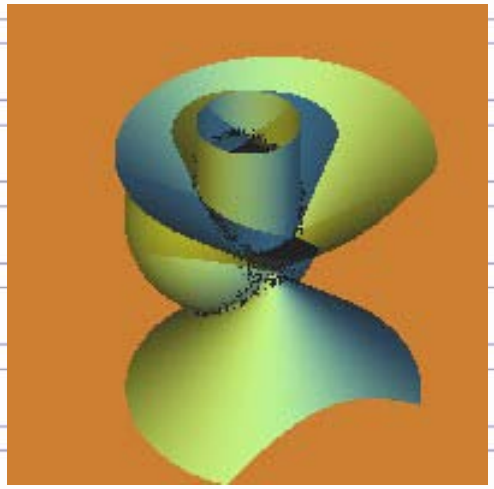
N° 117 – Octobre 2010

Feuille de Vigne

Irem de Dijon

- ✓ Cryptage par les groupes
- ✓ Une courbe méconnue : la bizarroïde
- ✓ Guide pratique d'utilisation de GéoGébra



Revue Trimestrielle

Issn 0246-5752

Sommaire

Articles

Éditorial

Le premier article de cette Feuille de Vigne est de Alma Selimovic et Marine Chargrasse, toutes deux étudiantes en deuxième année de master de mathématiques à Dijon. Elles ont écrit cet article lors de leur Travail d'Etude et de Recherche de M1 dirigé par leur enseignant Luis Paris. C'est une introduction à un domaine qui s'est beaucoup développé ces dernières années : la cryptographie sur les groupes. Elles vont toutes les deux passer l'écrit du CAPES en novembre ; nous leur souhaitons une bonne réussite.

Le second article nous présente une courbe qui, sous des airs de cercle dessiné de la main gauche par un droitier, possède une surprenante propriété : je n'en dis pas plus, allez-voir page 11 l'article de Michel Lafond !

En fin de revue, vous trouverez un article écrit par Nicolas Vissac, professeur au collège Les Amognes à Saint Bénin d'Azy. Il s'agit d'un guide très pratique sur l'utilisation du logiciel GeoGebra pour faire de la géométrie avec des élèves de collège. Nicolas Vissac appartient au groupe « Utiliser des logiciels libres pour faire de la géométrie » de l'IREM de Dijon.
Vous pouvez consulter le wiki du groupe à l'adresse :

http://geowiki.u-bourgogne;fr/.

Bonne lecture !

C. Labruère Chazal

Agenda

Dates des rallyes

Rallye des lycées de Bourgogne : mercredi 26 janvier 2011
Rallyes des collèges de Bourgogne : vendredi 21 janvier 2011

Connaissez-vous géowiki ?

Le groupe « Logiciels de géométrie » de l'IREM de Dijon dispose maintenant d'un wiki, hébergé par l'université, dont voici l'adresse : http://geowiki.u-bourgogne.fr/.

Nous vous invitons à vous y rendre de temps en temps pour suivre nos travaux et surtout à les influencer en nous posant des questions techniques ou pédagogiques concernant l'utilisation des logiciels de géométrie.

Pour poser des questions, c'est très simple. Il suffit de vous enregistrer. On vous demandera un nom d'utilisateur, votre nom et une adresse de courriel où vous sera envoyé votre mot de passe après quelques secondes. Dès cet instant vous pouvez vous connecter sur ***geowiki*** et vous disposez du droit d'écrire et même de déposer des fichiers dans la partie ***questions.*** Vous pouvez aussi vous abonner aux pages qui vous intéressent, vous serez ainsi tenu au courant des modifications de ces pages. Abonnez-vous à la page de votre question et vous saurez si un élément de réponse y a été apporté ! Un courriel vous sera envoyé automatiquement.

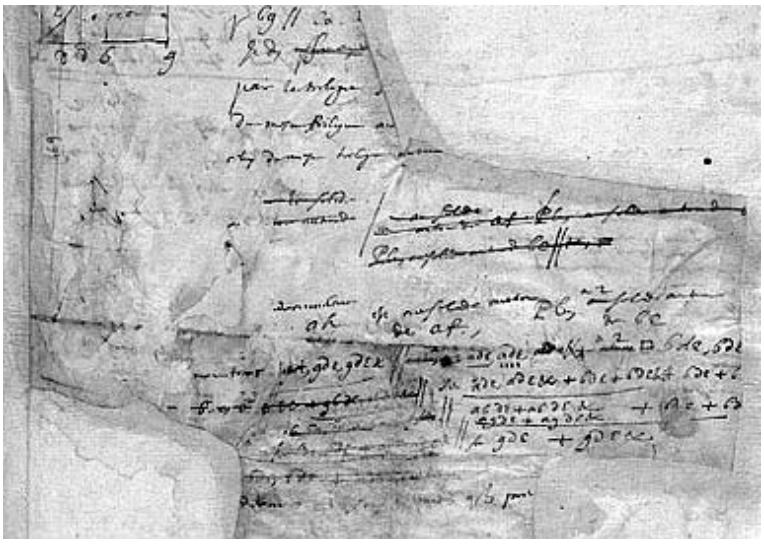
Nous vous tiendrons également au courant de nos activités dans la ***feuille de vigne.*** Dans celle-ci, par exemple, vous pourrez lire un mode d'emploi de ***géogébra*** pour les collèges, écrit par Nicolas Vissac.

Notre groupe est ouvert et si vous voulez en faire partie, il suffit de vous enregistrer et de m'écrire (mascret@ac-dijon.fr). Nos réunions se feront le plus souvent par internet ce qui permet aux membres du groupe d'être disséminés dans toute l'académie.

Alain Mascret, Collège La Champagne, 21220 Brochon

Un manuscrit de Blaise Pascal vient d'être découvert

Dominique Descotes, chercheur clermontois, a mis au jour un manuscrit inconnu de Blaise Pascal. Ce serait la seule note mathématique de la main de Pascal. Ce document se trouvait dans le manuscrit des « *pensées* » (conservé à la Bibliothèque Nationale de France).
C'est un morceau de papier, usé, découpé, sur lequel on peut voir une figure et des sommes de surfaces.



Ce document, même s'il est d'un intérêt scientifique limité, pourra donner des indications sur les méthodes de travail du philosophe-mathématicien et de « voir penser » Pascal ….

Sitographie :

http://www.lamontagne.fr/editions_locales/clermont_ferrand/un_manuscrit_de_blaise_pascal_mis_au_jour@CARGNjFdJSsGERkEBRw-.html
http://bibliophilie.blogspot.com/2010/09/un-manuscrit-de-blaise-pascal-decouvert.html
http://www.lexpress.fr/actualites/1/dominique-descotes-une-vie-sur-les-traces-de-blaise-pascal_920487.html
http://www.lefigaro.fr/sciences-technologies/2010/08/26/01030-20100826ARTFIG00638-decouverte-d-un-manuscrit-de-blaise-pascal-inconnu.php

Jeux et Problèmes

Michel LAFOND
mlafond001@yahoo.fr

JEU - 67

Quelle est la "suite logique" de :

$0{,}6^2 + 0{,}8^2 = 1$
$0{,}28^2 + 0{,}96^2 = 1$
$0{,}936^2 + 0{,}352^2 = 1$
$0{,}8432^2 + 0{,}5376^2 = 1$?

PROBLÈME - 67

Quel est le seul nombre premier qui peut s'écrire sous la forme :
$n^4 - 22\,n^3 + 148\,n^2 - 282\,n + 27$ avec n entier naturel ?

