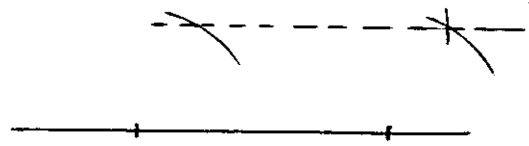
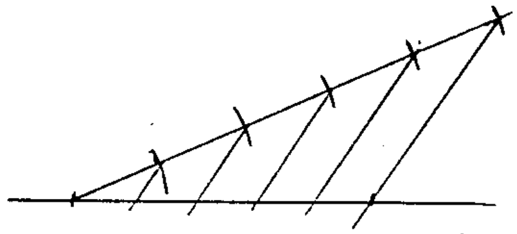
CHAPITRE XII - A PROPOS DE CONSTRUCTIONS GÉOMÉTRIQUES

§1 DE LA TRISECTION DE L'ANGLE À LA DUPLICATION DU CUBE

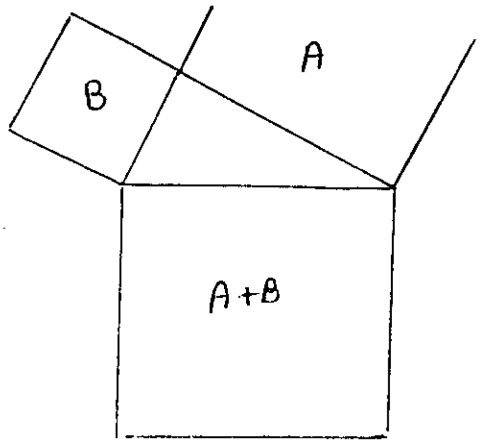
1.1 Les Grecs de l'époque classique ont très vite envisagé des problèmes de construction "à la règle et au compas". Comme on sait tracer avec ces outils la parallèle par un point à une droite en complétant un parallélogramme



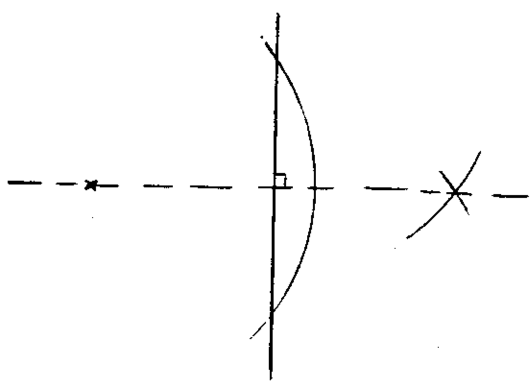
il est aisé de diviser (ou multiplier) une longueur par un entier :



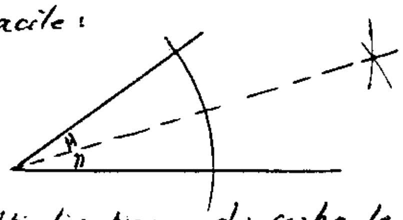
De même on sait, à partir de carrés d'aires A et B, tracer un carré d'aire NA (ou $\frac{A}{N}$) pour tout entier N, et même A+B, A−B, etc. Par exemple :



(puisqu'on sait obtenir la perpendiculaire par un point à une droite, à l'aide de la construction de la médiatrice de deux points :)

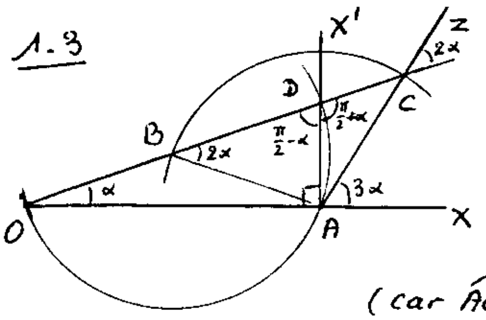


1.2 Il était naturel qu'on se posât la question de la division (par un entier) d'un angle (la multiplication est aisée !), ou de la multiplication ou division, toujours par un entier, d'un volume. La construction de la moitié, du quart, etc, d'un angle est facile :



mais peu de multiplications du cube le sont.
Sont donc devenues célèbres dès l'Antiquité les questions de la trisection de l'angle et de la duplication du cube. Échouant à les traiter "à la règle et au compas (et pour cause : cf. 5.3 et 5.4 plus loin), les Grecs introduisirent pour le faire de nouveaux outils de construction beaucoup plus controversés, parce que leur emploi systématique ébranlait le champ d'étude même de la géométrie. Donnons-en quelques exemples :

1.3

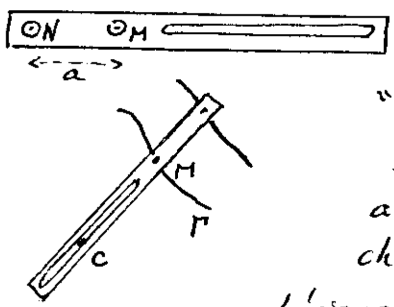


Une solution élégante à la "triplication" d'un angle $\widehat{XOY}$ est la suivante : soit B sur OY ; le cercle $\Gamma(B, BO)$ coupe OX en A, OY en D, et $\Gamma(A, AB)$ coupe OY en C. On a $\widehat{XAC} = 3\,\widehat{XOY}$

(car $\widehat{AOB} = \alpha$ implique $\widehat{BDA} = \frac{\pi}{2} - \alpha$ et $\widehat{BCA} = \widehat{CBA} = 2\alpha$, d'où $\widehat{ADC} = \frac{\pi}{2} + \alpha$, et $\widehat{DAC} = \pi - 2\alpha - (\frac{\pi}{2} + \alpha) = \frac{\pi}{2} - 3\alpha$)

De plus $DO = 2CA$. Si donc à l'inverse on part de l'angle $\widehat{XAZ} = 3\alpha$ pour reconstruire α, tout revient à construire une droite CY issue d'un point donné C et sur laquelle un angle droit donné $\widehat{X'AX}$ découpe une longueur donnée 2CA. (problème dit "de Pappus")

1.4 La solution proposée par Nicomède au problème de Pappus (et donc à la trisection de l'angle) est d'utiliser une règle à glissière idéale, où deux points sont marqués à la distance voulue a.



Si M décrit une courbe Γ, N décrit la "conchoïde" de Γ de centre C et de longueur a.
Dans notre cas, si M décrit AX', l'intersection avec AX de la conchoïde obtenue est le point O cherché.

L'équation polaire de pôle C de cette conchoïde est de la forme $\rho = \frac{d}{\cos\theta} + a$, et c'est donc un arc de la courbe du quatrième degré d'équation cartésienne

$$(x^2+y^2)(x-d)^2 - a^2x^2 = 0 .$$

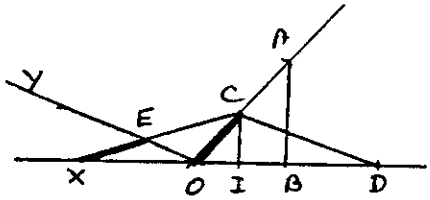
1.5 La même construction résout aussi le problème de la duplication du cube : il s'agit, connaissant a, de construire x tel que $x^3 = 2a^3$; on peut écrire plutôt $x^3 = \alpha^2\beta$, avec $\alpha = Na$, $\beta = \frac{2a}{N^2}$, et N entier assez grand pour que $\alpha > \beta$. On en tire

$$x^4 + \beta x^3 = \alpha^2\beta x + \alpha^2\beta^2$$

soit $x^2\left[\left(x+\frac{\beta}{2}\right)^2 - \frac{\beta^2}{4}\right] = \alpha^2\left[\left(\beta+\frac{x}{2}\right)^2 - \frac{x^2}{4}\right]$

ou encore $x^2\left[\left(x+\frac{\beta}{2}\right)^2 + \frac{\alpha^2-\beta^2}{4}\right] = \frac{\alpha^2}{4}(2\beta+x)^2$

et finalement : $\dfrac{\frac{\alpha}{2}}{x} = \dfrac{\sqrt{\left(x+\frac{\beta}{2}\right)^2 + \frac{\alpha^2-\beta^2}{4}}}{x+2\beta}$



