INVITATION À LA THÉORIE DE GALOIS

Nous allons esquisser, de manière assez informelle, deux succès historiquement importants de la théorie de Galois. Dans cette invitation, on n'utilisera que le fait bien connu que la donnée d'un sous-corps k d'un corps K munit K d'une structure de k-espace vectoriel. La dimension, finie ou non, se note $[\mathrm{K} : k]$ et s'appelle aussi le degré de *l'extension* K/k.
Le début du cours proprement dit commence au Chapitre 1.

0.1. Construction à la règle et au compas

On identifie le plan euclidien (orienté) à $\mathbf{C}$ muni de la norme usuelle $||z||=|z|$.
Pour deux points A, B distincts de $\mathbf{C}$, l'unique droite passant par A et B est notée $\langle \mathrm{A}, \mathrm{B} \rangle$. Pour A un point de $\mathbf{C}$ et R un nombre réel positif, le cercle de centre A et de rayon R est noté $\mathrm{C}(\mathrm{A}, \mathrm{R})$. Un lieu géométrique qui est une droite ou un cercle est appelé un « cercle-droite ».

Définition 0.1.1. — *On dira qu'un point* $\mathrm{P} \in \mathbf{C}$ *est* constructible *s'il existe une suite finie de points* $\mathrm{P}_0, \cdots, \mathrm{P}_\mathrm{N} = \mathrm{P}$ *telle que* $\mathrm{P}_0 = 0$, $\mathrm{P}_1 = 1$ *et pour tout* $n < \mathrm{N}$ *le point* P_{n+1} *est dans l'intersection de deux cercle-droites différents de type* $\langle \mathrm{P}_\alpha, \mathrm{P}_\beta \rangle$ *avec* $0 \leq \alpha < \beta \leq n$ *ou de type* $\mathrm{C}(\mathrm{P}_\gamma, |\mathrm{P}_\alpha - \mathrm{P}_\beta|)$ *avec* $0 \leq \alpha, \beta, \gamma \leq n$.

Notons que les deux cercle-droites différents dont on considère l'intersection peuvent être du même type.

Explicitons la définition : on décide d'abord que 0 et 1 sont constructibles. Puis, récursivement, étant donnée une famille de points constructibles, on construit les droites passant par deux points constructibles distincts, ou bien un cercle centré sur un de ces points, de rayon une distance entre deux points constructibles : ceci définit les cercle-droites admissibles. Les points constructibles au rang $n+1$ sont les points constructibles au rang n, ainsi que les intersections finies entre deux cercle-droites admissibles.

Par exemple, le nombre complexe i est constructible.

Le lecteur se souviendra des théorèmes de Thales et Pythagore et montrera les pro-

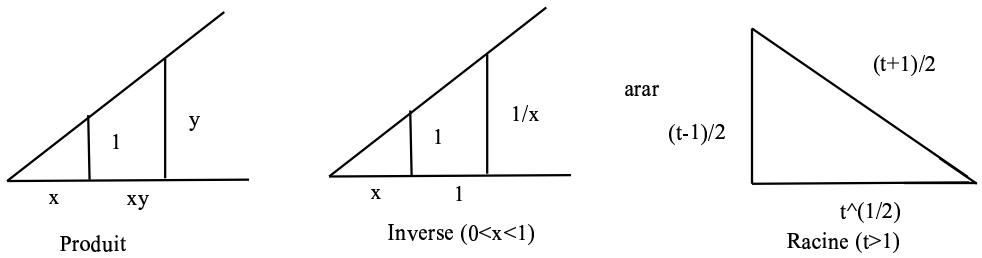

FIGURE 3. Constructions utiles

priétés de l'exercice suivant.

Exercice 0.1.2. — *L'ensemble des nombres réels constructibles est un sous-corps de* $\mathbf{R}$ *(en particulier il contient les nombres rationnels). Un nombre réel positif est constructible si et seulement si sa racine carrée l'est. Le nombre complexe z est constructible si et seulement ses parties réelles et imaginaires le sont, de sorte que les nombres complexes constructibles forment un sous-corps de* $\mathbf{C}$.

