2\pi}{5} > 0$ donc $\sin\frac{2\pi}{5} = \frac{1}{2}\sqrt{\frac{5+\sqrt{5}}{2}}$

2) Déterminons $\cos 3°$, $\sin 3°$, $\tan 3°$.

* Calcul de $\cos 18°$ et $\sin 18°$

$$\cos 18° = \cos(90° - 72°)$$
$$= \cos 90° \cos 72° + \sin 90° \sin 72°$$
$$= \sin 72° = \frac{1}{2}\sqrt{\frac{5+\sqrt{5}}{2}}$$

$$\sin 18° = \sin(90° - 72°)$$
$$= \sin 90° \cos 72° - \sin 72° \cos 90°$$
$$= \cos 72° = \frac{\sqrt{5}-1}{4}$$

* Calcul de $\cos 15°$ et $\sin 15°$

$$\cos 15° = \cos(45° - 30°) = \cos 45° \cos 30° + \sin 45° \sin 30°$$
$$= \frac{\sqrt{2}}{2} \times \frac{\sqrt{3}}{2} + \frac{\sqrt{2}}{2} \times \frac{1}{2} = \frac{\sqrt{6}+\sqrt{2}}{4}$$

$$\sin 15° = \sin(45° - 30°)$$
$$= \sin 45° \cos 30° - \sin 30° \cos 45°$$
$$= \frac{\sqrt{2}}{2} \times \frac{\sqrt{3}}{2} - \frac{\sqrt{2}}{2} \times \frac{1}{2} = \frac{\sqrt{6}-\sqrt{2}}{4}$$

* Calcul de $\cos 3^\circ$

$$\cos 3^\circ = \cos(18^\circ - 15^\circ)$$

$$= \cos 18^\circ \cos 15^\circ + \sin 18^\circ \sin 15^\circ$$

$$= \frac{1}{2}\sqrt{\frac{5+\sqrt{5}}{2}}\,\frac{\sqrt{6}+\sqrt{2}}{4} + \frac{\sqrt{5}-1}{4}\,\frac{\sqrt{6}-\sqrt{2}}{4}$$

$$= \frac{1}{2}\times\frac{1}{\sqrt{2}}\times\sqrt{5+\sqrt{5}}\times\frac{1}{4}\times\sqrt{2}(\sqrt{3}+1) + \frac{1}{16}(\sqrt{5}-1)(\sqrt{6}-\sqrt{2})$$

$$\boxed{\cos 3^\circ = \frac{1}{16}\left(2\sqrt{5+\sqrt{5}}\times(\sqrt{3}+1) + (\sqrt{5}-1)(\sqrt{6}-\sqrt{2})\right)}$$

* Calcul de $\sin 3^\circ$

$$\sin 3^\circ = \sin(18^\circ - 15^\circ)$$

$$= \sin 18^\circ \cos 15^\circ - \sin 15^\circ \cos 18^\circ$$

$$= \frac{\sqrt{5}-1}{4}\times\frac{\sqrt{6}+\sqrt{2}}{4} - \frac{\sqrt{6}-\sqrt{2}}{4}\times\frac{1}{2}\times\frac{1}{\sqrt{2}}\sqrt{5+\sqrt{5}}$$

$$= \frac{1}{16}(\sqrt{5}-1)(\sqrt{6}+\sqrt{2}) - \frac{1}{8}(\sqrt{3}-1)\sqrt{5+\sqrt{5}}$$

$$\boxed{\sin 3^\circ = \frac{1}{16}\left[(\sqrt{5}-1)(\sqrt{6}+\sqrt{2}) - 2(\sqrt{3}-1)\sqrt{5+\sqrt{5}}\right]}$$

* Calcul de $\tan 3^\circ$

$$\tan 3^\circ = \frac{\sin 3^\circ}{\cos 3^\circ} = \frac{(\sqrt{5}-1)(\sqrt{6}+\sqrt{2}) - 2(\sqrt{3}-1)\sqrt{5+\sqrt{5}}}{(\sqrt{5}-1)(\sqrt{6}-\sqrt{2}) + 2(\sqrt{3}+1)\sqrt{5+\sqrt{5}}}$$

$$= \frac{(\sqrt{5}-1)(\sqrt{3}+1) + (1-\sqrt{3})\sqrt{10+2\sqrt{5}}}{(\sqrt{3}-1)(\sqrt{5}-1) + (1+\sqrt{3})\sqrt{10+2\sqrt{5}}}$$