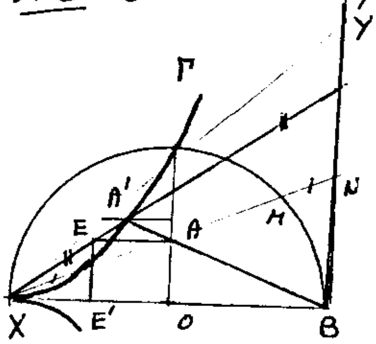
Sur un triangle rectangle de coté $OB = \beta$ et d'hypoténuse $OA = \alpha$, on construit les milieux C de OA et I de OB, puis D et X sur <OB>, tels que $OD = 2\beta$ et $OX = x$. On a :

$XD = x + 2\beta$, $XC = \sqrt{\left(x+\frac{\beta}{2}\right)^2 + \frac{\alpha^2-\beta^2}{4}}$, et la relation devient : $\dfrac{\frac{\alpha}{2}}{XO} = \dfrac{XC}{XD}$

La parallèle OY à CD par O coupe CX en E. La dernière proportion donne $XE = \frac{\alpha}{2} = OC$.

Il s'agit donc de construire une droite issue de C qui découpe sur un angle donné XOY une longueur donnée OC, et la solution est encore fournie par le tracé de la conchoïde de Nicomède.

1.6 Une solution plus élégante en principe est due à Dioclès : on "construit" la cissoïde Γ relative au cercle $\Gamma(O, OB)$, avec $OB = \beta$, et à sa tangente en B : la définition est analogue à celle de la conchoïde, sur toute droite issue de X et coupant Γ en M et BY en N, on porte la distance MN.



L'équation polaire de pole X de la cissoïde est $\rho = 2\beta\left(\frac{1}{\cos\theta} - \cos\theta\right)$, soit $(x^2+y^2)x = 2\beta y^2$.

Portons $OA = \alpha$ sur un axe perpendiculaire, puis $A' = AB \cap \Gamma$. La parallèle en A à OB coupe XA' en E qui se projette en E' sur OB.

L'équation de AB est $\alpha x + \beta y = 2\alpha\beta$, et l'angle polaire θ_0 de A' vaut $\operatorname{arc}\operatorname{Tg}\sqrt[3]{\frac{\alpha}{\beta}}$. D'où $XE' = EE' \operatorname{Cotg}\theta_0 = \alpha\sqrt[3]{\frac{\beta}{\alpha}} = \sqrt[3]{\alpha^2\beta} = x$.

1.7 Les Grecs ne connaissaient pas de tracé mécanique de la cissoïde de Dioclès, même à l'aide d'instruments bizarres (un tel tracé ne fut inventé que par Newton). Ils ne pouvaient donc construire la courbe que "par points". Cette résolution "graphique" (discrète) du problème était encore moins appréciée qu'une solution "mécanique" (continue). Les deux types de construction intéressèrent les plus grands géomètres (comme Newton, qui construisait mécaniquement les solutions d'équations des 3ème et 4ème degrés, ou encore Descartes, qui proposait des instruments farfelus pour construire une racine n-ième), mais ils furent toujours considérés comme "à la limite" du champ d'étude de la géométrie. Seuls les points constructibles et les problèmes résolubles "par la règle et le compas" à partir des données paraissaient incontestablement "géométriques."

1.8 Il ne s'agit pas de mode, mais d'une question de fond : de quoi sont faits les plans, les droites, les courbes, etc, de la géométrie ? Raisonne-t-elle vraiment sur des courbes "continues" au sens moderne (paramétrées par $\mathbb{R}$) ? Les Grecs auraient visiblement préféré s'en tenir aux points "rationnels" (disons à coordonnées rationnelles dans un repère lié aux données ; on disait "commensurables"). Mais la diagonale d'un carré, reportée sur un coté, introduit déjà une irrationnalité. Plus généralement, on ne pouvait guère éviter les points "euclidiens" (c'est-à-dire dont les coordonnées s'obtiennent à partir des données en résolvant une suite finie d'équations du second degré), surtout dans l'étude des coniques. Mais ceux-ci sont tous, comme on va le voir, constructibles à la règle et au compas, comme par exemple l'intersection d'une conique et d'une droite (ce qui n'est plus le cas pour des courbes du type 1.4 ou 1.6).

§2 DES CONSTRUCTIONS À LA RÈGLE ET AU COMPAS

2.1 C'est Descartes qui donne dans sa "Géométrie" des constructions à la règle et au compas des longueurs $a+b$, $a-b$, $a\times b$, $\frac{a}{b}$, et $\sqrt{a}$ à partir de longueurs données a et b, et énonce la réciproque (en gros que toute longueur constructible de cette façon est "euclidienne" au sens de 1.8), qui ne fut clairement énoncée et prouvée que par Kronecker au 19ème siècle.

2.2 Un remarquable théorème fut démontré par le danois Mohr en 1672, et retrouvé indépendamment par l'italien Mascheroni en 1797 :

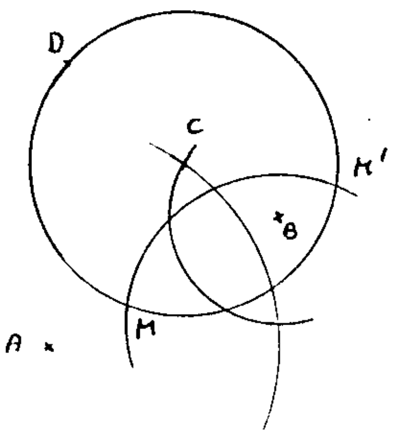
<u>Théorème : Toute construction possible à la règle et au compas l'est aussi au compas seul.</u>

Nous consacrons les numéros 2.3, 4, 5 à une preuve dûe à Lebesgue.
Il est clair que le problème revient à donner des constructions au compas seul de

- l'intersection d'une droite et d'un cercle,
- l'intersection de deux droites,

les droites étant définies par deux points, les cercles par leur centre et leur rayon. On notera $\langle AB \rangle$ la droite passant par A et B, $C(r)$ le cercle de centre C et de rayon r, $C(D)$ le cercle de centre C et de rayon CD.

2.3 Construction de $\langle AB \rangle \cap C(D)$ quand $C \notin \langle AB \rangle$

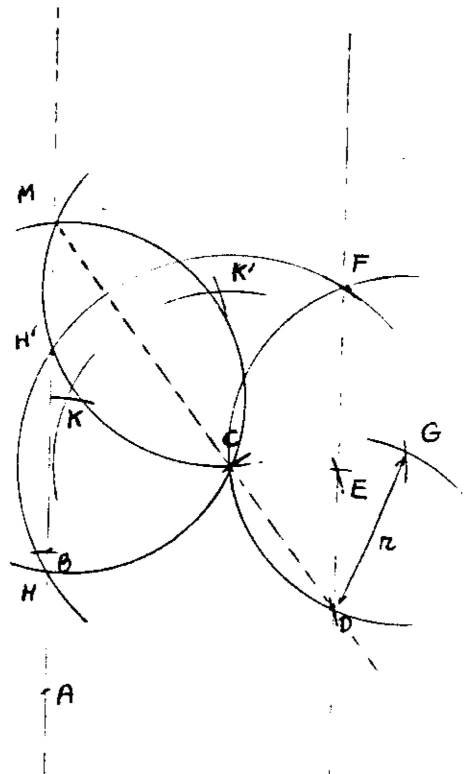


Si $\{C, C'\} = A(C) \cap B(C)$,
C' est le symétrique de C par rapport à $\langle AB \rangle$
D'où $\langle AB \rangle \cap C(D) = C(D) \cap C'(CD) = \{H, H'\}$. ■

