Introduction à la théorie de Galois
Transparents cours 1

Yves Laszlo

École polytechnique

27 janvier 2010

Évariste Galois, 1811-1832

Trois problèmes classiques

1) Quadrature du cercle : construire à la règle et au compas un disque d'aire 1.

2) Constructibilité à la règle et au compas des polygones réguliers à n côtés.

3) Résolution des équations polynomiales en n'utilisant que des expressions polynomiales en des racines n-ièmes successives de polynômes en les coefficients.

Définition

La dimension $\dim_k L$ d'une k-algèbre L se note $[L : k]$.

Si L est de plus un corps, la donnée de l'inclusion $k \subset L$ est appelée une extension de corps.

Point commun : les solutions de 1), 2) et 3) font intervenir la théorie des extensions de corps, 2) et 3) la théorie de Galois de ces extensions, un dictionnaire entre théorie des groupes et théorie des extensions de corps.

Constructibilité à la règle et au compas

On se donne un ensemble X de n points du plan complexe euclidien $\mathbf{C}$.

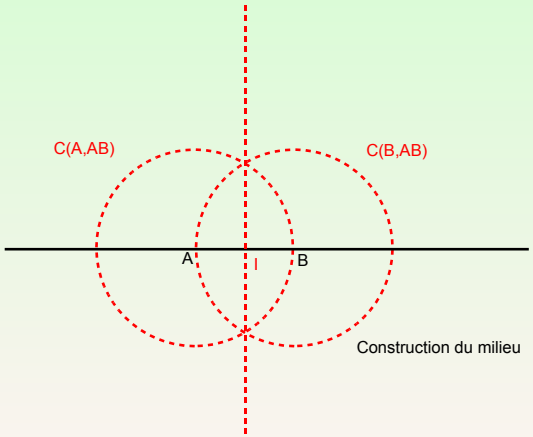
Définition

Les droites constructibles à partir de X sont les droites $(x, y), x \neq y \in X$.
Les cercles constructibles à partir de X sont les cercles $C(x, |y - z|)$ avec $x, y, z \in X$ et $y, z \in X$ distincts.
Les points constructibles à partir de X sont les points de X et ceux parmi les intersections propres entre droites ou cercles constructibles.

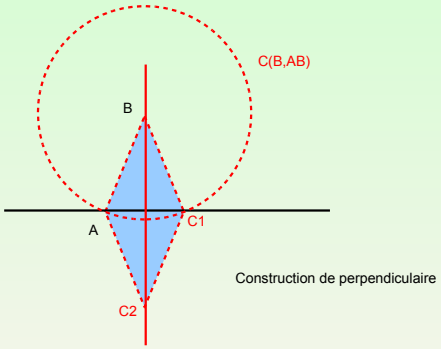
Ceci permet de définir récursivement les points constructibles en déclarant que 0 et 1 sont constructibles.

De même,les droites et cercles constructibles sont ceux obtenus récursivement à partir de $\mathbf{R} = (0, 1)$ et de $C(0, 1), C(1, 0)$.

On peut construire la médiatrice de deux points constructibles, donc le milieu et ainsi construire le 4 ème sommet d'un losange à partir de 3 de ses sommets.

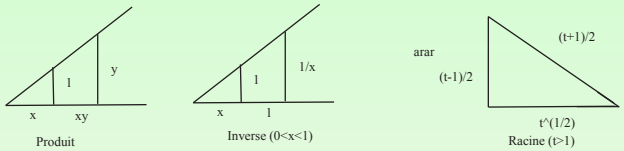


On obtient donc la droite perpendiculaire, parallèle à une droite passant par un point donné.



On déduit z constructible si et seulement $\mathrm{Re}(z), \mathrm{Im}(z)$ le sont.

Des constructions (et du théorème de Thales)



on déduit que l'ensemble des réels et donc également des complexes constructibles est un sous-corps (dénombrable) de $\mathbf{C}$ stable par racine carrée.

