# DEMONSTRATION AUTOMATIQUE EN GEOMETRIE : UNE APPROCHE PAR L'ALGEBRE

Marie-Françoise ROY

Les grandes étapes me semblent être en Occident
-le rêve de Descartes:
"remplacer les démonstrations de géométrie par les calculs"
-les succès de la géométrie analytique au 18° 19° siècle,
-avec le développement de la logique mathématique au 20 ° siècle, l'existence de théorèmes généraux comme le principe de Tarski-Seidenberg établi autour des année 1930 mais publié vers 1950 qui montre qu'on peut décider mécaniquement des classes très générales d'énoncés dans la géométrie réelle.

**Avec l'apparition des ordinateurs**
Les premiers essais de démonstration automatique remontent à 1960.

**Depuis le milieu des années 75**
Les progrès algorithmiques sont importants:
-les bases standard ou bases de Gröebner,
-la méthode de Wu (1977).

Wu est un mathématicien qui appartient à l'Académie des Sciences de Pékin. Il étudie aussi l'histoire des mathématiques chinoises et se place explicitement dans leur tradition "calculatoire". Dans la tradition mathématique en Chine il n'y a pas de démonstration mais des calculs (calculs de déterminants ...)

**Le principe de la méthode de Wu**
on a des hypothèses et une conclusion
on les traduit en égalités
on réarrange l'ensemble des hypothèses
on divise la conclusion par les hypothèses
si le reste est nul, le théorème est vrai.

*Référence*
Chou: Mechanical theorem proving, Reidel (1988).

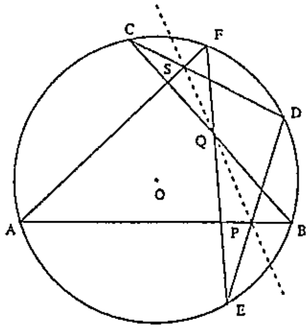
*Remarque*
La méthode ne produit pas les conclusions correctes, il ne fait que répondre par oui ou par non à des questions comme "telle conclusion est-elle conséquence de telles hypothèses?"

Le calcul produit les conditions de dégénérescence où l'énoncé devient faux: triangle aplati, droites parallèles.

**Un exemple: le théorème de Pascal**

Soient A,B C, D E, F six point sur un cercle (O). Soit $P=AB\cap DF$, $Q=BC\cap FE$ et $S=CD\cap EA$. Montrer que P,Q et S sont alignés.

Soit $A(0,0)$, $0(u_1,0)$, $B(x_1,u_2)$, $C(x_2,u_3)$ $D(x_3,u_4)$ $F(x_4,u_5)$ $E(x_5,u_6)$ $P(x_7,x_6)$ $Q(x_9,x_8)$ et $S(x_{11},x_{10})$.




Remarque: Il y a des u et des x: les u sont "libres" et les x "liés".

*Mise en équation des hypothèses*

| | |
|---|---|
| $h_1:=x_1^2-2u_1x_1+u_2^2$ | OA=OB |
| $h_2:=x_2^2-2u_1x_2+u_3^2$ | OA=OC |
| $h_3:=x_3^2-2u_1x_3+u_4^2$ | OA=OD |
| $h_4:=x_4^2-2u_1x_4+u_5^2$ | OA=OF |
| $h_5:=x_5^2-2u_1x_5+u_6^2$ | OA=OE |
| $h_6:=(u_5-u_4)x_7+(-x_4+x_3)x_6+u_4x_4-u_5x_2$ | P est sur DF |
| $h_7:=u_2x_7-x_1x_6$ | P est sur AB |
| $h_8:=(u_6-u_5)x_9+(-x_5+x_4)x_8+u_5x_5-u_6x_4$ | Q est sur FE |
| $h_9:=(u_3-u_2)x_9+(-x_2+x_1)x_8+u_2x_2-u_2x_1$ | Q est sur BC |
| $h_{10}:=u_6x_{11}-x_5x_{10}$ | S est sur AE |
| $h_{11}:=(u_4-u_3)x_{11}+(-x_3+x_2)x_{10}+u_2x_2-u_4x_2$ | S est sur CD |

*Mise en équation de la conclusion*

$g:=(x_8-x_6)x_{11}+(-x_9+x_7)x_{10}+x_6x_9-x_7x_8$ P,Q et S sont alignés.

