III. Applications

Baptiste Calmès

19 février 2021

Table des matières

1 Rappels de théorie des groupes

Rappelons brièvement quelques définitions de théorie des groupes.

1.1 Définition. Un groupe fini G est dit *résoluble* s'il existe une suite finie de sous-groupes

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

avec G_i normal dans G_{i+1} et G_{i+1}/G_i abélien pour tout i.

1.2 Lemme. *Soit H un sous-groupe d'un groupe fini G. Alors si G est résoluble, H l'est aussi. De plus, si H est normal, G est résoluble si et seulement si H et G/H sont résolubles.*

1.3 Lemme. *Si G est résoluble, on peut toujours raffiner une série de sous-groupes comme dans la définition pour que les quotients successifs soient cycliques (isomorphes à $\mathbb{Z}/n\mathbb{Z}$ pour certaines valeurs de n).*

1.4 Exemple. Le groupe $\mathcal{A}_5$ n'est pas résoluble (c'est en fait le plus petit groupe non résoluble) et donc $\mathcal{S}_5$ non-plus.

1.5 Lemme ($\mathrm{car}(K) = 0$)**.** *Si L/F, F/K et leur composée L/K sont toutes finies et normales, alors $\mathrm{Gal}(L/K)$ est résoluble si et seulement si $\mathrm{Gal}(L/F)$ et $\mathrm{Gal}(F/K)$ sont résolubles.* [1]

2 Résolubilité par radicaux

2.1 Définition. Une extension finie L/K est dite *résoluble* ou *résoluble par radicaux* s'il existe une extension (finie) M/L telle que M/K soit radicale.

2.2 Remarque. Concrètement, L/K est résoluble par radicaux si tout élément de L peut s'exprimer à partir d'éléments de K par sommes, produits et "racines n-ièmes" pour différentes valeurs de n.

1. Pour que ce lemme soit vrai sans hypothèse de caractéristique, il suffit de remplacer normales par galoisiennes.

2.3 Théorème (Galois)**.** *Si une extension finie d'un corps de caractéristique* 0 *est résoluble par radicaux alors son groupe de Galois est résoluble.*

2.4 Corollaire. *Il existe des polynômes sur* $\mathbb{Q}$ *(de degré* ≥ 5*) dont les racines ne peuvent s'exprimer par sommes, produits inverses et radicaux à partir d'éléments de* $\mathbb{Q}$*.*

En fait, on a aussi la réciproque suivante :

2.5 Théorème. *Si* K *est un corps de caractéristique* 0 *et* L/K *est une extension normale, alors si son groupe de Galois est résoluble, elle est résoluble par radicaux.*

2.6 Corollaire. *Soit* $P \in F[X]$ *où* F *est un corps de caractéristique* 0*, avec* $\deg(P) \leq 4$*. Une extension de décomposition de* P *est résoluble : les racines de* P *s'expriment par sommes, produits, inverses et racines* n*-ièmes itérées à partir d'éléments de* $\mathbb{Q}$ *et des coefficients de* P*.*

3 Nombres constructibles à la règle et au compas

3.1 Définition. Soit $\mathcal{E}$ un ensemble de points du plan. On dit qu'un point du plan est constructible à la règle et au compas à partir de $\mathcal{E}$ s'il s'obtient à partir de points de $\mathcal{E}$ en itérant un nombre fini de fois les étapes suivantes (on suppose A, B, C et D déjà obtenus) :

— Si (A, B) et (C, D) ne sont pas parallèles, et rajouter le point d'intersection $E = (A, B) \cap (C, D)$.

— Si $C \neq D$ et si le cercle de centre A passant par B coupe la droite passant par C et D, rajouter leur(s) point(s) d'intersection.

— Si $A \neq C$, et si le cercle de centre A passant par B coupe le cercle de centre C passant par D, alors rajouter leur(s) point(s) d'intersection.

3.2 Définition. Soit $\mathcal{E}$ une partie de $\mathbb{C}$ contenant $\{0, 1\}$. En identifiant le plan $\mathbb{R}^2$ avec $\mathbb{C}$ par $(x, y) \mapsto x + iy$, on obtient une définition de la constructibilité d'un nombre complexe à la règle et au compas, et en identifiant $\mathbb{R}$ aux nombres complexes de partie imaginaire nulle, on obtient également la définition d'un nombre réel constructible à la règle et au compas à partir de $\mathcal{E}$.

3.3 Définition. Soit $\mathcal{E}$ une partie de $\mathbb{C}$ contenant $\{0, 1\}$. On note

— $\mathrm{Cons}_{\mathbb{C}}(\mathcal{E})$ (resp. Cons) l'ensemble des nombres complexes constructibles à la règle et au compas à partir de $\mathcal{E}$ (resp. de $\{0, 1\}$).

