NON RÉSOLUBILITÉ PAR RADICAUX DE L'ÉQUATION POLYNOMIALE GÉNÉRALE DE DEGRÉ $\geqslant 5$.

MARC ABBOUD

Ceci est une note de mon exposé à l'édition 2025 des Gustins. Le but de l'exposé est de prouver le résultat suivant. Les références principales sont le poly d'algèbre 1 (pour la théorie des groupes) et algèbre 2 (théorie des corps) d'Olivier Debarre. Voir [Deba] et [Debb].

Théorème 0.1 (Abel, Galois, Artin)**.** *L'équation polynomiale générale de degré $\geqslant 5$ n'est pas résoluble par radicaux.*

Il faut expliquer les différents termes de cet énoncé. On donnera des énoncés précis dans la suite. Soit $P = a_0 t^n + a_1 t^{n-1} + \cdots + a_n$ un polynôme à coefficients rationnels. On dit que P est résoluble par radicaux si toutes ces racines sont obtenues à partir de sommes, produits et extractions de racines k-ièmes des coefficients $a_0, \ldots, a_n$.

1. Équations de degré 2 et 3

On connaît les formules pour résoudre les équations de degré 2. Considérons l'équation

$$aX^2 + bX + c = 0. \tag{1}$$

Les solutions s'écrivent

$$x_1 = \frac{-b + \sqrt{\Delta}}{2a}, \quad x_2 = \frac{-b - \sqrt{\Delta}}{2a} \tag{2}$$

où

$$\Delta = b^2 - 4ac. \tag{3}$$

Ici je ne m'embête pas de savoir si Δ est réel, ou positif. Je prends une racine carré de Δ.

Pour les équations de degré 3, on a aussi des formules. Ce sont les formules de Cardan qui utilisent les coefficients de l'équation, des racines carrés et des racines cubiques. Si on considère l'équation

$$X^3 + pX + q, \tag{4}$$

alors les solutions sont de la forme

$$x_k = j^k \sqrt[3]{\frac{1}{2}\left(-q + \sqrt{\frac{-\Delta}{27}}\right)} + j^{-k} \sqrt[3]{\frac{1}{2}\left(-q - \sqrt{\frac{-\Delta}{27}}\right)} \tag{5}$$

pour $k = 0, 1, 2$ et $j = e^{\frac{2i\pi}{3}}$.

En degré 4, il y a également des formules du même acabit. Mais en degré 5 et plus, pas de formules ! On va voir pourquoi dans cet exposé.

2. Un peu de théorie des groupes

2.1. **Définitions et exemples.**

Définition 2.1. Un *groupe* est la donné d'un ensemble G muni d'une loi de composition $\cdot : G \times G \to G$ tel que

(i) G possède un neutre.
(ii) Tout élément a un inverse.
(iii) La loi est associative: $(ab)c = a(bc)$.

On dit que G est un groupe *abélien* ou *commutatif* si la loi vérifie $ab = ba$.

Définition 2.2. Soit G un groupe. Un *sous-groupe* $H \subset G$ est une partie de G vérifiant les propriétés suivantes.

(i) $e_G \in H$.
(ii) $\forall x, y \in H, xy \in H$.
(iii) $\forall x \in H, x^{-1} \in H$.

Définition 2.3. Un *morphisme de groupes* est une application $\phi : G \to G'$ entre deux groupes telle que

(i) $\phi(e_G) = \phi(e_{G'})$.
(ii) $\phi(xy) = \phi(y)\phi(y)$.

Le *noyau* de ϕ est l'ensemble des $x \in G$ tels que $\phi(x) = e_{G'}$. On le note $\ker\phi$.

Un *isomorphisme* de groupes est un morphisme de groupe $\phi : G \to G'$ tel qu'il existe un morphisme $\psi : G' \to G$ tel que

$$\psi \circ \phi = \mathrm{id}_G, \quad \phi \circ \psi = \mathrm{id}_{G'}. \tag{6}$$

Exercice 2.4. Montrer que ϕ est injectif si et seulement si $\ker\phi = \{e_G\}$.

Exercice 2.5. Montrer que l'image et le noyau d'un morphisme sont des sous-groupes.

Exemple 2.6. $(\mathbf{R}, +)$ est un groupe, $(\mathbf{C}, +)$ aussi. L'ensemble des matrices inversibles sur un corps est un groupe.