*Arrangement des hypothèses*

A chaque étape, une seule nouvelle variable $x_i$ apparait.

$f_1:=h_1$

$f_2:=h_2$

$f_3:=h_3$

$f_4:=h_4$

$f_5:=h_5$

$f_6:=\text{reste}((u_5-u_4)h_7,h_6,x_7)$

$f_7:=h_7$

$f_8:=\text{reste}((u_6-u_5)h_9,h_8,x_9)$

$f_9:=h_9$

$f_{10}:=\text{reste}(u_6h_{11},h_{10},x_{11})$

$f_{11}:=h_{11}$

*Division de la conclusion par les hypothèses*

Chacune des "hypothèses modifiées" $f_i$ a comme variable principale $x_i$. Quand on divisera par $f_i$ on considérera tout comme polynomial en $x_i$ .

On ne veut pas de dénominateur. On multiplie donc à chaque fois le reste par le coefficient dominant du diviseur.

$r_{10}:=\text{reste}(\text{coefdom}(f_{11},x_{11})g,f_{11},x_{11})$

$r_9:=\text{reste}(\text{coefdom}(f_{10},x_{10})r_{10},f_{10},x_{10})$

$r_8:=\text{reste}(\text{coefdom}(f_9,x_9)r_9,f_9,x_9)$

$r_7:=\text{reste}(\text{coefdom}(f_8,x_8)r_8,f_8,x_8)$

etc ....

$r_0:=\text{reste}(\text{coefdom}(f_1,x_1)r_1,f_1,x_1)$

*Résultat du calcul*

$r_0 := 0$

*Interprétation du calcul*

Le théorème est démontré sous l'hypothèse que les coefficients dominants des $f_i$ sont non nuls, ce qui donne les conditions:

$I_5 := u_1 \neq 0$

$I_6 := x_1(u_4 - u_5) + (-x_3 + x_4) u_2 \neq 0$

$I_7 := u_2 \neq 0$

$I_8 := (u_6 - u_5)x_1 - (u_6 - u_5)x_2 - (u_2 - u_3)x_4 + (u_2 - u_3)x_5 \neq 0$

$I_9 := u_2 - u_3 \neq 0$

$I_{10} := (- x_2 + x_3)u_6 + (u_3 - u_4)x_5 \neq 0$

$I_{11} := (u_3 - u_4) \neq 0$

Ces conditions peuvent se réinterpréter géométriquement ainsi:
Le rayon n'est pas nul ($I_5$),
B n'est pas sur l'axe des x ($I_7$),
C n'a pas même abscisse que B ($I_9$),
D n'a pas même abscisse que C ($I_{11}$),
Les droites AB et DF ne sont pas parallèles ($I_6$),
Les droites BC et FE ne sont pas parallèles ($I_8$),
Les droites CD et EA ne sont pas parallèles ($I_{10}$).

*Remarques*

On a deux sortes de variables: les paramètres (u..) qui sont indépendants, les variables (x..) qui sont liées.

En arrangeant les hypothèses on fait apparaître une forme triangulaire.

En divisant il apparaît des dénominateurs (qui s'interprètent a posteriori comme des conditions de dégénérescence).

**Plus de détails sur la méthode de Wu**

*Mise en équation*

On a une "variété des hypothèses": un ensemble fini d'équations algébriques.

On doit avoir une idée claire (non mécanisée) de ce qui est paramètre indépendant et de ce qui ne l'est pas.