Les points d'intersection z, z' du cercle C d'équation d'équation

$$z\bar{z} + az + b\bar{z} + c = 0$$

et de la droite D d'équation

$$a'z + b'\bar{z} + c' = 0, a'b' \neq 0$$

avec

$$a, b, c, a', b', c' \in k \text{ corps} \subset \mathbf{R}$$

sont les solutions d'une équation de degré 2 à coefficients dans k (éliminer $\bar{z}$).

On déduit que les points d'intersection z, z' du cercle C et du cercle C' d'équation

$$z\bar{z} + a'z + b'\bar{z} + c' = 0, \ \ a', b', c' \in k \subset \mathbf{R}$$

sont les solutions d'une équation de degré 2 à coefficients dans k (éliminer $z\bar{z}$).

Donc, tout z constructible à partir de points de k est sol. d'une eq. du second degré à coefficients dans k.

Inversement, si $z^2 + az + b = 0$ avec a, b constructible, alors $z = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$ est constructible.

Interprétation algébrique

Définition

Soit L/k une extension de corps, E une *partie* de L. On note

$$k[E] = \bigcap_{\substack{k-\text{algèbres } A \\ E\subset A\subset L}} A$$

la plus petite sous-algèbre de L contenant E et

$$k(E) = \mathrm{Frac}(k[E]) = \bigcap_{\substack{\text{corps } K \\ k,E\subset K\subset L}} K.$$

$k(E)/k$ est la plus petite sous-extension de l'extension de corps L/k contenant E. Si

$$z^2 + az + b = 0,\ a, b \in k,$$

on a alors

$$k(z) = k[z] = k + zk$$

de dimension ≤ 2 sur k.

La discussion précédente assure

Théorème

Le complexe z est constructible si et seulement si il existe une suite finie de corps $L_0 = \mathbf{Q} \subset L_1 \subset \cdots \subset L_n$ et $[L_{i+1} : L_i] = 2$ avec $z \in L_n$.

Mais on a l'énoncé crucial suivant

Théorème de la base télescopique

Soit L une K-algèbre où K est un corps contenant k de sorte qu'on a des inclusions $k \subset K \subset L$. On a

$$[L : k] = [L : K][K : k].$$

Plus précisément,

si $\lambda_i, i \in I$ base de L/K et $\kappa_j, j \in J$ base de K/k alors $\lambda_i\kappa_j, i \in I, j \in J$ base de $L/k/$.

On déduit le critère

Si z constructible, alors $[\mathbf{Q}(z) : \mathbf{Q}]$ puissance de 2.

Les nombres constructibles sont donc algébriques sur $\mathbf{Q}$.

Nombres algébriques

Définition

Un élément $x \in K$ est dit **algébrique** sur $k \subset K$ si il existe $P \in k[X]$ non nul annulant x. Sinon, il est dit **transcendant**. Une extension K/k est dite algébrique si tous les éléments de K sont algébriques (sur k).

On a

Proposition

Les propositions suivantes sont équivalentes.

- i) x est algébrique sur k ;
- ii) l'algèbre $k[x]$ est de dimension finie sur k ;
- iii) l'algèbre $k[x]$ est un corps.
- iv) $k[x] = k(x)$.

Le polynôme unitaire P de degré minimal annulant x algébrique sur k s'appelle le polynôme minimal de x : il est irréductible sur k et divise tous les polynômes de $k[X]$ annulant x et on a

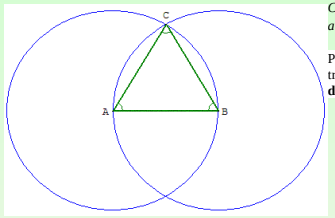
$$[k[x] : k] = \deg(P).$$

Comme $x + y, xy, 1/x \in k[x, y]$, on déduit (base télescopique)

l'ensemble des éléments de K algébriques sur k est un sous-corps de K.

Lindemann (1882) a prouvé que π, donc $\sqrt{\pi}$ est transcendant sur $\mathbf{Q}$:
la quadrature du cercle est impossible.

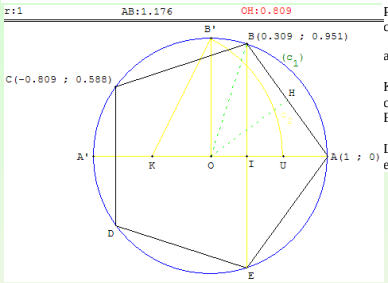
3. Triangle équilatéral



Construction de la proposition 1 du I^er livre d'Euclide (Alexandrie 300 avant Jésus-Christ).