Solutions

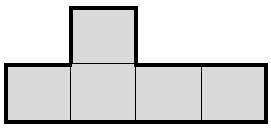
JEU - 66

Soit F un ensemble du plan sans axe de symétrie.

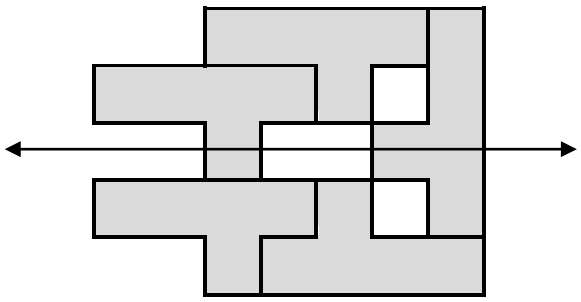
Le jeu consiste à disposer dans le plan un nombre impair de figures F, sans empiètement, de manière à obtenir une figure ayant un axe de symétrie. Le retournement est autorisé.

Exemple :

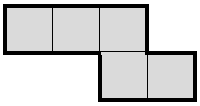
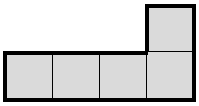
À partir de 5 figures F =



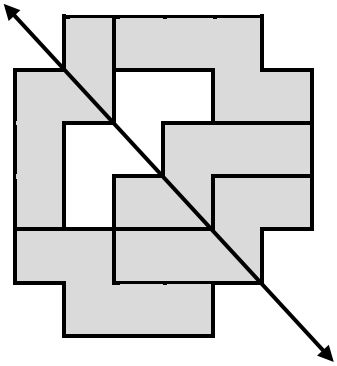
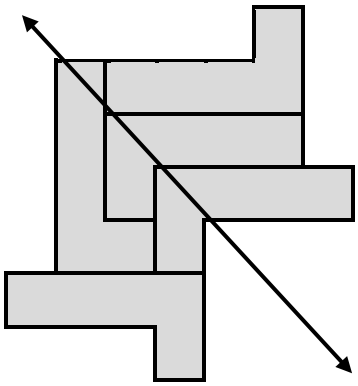
On obtient :



Faire de même avec les figures ci-dessous :

 puis 

Solution :

PROBLÈME - 66

Démontrer que tous les entiers dont l'écriture décimale commence et finit par 1, et qui alternent les 1 et les 0, c'est-à-dire N = 1 0 1 0 1 0 --- 1 0 1 sont des nombres composés (non premiers) sauf 101.

Solution :

Distinguons 2 cas :

- Si on a un nombre pair de "1" alors N est multiple de 101.
  Exemple 101010101010101 = 101 × 1000100010001
- Si on a un nombre impair de "1" disons $2p + 1$ alors :

$$N = 10^{4p} + 10^{4p-2} + 10^{4p-4} + 10^{4p-2} + \ldots + 10^2 + 1 = \frac{10^{4p+2} - 1}{10^2 - 1} = \frac{10^{2p+1} - 1}{9} \times \frac{10^{2p+1} + 1}{11}$$

et N est le <u>produit de deux entiers</u> puisque $10^{2p+1} \equiv 1$ modulo 9 et $10^{2p+1} \equiv -1$ modulo 11.

Le cas $p = 0$ donne $N = 1 \times 1 = 1$ qui n'est pas premier, et à partir de $p = 1$ les deux facteurs sont au moins égaux à 91. N est encore composé.

Cryptage par les groupes

A.Selimovic & M.Chargrasse
Mémoire 1ère année de Master

La cryptologie (étymologiquement « la science du secret ») n'est vraiment considérée comme une science que depuis peu. La cryptographie quant à elle est une des disciplines de la cryptologie s'attachant à protéger des messages en s'aidant de secrets ou de clés. Aujourd'hui considérée comme une branche des mathématiques, de l'informatique et des sciences de la communication, la cryptographie donne des moyens pour envoyer des messages confidentiels à travers des canaux publics de communication (internet, ...). Les différents systèmes de cryptage existant de nos jours utilisent divers algorithmes et protocoles afin d'envoyer et de recevoir des messages cryptés. Cet article permettra l'initiation aux systèmes de cryptage basés sur la théorie des groupes. Le sujet ici concerne la cryptographie à clé publique : l'expéditeur utilise la clé publique du destinataire pour coder le message que seul ce destinataire (en possession de la clé privée) peut décoder. L'objectif de cet article est, une fois le terrain classique exploré (RSA et autres, fondés sur des difficultés liées à l'arithmétique), d'aborder de nouveaux protocoles fondés sur l'algorithmique de théorie des groupes de type fini non commutatifs.

Donnons un exemple classique de crypto système (utilisé par Jules César!) pour commencer. Considérons les lettres de l'alphabet et une modification quelconque de cet ensemble. Par exemple la permutation cyclique qui envoie a sur b, b sur c, ..., z sur a. Si on applique cette transformation à un mot, on obtient par exemple pour le mot *oui,* le mot *pvj* . Pour déchiffrer le message, on applique évidemment la transformation inverse. Le problème avec cet exemple classique est que cette transformation et son inverse peuvent être facilement déduites à partir de quelques messages. Il suffit en effet de connaître la fréquence d'apparition des lettres dans un texte. A partir d'un échantillon de messages suffisant, le décryptage est rapide. Le problème est donc de rendre pratiquement impossible la détermination de l'application inverse.

Dans le modèle classique de la cryptographie, deux individus Bob et Patrick choisissent secrètement une clé K qui définit des règles e_K (cryptage) et d_K (décryptage). Lorsque e_K et d_K sont identiques ou peuvent se déduire facilement, on dit que ces systèmes cryptographiques sont *à clé privée* ou *à clé symétrique*, car la publication de e_K rend le système peu sûr. Les systèmes à clé privée ont un défaut : ils nécessitent la communication au préalable de la clé K entre Bob et Patrick, par un canal sûr avant la transmission du message chiffré.

Dans la pratique, cela peut s'avérer difficile à réaliser. Par exemple si Patrick et Bob vivent à des endroits éloignés et s'ils décident de communiquer par courrier électronique, ils n'ont raisonnablement pas accès à un canal sûr. L'objectif des systèmes *à clé publique* est de rendre la règle d_K impossible à retrouver à partir de e_K. Ainsi la règle de cryptage e_K peut être publiée dans un répertoire (d'où le nom du

Historique :

- XVI^{ème} avt J-C — Un potier grave sa recette secrète sur une tablette d'argile en modifiant l'orthographe des mots.
- V^{ème} avt J-C — Utilisation des premières techniques de chiffrement dans des textes religieux ; la plus connue « atbash », une méthode de substitution inversée : A devient Z, B devient Y, ...
- II^{ème} avt JC — Le code César.
- 1379 — Le secrétaire du Pape écrit un recueil de codes et de clés : « nomenclateur », permet de crypter des mots courants et sera utilisé pendant plusieurs siècles par des diplomates américains et européens.
- 1412 — Première encyclopédie en 14 volumes dans le domaine de la cryptographie par l'égyptien al Qalquashandi.
- 1467 — Leone Battista Alberti expose pour la première fois le chiffrement par substitution polyalphabétique. Le procédé consiste à remplacer chaque lettre du texte par une lettre d'un autre alphabet et à changer plusieurs fois d'alphabet de substitution au cours du codage, rendant la cryptanalyse par analyse de fréquence inefficace.
- 1518 — Le premier livre traitant de cryptologie, il expose notamment le procédé sténographique consistant à rempla cer chaque lettre par un groupe de mot, le texte crypté ressemblant ainsi à un poème.
- 1854 — Un pionnier du télégraphe, Charles Weatstone, invente le chiffrement de Playfair, qui est basé sur une métho de de substitution diagrammatique consistant à remplacer un couple de lettres adjacentes par un autre couple choisi qui constitue la clé.
- 1919 — La machine Enigma (machine à chiffrer électromécanique) a été inventée pour les civils. Elle fut reprise par les militaires. Elle remplace chaque lettre par une autre et la substitution change d'une lettre à l'autre. Quand on appuie sur une touche du clavier, un circuit électrique est formé et une lampe s'allume indiquant que la lettre a été codée. Ses points forts : le nombre de clés, énorme pour l'époque, et la réversibilité. Ses point faibles : les opérateurs commençaient souvent leurs messages par « mon général », de ce fait connaissant le début en clair et en codé, il était facile de trouver la clé, qui était la même pour toutes les machines Enigma.