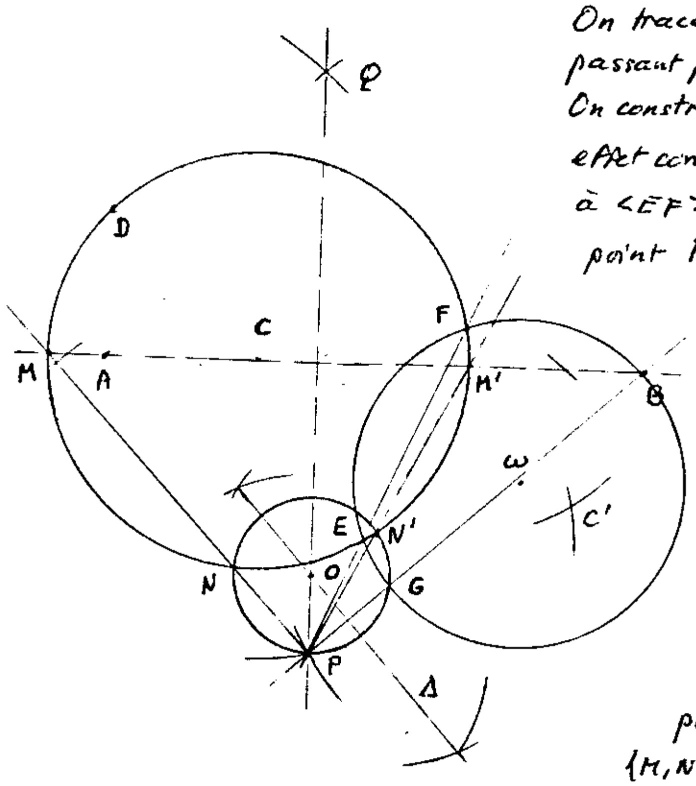
2.4 Construction de $\langle AB \rangle \cap \langle CD \rangle$

On construit E tel que $\overrightarrow{AB} = \overrightarrow{DE}$ (cf. 1.1), puis on choisit une longueur r arbitraire (mais pas trop petite ...) et on construit $G \in C(r) \cap D(r)$, puis F tel que $\langle DE \rangle \cap G(r) = \{D, F\}$ (par 2.3)
Toujours par 2.3, on obtient $\{H, H'\} = \langle AB \rangle \cap C(F)$, puis les centres K et K' de deux cercles de rayon r passant respectivement par $\{C, H\}$ et $\{C, H'\}$, et tels que $(\overrightarrow{KC}, \overrightarrow{KH})$ et $(\overrightarrow{K'C}, \overrightarrow{K'H'})$ soient égaux.
(Ils le sont au signe près automatiquement, comme angles au centre sous-tendant des cordes égales $CH = CF = CH'$ sur des cercles égaux).
On construit enfin $K(C) \cap K'(C) = \{C, M\}$
On a $\widehat{HMC} = \frac{1}{2}\widehat{HKC} = \frac{1}{2}\widehat{FGC} = \widehat{FDC}$.
Comme $\langle AB \rangle \parallel \langle DF \rangle$, on en déduit $\langle MC \rangle \parallel \langle CD \rangle$, c'est-à-dire $M \in \langle CD \rangle$, et finalement

$$M = \langle AB \rangle \cap \langle CD \rangle. \quad ■$$



2.5 Construction de $\langle AB\rangle \cap C(D)$ quand $C \in \langle AB\rangle$



On trace un cercle $\omega(B)$ de centre arbitraire passant par B, mais sécant à $C(D)$ en E et F. On construit un autre point P de $\langle EF\rangle$: on peut en effet construire le symétrique C' de C par rapport à $\langle EF\rangle$, puisque $E(C) \cap F(C) = \{C, C'\}$, puis un point $P = C(r) \cap C'(r)$ pour r assez grand.

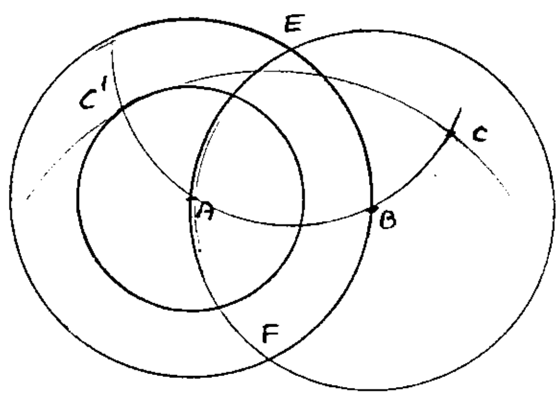
Par 2.3, on construit $G = \langle PB\rangle \cap \omega(B)$, puis par 2.4, $O = \langle PQ\rangle \cap \Delta$, où Q est le symétrique de P par rapport à $\langle AB\rangle$, et Δ est la médiatrice de $\{P, G\}$.

L'inversion de pôle P qui conserve $\omega(B)$ conserve aussi $C(D)$, et échange $\langle AB\rangle$ et $O(P)$.

On construit $\{N, N'\} = O(P) \cap C(D)$, puis $\{M, M'\}$ tels que $\{M, N\} = \langle PN\rangle \cap C(D)$ et $\{M', N'\} = \langle PN'\rangle \cap C(D)$.

Il est clair que $\{M, M'\} = \langle AB\rangle \cap C(D)$. ■

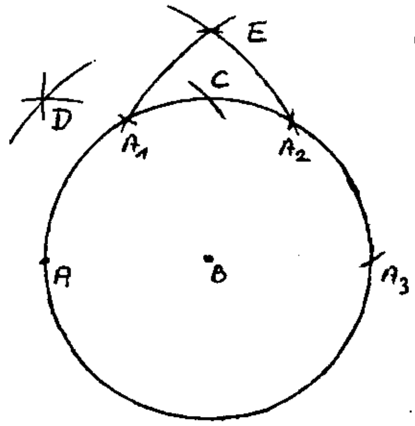
2.6 Il faut noter qu'on a utilisé le compas pour <u>tracer</u> des cercles, mais aussi pour <u>reporter</u> des longueurs. A vrai dire le second rôle se réduit au premier, car pour tracer $A(BC)$, il suffit de tracer $A(B)$ et $B(A)$ qui se coupent en E et F, puis le symétrique C' de C par rapport à $\langle EF\rangle$: $\{C, C'\} = E(C) \cap F(C)$, enfin $A(C') = A(BC)$.



On peut donc parler de l'usage du compas sans préciser.

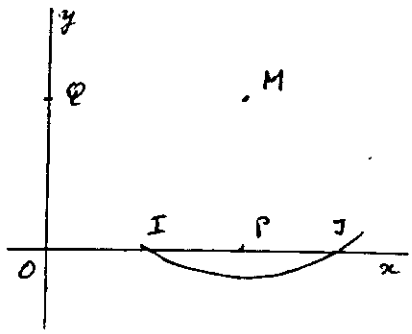
On va donner les six constructions de base de la géométrie de la règle et du compas, qui impliquent l'existence des autres (visiblement, pour un esprit algébrique !), et dans l'esprit du théorème de Mohr et Mascheroni, on donnera des constructions au compas seul.