Nous montrerons (6.5.1) le résultat suivant.

Théorème 0.1.3 **(Wantzel[7])**. — *Un nombre complexe z est constructible si et seulement si il existe une suite finie de corps $\mathrm{L}_0 = \mathbf{Q} \subset \mathrm{L}_1 \cdots \subset \mathrm{L}_n$ tels que pour chaque i, $[\mathrm{L}_{i+1} : \mathrm{L}_i] = 2$ et $z \in \mathrm{L}_n$.*

Lorsque cette condition est vérifiée, on a en particulier que $[\mathbf{Q}[z] : \mathbf{Q}]$ est finie et est une puissance de 2.

Par exemple, π étant transcendant (9.3), on en conclut l'impossibilité de la quadrature du cercle : on ne peut pas construire à la règle et au compas un carré de même aire que le disque unité.

On peut aussi en déduire par exemple que l'on ne peut pas construire à la règle et au compas un heptagone régulier. En effet, sinon, la dimension de $\mathbf{Q}[\exp(\frac{2i\pi}{7})]$ sur $\mathbf{Q}$ serait une puissance de 2. Or, nous montrerons le résultat suivant (6.3.8).

Proposition 0.1.4 **(Gauss[8]).** — *On a* $[\mathbf{Q}[\exp(\frac{2i\pi}{n})], \mathbf{Q}] = \varphi(n)$ *où* φ *est l'indicateur d'Euler*[9] *et* $\mathbf{Q}[\exp(\frac{2i\pi}{n})]$ *est le corps engendré par* $\exp(\frac{2i\pi}{n})$*, qui est aussi l'ensemble des polynômes en* $\exp(\frac{2i\pi}{n})$ *à coefficients rationnels.*

La formule $\varphi(7) = 7 - 1 = 6$ implique le résultat.

Généralement donc, si le polygone régulier à n côtés est constructible, alors $\varphi(n)$ est une puissance de 2. On verra qu'alors n est le produit d'une puissance de 2 par un nombre fini de nombres premiers de Fermat F_m. On rappelle ici que le nombre de Fermat F_m est $\mathrm{F}_m = 2^{2^m} + 1$. Ce résultat est dû à Gauss.

Ces résultats *ne font pas* intervenir la théorie de Galois[10]. Cette dernière est par contre cruciale pour la réciproque, qui avait été conjecturée semble-t-il par Gauss.

FIGURE 4. Karl Friedrich Gauss

FIGURE 5. Leonhard Euler

Il avait deviné juste :

[7] 1814-1848
[9] 1777-1855
[9] 1707-1783
[10] 1811-1832

***Théorème 0.1.5* (Gauss-Wantzel).** — *La réciproque est vraie : si n est un produit d'une puissance de 2 et d'un nombre fini de nombre premiers de Fermat distincts, alors le polygone régulier à n côtés est constructible.*

En fait la preuve donne presque un algorithme pour construire un polygone régulier à n côtés (lorsque c'est possible !) : on doit décomposer n en facteurs premiers *et* trouver un générateur du groupe cyclique $(\mathbf{Z}/p\mathbf{Z})^*$. Notons qu'on a $\mathrm{F}_0 = 3, \mathrm{F}_1 = 5, \mathrm{F}_2 = 17, \mathrm{F}_3 = 257, \mathrm{F}_4 = 65537$ et qu'ils sont tous premiers. Si les constructions des triangles équilatéraux, carrés, et pentagones réguliers sont élémentaires, celle du polygone régulier à 17 côtés est moins évidente[(11)]...

Rappelons d'abord la construction (connue de Ptolémée[(12)], premier siècle de notre ère) du pentagone régulier, simple conséquence de la formule élémentaire

$$\cos\left(\frac{2\pi}{5}\right) = \frac{\sqrt{5}-1}{4}.$$

Gauss, encore lui, a donné une construction du polygone à 17 côtés ; voici une construction :

On a ici déjà une formule assez compliquée

$$16\cos\left(\frac{2\pi}{17}\right) = -1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+\sqrt{68+12\sqrt{17}-4\sqrt{34-2\sqrt{17}}-8\sqrt{34+2\sqrt{17}}},$$

formule qui se déduit d'ailleurs de la théorie de Galois et qui permet de donner effectivement une construction.