Placer les points libres A, B et dessiner le segment [AB],
tracer les cercles de centre A et B et de rayon AB, C est le **point d'intersection** C des deux cercles.

5. Pentagone - Construction de Ptolémée (90-168 AC).

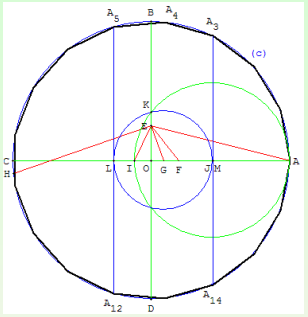


Pour construire un pentagone régulier convexe inscrit dans un cercle à la « *règle et au compas* » il suffit de savoir construire un angle au centre de $\frac{2\pi}{5}$ dont le cosinus est égal à $\frac{\sqrt{5}-1}{4}$.

K est le milieu de [OA'], le cercle de centre K et de rayon KB' coupe [OA] en U. La longueur du côté du pentagone est égale à B'U.

La médiatrice de [OU] coupe le premier cercle (c_1) aux points B et E qui sont deux sommets du pentagone.

17. Heptadécagone (construction de Gauss)



Pour inscrire un polygone régulier dans un cercle (c), de centre O, tracer deux diamètres [AC] et [BD] perpendiculaires.

Soit E le point de [OB] tel que OE = $\frac{1}{4}$OB,

La droite (EF) est la bissectrice de OÊA et la droite (EG) est la bissectrice de OÊF

(OÊG = $\frac{1}{4}$OÊA).

(HE) est la perpendiculaire en E à (EG),
La droite (EI) est la bissectrice de H ÊG.

Le cercle de diamètre [IA], centré en J, rencontre [OB] en K.

Le cercle de centre G, passant par K coupe [AC] en L et M (presque confondu avec J).

Les parallèles à (BC) passant L et M coupent le cercle (c) en A_5, A_{12}, A_3, A_{14}, points de l'heptadécagone.

La médiatrice de [A_3 A_5] coupe le cercle en A_4. [A_3 A_4] et [A_4 A_5] sont deux côtés de l'heptadécagone.

Les polygones réguliers à $3, 5, 17$ sont donc constructibles[1]. Ils ont

$$F_n = 2^{2^n} + 1, n = 0, 1, 2$$

côtés avec F_n premier.

Dire que P_n est constructible, c'est dire que $\mathbf{e}^{\frac{2i\pi}{n}}$ l'est.
Or, si $\mathbf{e}^{2i\pi\alpha}, \mathbf{e}^{2i\pi\beta}$ constructibles, $\mathbf{e}^{2i\pi(x\alpha+y\beta)}$ constructible pour $x, y \in \mathbf{Z}$.
Donc,

$$P_n, P_m \text{ constructibles avec } (m, n) = 1 \rightarrow P_{nm} \text{ constructible}$$

car Bézout donne

$$\exists x, y \in \mathbf{Z} | \ \frac{2i\pi}{nm} = x\frac{2i\pi}{m} + y\frac{2i\pi}{n}.$$

Mais on verra

Théorème [Gauss]

On a $[\mathbf{Q}[\exp\frac{2i\pi}{n}], \mathbf{Q}] = \varphi(n)$ où φ est l'indicateur d'Euler.

1. Voir http ://pagesperso-orange.fr/debart/geoplan/polygone_regulier.html, dont les constructions explicites précédentes sont tirées.

Mais $\varphi(n)$ puissance de 2 si et seulement si n est un produit d'une puissance de 2 et d'un nombre de Fermat $F_m = 2^{2^m}+1$ qui est *premier*.

Donc, si P_n constructible, alors n est un produit d'une puissance de 2 et d'un nombre de Fermat $F_m = 2^{2^m}+1$ qui est *premier*.