2.2. **Quotients et sous-groupe dinstingué.**

Soit G un groupe et $H \subset G$ un sous-groupe. On aimerait définir le *groupe quotient* G/H qui hérite de la loi de groupe de G mais dans lequel tous les éléments de H sont envoyés sur l'élément neutre (penser par exemple au groupe $\mathbf{Z}/3\mathbf{Z}$). Autrement dit on veut construire un groupe G/H avec un morphisme de groupes surjectif

$$\phi : G \to G/H \tag{7}$$

tel que $\ker\phi = H$. Supposons avoir construit un tel groupe. On note $\overline{g} = \phi(g)$. On doit nécessairement avoir la propriété suivante.

$$\forall g \in G, \forall h \in H, \quad ghg^{-1} \in H. \tag{8}$$

C'est à dire que H est *stable par conjugaison*. Un tel sous-groupe sera dit *distingué*. En effet, on a

$$\overline{ghg^{-1}} = \overline{g}\overline{h}\overline{g^{-1}} = \overline{g}\overline{g^{-1}} = e_{G/H}. \tag{9}$$

Exercice 2.7. Montrer que pour tout morphisme de groupes ϕ, $\ker\phi$ est un sous-groupe distingué.

Théorème 2.8. *Soit G un groupe et $H \lhd G$ un sous-groupe distingué. Il existe un unique groupe G/H à isomorphisme près tel que on a un morphisme de groupes surjectifs $\phi : G \to G/H$ et $\ker\phi = H$.*

Corollaire 2.9. *Soit $\phi : G \to G'$ un morphisme de groupes, alors*

$$\mathrm{Im}\,\phi \simeq G/\ker\phi. \tag{10}$$

2.3. **Groupes abéliens finis.** Une version faible du théorème de structure des groupes abéliens finis.

Théorème 2.10. *Soit G un groupe fini, alors il existe des entiers $n_1, \ldots, n_r$ tels que*

$$G = \mathbf{Z}/n_1\mathbf{Z} \times \cdots \mathbf{Z}/n_r\mathbf{Z}. \tag{11}$$

Étudions un peu plus le groupe $\mathbf{Z}/n\mathbf{Z}$.

Proposition 2.11. *Tout $x \in \mathbf{Z}/n\mathbf{Z}$ est d'ordre $d|n$. Et l'ordre de x est n si et seulement si $n \wedge d = 1$. En particulier l'ensemble des d tels que $d \wedge n = 1$ est un groupe de taille $\phi(n)$ qu'on note $(\mathbf{Z}/n\mathbf{Z})^\times$.*

Corollaire 2.12. *On a*

$$\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) = (\mathbf{Z}/n\mathbf{Z})^\times. \tag{12}$$

Proof. Le groupe $\mathbf{Z}/n\mathbf{Z}$ est engendré par $\overline{1}$. Donc tout automorphisme est entièrement déterminé par l'image de $\overline{1}$. Donc on doit avoir que $\sigma(\overline{1})$ est un générateur de $\mathbf{Z}/n\mathbf{Z}$ et donc $\sigma(\overline{1}) = \overline{d}$ avec $d \in (\mathbf{Z}/n\mathbf{Z})^\times$. □

Proposition 2.13. *Un sous-groupe de $\mathbf{Z}/n\mathbf{Z}$ est isomorphe à $\mathbf{Z}/d\mathbf{Z}$ avec $d|n$. En particulier c'est aussi un groupe cyclique.*

Proof. Soit $G = \mathbf{Z}/n\mathbf{Z}$ et $H \subset G$ un sous-groupe. Soit $k = 1, \ldots . n-1$ le plus petit entier tel que $k \in H$. Alors on montre que $H = \langle k \rangle$. Soit $\ell \in H$. On écrit la division euclidienne de ℓ par k. On a

$$\ell = qk + r \tag{13}$$

avec $0 \leqslant r < k$. On a $\ell - qk = r \in H$. Par minimalité de k on a que $r = 0$ et donc $\ell = qk$ et $\ell \in \langle k \rangle$. On a donc l'égalité. □