système à clé publique). L'avantage du système à clé publique est que Patrick (ou toute autre personne) peut envoyer un message chiffré par e_K à Bob, sans communication privée au préalable. Bob est la seule personne capable de le déchiffrer en utilisant sa règle secrète d_K. Ceci est analogue à la situation suivante : Patrick place un objet dans un coffre fort, dont Bob seul connaît la combinaison et le ferme. Bob pourra ensuite (et lui seul) récupérer l'objet grâce à la combinaison secrète. L'idée de ce système à clé publique, qui date de 1976, est due à Diffie et Hellman. La première réalisation d'un système à clé publique fut publiée en 1977 par Rivest, Shamir et Adleman : le système RSA.

Le système RSA

On veut coder par exemple le mot «cryptage». On considère A l'alphabet usuel auquel on adjoint des symboles (virgule, point, blanc, ...) et B un ensemble. Au lieu de remplacer une lettre par une autre, on peut remplacer une suite de lettres, disons 2 lettres (k dans le cas général), par un élément de B. Cette transformation est appelée *fonction de hachage*. Ici, supposons par exemple que B est l'ensemble des mots de deux lettres et que la fonction de hachage envoie le mot «cryptage» sur (cr,yp,ta,ge).
On définit également une application β qui à un élément de B associe un entier. Cette application sert à remplacer les lettres par des chiffres pour pouvoir coder. Supposons par exemple que β(cr) =2, β(yp)=11, β(ta)=3, β(ge)=8. Alors (cr, yp, ta, ge) devient (2, 11, 3, 8).

Pour utiliser le système RSA, Bob choisit une paire de nombres entiers assez grands. Pour l'exemple, p=19 et q=43. Puis il calcule n=pq=817 et le rend « publique ».

Il calcule ensuite $\varphi(n)=(p-1)(q-1)=756$ (qui se trouve être le nombre d'entiers inférieurs à n et premiers avec n) et choisit au hasard un entier c de façon à ce qu'il soit premier avec $\varphi(n)$. Dans cet exemple choisissons c=11. Bob rend c également « publique ».
Pour coder le message, Patrick qui connaît la valeur de c, calcule :

$$(2^{11},11^{11},3^{11},8^{11})$$

puis réduit ces entiers modulo 817 (i.e. tous les entiers entre 1 et 816 ne changent pas et on remplace chaque entier supérieur à 816 par le reste de la division euclidienne par 817) . Voilà le message « codé » :

$$(414,64,675,677)$$

Désignons par d l'inverse de c dans le groupe Z/756Z. Grâce à l'algorithme d'Euclide, on obtient d=275. Remarquons que Bob est le seul à pouvoir faire ce calcul car p et q n'étant pas publiques, $\varphi(n)=756$ ne l'est pas non plus.
Pour décoder le message, Bob fait alors le calcul suivant :

$$(414^{275},64^{275},675^{275},677^{275})$$

Il réduit ces entiers modulo 817 et retrouve le message de départ (2,11,3,8). Ceci est obtenu grâce au
Théorème de Fermat-Euler : *si a est premier avec n alors a à la puissance $\varphi(n)$ est un multiple de n.*

Le triplet <p,q,d> est la clé privée tandis que <n,c> est la clé publique. La sécurité du système RSA repose sur la difficulté à trouver les entiers p et q, c'est-à-dire à factoriser de grands nombres premiers.

Afin de pouvoir travailler sur le cryptage par les groupes, il est important de bien connaître le cryptage « Diffie-Hellman » que nous allons présenter ci-après.

Le système de Diffie-Hellman

On se place dans un groupe cyclique, ici Z/pZ, où p est un nombre premier. On choisit α un générateur de Z/pZ. Comme pour RSA, Patrick et Bob ne disposent pour communiquer que d'un canal non sûr. Il leur faut donc se mettre d'accord publiquement sur un procédé de communication assurant la confidentialité. Bob choisit un nombre secret a compris entre 0 et p-2. Il calcule

$$b = \alpha^a$$

réduit b modulo p puis transmet b.
Patrick choisit de même un nombre secret c. Il calcule

$$d = \alpha^c$$

réduit d modulo p puis transmet d.
Bob et Patrick décident ensuite que leur clé secrète commune sera :

$$s = b^c = d^a = \alpha^{ac}$$

réduite aussi modulo p. Remarquons qu'ils peuvent bien la calculer tous les deux, sans transmission supplémentaire.
Si Patrick veut transmettre le message x, il transmet e(x) = s*x.

Désignons par b' l'inverse de b dans Z/pZ. Bob décode alors le message e(x) en le multipliant par b'^c et en réduisant modulo p. En effet, $b'^c * e(x)=b'^c * d^a * x = x$ modulo p.

Il n'y a pas de manière facile d'obtenir s à partir des seules indications transmises publiquement . Trouver s revient à résoudre un problème difficile (en temps raisonnable) appelé *problème du logarithme discret* : Il s'agit de trouver α connaissant α^a et a. De la même manière que le problème de factorisation des grands nombres premiers est garant de la sécurité du système RSA, le problème du logarithme discret l'est de la sécurité du système de Diffie-Hellman.

Les crypto-systèmes basés sur la théorie des groupes n'ont pas encore abouti à des systèmes rivalisant avec RSA et Diffie-Hellman mais les idées sont intéressantes et les différentes perspectives conduisent à des problèmes intéressants en théorie des groupes. Nous allons en voir quelques-uns ci-après.

Système de Ko-Lee

Soit G un groupe non commutatif. On choisit publiquement un élément g de G. Soient A et B deux sous groupes de G commutant l'un avec l'autre (i.e. tout élément de A commute avec tout élément de B). Pour envoyer un message à Bob, Patrick choisit un élément a de A, calcule $a^{-1}ga$ (noté g^a) où a^{-1} est l'inverse de a dans A et transmet à Bob. De même, Bob choisit un élément de B, calcule $g^b=b^{-1}gb$ et transmet à Patrick. Comme ba=ab, chacun peut alors calculer la clé secrète :

$$s=(g^b)^a=(g^a)^b$$

On crypte le message de la même manière que pour le système de Diffie-Hellman. La sécurité de cette méthode réside dans la difficulté à déterminer a à partir de $a^{-1}ga$ et g (ou b à partir de $b^{-1}gb$ et g). Ce problème, bien connu en théorie des groupes, est appelé *problème de conjugaison*. Ce protocole est notamment plus facile à construire sur *le groupe des tresses*.

Le groupe des tresses :

Pour étudier ce groupe, on doit déjà fixer un entier n qui représente le nombre de brins. Une tresse est, comme on peut se l'imaginer, définie par plusieurs brins que l'on passe les uns sur les autres mais sans revenir en arrière. La tresse triviale est le brin. Avec deux tresses, on peut construire une troisième : la composée. On obtient ainsi le groupe des tresses : les tresses ainsi que leurs compositions. Le groupe des tresses B_n n'est pas commutatif à partir de n =3.