Le reste se fait mécaniquement:

on triangularise les hypothèses pour qu'elles soient sous la forme $f_i$ : polynôme des $u_i$ et des seules variables $x_1,...,x_i$

on fait la division. Lors de la division il apparaît des conditions de dégénérescence correspondant aux coefficients dominants des diviseurs.

Si le reste est nul on peut conclure que le théorème est vrai (sous les conditions de dégénérescence)

Si le reste n'est pas nul et que la variété des hypothèses est irréductible on peut conclure que le théorème est faux.

Si le reste n'est pas nul et que la variété des hypothèses n'est pas irréductible il faut la factoriser par la "méthode de Wu améliorée "(dont je ne parlerai pas ici) ...

Reste à analyser les conditions de dégénérescence (de manière non mécanisée): on réintroduit un contenu géométrique.

*Du point de vue informatique*

Cette méthode nécessite de faire de gros calculs symboliques avec des variables et des entiers longs. Il existe pour cela des systèmes appelés systèmes de calcul formel: MACSYMA, REDUCE, MAPLE disponibles sur stations de travail, de plus en plus sur ordinateurs personnels.

*Exemple de déroulement d'une session.*

(ici la session est interactive mais on pourrait travailler par programme)

*appel de REDUCE*

```
Emmy% reduce
REDUCE 3.3, 15-Jul-87 ...
```

*rentrée des hypothèses*

```
1: h1:=x1^2-2*u1*x1+u2^2;
       2                 2
H1 := X1  - 2*X1*U1 + U2

2: 2: h2:=x2^2-2*u1*x2+u3^2;
       2                 2
H2 := X2  - 2*X2*U1 + U3

3: 3: h3:=x3^2-2*u1*x3+u4^2;
       2                 2
H3 := X3  - 2*X3*U1 + U4

4: h4:=x4^2-2*u1*x4+u5^2;
       2                 2
H4 := X4  - 2*X4*U1 + U5

5:  h5:=x5^2-2*u1*x5+u6^2;
                      2    2
H5 :=  - (2*U1*X5 - X5  - U6 )

6: h6:=(u5-u4)*x7+(-x4+x3)*x6+u4*x4-u5*x3;

H6 :=  - (X3*U5 - X3*X6 - X4*U4 + X4*X6 + U4*X7 - U5*X7)

7: h7:=u2*x7-x1*x6;

H7 :=  - (X1*X6 - U2*X7)

8: h8:=(u6-u5)*x9+(-x5+x4)*x8+u5*x5-u6*x4;

H8 :=  - (X4*U6 - X4*X8 - U5*X5 + U5*X9 + X5*X8 - U6*X9)

9: h9:=(u3-u2)*x9+(-x2+x1)*x8+u2*x2-u3*x1;

H9 :=  - (X1*U3 - X1*X8 - X2*U2 + X2*X8 + U2*X9 - U3*X9)

10: h10:=u6*x11-x5*x10;

H10 :=  - (X5*X610 - U6*X11)

11:  h11:=(u4-u3)*x11+(-x3+x2)*x10+u3*x3-u4*x2;

H11 :=  - (X2*U4 - X2*X10 - X3*U3 + X3*X10 + U3*X11 - U4*X11)
```

*rentrée de la conclusion*

```
12: g:=(x8-x6)*x11+(-x9+x7)*x10+x6*x9-x7*x8;

G :=  - (X7*X8 - X7*X10 - X6*X9 + X6*X11 + X9*X10 - X8*X11)
```

*ordre d'élimination des variables*

```
13: korder x11,x10,x9,x8,x7,x6,x5,x4,x3,x2,x1;
```