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

La réciproque, elle, fait intervenir la théorie de Galois : c'est une conséquence du calcul du groupe de Galois $\mathrm{Gal}(\mathbf{Q}[\exp(\frac{2i\pi}{n})], \mathbf{Q})$ (cf. 6.3.10).

(11) Cf. http ://pagesperso-orange.fr/debart/geoplan/polygone_regulier.html, dont les constructions explicites suivantes sont tirées.

(12) ∼90-168

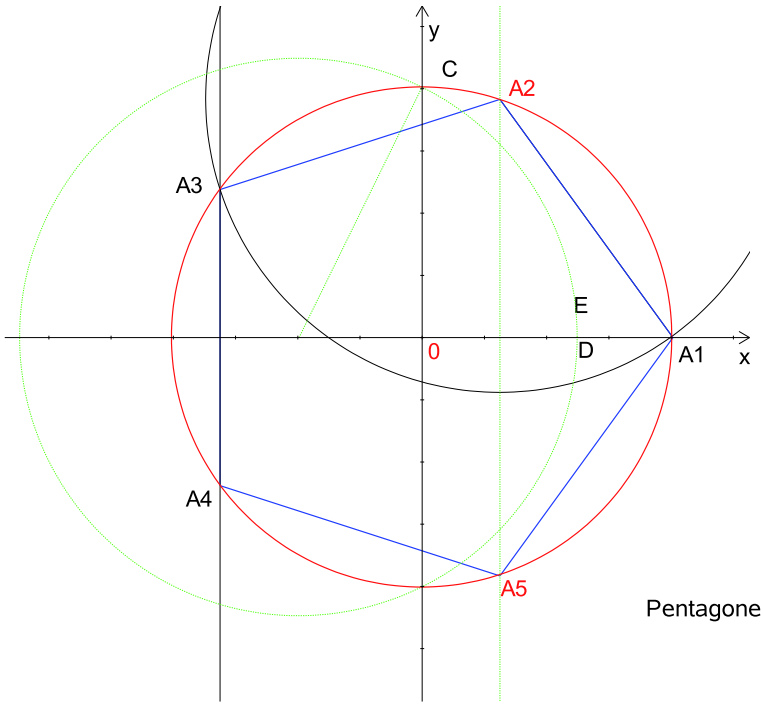

FIGURE 6. Construction du pentagone régulier

FIGURE 7. Claudius Ptolémée

0.2. Résolution d'équations

Les solutions $x = \pm\sqrt{a}$ de l'équation quadratique $x^2 + a = 0$, $a \in \mathbf{C}$, sont bien connues. En général, pour l'équation de degré n, une habile translation de la variable annule

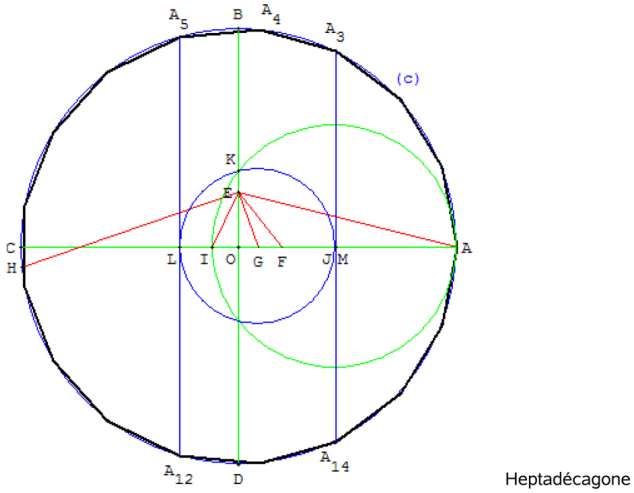

FIGURE 8. Construction de l'heptadécagone régulier

le terme de degré $n-1$. En degré 3, on a donc affaire à l'équation $x^3+ax+b=0$ dont les solutions ont été achetées au 16ème siècle par Cardan[13] au mathématicien Tartaglia[14] (mais étaient sans doute connues de del Ferro[15]). Elles s'écrivent