Pour le moment, on sait mal construire des tresses aléatoires pour lesquels il soit certain que le problème de conjugaison est difficile, ce qui pose problème pour le choix de clés.

Système Anshel-Anshel-Goldfeld

On suppose toujours que G est un groupe non commutatif. Il n'est pas nécessaire que A et B commutent. On choisit publiquement un certain nombre d'éléments $a_1, \dots, a_k, b_1, \dots, b_m$ de ce groupe G.

Patrick choisit en secret x parmi $a_1, \dots, a_k$ et envoie à Bob $xb_1x^{-1}, \dots, xb_mx^{-1}$. De la même manière Bob choisit y parmi $b_1, \dots, b_m$ et envoie $ya_1y^{-1}, \dots, ya_ky^{-1}$.
Patrick calcule yxy^{-1} et Bob xyx^{-1}.

La clé secrète du protocole est :
$s=x^{-1}y^{-1}xy$ où x^{-1} et y^{-1} sont les inverses de x et y respectivement.

Notons que Patrick et Bob peuvent tous les deux calculer la clé secrète. Comme dans le système précédent, on préfère travailler pour l'instant avec le groupe des tresses à cause du problème de conjugaison qui semble être difficile à résoudre dans un temps raisonnable.

La clé Stickel

On prend comme groupe G le groupe des matrices n,n inversibles à coefficients dans Z/pZ et g un élément de G. Soient a et b des éléments de G qui commutent. Soient m l'ordre de b (i.e. le plus petit entier tel que $b^m=1$) et n l'ordre de a. Pour créer une clé secrète, Patrick et Bob doivent procéder de la manière suivante :
Patrick choisit l, k au hasard tels que l est compris entre 0 et n et k est compris entre 0 et m. Il calcule $u=a^lgb^k$ et l'envoie à Bob.
De même Bob choisit r et s tels que r est compris entre 0 et n et s est compris entre 0 et m. Il calcule $v=a^rgb^s$ et l'envoie à Patrick.
Patrick calcule $k_a = a^lvb^k = a^{l+r}gb^{k+s}$.
Bob calcule $k_b = a^rub^s = a^{l+r}gb^{k+s}$.
La clé partagée secrètement est donc $s=k_a=k_b$.

Les hommes ont toujours voulu protéger les messages qu'ils transmettent que ce soit des messages amoureux, de guerre, ou encore des coordonnées bancaires. Depuis une dizaine d'années, beaucoup de crypto-systèmes sont apparus afin d'essayer d'augmenter la sécurité des messages transmis. Les systèmes de cryptographie par les groupes se sont développés : les protocoles de Ko-Lee ou de Anshel-Anshel-Goldfeld sont les premières idées de cryptages par les groupes, en attendant de trouver le « bon » groupe, celui où les éléments pourront être efficacement manipulés et stockés.

Références :

- www.wikipedia.org
- Lionel Schwarz, « algèbre troisième année », DUNOD
- Patrick Dehornoy, « Mathématiques de l'informatique », DUNOD
- Douglas Stinson, « Cryptographie, théorie et pratique », THOMSON
- G. Brassard, « Cryptographie contemporaine », MASSON
- math.u-bourgogne.fr/topolo/paris/LesTresses.pdf
- Sciences1.univ-oujda.ac.ma/CIMPA/Cours/11.Marraki/marakibraidPartie2.pdf
- Simon R. Blackburn, Carlos Cid and Ciaran Mullan, *Group theory in cryptography.*

Une courbe méconnue : la bizarroïde

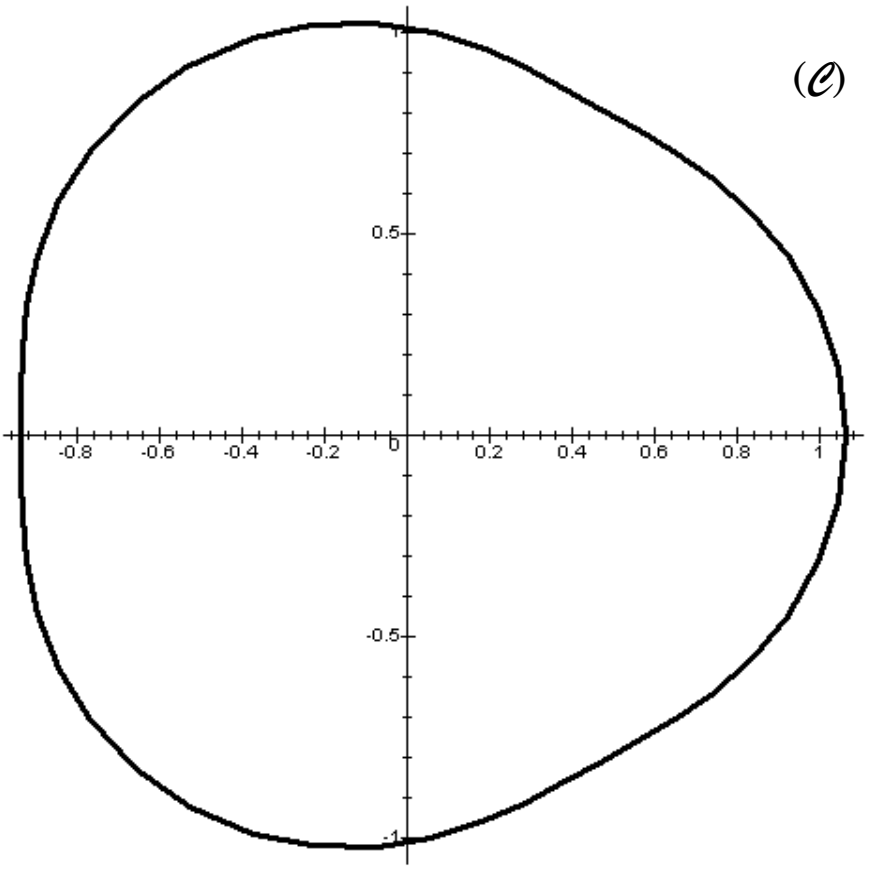
Michel LAFOND,

Mots clé : courbe, carré, carré inscrit, paramétrage, trigonométrie.

Résumé : Une curieuse propriété concernant un carré inscrit dans une courbe. Tout est facilement vérifiable en terminale.

- Considérons et admirons la courbe plane ayant pour équations paramétrées :

(C) $\begin{cases} x = \cos(t) + \dfrac{1}{16}\cos(4t) \\ y = \sin(t) + \dfrac{1}{16}\sin(4t) \end{cases}$ le paramètre t variant de 0 à 2π.



Qu'a-t-elle de si remarquable ?
Cela ne se voit pas, mais il se trouve qu'un carré peut tourner complètement à l'intérieur de (C) tout en ayant ses 4 sommets sur (C) et bien sûr, en gardant ses dimensions !

- ***Démontrons-le !***

Notons M (t) le point de (C) correspondant au paramètre t.
Posons

$A = M(t)$ $\quad B = M\left(t + \frac{\pi}{2}\right)$ $\quad C = M(t + \pi)$ $\quad$ et $\quad D = M\left(t + \frac{3\pi}{2}\right)$

et notons pour simplifier : $k = \frac{1}{16}$.