2.7 Construire sur A et B un carré ABCD (= fixer le repère orthonormé)



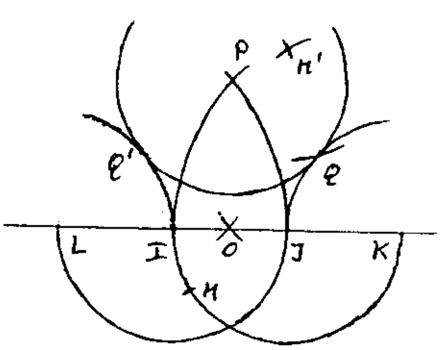
On trace B(A), de rayon $r = AB$, puis les sommets successifs de l'hexagone régulier : $A_1 \in A(r) \cap B(r)$, $A_2 \in A_1(r) \cap B(r)$, $A_3 = A_2(r) \cap B(r)$. On choisit E dans $A(A_2) \cap A_3(A_1)$, cercles de rayon $r\sqrt{3}$. Il vient $BE = a\sqrt{2}$, d'où $C \in A(BE) \cap B(A)$, puis D par la construction élémentaire du parallélogramme. ∎

2.8 Passer d'un point à ses projections sur les axes, et réciproquement
(c'est ramener les questions algébriques qui se posent dans le plan aux mêmes sur la droite)

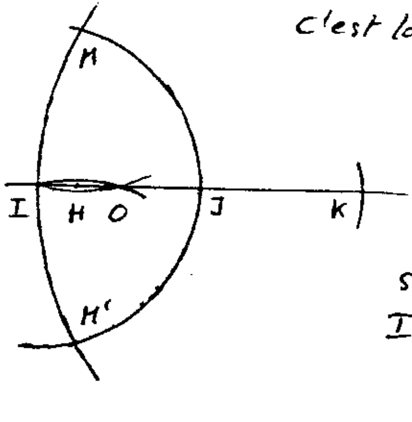


Si P et Q sont connus, le point M dont ce sont les projections est dans $P(OQ) \cap Q(OP)$ (parallélogramme). Réciproquement si M est connu, un cercle de centre M et de rayon suffisant coupe l'axe Ox en I et J, dont le point P cherché est le milieu.
(On construit $M(r) \cap \langle Ox \rangle$ par 2.3)
Reste à résoudre le problème auxiliaire :

Construction du milieu d'un segment IJ

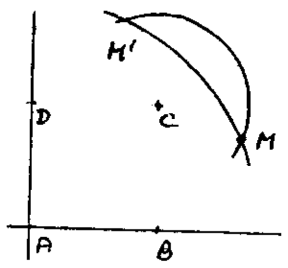


On construit d'abord les points K et L de $\langle IJ \rangle$ tels que $LI = IJ = JK = r$ (par exemple comme sommets d'un hexagone régulier inscrit dans J(I) ou dans I(J))
On obtient ensuite $P \in K(I) \cap L(J)$, puis $Q = P(r) \cap K(r)$ et $Q' = P(r) \cap L(r)$
(mais ces derniers cercles sont tangents, et si l'on veut éviter une construction aussi peu précise, on prend M arbitraire sur J(I), puis M' tel que $KIM = KPM'$: $M' \in P(IM) \cap K(M)$. On a alors $Q = M'(r) \cap P(r) \cap Q(r)$)
Le milieu O cherché est alors le symétrique de P par rapport à $\langle QQ' \rangle$: $O \in Q(r) \cap Q'(r)$. ∎



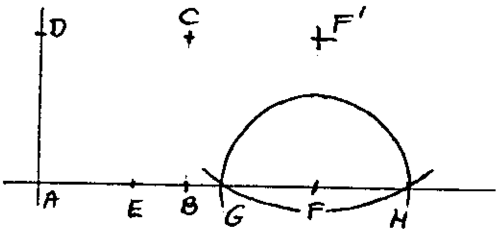
C'est la solution de Mohr. Celle de Mascheroni est plus rapide :
On construit K sur $\langle IJ \rangle$ et tel que $JK = IJ = r$, comme ci-dessus, puis $\{M, M'\} = K(2r) \cap I(r)$. On obtient le milieu O de IJ en remarquant que $\{O, I\} = M(I) \cap M'(I)$.
En effet $IM = r$ et $KM = 2r$ impliquent que M et M' se projettent en H sur $\langle IJ \rangle$ tel que $IH \cdot 4r = IM^2 = r^2$, d'où $IO = 2\,IH = \frac{r}{2}$. ∎
(exercice !)

2.9 Passer du point de coordonnées (x,y) au point (y,x) (= s'assurer que les questions d'algèbre sont les mêmes "dans les deux directions")



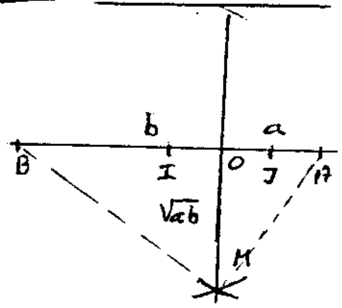
Il s'agit de construire le symétrique M' d'un point M par rapport à la diagonale AC du carré de base $ABCD$ supposé déjà construit, par exemple par 2.7. On a $\{M,M'\} = A(M) \cap C(M)$. ■

2.10 Construire la longueur $a \pm b$ (a,b donnés)



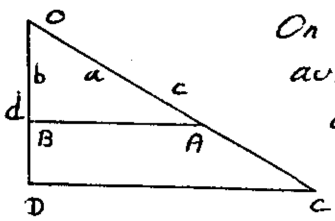
De nouveau, on peut supposer le carré-unité $ABCD$ connu. Si $AE = a$, et $AF = b$, on construit $F' \in D(AF) \cap F(AD)$, puis $\{G,H\} = F(AE) \cap F'(DE)$
Les triangles $FF'G$ et $FF'H$ sont égaux à ADE, d'où $AH = a+b$ et $AG = b-a$. ■

2.11 Construire $\sqrt{ab}$:



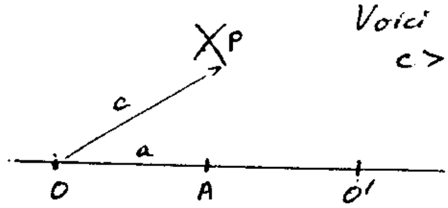
Si A, B sont, sur l'un des axes, d'origine O, les points d'abscisses a et $-b$, on construit (cf. 2.8) le milieu I de AB puis (cf. 2.9) son symétrique par rapport à l'autre axe.
Si $M \in I(IA) \cap J(IA)$, le triangle AMB est rectangle en M, d'où $OM = \sqrt{ab}$. ■

2.12 Construire $d = \frac{bc}{a}$ (a,b,c donnés)



On va construire une "figure de Thalès" adaptée aux données : ayant C et A tels que $OA = a$, on construit le milieu de OA (cf. 2.8), puis le cercle de diamètre OA, et son intersection B avec $O(b)$. Ayant le triangle rectangle OBA, si l'on sait reporter la longueur $c = OC$ sur la droite OA, projetant C sur OB en D (cf. 2.8), on aura $OD = d$.
Reste à résoudre le problème auxiliaire (mais essentiel !) :

Porter une longueur donnée $OC = c$ sur un axe OA (avec $OA = a$ connu), autrement dit : construire l'intersection d'un cercle et d'un de ses diamètres (cf. 2.5)

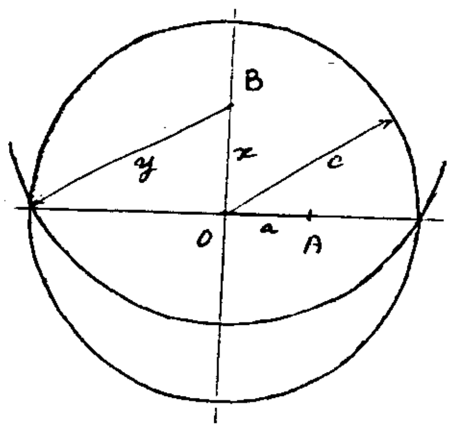


Voici l'élégante solution de Mohr : on peut supposer $c > a$ (sinon $Nc > a$ ...) On obtient d'abord $\sqrt{c^2-a^2}$ en construisant le point $P \in O(c) \cap O'(c)$, où O' est le symétrique de O par rapport à A

(obtenu comme en 2.7 par un hexagone régulier) : AP est orthogonal à OA, d'où $AP = \sqrt{c^2 - a^2}$.