— $\mathrm{Cons}_{\mathbb{R}}(\mathcal{E})$ (resp. $\mathrm{Cons}_{\mathbb{R}}$) l'ensemble des nombres réels constructibles à la règle et au compas à partir d'une partie $\mathcal{E}$ de $\mathbb{R}$ (resp. de $\{0, 1\}$), i.e. $\mathrm{Cons}_{\mathbb{R}}(\mathcal{E}) = \mathrm{Cons}_{\mathbb{C}}(\mathcal{E}) \cap \mathbb{R}$.

3.4 Lemme. *Si* $\{0, 1\} \subset \mathcal{E}$*, alors un nombre complexe* z *est dans* $\mathrm{Cons}_{\mathbb{C}}(\mathcal{E})$ *si et seulement si ses parties réelles et imaginaires sont dans* $\mathrm{Cons}_{\mathbb{R}}(\mathcal{E})$*.*

3.5 Proposition. *Si* $\{0, 1\} \subset \mathcal{E} \subset \mathbb{R}$ *(resp.* $\{0, 1\} \subset \mathcal{E} \subset \mathbb{C}$*), l'ensemble* $\mathrm{Cons}_{\mathbb{R}}(\mathcal{E})$ *des nombres réels (resp. complexes) constructibles à la règle et au compas est un sous-corps de* $\mathbb{R}$ *(resp. de* $\mathbb{C}$*) contenant* $\mathbb{Q}(\mathcal{E})$*. Si* $\mathcal{E} \subset \mathbb{R}$*, alors* $\mathrm{Cons}_{\mathbb{C}}(\mathcal{E}) = \mathrm{Cons}_{\mathbb{R}}(\mathcal{E})[i]$*.*

3.6 Remarque. En particulier $\mathrm{Cons}_{\mathbb{R}} = \mathrm{Cons}_{\mathbb{R}}(\mathbb{Q})$ et de même avec $\mathrm{Cons}_{\mathbb{C}} = \mathrm{Cons}_{\mathbb{C}}(\mathbb{Q})$.

Rappel :

3.7 Lemme. *Si* $\mathrm{car}(K) \neq 2$*, et si* L/K *est de degré* 2*, alors il existe de* $a \in L$ *avec* $a^2 \in K$ *tel que* $L = K[a]$*.*

3.8 Lemme. *Si* $\{0, 1\} \subset \mathcal{E}$*, alors* $x \in \mathrm{Cons}_{\mathbb{R}}(\mathcal{E})$ *si et seulement si* $\sqrt{x} \in \mathrm{Cons}_{\mathbb{R}}(\mathcal{E})$*. En particulier,* $\mathrm{Cons}_{\mathbb{R}}(\mathcal{E})$ *n'a pas d'extension quadratique. Il en est de même pour* $\mathrm{Cons}_{\mathbb{C}}(\mathcal{E})$*.*

3.9 Théorème. *Soit E un sous-corps de $\mathbb{R}$. Un nombre réel x est constructible à la règle et au compas à partir de E si et seulement s'il existe une tour de sous-corps de $\mathbb{R}$*

$$E = L_0 \subset L_1 \subset \ldots \subset L_n$$

avec $x \in L_n$ et $[L_i : L_{i-1}] = 2$ pour tout i, $1 \leq i \leq n$.

3.10 Corollaire. *Un nombre réel constructible à la règle et au compas à partir de K est algébrique sur K, de degré une puissance de 2.*

3.11 Théorème (impossibilité de la quadrature du cercle)**.** *Il n'est pas possible de construire à la règle et au compas un carré dont l'aire est celle du cercle unité.*

3.12 Théorème (impossibilité de la trisection de l'angle)**.** *Il existe des angles qu'on ne peut couper en trois angles égaux à la règle et au compas.*

3.13 Lemme. *Soit θ un réel. Le réel $\cos(\theta/3)$ est constructible à la règle et au compas à partir de $\{0, 1, \cos(\theta)\}$ si et seulement si le polynôme $X^3 - 3X - 2\cos(\theta)$ n'est pas irréductible sur $\mathbb{Q}(\cos(\theta))$.*

3.14 Remarque. En particulier, $\pi/3$ ne peut être trisecté à la règle et au compas, puisque $\cos(\pi/3) = \frac{1}{2}$ et $X^3 - 3X - 1$ est irréductible sur $\mathbb{Q}$ (exercice). En d'autres termes, l'angle $\pi/9$ n'est pas constructible à la règle et au compas (à partir de $\{0, 1\}$).