A a pour coordonnées $\quad x_A = \cos(t) + k\cos(4t)$
$\qquad\qquad\qquad\qquad\quad y_A = \sin(t) + k\sin(4t)$

B a pour coordonnées

$$x_B = \cos\left(t + \frac{\pi}{2}\right) + k\cos\left(4\left(t + \frac{\pi}{2}\right)\right) = -\sin(t) + k\cos(4t)$$

$$y_B = \sin\left(t + \frac{\pi}{2}\right) + k\sin\left(4\left(t + \frac{\pi}{2}\right)\right) = \cos(t) + k\sin(4t)$$

C a pour coordonnées

$$x_C = \cos(t + \pi) + k\cos(4(t + \pi)) = -\cos(t) + k\cos(4t)$$
$$y_C = \sin(t + \pi) + k\sin(4(t + \pi)) = -\sin(t) + k\sin(4t)$$

D a pour coordonnées

$$x_D = \cos\left(t + \frac{3\pi}{2}\right) + k\cos\left(4\left(t + \frac{3\pi}{2}\right)\right) = \sin(t) + k\cos(4t)$$

$$y_D = \sin\left(t + \frac{3\pi}{2}\right) + k\sin\left(4\left(t + \frac{3\pi}{2}\right)\right) = -\cos(t) + k\sin(4t)$$

Si on pose
$s = \sin(t)$ et $c = \cos(t)$ alors les vecteurs $\overrightarrow{AB}$, $\overrightarrow{BC}$, $\overrightarrow{CD}$, $\overrightarrow{DA}$, ont pour composantes :

$$\overrightarrow{AB}\begin{pmatrix} -s-c \\ -s+c \end{pmatrix} \qquad \overrightarrow{BC}\begin{pmatrix} s-c \\ -s-c \end{pmatrix} \qquad \overrightarrow{CD}\begin{pmatrix} s+c \\ s-c \end{pmatrix} \qquad \overrightarrow{DA}\begin{pmatrix} c-s \\ c+s \end{pmatrix}$$

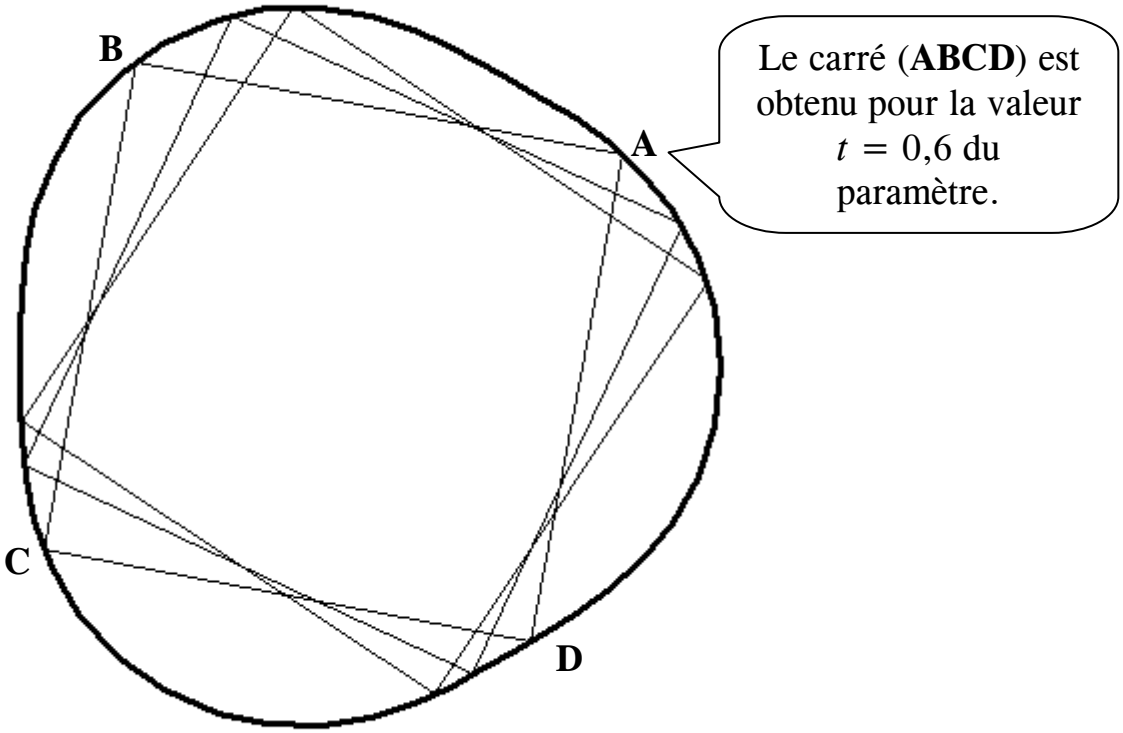
On a donc : $AB^2 = (-s-c)^2 + (-s+c)^2 = 2(s^2 + c^2) = 2$ d'où $AB = \sqrt{2}$.
On vérifie de même que $BC = CD = DA = \sqrt{2}$.

Ensuite le produit scalaire $\overrightarrow{AB}.\overrightarrow{BC}$ vaut

$$(-s-c)\times(s-c) + (-s+c)\times(-s-c) = 0.$$

On vérifie de même que les produits scalaires $\overrightarrow{BC}.\overrightarrow{CD}$; $\overrightarrow{CD}.\overrightarrow{DA}$; $\overrightarrow{DA}.\overrightarrow{AB}$ valent 0.

Le quadrilatère ABCD est donc un carré de côté $\sqrt{2}$ dont les 4 sommets sont sur (C).
Comme *t* est quelconque les points M (*t*) décrivent complètement la courbe. CQFD.



Guide pratique d'utilisation de GéoGébra pour le collège

Nicolas VISSAC, Collège les Amognes, Saint Benin d'Azy

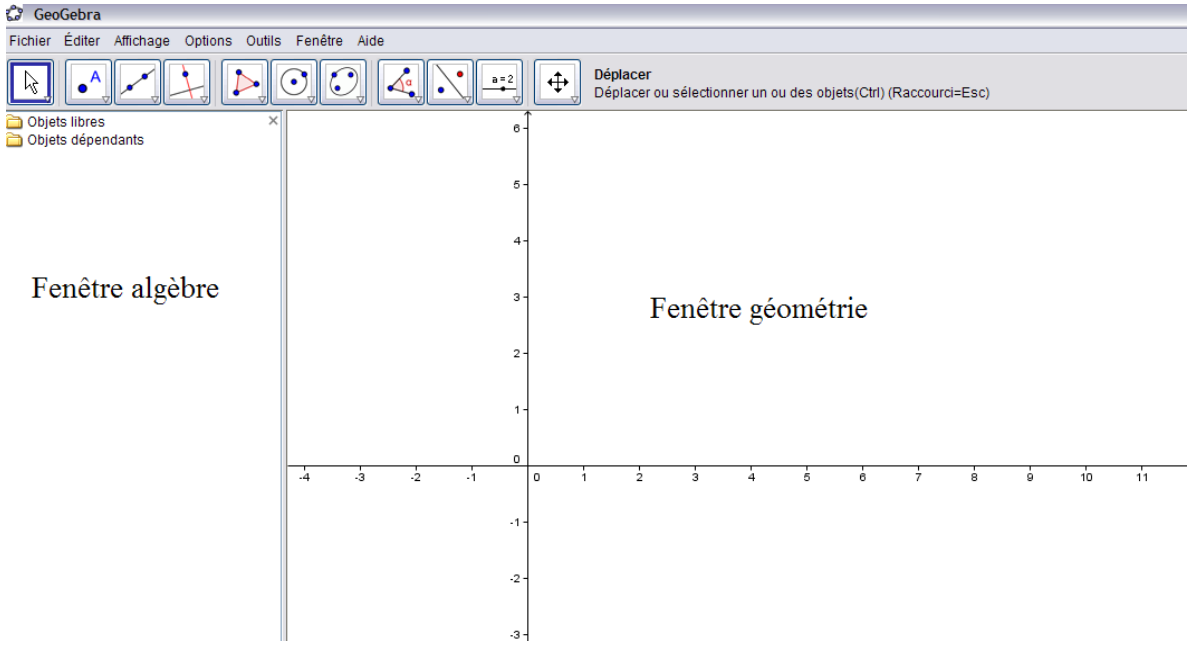
Mots clé : Géométrie dynamique, géogébra, collège.