Soit $\alpha = \sqrt{10+2\sqrt{5}}$

$$\tan 3^\circ = \frac{(\sqrt{3}+1)(\sqrt{5}-1)+(1-\sqrt{3})\alpha}{(\sqrt{3}-1)(\sqrt{5}-1)+(1+\sqrt{3})\alpha}$$

$$\tan 3^\circ = \frac{2(\sqrt{5}-1)^2+2(10+2\sqrt{5})+\alpha\left[(\sqrt{5}-1)(2\sqrt{3}-4)-(\sqrt{5}-1)(4+2\sqrt{3})\right]}{(4-2\sqrt{3})(6-2\sqrt{5})-(4+2\sqrt{3})(10+2\sqrt{5})}$$

$$= \frac{32+8\alpha(1-\sqrt{5})}{-16-32\sqrt{3}-16\sqrt{5}} = -\frac{1}{2}\,\frac{4+\alpha(1-\sqrt{5})}{1+2\sqrt{3}+\sqrt{5}}$$

$$= -\frac{1}{2}\,\frac{4(1+2\sqrt{3}-\sqrt{5})+\alpha(1-\sqrt{5})(1+2\sqrt{3}-\sqrt{5})}{8+4\sqrt{3}}$$

$$= -\frac{1}{8}\,\frac{4(1+2\sqrt{3}-\sqrt{5})+\alpha(6+2\sqrt{3}-2\sqrt{5}-2\sqrt{15})}{2+\sqrt{3}}$$

$$= -\frac{1}{4}\left[(2-\sqrt{3})(2+4\sqrt{3}-2\sqrt{5})+\alpha(2-\sqrt{3})(3+\sqrt{3}-\sqrt{5}-\sqrt{15})\right]$$

$$= -\frac{1}{8}(\sqrt{3}-1)\left[(\sqrt{3}-1)(2+4\sqrt{3}-2\sqrt{5})+\alpha(\sqrt{3}-1)(3+\sqrt{3}-\sqrt{5}-\sqrt{15})\right]$$

$$= -\frac{1}{8}(\sqrt{3}-1)\left[10-2\sqrt{3}+2\sqrt{5}-2\sqrt{15}+\alpha(2\sqrt{3}-2\sqrt{5})\right]$$

$$= \frac{1}{4}(\sqrt{3}-1)\left[\alpha(\sqrt{5}-\sqrt{3})+\underbrace{\sqrt{15}-\sqrt{5}+\sqrt{3}-5}_{(\sqrt{5}+1)(\sqrt{3}-\sqrt{5})}\right]$$

$$= \frac{1}{4}(\sqrt{3}-1)(\sqrt{5}-\sqrt{3})\left[\alpha-\sqrt{5}-1\right]$$

$$\boxed{\tan 3^\circ = \frac{1}{4}(\sqrt{3}-1)(\sqrt{5}-\sqrt{3})\left(\sqrt{10+2\sqrt{5}}-\sqrt{5}-1\right)}$$

## ÉNONCÉ DU PROBLÈME 5

Problème sur le jeu des sauvages, appelé jeu des noyaux

Le baron de la Hontan fait mention de ce jeu dans le second tome de ses Voyages de Canada. Voici comment il s'explique :

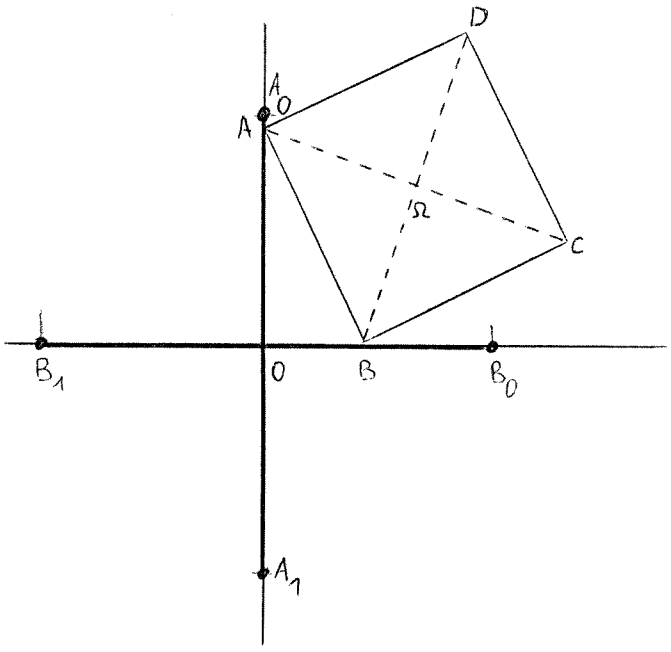
On y joue avec huit noyaux noirs d'un côté et blancs de l'autre; on jette les noyaux en l'air : alors si les noirs se trouvent impairs, celui qui a jeté les noyaux gagne ce que l'autre Joueur a mis au jeu. S'ils se trouvent ou tous noirs ou tous blancs, il en gagne le double; et hors de ces deux cas il perd sa mise.