2.4. **Les permutations.** On note S_n le groupe des permutations de l'ensemble $\{1,\dots,n\}$. C'est un groupe fini de cardinal $n!$. La loi est donné par

$$\sigma \circ \tau(k) = \sigma(\tau(k)). \tag{14}$$

L'élément neutre est la permutation id qu'on appelle *identité* qui vérifie,

$$\forall n, \sigma(n) = n. \tag{15}$$

Définition 2.14. Soit $n \geqslant 1$ et $2 \leqslant p \leqslant n$. Un p-cycle γ est une permutation de la forme suivante. Il existe $a_1,\dots,a_p \in \{1,\dots,n\}$ 2 à 2 distincts telle que

$$\gamma(a_i) = a_{i+1} \tag{16}$$

et pour tout $x \neq a_i, \gamma(x) = x$. On note

$$\gamma = (a_1\ a_2 \cdots a_p). \tag{17}$$

Un $2-$cycle est appelé une *transposition*.

Proposition 2.15. *Soit $\gamma = (a_1 \cdots a_p)$ un p-cycle et $\sigma \in S_n$, alors*

$$\sigma\gamma\sigma^{-1} = (\sigma(a_1)\cdots\sigma(a_p)). \tag{18}$$

Théorème 2.16. *Pour tout $n \geqslant 2$, S_n est engendré par les transpositions.*

Proof. Par récurrence. C'est vrai si $n = 2$. Supposons que le théorème soit vrai pour S_n et soit $\sigma \in S_{n+1}$. Si $\sigma(n+1) = n+1$, alors σ induit naturellement une permutation de $\{1,\dots,n\}$ et on peut l'écrire comme un produit de transpositions par récurrence. Sinon, on a

$$\sigma' = (n+1 \quad \sigma(n+1))\sigma \tag{19}$$

qui vérifie $\sigma'(n+1) = n+1$. On écrit alors σ' commme produit de transpositions et comme $\sigma = n+1 \quad \sigma(n+1))\sigma'$ on a le résultat. □

Définition 2.17. Soit $\sigma \in S_n$. Une *inversion* de σ est la donnée de $i, j \in \{1,\dots,n\}$ tels que $i < j$ et $\sigma(i) > \sigma(j)$.

La *signature* de σ est définie par

$$\varepsilon(\sigma) := (-1)^{I(\sigma)} \tag{20}$$

où $I(\sigma)$ est le nombre d'inversions de σ.

Proposition 2.18. *L'application signature $\varepsilon : S_n \to \{\pm 1\}$ est un morphisme de groupes surjectif. On a en particulier pour tout p-cycle γ,*

$$\varepsilon(\gamma) = (-1)^{p-1}. \tag{21}$$

Le noyau du morphisme signature est appelé le *groupe alterné*, on le note A_n.

Proposition 2.19. *Soit $n \geqslant 3$, le sous-groupe alterné A_n est engendré par les 3-cycles.*

Proof. On a que toute permuation est produit de transposition. Par la proposition 2.18, on a que $\varepsilon(\sigma) = 1$ si et seulement si σ est un produit d'un nombre pair de transpositions. Il suffit donc de montrer que n'importe quelle double transposition $(ab)(cd)$ est une produit de 3-cycles.

Si $\#\{a,b\} \cap \{c,d\} = 2$, alors $a = c$ et $b = d$ à permutations près et alors $(ab)(cd) = \mathrm{id}$.

Si $\#\{a,b\} \cap \{c,d\} = 1$, alors par exemple $b = c$ et

$$(ab)(bd) = (abd). \tag{22}$$

Enfin si a,b,c,d sont deux à deux distincts, on a

$$(ab)(cd) = (abc)(bcd). \tag{23}$$

□

2.5. **Théorème de décomposition en cycles à supports disjoints.** Soit $\sigma \in S_n$, le *support* de σ est défini par

$$\mathrm{Supp}\,\sigma := \{i \in \{1,\dots,n\} : \sigma(i) \neq i\}. \tag{24}$$

Exercice 2.20. Montrer que si $\mathrm{Supp}\,\sigma \cap \mathrm{Supp}\,\tau = \varnothing$, alors

$$\sigma\tau = \tau\sigma. \tag{25}$$

Théorème 2.21. *Soit $\sigma \in S_n$, alors il existe des p_i-cycles γ_i à supports dijoints tels que*

$$\sigma = \gamma_1 \cdots \gamma_r. \tag{26}$$

Et cette décomposition est unique.