*triangulation des hypothèses*

```
14: f1:=h1;

          2              2
F1 := X1   - 2*X1*U1 + U2

15: f2:=h2;

          2              2
F2 := X2   - 2*X2*U1 + U3

16: f3:=h3;

          2              2
F3 := X3   - 2*X3*U1 + U4

17: f4:=h4;

          2              2
F4 := X4   - 2*X4*U1 + U5

18: f5:=h5;

                       2     2
F5 :=  - 2*U1*X5 + X5   + U6

19: f6:=remainder((u5-u4)*h7,h6,x7);

F6 := X1*U4*X6 - X1*U5*X6 + X3*U2*U5 - X3*U2*X6 - X4*U2*U4 + X4*U2*X6

20: f7:=h7;

F7 :=  - X1*X6 + U2*X7

22: f8:=remainder((u6-u5)*h9,h8,x9);

F8 :=  - ( - X1*U3*U5 + X1*U3*U6 + X1*U5*X8 - X1*U6*X8 + X2*U2*U5 -
          X2*U2*U6 - X2*U5*X8 + X2*U6*X8 + X4*U2*U6 - X4*U2*X8 - X4*
          U3*U6 + X4*U3*X8 - U2*U5*X5 + U2*X5*X8 + U3*U5*X5 - U3*X5*
          X8)

23: 23: f9:=h9;

F9 :=  - (X1*U3 - X1*X8 - X2*U2 + X2*X8 + U2*X9 - U3*X9)

25: f10:=remainder(u6*h11,h10,x11);

F10 :=  - (X2*U4*U6 - X2*U6*X10 - X3*U3*U6 + X3*U6*X10 + U3*X5*X10 -
           U4*X5*X10)
```

```
30: f11:=h11;

F11 :=  - (X2*U4 - X2*X10 - X3*U3 + X3*X10 + U3*X11 - U4*X11)
```

*division de la conclusion par les hypothèses*

```
31: r10:=remainder(g*(u4-u3),f11,x11);

R10 :=  - X2*U4*X6 + X2*U4*X8 + X2*X6*X10 - X2*X8*X10 + X3*U3*X6 - X3
        *U3*X8 - X3*X6*X10 + X3*X8*X10 + U3*X7*X8 - U3*X7*X10 - U3*X6*
        X9 + U3*X9*X10 - U4*X7*X8 + U4*X7*X10 + U4*X6*X9 - U4*X9*X10
```

et ainsi de suite jusqu'à

```
75: r0:=remainder(lcof(f1,x1)*r1,f1,x1);

R0 := 0
```

YOUPIE !!!

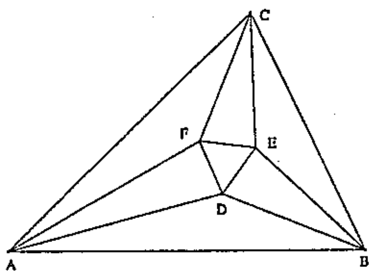
*Remarque*:
Il est clair qu'on n'aurait pas pu faire le calcul à la main: les calculs sont très gros, certain résultats intermédiaires occupant 9 pages de listing. Sur une station de travail SUN de l'IRMAR, le tout m'a pris en interactif moins d'une demi-heure (y compris l'affichage des résultats, qui est très long). Chou donne 2,5 secondes de temps CPU sur sa machine Symbolics 3600.

**A quoi ça sert?**

*a) A montrer des théorèmes non triviaux*

*-le théorème de Morley* (1899)

Les trois point d'intersection des trisecteurs adjacents d'un triangle forment un triangle équilatéral.




Donnons un petit historique de ce problème:

Cette propriété, aussi élégante que surprenante a été découverte par Morley en 1899. Elle s'est répandue à travers le monde. Une preuve trigonométrique a été donnée par Satyanarayana dix ans après. Une preuve élémentaire a été publiée par

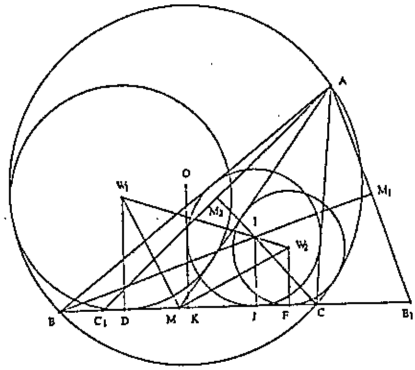
Naraniengar.