$$\begin{aligned}
x_1 &= \sqrt[3]{-\frac{b}{2}+\sqrt{(\frac{a}{3})^3+(\frac{b}{2})^2}}+\sqrt[3]{-\frac{b}{2}-\sqrt{(\frac{a}{3})^3+(\frac{b}{2})^2}}\\
x_2 &= j\sqrt[3]{-\frac{b}{2}+\sqrt{(\frac{a}{3})^3+(\frac{b}{2})^2}}+j^2\sqrt[3]{-\frac{b}{2}-\sqrt{(\frac{a}{3})^3+(\frac{b}{2})^2}}\\
x_3 &= \bar{j}\sqrt[3]{-\frac{b}{2}+\sqrt{(\frac{a}{3})^3+(\frac{b}{2})^2}}+\bar{j}^2\sqrt[3]{-\frac{b}{2}-\sqrt{(\frac{a}{3})^3+(\frac{b}{2})^2}}
\end{aligned}$$

avec $j=\exp(\frac{2i\pi}{3})$, les racines cubiques étant normalisées par

$$\sqrt[3]{-\frac{b}{2}+\sqrt{(\frac{a}{3})^3+(\frac{b}{2})^2}}\sqrt[3]{-\frac{b}{2}-\sqrt{(\frac{a}{3})^3+(\frac{b}{2})^2}}=-\frac{a}{3}.$$

[13] 1501-1576
[14] 1499-1557
[15] 1465-1526

Un élève de Cardan, Ferrari[16], a découvert comment ramener les équations de degré 4 à celles de degré 3. On part de l'équation

$$x^4 = ax^2 + bx + c$$

qui équivaut, y étant un paramètre, à l'équation

$$x^4 + 2yx^2 + y^2 = (a + 2y)x^2 + bx + (c + y^2).$$

On cherche y tel que $(a + 2y)x^2 + bx + (c + y^2)$ soit un carré $(\mathrm{A}x + \mathrm{B})^2$, autrement dit on résout l'équation

$$b^2 - 4(a + 2y)(c + y^2) = 0$$

qui est de degré 3 en y. Une fois qu'on a un tel y, il ne nous reste qu'à résoudre l'équation $x^4 + 2yx^2 + y^2 = (\mathrm{A}x + \mathrm{B})^2$ qui n'est autre que

$$(x^2 + y - \mathrm{A}x - \mathrm{B})(x^2 + y + \mathrm{A}x + \mathrm{B}) = 0,$$

soit deux équations de degré 2 !

FIGURE 9. Gerolamo Cardano

FIGURE 10. Niccolo Fontana dit Tartaglia

Dans tous ces cas de petit degré, les racines complexes de l'équation générale initiale s'obtiennent à l'aide de polynômes en ses coefficients ainsi que des racines de tels polynômes : on dit qu'elles s'expriment par radicaux. C'est impossible pour $n \geq 5$: c'est une conséquence du théorème des fonctions symétriques et de la théorie de Galois (cf. 7.4). C'est le succès le plus connu de la théorie de Galois. On a des résultats très précis. Par exemple, on peut montrer avec les méthodes développées ici que les racines de l'équation $\mathrm{X}^5 - \mathrm{X} - 1$ ne s'expriment pas par radicaux de nombres rationnels !

[16] 1522-1565

Pour finir cette invitation, insistons sur le fait que la théorie de Galois ne se limite pas, loin s'en faut, à ces applications à l'intérêt désormais historique. Elle a de multiples facettes, très profondes, gouvernant de vastes aspects tant de l'algèbre que de la théorie des nombres et de la géométrie. C'est l'étude fine des représentations linéaires du groupe de Galois « absolu »de $\bar{\mathbf{Q}}/\mathbf{Q}$ -au travers notamment d'un cas particulier des conjectures de Langlands- qui a permis à Wiles de prouver le théorème de Fermat : pour n nombre entier strictement supérieur à 2, il n'existe pas de nombres entiers non nuls x, y et z tels que $x^n + y^n = z^n$.
Ce cours n'est que le *début* d'une longue histoire, bien loin d'être terminée.