La réciproque est vraie et est une conséquence facile de la théorie de Galois.
Notons qu'on a

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$$

et sont tous premiers.
En revanche, F_5 est divisible par 641 (Euler), on ne sait pas si F_{33} est premier, alors qu'on sait que $F_{2478782}$ ne l'est pas : peu de choses sont connues sur la primalité des nombres de Fermat.

Résolution d'équations

On veut « Résoudre » $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0 = 0, a_i \in \mathbf{C}$, (on peut supposer $a_{n-1} = 0$).
Pour $n = 2$, on a $z_i = \pm\sqrt{-a_0}$.
Pour $n = 3$, on a les formules de Cardan

$$z_i = \rho^i \sqrt[3]{-\frac{a_0}{2}+\sqrt{\frac{\Delta}{4.27}}} + \rho^{2i}\sqrt[3]{-\frac{a_0}{2}-\sqrt{\frac{\Delta}{4.27}}}.$$

où $\Delta = 4{a_1}^3 + {a_0}^2$ et la normalisation

$$\sqrt[3]{-\frac{a_0}{2}+\sqrt{\frac{\Delta}{4.27}}}\cdot\sqrt[3]{-\frac{a_0}{2}-\sqrt{\frac{\Delta}{4.27}}} = -\frac{a_1}{3}.$$

et $\rho = \exp(2\sqrt{-1}\pi/3)$.
Pour $n = 4$, on se ramène à $n = 3$ (méthode de Ferrari).
L'idée est de se ramener à l'équation

$$A^2 - B^2 = (A-B)(A+B) = 0$$

avec $A, B \in k_2[X]$, qu'on sait résoudre.

On part de

$$X^4 - aX^2 - bX - c = 0$$

qu'on écrit

$$X^4 = aX^2 + bX + c.$$

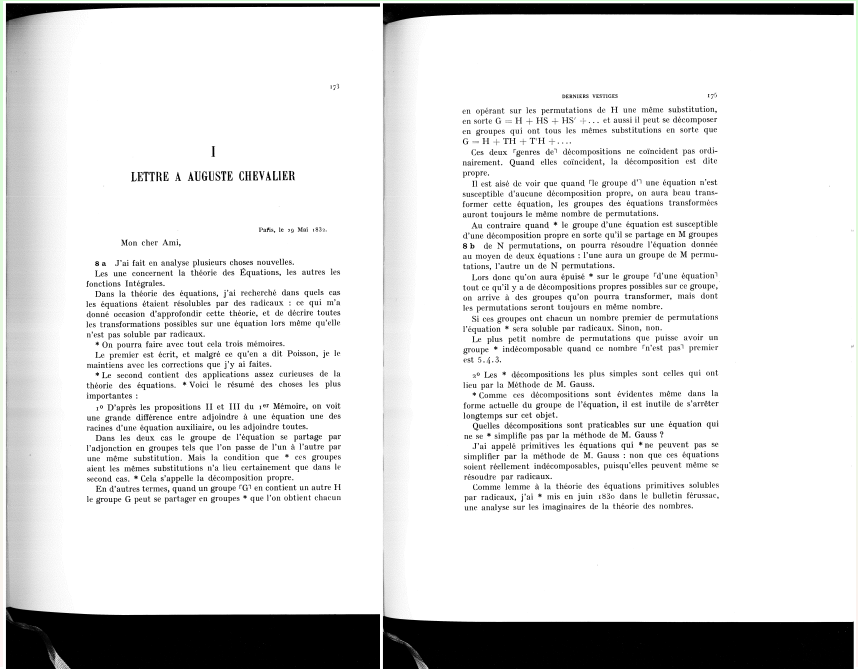
On ajoute $2yX^2 + y^2$ (y paramètre) pour avoir

$$\begin{aligned} X^4 + 2yX^2 + y^2 &= aX^2 + bX + c + 2yX^2 + y^2 \\ (X^2+y)^2 &= (a+2y)X^2 + bX + (c+y^2) \end{aligned}$$

Reste à choisir y racine du discriminant

$$\Delta(y) = b^2 - 4(a+2y)(c+y^2)$$

(de degré 3 en y !) qui assure que $(a+2y)X^2 + bX + (c+y^2)$ carré.□



173

I

LETTRE A AUGUSTE CHEVALIER

Paris, le 29 Mai 1832.