On demande lequel des deux Joueurs a de l'avantage, en supposant qu'ils mettent également au jeu.

## ÉNONCÉ DU PROBLÈME 6

Les segments $[A_0A_1]$ et $[B_0B_1]$ sont perpendiculaires, ont même milieu $O$ et même longueur $4a$.

Un carré $ABCD$ **direct** de côté $2a$ varie de telle façon que
$A$ décrit le segment $A_0A_1$
$B$ décrit le segment $B_0B_1$.




**1)** Trouver le lieu que décrit le centre $\omega$ du carré.
**2)** Montrer qu'il y a une infinité de points fixés solidement au carré qui décrivent chacun respectivement un segment de droite.
**3)** Trouver le lieu décrit par un point $P$ fixé quelconque du carré.

# RALLYE MATHÉMATIQUE D'ALSACE 1994

Voici les sujets proposés au vingt et unième Rallye Mathématique d'Alsace, le mercredi 23 mars de 14 à 18 heures pour les Terminales et le mercredi 6 avril de 14 à 18 heures pour les Premières. Il y eut cette année 1600 participants. Nous publierons des solutions dans le prochain "*Ouvert*".

---

## RALLYE DE PREMIÈRE

### 1e exercice

Un hexagone inscrit dans un cercle a 3 côtés de longueur a et 3 côtés de longueur b. Quel est le rayon du cercle ?

### 2e exercice

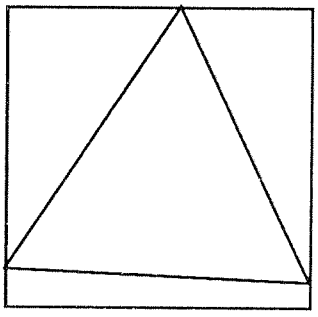
Alice, Betty et Carole ont subi une même série de tests notés de 1 à 10. Le professeur de Mathématiques leur annonce que l'ensemble de toutes les notes enregistrées comporte trois valeurs différentes apparaissant toutes le même nombre de fois. Le professeur de Physique ajoute que Betty est la première en Physique. En consultant leur Minitel, elles apprennent leurs totaux respectifs :

| |
|---|
| Alice : 20<br>Betty : 10<br>Carole : 9 |

Qui est première en Mathématiques ?

### 3e exercice

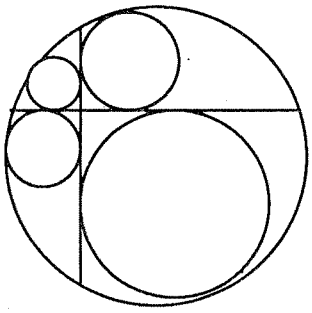
Un triangle dont tous les côtés sont de longueur strictement supérieure à 1 est inscrit dans un carré de côté 1. Montrez que le centre du carré est à l'intérieur du triangle.



---

# RALLYE DE TERMINALE

## 1e exercice



La construction du Tramway de Strasbourg a nécessité d'enterrer 4 câbles. Une des solutions techniques envisagées a été de choisir une gaine de diamètre intérieur D compartimentée par deux parois perpendiculaires, les câbles étant collés aux deux parois. Montrer que la somme des diamètres des 4 câbles est inférieure à $4(\sqrt{2}-1)D$.

## 2e exercice

Déterminez les entiers naturels x, y, z tels que :

$$x^{(y^z)}y^{(z^x)}z^{(x^y)} = 1994^{1994}xyz$$

## 3e exercice

Madame Lacraie, professeur de Mathématiques, enseigne dans deux classes de même niveau ayant chacune deux heures de Mathématiques par semaine. La classe A a une heure le lundi et une heure le jeudi. La classe B a une heure le mardi et une heure le vendredi. Normalement Madame Lacraie traite un paragraphe par heure, mais lorsqu'elle refait un cours pour la deuxième fois, elle va deux fois plus vite. Au bout de dix semaines de classe combien de paragraphes auront été traités dans chaque classe ?


---

Nous rappelons que l'IREM de Strasbourg a publié aux éditions Bordas (1990) "*Mathématiques de compétition – 2nde/1ère/Terminale*", dans la collection Jokers-Jeux.
Jean Lefort a rassemblé dans cet ouvrage les Rallyes Mathématiques d'Alsace avec les corrigés, de 1981 à 1989.
En vente dans les bonnes librairies (environ 63 F).