Résumé : Le logiciel géogébra offre de nombreuses possibilités qui peuvent freiner sa prise en main par de jeunes élèves. Ce guide pratique présente les commandes qui sont utiles aux élèves des collèges.

1. Généralités

GéoGébra est un logiciel qui allie dessin géométrique et calcul.
Pour cela le logiciel est composé à son ouverture de deux parties :

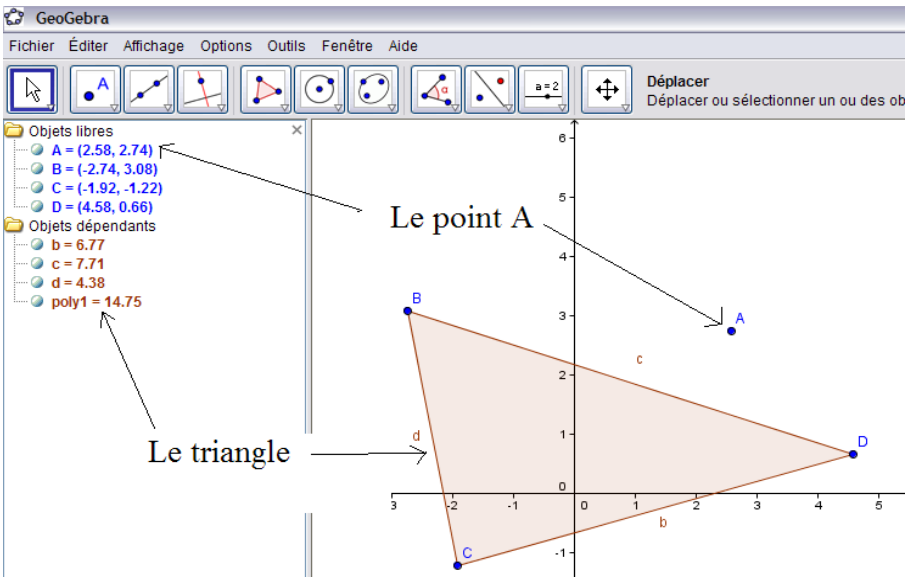
- Une fenêtre algèbre (sur la gauche) qui sert au calcul.
- Une fenêtre géométrie pour les tracés.

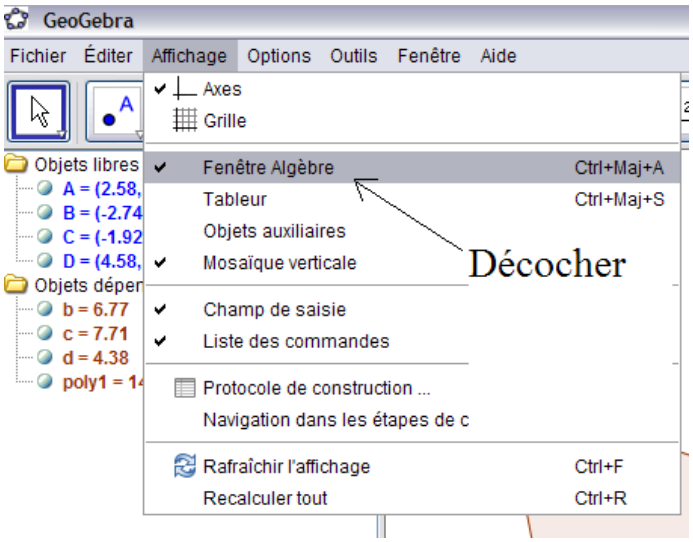


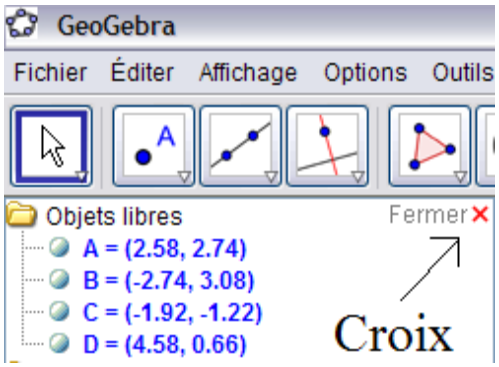
Une particularité de ce logiciel est que tout objet géométrique apparaît également dans la fenêtre algèbre comme sur l'exemple ci dessous :

En collège, **<u>on utilise essentiellement la fenêtre géométrie</u>**.
Il est possible de faire disparaître la fenêtre algèbre :

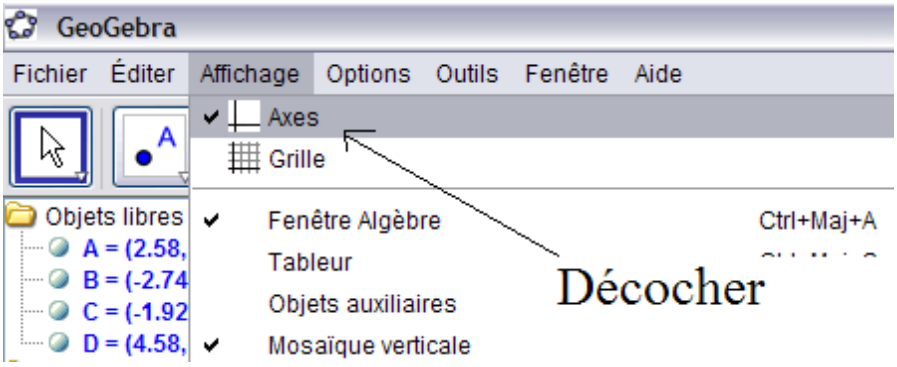
- soit en utilisant la croix en haut à droite de la fenêtre algèbre,
- soit en décochant "*fenêtre algèbre*" dans le menu affichage.





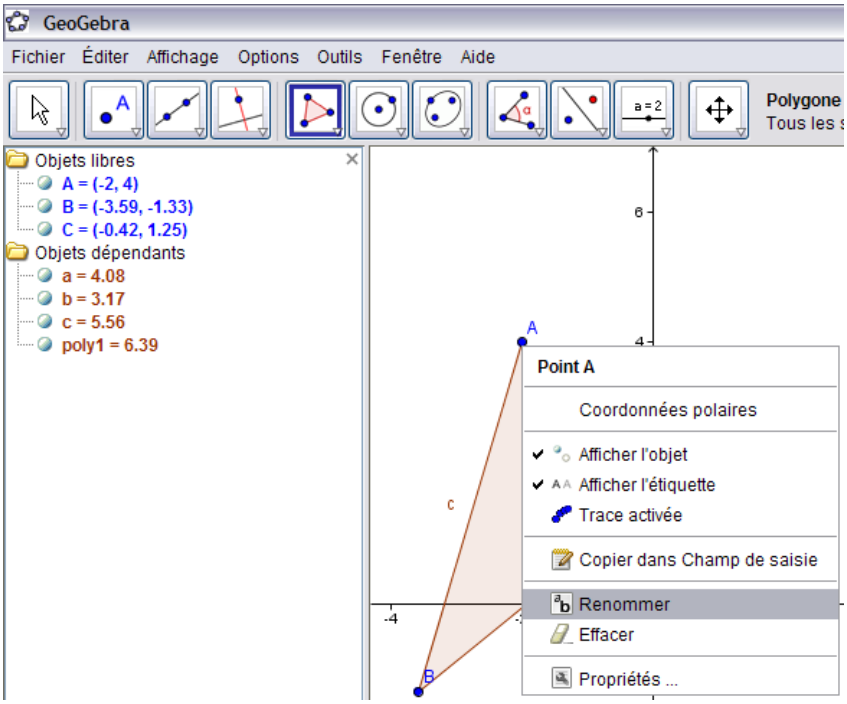


De même il est souvent inutile d'avoir des axes dans la fenêtre géométrique. Pour les faire disparaître, il suffit de décocher *'axes'* dans le menu affichage.