La preuve mécanique de Chou prouve en fait une généralisation, peut-être nouvelle, de ce théorème: parmi les 27 triangles qu'on peut réaliser avec les trisecteurs, 18 sont équilatéraux.

*-le théorème de Thébault*

Soit ABC un triangle, et M un point de BC. Soient (O) le cercle circonscrit et (I) le cercle inscrit au triangle ABC.

Soient ($w_1$) et ($w_2$) deux cercles de centre $w_1$ et $w_2$ tangent au cercle (O) avec ($w_1$) tangent aux deux côtés de l'angle AMB, et ($w_2$) tangent aux deux côtés de l'angle AMC. Montrer que la droite joignant $w_1$et $w_2$ passe par I.




Il s'agit d'une conjecture de Thébault en 1938. La première démonstration date de 1983. Chou a réussi mécaniquement en 1987: 44 heures de CPU, consistant surtout à manipuler des polynômes de 100 000 termes.

Là encore la démonstration mécanique crée un nouvel énoncé:

Pour chacun des quatre centres des cercles tritangents (inscrits ou exinscrits), noté I, il existe $w_1$et $w_2$ tels que $w_1$, $w_2$ et I sont alignés.

*b) A poser des questions de mathématique intéressantes*

*-Reposer certaines questions de la géométrie classique*

*La notion de condition de dégénérescence*: les conditions de dégénérescence ne dépendent pas de la figure mais du problème qu'on se pose sur la figure.

*Les quatre cercles tritangents*: nombre de propriétés montrées pour le cercle inscrit sont encore valables pour les cercles exinscrits. La raison en est que les abscisses des centres des cercles tritangents vérifient une équation du 4° degré (puisqu'il y a quatre solutions) en général irréductible, et ne peuvent donc pas être distingués pour tout une classe de problèmes.

*-Permettre l'illustration de concepts fondamentaux de la géométrie*

*algébrique moderne*:

variables algébriquement indépendantes,

théorie de la dimension,

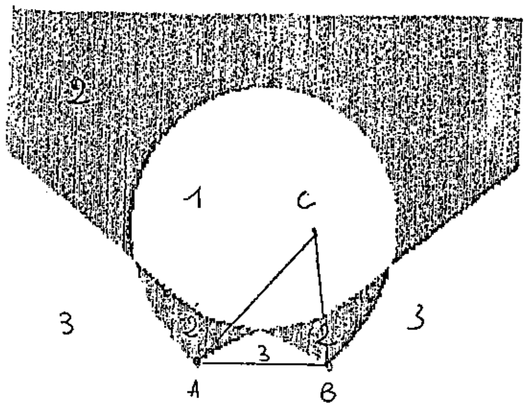
notion de variété algébrique irréductible.

-*Eclaire les relations entre géométrie réelle et géométrie complexe*:
la méthode de Wu ne traite que des égalités et inéquations, jamais des inégalités.

*Un exemple avec des inégalités: l'espace des triangles.*

Le problème initial était le suivant : montrer que le rayon du cercle inscrit est inférieur ou égal à la moitié du rayon du cercle circonscrit.

En faisant le calcul, il est apparu que suivant la forme du triangle, il y a un deux ou trois des cercles tritangents qui vérifient la propriété. La mise en évidence de cette propriété vient donc du calcul automatique.




On peut donc se poser encore de nouvelles questions sur les triangles...
La courbe qui apparaît sur le dessin est une courbe irréductible du 8° degré. Elle a été étudiée par des techniques de géométrie réelle, à Rennes, par Ahmed Guergueb.

*c) A poser des questions d'épistémologie des mathématiques intéressantes*

Par exemple:

- L'interaction algèbre/géométrie: Dans les calculs on oublie le contenu géométrique. Il faut revenir à la géométrie dans l'interprétation.

-L'intérêt d'une approche automatique des mathématiques pour affiner les énoncés.