On pourra construire de même $c\sqrt{2} = \sqrt{(c\sqrt{3})^2 - c^2}$, puisque $c\sqrt{3}$ s'obtient à l'aide d'un hexagone comme en 2.7, puis

$$\sqrt{a^2+c^2} = \sqrt{(c\sqrt{2})^2 - (\sqrt{c^2-a^2})^2}.$$



Soit alors B un point arbitraire de la perpendiculaire en O à OA (que l'on peut construire comme médiatrice de AA', où le symétrique A' de A par rapport à O se construit comme en 2.7 ...).

Si $OB = x$, on sait donc construire la longueur $y = \sqrt{c^2 + x^2}$, et les points $\{M, M'\} = B(y) \cap O(c)$ sont les points d'intersection cherchés. ∎

§3 DE LA RÈGLE SEULE

<u>3.1</u> La première remarque à faire est qu'avec la règle seule on ne peut construire que des intersections de droites, autrement dit résoudre des équations linéaires (du <u>premier</u> degré). Il est clair qu'on n'obtiendra donc que des points <u>rationnels</u> à partir des données (c'est-à-dire dont les coordonnées sont rationnelles dans un système lié aux données). Mais on est loin de les obtenir tous : par exemple le <u>milieu</u> d'un segment se construit aisément à la règle et au compas comme sur la

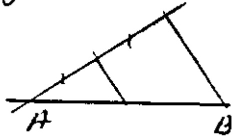
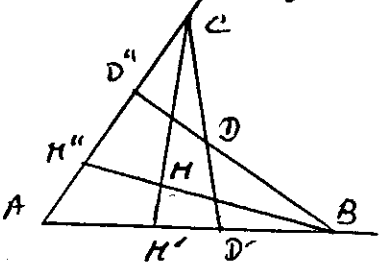


figure. Le compas sert ici à reporter deux fois une longueur quelconque, puis à tracer une parallèle : on pourrait le remplacer par d'autres instruments, règle avec deux points gravés, règle à deux bords parallèles ..., mais certainement pas par la règle seule. En effet, si une construction était possible à la règle seule, elle serait conservée dans toute transformation qui respecte l'alignement, par exemple par une perspective. Or celle-ci ne conserve pas le milieu ! Les constructions possibles à la règle seule sont du domaine de la géométrie <u>projective</u>.

De plus, la notion de problème "du premier degré" dépend du système d'axes choisi : le point $(1,1)$ a pour coordonnées $(\sqrt{2}, 0)$ dans le système des bissectrices ...

3.2 Pour la clarté, on supposera donc que ce qui est donné est en fait un repère projectif du plan, c'est-à-dire quatre points A, B, C, D, trois à trois non alignés. Les "coordonnées trilinéaires" d'un point M



du plan sont les birapports

$x = (CM, CD, CA, CB) = (M', D', A, B)$, et

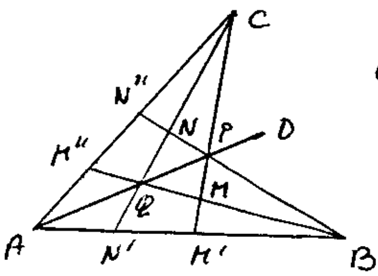
$y = (BM, BD, BA, BC) = (M'', D'', A, C)$

par exemple. On a alors le théorème:

Si $x_1, \ldots, x_{2n}$ sont les coordonnées de tous les points donnés, les points constructibles à la règle seule à partir de ceux-ci sont ceux dont les coordonnées sont dans $\mathbb{Q}(x_1, \ldots, x_{2n})$.

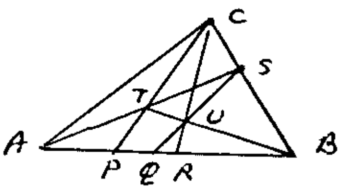
Preuve: Qu'elles y soient résulte de 3.1. Pour démontrer la réciproque, il suffit de produire des constructions à la règle des opérations fondamentales, analogues aux questions qu'on s'est déjà posées au paragraphe précédent, en 2.7, 2.8, 2.9, 2.10, et 2.12 (2.11 n'est évidemment plus en cause); mais l'équivalent de 2.7 (tracer le repère de base) est supposé déjà fait, et celui de 2.8 (passer d'un point M à ses projections M' et M'' sur les axes, et réciproquement) est trivial. Les trois autres opérations font l'objet de 3.3, 3.4, 3.5. ∎

3.3 Construire (y, x) à partir de (x, y)



On le fait comme l'indique la figure:
(si le point est sur un axe, c'est encore plus simple!)
de $M\binom{x}{y}$ on obtient $P\binom{x}{x}$ et $Q\binom{y}{y}$, d'où $N\binom{y}{x}$. Le point crucial est que $\langle AD \rangle$ est la "diagonale", c'est-à-dire l'ensemble des points de coordonnées égales. ∎

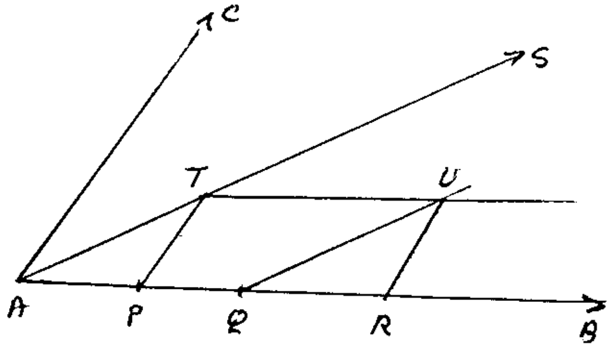
3.4 Construire $a \pm b$



Soient $P = (a, 0)$ et $Q = (b, 0)$. On prend S arbitraire sur BC, d'où $T = AS \cap CP$, $U = BT \cap SQ$, et enfin $R = CU \cap AB$. On a bien

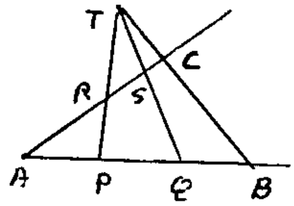
$$R = (a+b, 0),$$

car pour la structure affine où B et C sont à l'infini, on a construit la figure:



où $AQUT$ et $PRUT$ sont des parallélogrammes.
On construirait de la même manière $(b-a, 0)$ ou $(a-b, 0)$. ∎

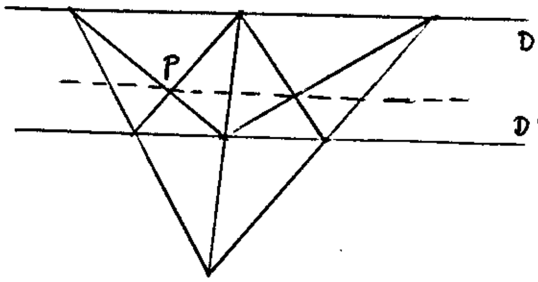
<u>3.5</u> <u>Construire $d = \frac{bc}{a}$</u> : Il s'agit de même d'une "figure de Thalès" projective : si $P = (a,0)$ $Q = (b,0)$, $R = (0,c)$ (cf. 3.3 pour changer d'axe éventuellement), on construit $T = PR \cap BC$, puis $S = TQ \cap AB$, et on a bien $S = (0,d)$, en considérant la structure affine où B et C sont à l'infini ■



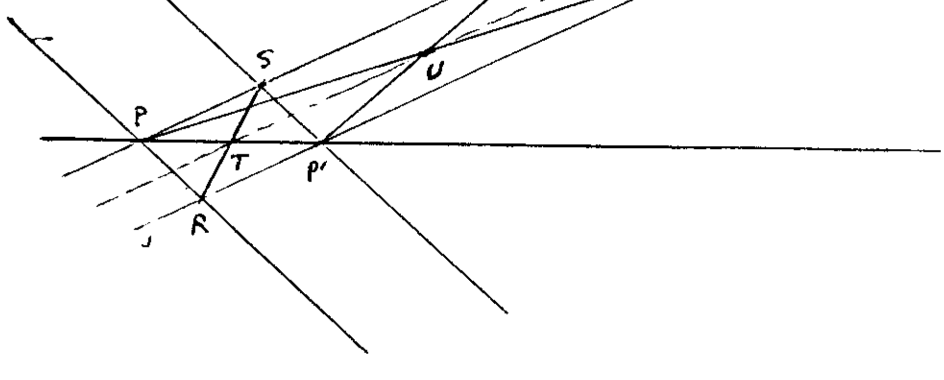
<u>3.6</u> Notons toutefois que ces constructions "projectives" ne sont utilisables dans l'espace affine que si l'on sait résoudre les "problèmes à l'infini" (même à l'infini "approché"!) qu'elles peuvent poser, c'est-à-dire répondre, à l'aide de la règle seule aux deux questions posées (et résolues) en 3.7 et 3.8.