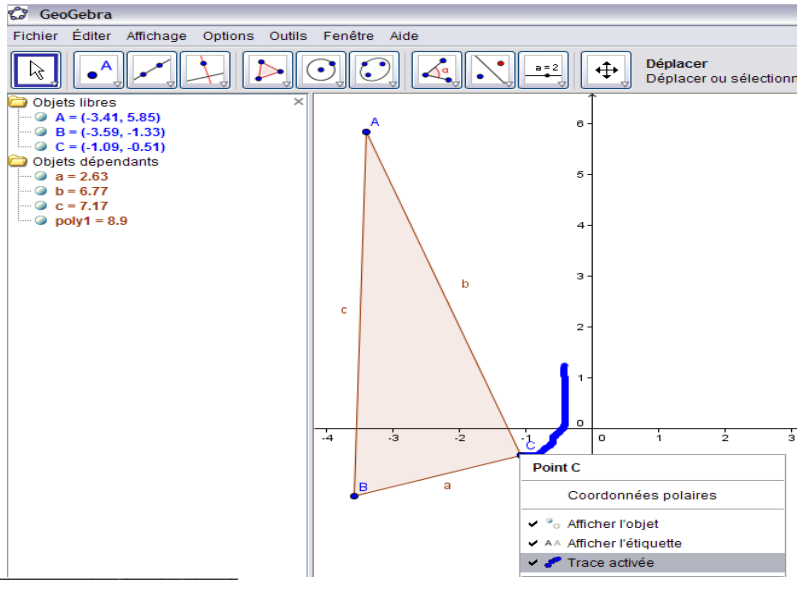
Chaque objet créé par le logiciel possède un nom que le logiciel appelle étiquette. Pour chaque objet, il est possible de faire apparaître ou disparaître l'objet ou son étiquette : pour cela, il faut faire un clic droit sur l'objet et cocher ou décocher *« afficher l'objet »* ou *« afficher l'étiquette »*.

Il est également possible de renommer un objet : faire un clic droit sur l'objet et sélectionner *« renommer »*.



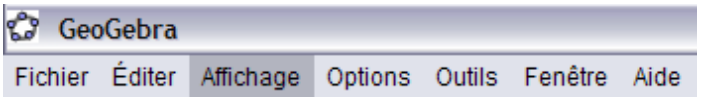
Il est également possible d'effacer un objet ou d'afficher ses propriétés en faisant un clic droit sur cet objet.

Enfin le logiciel possède également un mode Trace (clic droit et cocher « trace activée ») qui permet d'afficher la trace d'un objet lors du déplacement de la figure ou de sa déformation :

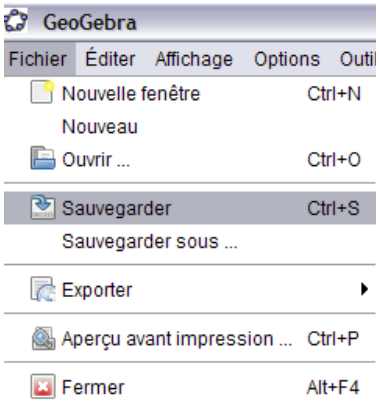


2. Barre des menus

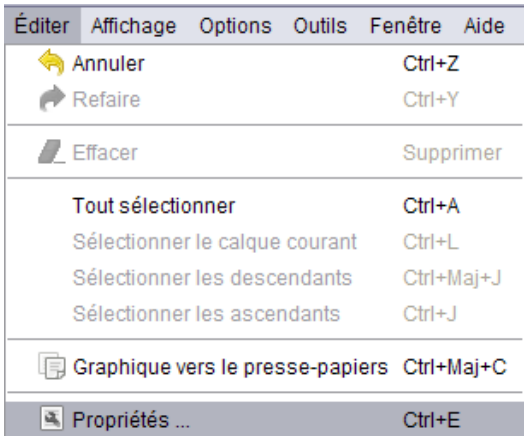
Tout en haut du logiciel apparaît la barre de menus :



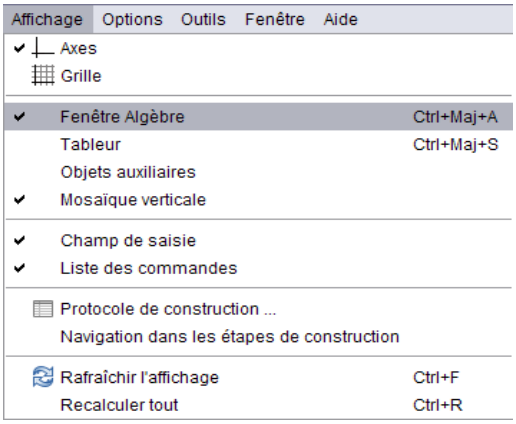
1. Fichier : Pour créer un nouveau fichier, enregistrer, imprimer …..



2. Éditer : Pour annuler la dernière action ou pour **voir les propriétés d'un objet** (ceci peut être très utile pour modifier l'apparence de l'objet : couleur, épaisseur des traits, etc.).

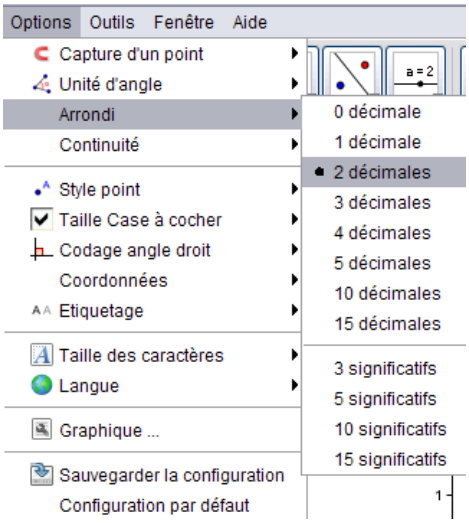


3. Affichage : Les fonctionnalités utiles de ce menu ont été vues précédemment, c'est-à-dire faire apparaître ou disparaître les axes ou la fenêtre algèbre.



Le protocole de construction permet de se « relire » et même de faire refaire la figure étape par étape.

4. Options : Ce menu sert à choisir l'unité de mesure des angles ou la précision d'arrondi des nombres.

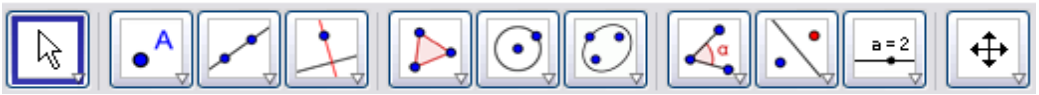


5. Les autres menus n'ont pas grand intérêt pour l'utilisation du logiciel en collège :

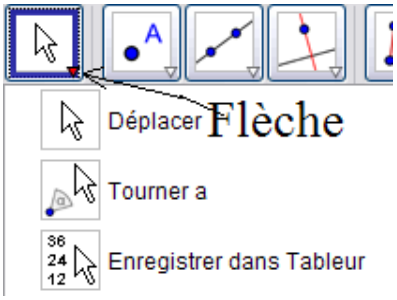
Outil permet de fabriquer un nouvel outil à partir des outils de base et ***fenêtre*** ouvre une nouvelle fenêtre sans fermer celle qui était utilisée.