## A VOS STYLOS

### 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.

**Solution (E. Kern, M. Krier et D. Schneider)**

Il est clair que les $x_n$ sont strictement positifs et strictement croissants; ne pouvant avoir de limite finie (une telle limite, soit $l$, devrait vérifier $l = l + \frac{\alpha}{l}$), ils tendent vers l'infini. En additionnant les relations

$$x_{n+1}^2 = x_n^2 + 2\alpha + \frac{\alpha^2}{x_n^2},$$

on obtient

$$x_n^2 = 2n\alpha + x_0^2 + \alpha^2(\frac{1}{x_0^2} + \cdots + \frac{1}{x_{n-1}^2}).$$

Divisons les deux membres par $n$. Puisque la suite $1/x_n^2$ tend vers zéro, il en va de même de ses moyennes de Cesaro. Donc $x_n^2/n$ tend vers $2\alpha$, et $x_n$ est équivalent à $\sqrt{2n\alpha}$.

Nous avons reçu des solutions de F. Brassart (Arras), J. Dautrevaux (06 Saint-André), X. Fernique (Strasbourg), G. Hecquet (Toulouse), E. Kern (Strasbourg), M. Krier (Strasbourg), P. Renfer (Ostwald), D. Schneider (Strasbourg) et A. Trœsch (Strasbourg).

Trois d'entre elles (celles de X. Fernique, E. Kern et, par une méthode non-standard, A. Trœsch) mettent en évidence le lien entre le comportement de $x_n$ et celui de la solution de l'équation différentielle $\frac{dx}{dt} = \frac{\alpha}{x}$.

Plus généralement, E. Kern pose $g(x) = \alpha x^{1-\beta}$ ou $g(x) = \alpha e^{-\beta x}$ (avec $\alpha > 0$ et $\beta > 0$) et montre que, pour $f > 0$, continue et équivalente à $g$ au voisinage de $+\infty$, les suites $(x_n)_{n\in\mathbb{N}}$ vérifiant $x_{n+1} = x_n + f(x_n)$ sont équivalentes, quand $n$ tend vers l'infini, entre elles et à $y(n)$, où $y$ est n'importe quelle solution de l'équation différentielle $\frac{dy}{dt} = g(y)$. Il demande pour quelles autres fontions $g$ ce résultat subsiste.

G. Hecquet nous signale un résultat plus précis, figurant en exercice dans le livre de J.-M. Arnaudiès et H. Fraysse, "Cours de mathématiques - 2 : Analyse",

Chapitre II.4 (éd. Dunod, 1988) (nos excuses aux lecteurs; nous tâcherons d'être plus originaux la prochaine fois) : la différence

$$x_n - \sqrt{x_0^2 + 2\alpha n}$$

tend vers zéro. Ceci peut s'obtenir en l'écrivant

$$\frac{x_n^2 - (x_0^2 + 2\alpha n)}{x_n + \sqrt{x_0^2 + 2\alpha n}}$$

et en remarquant que le numérateur, égal à $\frac{\alpha^2}{x_0^2} + \cdots + \frac{\alpha^2}{x_{n-1}^2}$, croît logarithmiquement en $n$ alors que le dénominateur est en $\sqrt{n}$. Bien entendu, la constante $x_0^2$ sous le radical n'a aucune influence et peut être omise.

---

## PROBLÈME 28

### Énoncé

Etant donnés 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 $S$,

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

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

### Indication

La formule dépend de la parité de $n$.

---

## PROBLÈME 29

### Énoncé

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.

---

## PROBLÈME 30

### Énoncé

Pour quels entiers $p \geq 2$ et $q \geq 2$ le rectangle de dimensions $p \times q$ peut-il être pavé par des dominos $1 \times 2$ de manière que toute droite traversant le rectangle coupe en deux l'un (au moins) des dominos du pavage?

NOUVELLE BROCHURE :

# ENSEIGNER LES PROBABILITÉS EN TERMINALE

Après "Enseigner les probabilités en classe de première" (réédition mars 1994 - prix sur place : 55 F, 68 F en cas d'envoi), voici la nouvelle brochure du groupe "Probabilités" de l'IREM de Strasbourg.

Table des matières



---

Pour se la procurer veuillez vous adresser à la bibliothécaire et établir le chèque à l'ordre de M. l'Agent Comptable de l'ULP - IREM.
Prix de vente sur place 55 F, si envoi 70 F