<u>3.7</u> <u>Construire à la règle la parallèle issue d'un point à deux droites parallèles données :</u>

La construction est claire sur la figure. ■



<u>3.8</u> <u>La droite de l'infini étant définie par deux couples de droites parallèles, construire par un point donné la parallèle à une droite donnée :</u>
Au vu de 3.7, il suffit de savoir construire <u>une</u> parallèle à la droite D donnée. On prend P, P' sur D puis on trace $P + \vec{\partial}$, $P' + \vec{\partial}$, $P + \vec{\partial}'$, $P' + \vec{\partial}'$, d'où R et S, puis $T = RS \cap D$, et par 3.7 $T + \vec{\partial}$, sur laquelle on choisit U arbitraire (mais pas sur D !). On obtient alors Q et Q' comme l'indique la figure, et $\langle QQ' \rangle$ est parallèle à D.



■

3.9 L'usage d'une règle est évidemment équivalent à faire un "pliage de première espèce", c'est-à-dire plier le plan de la figure sur une arête passant par deux points donnés. Ceci ne doit pas être confondu avec un

"pliage de deuxième espèce" qui consiste à plier le plan de la figure sur une arête de façon à faire coïncider les deux cotés d'un angle. Cette deuxième espèce de pliage équivaut au tracé de la bissectrice d'un angle quelconque et offre des possibilités nouvelles (qui ne dépassent pourtant pas celles du compas, qui permet lui aussi la construction des bissectrices).
Comme on vient de voir que les pliages de première espèce, (c'est : la règle) permettent d'obtenir des parallèles, on peut se contenter de discuter de la portée des pliages de sommet donné S. On raisonnera en termes de pentes de droites passant par S, ce qui n'est guère dramatique, au vu de 3.5.

Comme $Tg\left(\frac{\alpha+\beta}{2}\right) = -Cotg(\alpha+\beta) \pm \sqrt{1+Cotg^2(\alpha+\beta)}$,

et que $Cotg\,(\alpha+\beta) = \dfrac{1-Tg\alpha\,Tg\beta}{Tg\alpha+Tg\beta}$ est fonction rationnelle de $Tg\alpha$ et $Tg\beta$, il est clair (en tenant compte de 3.5 et 3.4) que si λ et μ sont des pentes de droites données, la bissectrice obtenue par pliage permet de construire $\sqrt{\lambda^2+\mu^2}$. Le domaine de constructibilité est donc au moins le plus petit corps contenant les données, leurs fonctions rationnelles, et stable par $(\lambda,\mu) \longmapsto \sqrt{\lambda^2+\mu^2}$.
Comme $\sqrt{\lambda^2+(\sqrt{\mu^2+\nu^2})^2} = \sqrt{\lambda^2+\mu^2+\nu^2}$, ce corps est stable par $(\lambda_1,\dots,\lambda_p) \longmapsto \sqrt{\lambda_1^2+\dots+\lambda_p^2}$.

Ce corps est cependant strictement plus petit que celui du compas (nombres "euclidiens"), comme le prouve la remarque qui suit, due à Lebesgue adaptant une idée de Hilbert : la construction à la règle et au compas de l'intersection d'un cercle et d'une droite par exemple, ne donne évidemment rien lorsque cette intersection est vide ; or des pliages sont toujours possibles, et s'il existait une construction par pliage, elle marcherait ! Donc il n'y en a pas !

(§4) DE LA QUADRATURE DU CERCLE

4.1 L'un des plus célèbres problèmes posés par les Grecs est celui de la "quadrature du cercle" : construction d'un carré de même périmètre que la circonférence d'un cercle donné (ou de même aire qu'un cercle donné). A vrai dire le problème est sans doute plus ancien : des papyrus égyptiens semblent indiquer des solutions approchées...

Comme l'aire d'un cercle de rayon R est πR^2, et sa circonférence $2\pi R$, il est clair que la question est d'abord de nature algébrique : π est-il un nombre rationnel (si oui, une construction serait possible à la règle), ou un nombre "quadratique" ($a \pm \sqrt{b}$, $a, b \in \mathbb{Q}$), ou plus généralement "euclidien" (cf. 1.8 ; auquel cas une construction à la règle et au compas serait possible — c'est d'ailleurs celle-ci que les Grecs cherchaient), ou seulement "algébrique" (id est : racine d'une équation algébrique, $P(\pi)=0$, où P est un polynôme à coefficients entiers), ou même "transcendant" (id est : non algébrique) ?

En 1761, Lambert montra que π est irrationnel (e aussi d'ailleurs, et même e^n pour tout n), et il était déjà convaincu de leur transcendance. Cependant celle-ci ne fut démontrée que par Hermite en 1872 pour e, et par Lindemann en 1882 pour π.

Comme π et e ont des définitions géométriques naturelles (le rôle de π est évidemment fondamental ; celui de e est plus discret, mais la spirale logarithmique, par exemple, est une courbe plane dont la définition géométrique est simple : c'est la courbe dont les tangentes font avec le rayon issu d'un point fixe un angle constant), ces résultats s'intègrent logiquement dans un cours de "géométrie".

Nous allons en donner des preuves dues, pour e à Hermite simplifié par Hilbert, et pour π à Lindemann simplifié par Lebesgue.

4.2 Rappelons d'abord que e est irrationnel puisque

$$e = 1 + \frac{1}{1!} + \cdots + \frac{1}{n!} + \frac{e^{\theta_n}}{(n+1)!} \quad \text{avec } 0 < \theta_n < 1$$

d'où $n!e = \dfrac{e^{\theta_n}}{n+1}$ modulo $\mathbb{N}$, où le second membre, qui tend vers zéro quand n tend vers ∞, sans jamais être nul, ne peut donc être entier pour aucune valeur de n. ■

Mais il est presque aussi facile de montrer que e n'est pas quadratique : si $A, B, C \in \mathbb{Z}$, on a modulo $\mathbb{Z}$ et pour tout entier n :

$$\frac{n!}{e}(Ae^2+Be+C)=n!(Ae+B+Ce^{-1})\equiv r_n \quad ,$$

avec $r_n = \dfrac{Ae^{\theta_n}+(-1)^{n+1}Ce^{-\theta_n}}{n+1}$, et $0<\theta_n<1$

Pour n impair si $AC<0$, pair si $AC>0$, et assez grand dans tous les cas, il est clair que $0<r_n<1$. En particulier $Ae^2+Be+C\neq 0$. ∎

Les deux numéros suivants sont consacrés à la transcendance de e, et le dernier à celle de π. Quoique assez techniques, ces preuves sont fondées sur la même idée que celles ci-dessus.