Proof. On donne l'algorithme pour trouver la décomposition en cycles à support disjoints. On raisonne par récurrence descendante sur le nombre de points fixes de σ. Si $\#\mathrm{Fix}(\sigma) = n$, alors $\sigma = \mathrm{id}$ et il est clair que la décomposition est unique. Soit σ tel que $\#Fix(\sigma) = k < n$. Soit x tel que $\sigma(x) \neq x$, alors soit ℓ le plus petit entier > 0 tel que $\sigma^\ell(x) = x$. Soit γ le cycle

$$\gamma = \left(x\ \sigma(x)\ \sigma^2(x) \cdots \sigma^{\ell-1}(x)\right). \tag{27}$$

Alors $\mathrm{Fix}(\gamma^{-1}\sigma) > \mathrm{Fix}(\sigma)$ et par récurrence il existe $\gamma_1,\dots,\gamma_r$ des cycles à supports disjoints tels que

$$\gamma^{-1}\sigma = \gamma_1 \cdots \gamma_r \tag{28}$$

et donc

$$\sigma = \gamma \cdot \gamma_1 \cdots \gamma_r. \tag{29}$$

On laisse l'unicité en exercice. □

Exercice 2.22. Donner le nombre de classes de conjugaison de S_n. Donner un équivalent pour $n \to +\infty$ (On pourra demander à Ramanujan).

2.6. **Groupes résolubles.**

Définition 2.23. On dit qu'un groupe G est *résoluble* s'il existe une suite de sous groupes $G_0 = G \supset G_1 \supset \cdots \supset G_n = 0$ telle que G_{i+1} soit un sous-groupe distingué de G_i et G_i/G_{i+1} est abélien.

Définition 2.24. Soit G un groupe. On définit la *suite dérivée* $D_n(g)$ de G par

$$D_0(G) := G, \quad D_{i+1}(G) := D(D_i(G)) \tag{30}$$

où $D(H)$ est le sous-groupe de H engendré par les commutateurs de H. On l'appelle le *sous-groupe dérivé* de H.

Lemme 2.25. *Soit G un groupe. Le sous-groupe dérivé de G est le plus petit-sous-groupe distingué de G tel que le quotient $G/D(G)$ soit abélien.*

Proof. Il faut tout d'abord montrer que $D(G)$ est distingué et que son quotient est abélien. Supposons que $D(G)$ soit distingué et soit $\overline{a}, \overline{b} \in G/D(G)$. On a que $\overline{a}$ et $\overline{b}$ commutent si et seulement si $[\overline{a}, \overline{b}] = 0$. Mais si a, b sont des relevés respectifs de $\overline{a}$ et $\overline{b}$, alors

$$[\overline{a}, \overline{b}] = \overline{[a,b]} = 0 \tag{31}$$

car $[a,b] \in D(G)$ et on a bien que $G/D(G)$ est abélien.

Pour montrer que $D(G)$ est distingué, il suffit de montrer que le conjugué de tout commutateur est un commutateur. Or si $a, b, c \in G$, on a

$$c[a,b]c^{-1} = caba^{-1}b^{-1}c^{-1} = [cac^{-1}, cbc^{-1}]. \tag{32}$$

Maintenant, si $H \subset G$ est un sous-groupe distingué tel que G/H est abélien, alors pour tout $a, b \in G$, on a que $\overline{[a,b]} = [\overline{a}, \overline{b}] = 0$ dans G/H car c'est un groupe abélien. Donc $[a,b] \in H$ et $D(G) \subset H$. □

Proposition 2.26. *G est résoluble si et seulement si il existe $n \geqslant 0$ tel que $D_n(G) = 0$.*

Proof. S'il existe $n \geqslant 0$ tel que $D_n(G) = 0$, alors la suite dérivée vérifie la définition de résolubilité. Réciproquement, si $G = G_0 \supset G_1 \supset \cdots \supset G_l = 0$ est une suite qui vérifie la définition de résolubilité alors on montre par récurrence le résultat suivant: Pour tout $k \geqslant 0, D_k(G) \subset G_k$. C'est vrai pour $k = 0$. Supposons le résultat vrai pour un indice $k \geqslant 0$ et montrons que $D_{k+1}(G) \subset G_{k+1}$. Par définition on a $D_{k+1}(G) = D(D_k(G))$ et par hypothèse de récurrence $D_k(G) \subset G_k$. Par le lemme 2.25, comme G_k/G_{k+1} est abélien on a que $D_{k+1}(G) \subset G_{k+1}$. En particulier pour $k = l$, on a $D_l(G) \subset G_l = 0$. □

Exercice 2.27. Soit G un groupe et $H \lhd G$ un sous-groupe distingué, alors G est résoluble si et seulement si H et G/H sont résolubles.