3. Barre d'outils

Afin de pouvoir effectuer les diverses actions, le logiciel dispose d'une barre d'outils :



L'outil sélectionné est encadré en bleu. (Ci-contre, c'est la flèche qui est sélectionnée).
Chacun de ces onglets est en fait un menu déroulant si on clique sur la petite flèche en bas à droite de chaque onglet comme on peut le voir ci-contre :

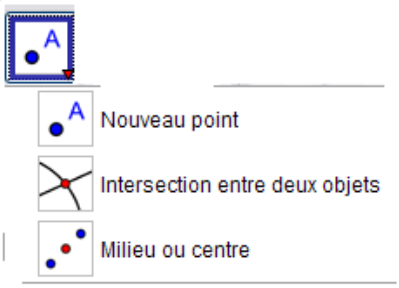


1. *Le menu déplacer*

Les fonctionnalités sont indiquées à côté de chaque icône.

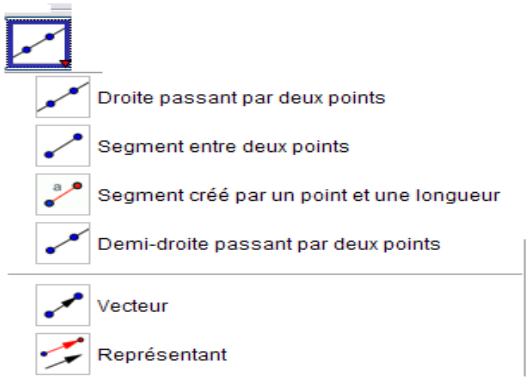
2. Le menu point

Ce menu sert à créer des points libres ou définis comme une intersection de deux objets géométriques ou comme un milieu de segment.



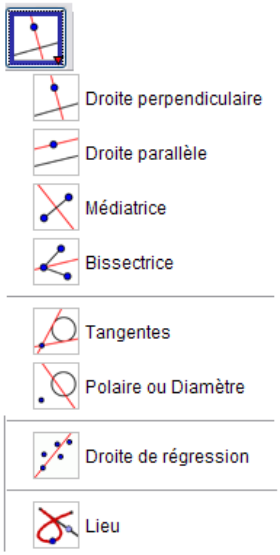
3. Le menu droite

Ce menu sert à construire des droites, des segments, des demi-droites.



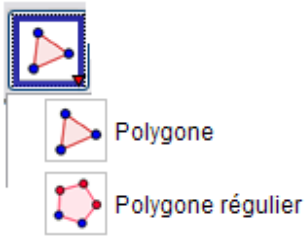
4. Le menu droites remarquables

Ce menu sert à construire des parallèles ou des perpendiculaires à une droite, passant par un point. Il sert également à tracer des médiatrices ou des bissectrices



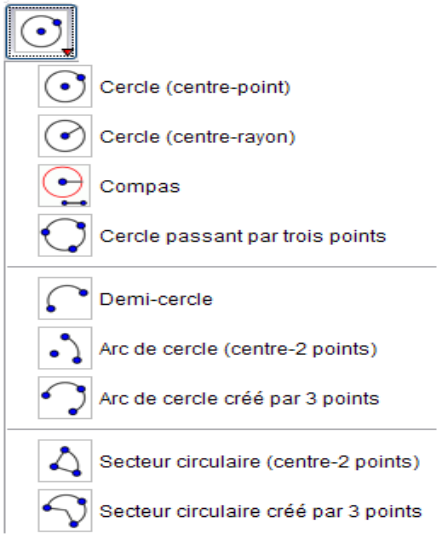
5. Le menu polygones

Ce menu sert à construire des polygones (triangles, quadrilatères, pentagones …...)



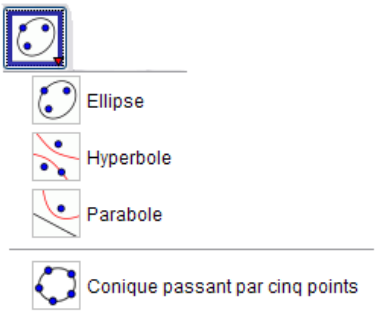
6. Le menu cercle

Ce menu sert à construire des cercles (défini par un centre et un point ou par un centre et un rayon) ou des arcs de cercles. L'outil compas est également utile pour reporter des longueurs



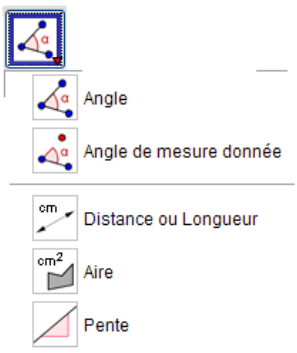
7. Le menu coniques

Ce menu est inutile au collège (sauf si on veut dessiner un cercle vu en perspective).



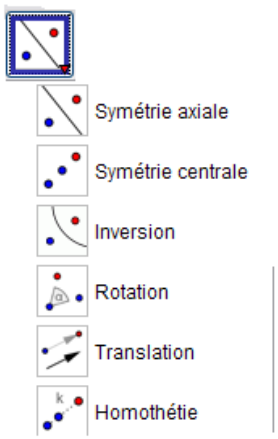
8. Le menu angles et mesures

Ce menu sert à marquer et mesurer un angle, à construire un angle donné, à mesurer des longueurs ou des aires.



9. Le menu des transformations

Ce menu sert à effectuer des symétries centrales ou axiales, les autres transformations n'étant pas au programme du collège.



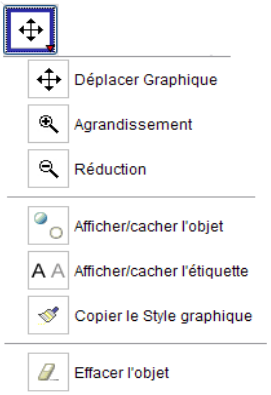
10. Le menu d'insertion

L'outil le plus utile de ce menu est l'outil ***relation entre deux objets*** qui permet de comparer deux objets. (Dire si deux droites sont parallèles par exemple).

Les ***curseurs*** permettent d'animer certaines figures.

11. Le menu d'affichage

Ce menu sert à modifier l'affichage. (le déplacer, l'agrandir ou le rétrécir...).



Géogébra est un logiciel très complet. Ce petit guide n'en aborde que les aspects géométriques de base et permet ainsi une prise en main rapide pour les élèves et aussi pour les professeurs.

Passé cette phase d'initiation, l'utilisateur curieux pourra se familiariser avec les autres possibilités de ce logiciel. C'est le souhait de l'auteur.

MISE EN PAGE :
Françoise BESSE

COMITE DE REDACTION ET DE LECTURE :
Catherine LABRUERE CHAZAL
Alain MASCRET
Marie-Noëlle RACINE

REDACTEUR EN CHEF :
Catherine LABRUERE CHAZAL

DIRECTEUR DE LA PUBLICATION :
Catherine LABRUERE CHAZAL, Directrice de l'IREM

DÉPÔT LÉGAL :
n° 194 – 2E semestre 2010

IMPRESSION :
Service Reprographie

FEUILLE DE VIGNE
Université de Bourgogne – UFR Sciences et Techniques
IREM
9 Avenue Alain Savary – BP 47870 – 21078 Dijon cedex
☎ 03 80 39 52 30 – Fax 03 80 39 52 39
@ : iremsecr@u-bourgogne.fr.
http://math.u-bourgogne.fr/IREM