4.3 Pour tout entier p, on peut trouver des entiers n et N arbitrairement grands tels que $(1+\frac{1}{p})n<N<(1+\frac{1}{p-\frac{1}{2}})n$. Posant $m=N-n$, il vient en particulier $0<N-pm<m$. Considérons le polynôme de degré N

$$F(z)=\frac{1}{(N-pm)!}\,z^{N-pm}(z-1)^m(z-2)^m\cdots(z-p)^m ,$$

et $\Phi(x)=F^{(N)}(0)+xF^{(N-1)}(0)+\cdots+x^{N-pm}F^{(N-pm)}(0)$.

Il est clair que Φ est à coefficients entiers. Posons

$$\Phi(x)e^{zx}=S_n(x,z)+S_{n,N}(x,z)+r_N(x,z) ,$$

avec $S_n(x,z)=\sum_{k=0}^{n}A_k(z)x^k$, et $S_{n,N}(x,z)=\sum_{k=n+1}^{N}A_k(z)x^k$.

De $\left(\frac{\partial}{\partial z}\right)^k\left[\Phi(x)e^{zx}\right]=e^{zx}\left[z^k\Phi(x)+C_k^1 z^{k-1}\Phi'(x)+\cdots+C_k^k\Phi^{(k)}(x)\right]$

on déduit $A_k(z)=\dfrac{z^k\Phi(0)}{k!}+\dfrac{z^{k-1}\Phi'(0)}{(k-1)!\,1!}+\cdots+\dfrac{\Phi^{(k)}(0)}{k!}$, d'où $A_{k-1}=\frac{d}{dz}A_k$.

Comme $\Phi(0)=F^{(N)}(0),\ldots,\Phi^{(N)}(0)=F(0)$, il vient, par l'identité de Taylor, $A_N(z)=F(z)$, et par suite $A_k(z)=\left(\frac{d}{dz}\right)^{N-k}F(z)$.

On a donc $A_k(z)=0$ pour $k=n+1,\ldots,N$ et $z=1,2,\ldots,p$, d'où

$S_{n,N}(x,z)=0$ pour $z=1,2,\ldots,p$, et pour tout x.

Pour $k=0,\ldots,n$, les seuls termes de la dérivée d'ordre $N-k$ de F qui ne s'annulent pas au point $z=j$ $(1\le j\le p)$ s'obtiennent en dérivant au moins m fois le facteur $(z-j)^m$, de sorte que, puisque $m!>(N-pm)!$, $A_k(j)$ est un entier ; plus particulièrement $F^{(N-pm)}(0)=(-1)^p(p!)^m$, tandis que les autres dérivées non nulles $F^{(k)}(0)$ sont des entiers multiples de m.

Posons maintenant $\Psi(x,z)=S_n+S_{n,N}=\sum_{0}^{N}A_k(z)x^k$

$$=F^{(N)}(z)+xF^{(N-1)}(z)+\cdots+x^N F(z).$$

On a $\Psi(x,0)=\Phi(x)$, et $\Psi(x,0)e^{zx}-\Psi(x,z)=r_n(x,z)$.

4.4 Soit $P(u) = a_p u^p + a_{p-1} u^{p-1} + \dots + a_0$ un polynôme à coefficients entiers. (On peut supposer $a_0 \neq 0$ pour la suite). On a :

$$\Psi(x,0)\,P(e^x) - \{a_0 \Psi(x,0) + a_1 \Psi(x,1) + \dots + a_p \Psi(x,p)\}$$

$$= a_0 r_N(x,0) + a_1 r_N(x,1) + \dots + a_p r_N(x,p) = R_N(x).$$

S'il existait un tel polynôme P tel que $P(e) = 0$, on aurait donc

$$E = a_0 \Psi(1,0) + a_1 \Psi(1,1) + \dots + a_p \Psi(1,p) = -R_N(1).$$

Or on va montrer que a) E est un entier non nul si m est premier assez grand

b) $R_N(1) \xrightarrow[N\to\infty]{} 0$.

Preuve du a) On a vu à la fin de 4.3 que pour $j = 1, \dots, p$, tous les termes de $\Psi(1,j)$ sont des multiples de $\dfrac{m!}{(N-pm)!}$, donc de m puisque $m > N-pm$, et tous les termes de $\Psi(1,0)$ aussi, sauf un qui vaut $(-1)^p (p!)^m$.

Donc $E \equiv a_0 (-1)^p (p!)^m$ modulo m, et il suffit que m soit premier et plus grand que p et a_0, pour que $E \neq 0$. ∎

Preuve du b) Il suffit de montrer que chaque $r_N(1,j)$ tend vers zero ($j = 0, \dots, p$). Or

$$r_N(x,z) = e^{-xz}\left[\Psi(x,z)e^{-xz} - \Psi(x,0)e^{-x.0}\right] = e^{-xz}\cdot z\left[\frac{\partial}{\partial t}\left(\Psi(x,t)e^{-xt}\right)\right]_{t=\theta z}$$

$$= -z\, x^{N+1} e^{(1-\theta)xz} F(\theta z),$$

par la définition de Ψ comme polynôme de Taylor, et avec $0<\theta<1$.

Posons $C = \sup\limits_{\substack{j=1,\dots,p \\ \theta\in[0,1]}} |\theta j(\theta j - 1)\cdots(\theta j - p)|$. Il vient

$$|r_N(1,j)| \leq p e^p \frac{C^{(N-pm)+m}}{(N-pm)!} \leq p e^p \frac{(C^3)^{N-pm}}{(N-pm)!}$$

puisque $N-pm < m < 2(N-pm)$

et le terme de droite tend vers zéro quand $N\to\infty$, puisque la double inégalité ci-dessus implique $m \xrightarrow[N\to\infty]{} \infty$ (ce qui achève aussi la preuve du a) !) ∎

Finalement, un tel polynôme P n'existe pas, autrement dit,

e est transcendant.

4.5 Il se trouve que la preuve ci-dessus s'adapte aussi à l'étude de la transcendance de π. On se contentera d'indiquer ici les grandes lignes de la démonstration. On part de la fameuse formule d'Euler :

$$1 + e^{i\pi} = 0$$

Soit Q un polynôme à coefficients entiers, et $z_1, \dots, z_n$ ses racines complexes. Il s'agit de montrer que $(1+e^{z_1})\dots(1+e^{z_n}) \neq 0$, soit $1+\sum_i e^{z_i} + \sum_{i,j} e^{z_i+z_j} + \sum_{i,j,k} e^{z_i+z_j+z_k} + \dots \neq 0$.

Or les sommes 2 à 2, 3 à 3, etc., des z_i sont elles-mêmes racines de polynômes à coefficients entiers. On est donc ramené à montrer (en séparant les racines nulles des autres) que

$$P = K + e^{z_1} + \dots + e^{z_p} \neq 0$$

dès que $K \in \mathbb{N}$, et $z_1, \dots, z_p$ sont les racines (non nulles) d'un polynôme Q à coefficients entiers : $Q(z) = b_0 z^p + b_1 z^{p-1} + \dots + b_p$, avec $b_0 \neq 0$ et $b_p \neq 0$.

Choisissant n, N, m comme en 4.3, et posant cette fois-ci

$$F(z) = \frac{A b_0^m}{(N-pm)!} z^{N-pm} (z-z_1)^m \cdots (z-z_p)^m = A \frac{z^{N-pm}}{(N-pm)!} (Q(z))^m,$$

avec $A \in \mathbb{N}$, puis $\Psi(x,z) = F^{(N)}(z) + x F^{(N-1)}(z) + \dots + x^N F(z)$,

on arrive comme en 4.4 à l'égalité

$$R_N = \Psi(1,0)P - \{K\Psi(1,0) + \Psi(1,z_1) + \dots + \Psi(1,z_p)\}.$$

Les $\Psi(1,z_i)$ sont maintenant complexes, mais leur somme est rationnelle, et même entière dès que A est un multiple de b_0^{N-m}. Si on prend $A = b_0^{N-m}$, comme $N-pm < m$, c'est même un multiple de m, et tous les termes non nuls de $\Psi(1,0)$ le sont aussi (en analogie à 4.3), sauf peut-être $F^{(N-pm)}(0) = b_0^{N-m}(Q(0))^m = b_0^{N-2m} b_p^m$.