Mon cher Ami,

8 a J'ai fait en analyse plusieurs choses nouvelles.
Les une concernent la théorie des Équations, les autres les fonctions Intégrales.
Dans la théorie des équations, j'ai recherché dans quels cas les équations étaient résolubles par des radicaux ; ce qui m'a donné occasion d'approfondir cette théorie, et de décrire toutes les transformations possibles sur une équation lors même qu'elle n'est pas soluble par radicaux.
* On pourra faire avec tout cela trois mémoires.
Le premier est écrit, et malgré ce qu'en a dit Poisson, je le maintiens avec les corrections que j'y ai faites.
* Le second contient des applications assez curieuses de la théorie des équations. * Voici le résumé des choses les plus importantes :
1° D'après les propositions II et III du 1er Mémoire, on voit une grande différence entre adjoindre à une équation une des racines d'une équation auxiliaire, ou les adjoindre toutes.
Dans les deux cas le groupe de l'équation se partage par l'adjonction en groupes tels que l'on passe de l'un à l'autre par une même substitution. Mais la condition que * ces groupes aient les mêmes substitutions n'a lieu certainement que dans le second cas. * Cela s'appelle la décomposition propre.
En d'autres termes, quand un groupe 'G' en contient un autre H le groupe G peut se partager en groupes * que l'on obtient chacun

DERNIERS VESTIGES 175

en opérant sur les permutations de H une même substitution, en sorte G = H + HS + HS' + ... et aussi il peut se décomposer en groupes qui ont tous les mêmes substitutions en sorte que G = H + TH + T'H + ...
Ces deux 'genres de' décompositions ne coïncident pas ordinairement. Quand elles coïncident, la décomposition est dite propre.
Il est aisé de voir que quand 'le groupe d'' une équation n'est susceptible d'aucune décomposition propre, on aura beau transformer cette équation, les groupes des équations transformées auront toujours le même nombre de permutations.
Au contraire quand * le groupe d'une équation est susceptible d'une décomposition propre en sorte qu'il se partage en M groupes
8 b de N permutations, on pourra résoudre l'équation donnée au moyen de deux équations : l'une aura un groupe de M permutations, l'autre un de N permutations.
Lors donc qu'on aura épuisé * sur le groupe 'd'une équation' tout ce qu'il y a de décompositions propres possibles sur ce groupe, on arrive à des groupes qu'on pourra transformer, mais dont les permutations seront toujours en même nombre.
Si ces groupes ont chacun un nombre premier de permutations l'équation * sera soluble par radicaux. Sinon, non.
Le plus petit nombre de permutations que puisse avoir un groupe * indécomposable quand ce nombre 'n'est pas' premier est 5.4.3.
2° Les * décompositions les plus simples sont celles qui ont lieu par la Méthode de M. Gauss.
* Comme ces décompositions sont évidentes même dans la forme actuelle du groupe de l'équation, il est inutile de s'arrêter longtemps sur cet objet.
Quelles décompositions sont praticables sur une équation qui ne se * simplifie pas par la méthode de M. Gauss ?
J'ai appelé primitives les équations qui * ne peuvent pas se simplifier par la méthode de M. Gauss ; non que ces équations soient réellement indécomposables, puisqu'elles peuvent même se résoudre par radicaux.
Comme lemme à la théorie des équations primitives solubles par radicaux, j'ai * mis en juin 1830 dans le bulletin férussac, une analyse sur les imaginaires de la théorie des nombres.

Par définition, le groupe G d'une équation $P(X) = 0$ est le groupe des automorphismes du corps $k[z_1, \cdots, z_n]$ engendré par les racines de P laissant k fixe.
Il permute les racines, donc est un sous-groupe de S_n.
En langage moderne, Galois dit que l'équation $P = 0$ est résoluble par radicaux si et seulement si G est résoluble au sens de la théorie des groupes.

Or, le groupe de l'équation $\ll$ générale $\gg$ de degré n est S_n, qui n'est pas résoluble justement pour $n \geq 5$!

C'est notamment ce qu'on va expliquer dans ce cours.