D'où : $P=0 \Rightarrow R_N = K b_0^{N-2m} b_p^m$ modulo m,

ce qui impliquerait que R_N est un entier non nul, dès que m est un nombre premier plus grand que K, b_0, et b_p. Mais on peut montrer, comme en 4.4, que $R_N \xrightarrow[N\to\infty]{} 0$.

Par suite $P \neq 0$, et π est transcendant. ■

§5 DES POLYGONES RÉGULIERS

5.1 On a appelé "euclidiennes" les longueurs constructibles à la règle et au compas à partir d'une longueur-unité, et on les a identifiées aux nombres réels qui sont dans un des corps K construits à partir de $\mathbb{Q}$ en résolvant un nombre fini d'équations du second degré, autrement dit $K = \bigcup_{j=0}^{p} K_j$, avec $K_0 = \mathbb{Q}$, et $K_{j+1} = K_j(\sqrt{r_j})$ où $r_j \in K_j$ et n'est pas un carré dans K_j.

Appelons conjugués d'un tel nombre x tous ceux qu'on obtient en changeant dans l'expression de x par radicaux, certains des signes qui les précèdent.

<u>Proposition (Abel) : Si $x \in K$ est racine de $F \in \mathbb{Q}[X]$, tous ses conjugués aussi.</u>

Preuve : Si $x = p_j + q_j \sqrt{r_j}$, avec $p_j, q_j, r_j \in K_j$, on a aussi
$0 = F(x) = P_j + Q_j \sqrt{r_j}$, avec $P_j, Q_j \in K_j$, et comme r_j n'est pas un carré dans K_j, $P_j = Q_j = 0$, d'où $F(p_j - q_j\sqrt{r_j}) = P_j - Q_j\sqrt{r_j} = 0$ ... ∎

5.2 <u>Corollaire : Le degré de l'équation irréductible que satisfait un nombre "euclidien" est une puissance de 2.</u>

Preuve : Si $x_1 \in K_j$, et $x_2, \dots, x_{2^j}$ sont ses conjugués (pas forcément distincts), posons $F(x) = \prod_{k=1,\dots,2^j} (x - x_k)$.
Il se peut que F soit réductible sur $\mathbb{Q}$, mais chaque facteur irréductible aura pour racine l'un des x_k, et par 5.1, toutes les autres.
Autrement dit, si $\{x_1, \dots, x_p\}$ est l'ensemble des conjugués <u>distincts</u> de x_1, on a
$$F(x) = \Big(\prod_{j=1,\dots,p} (x - x_k)\Big)^q, \quad \text{avec } pq = 2^j.$$
En particulier p est une puissance de 2. ∎

5.3 <u>Corollaire : La duplication du cube est impossible à la règle et au compas.</u>

Preuve : Il s'agirait en effet de construire une solution de $x^3 - 2a^3 = 0$; cette équation est irréductible sur $\mathbb{Q}(a)$ (sinon elle aurait une racine rationnelle ...), et de degré 3 : on conclut par 5.2. ∎

5.4. <u>Corollaire : La trisection de l'angle est impossible à la règle et au compas</u>

Preuve : Elle reviendrait en effet à la construction, par exemple, de $\sin\theta$ à partir de $\sin 3\theta$ connu, autrement dit à la résolution de
$$4x^3 - 3x + a = 0,$$
et on raisonne comme en 5.3. ∎

5.5 L'énoncé 5.4 ne signifie évidemment pas qu'on ne sache pas "trisecter" <u>certains</u> angles particuliers : on sait bien par exemple construire $\frac{\pi}{3}$, puisque $\cos\frac{\pi}{3} = \frac{1}{2}$. C'est d'ailleurs une construction qui nous a déjà beaucoup servi, celle de l'hexagone régulier (cf. §2). Et la question se pose de la constructibilité des autres polygones réguliers.

Si p et q sont premiers entre eux, il existe $a, b \in \mathbb{Z}$ tels que $ap + bq = 1$, d'où $\frac{1}{pq} = \frac{b}{p} + \frac{a}{q}$, et si l'on sait construire les polygones à p et à q cotés, on en déduira donc celui à pq coté. Il suffit donc de résoudre la question pour le polygone à n cotés, avec $n = p^\alpha$, $\alpha \in \mathbb{N}$, et p premier impair (le cas $p=2$ est connu). Nous n'indiquerons ici que le résultat final:

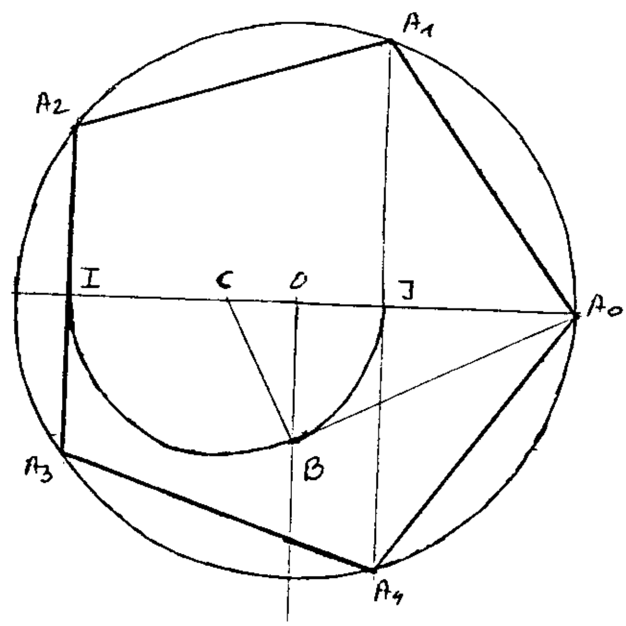
5.6 Théorème "de Gauss": Le polygone régulier à n cotés est constructible à la règle et au compas si et seulement si n est de la forme:

$\boxed{n = 2^m \left(2^{2^{m_1}}+1\right) \cdots \left(2^{2^{m_p}}+1\right)}$, où $m, m_1, \dots, m_p \in \mathbb{N}$, et où toutes les parenthèses sont des nombres premiers distincts.

La preuve en a été donnée par Gauss. Elle utilise évidemment l'énoncé 5.2 et la remarque ci-dessus, mais aussi le théorème de Fermat ($a^{p-1} \equiv 1$ mod. p), les propriétés de la fonction Φ d'Euler, les méthodes de Vandermonde et Lagrange pour la résolution des équations algébriques, et bien d'autres jolies choses. Elle a aussi le mérite d'être "constructive" (c'est le cas de le dire!); au moins en principe, car il convient de remarquer que les cinq premiers nombres de la suite $2^{2^m}+1$ sont 3, 5, 17, 257, et 65.537 (ceux-ci sont bien premiers, mais pas tous les suivants, tant s'en faut!)

Pour finir en beauté, on indiquera ici les constructions des polygones à 5 et à 17 cotés (sans les vérifier), laissant les cas suivants à la sagacité du lecteur!!!

5.7 Construction du pentagone régulier



B est le milieu du rayon perpendiculaire à OA_0

La perpendiculaire à BA_0 donne C sur OA_0

C(B) donne I et J, projections des autres sommets A_2, A_3, A_1, A_4.

5.8 Construction du polygone régulier à 17 cotés

On porte $OB = \frac{1}{4}$ sur la perpendiculaire à OA_0
La perpendiculaire en B à BA_0 donne C.
$C(CB)$ donne D_1 et D_2 . $D_1(B)$ et $D_2(B)$ donnent E_1, E_1', E_2, E_2'
Le cercle de diamètre A_0E_1' coupe OB en D, et
$E_2(CD)$ donne I et J ; projections de A_3 et A_5.
$A_3(A_5)$ donne A_1, et on obtient ainsi tous les autres...