Proposition 2.28. *Pour tout $n \geqslant 5$, on a*

$$D(S_n) = A_n \text{ et } D(A_n) = A_n. \tag{33}$$

En particulier, pour tout $n \geqslant 5$, S_n n'est pas résoluble.

Proof. Il est clair que tout commutateur de S_n est de signature 1. On a donc que $D(S_n) \subset A_n$. Comme A_n est engendré par les 3-cycles, il suffit de montrer que tout 3-cycle est un commutateur ce qui prouvera les deux assertions. Soient a,b,c des entiers compris entre 1 et n. Comme $n \geqslant 5$ on peut choisir deux entiers distincts d,e compris entre 1 et n distincts de a,b,c. On a alors

$$(abc) = (ab)(abc)(ab)^{-1}(abc)^{-1} = [(ab),(abc)]. \tag{34}$$

Ceci prouve que (abc) est un commutateur et donc que $S_n = D(A_n)$. Mais ce n'est pas un commutateur de A_n. Mais comme $(de)^2 = \mathrm{id}$ on a

$$(abc) = (ab)(de)(abc)(ab)^{-1}(de)^{-1}(abc)^{-1} = [(ab)(de),(abc)] \tag{35}$$

et donc (abc) est bien un commutateur dans A_n et donc $D(A_n) = A_n$. □

Proposition 2.29. *Pour tout $n \leqslant 4, S_n$ est résoluble.*

Proof. Si $n = 1, S_1 = 1$, ok. Si $n = 2$, alors $S_2 = \{\pm 1\}$ est abélien donc résoluble.

Si $n = 3$, alors $A_3 = \langle (123) \rangle \simeq \mathbf{Z}/3/Z$ et $S_3/A_3 = \mathbf{Z}/2\mathbf{Z}$ donc S_3 est résoluble.

Si $n = 4$, alors A_4 est de taille 12, non abélien. Il possède 8 3-cycles et 3 doubles transpositions de la forme $(ab)(cd)$ avec a,b,c,d deux à deux distincts. Le sous-groupe des doubles transpositions est appelé le *groupe de Klein*, on le note K et on a

$$[A_4, A_4] = K. \tag{36}$$

On a

$$K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}. \tag{37}$$

La suite dérivé de S_4 est alors

$$S_4 \rhd A_4 \rhd K \rhd \{\mathrm{id}\}. \tag{38}$$

Donc S_4 est résoluble. □

3. Un peu de théorie des corps

Définition 3.1. On dit que $(K,+,\cdot)$ est un *corps* si

(i) $\forall a,b \in K, \quad a+b \in K$ et $a+b = b+a$.
(ii) $\exists 0 \in K, \forall a \in K, 0+a = a$.
(iii) $\forall a,b \in K, \quad a \cdot b \in K$ et $ab = ba$.
(iv) $\exists 1 \in K, 1 \cdot a = a$.
(v) $\forall a \in K, \quad a \neq 0 \Rightarrow \exists b \in K, ab = 1$.

Exemple 3.2. Des exemples de corps sont $\mathbf{C}, \mathbf{R}, \mathbf{Q}$. En revanche, $\mathbf{Z}$ n'est pas un corps. Un autre exemple est si K est un corps, alors le corps des fractions rationnelles à n indéterminées $K(t_1, \ldots, t_n)$ est un corps.

Ici, on va supposer que tout nos corps contiennent $\mathbf{Q}$. En particulier, si vous regardez des polycopiés de cours de théorie des cours, il y a la notion de *séparabilité* qui apparaît. C'est un phénomène qu'il faut considérer en caractéristique positive mais pas en caractéristique nulle. Les notions et définitions que je donne ici ne sont valables qu'en caractéristique nulle.

Une *extension de corps* est un morphisme de corps $K \hookrightarrow L$. On dit qu'elle est *finie* si L est un K-espace vectoriel de dimension finie. Soit $x_1, \ldots, x_n \in L$, on dit que L est *engendrée* par $x_1, \ldots, x_n$ si tout élément de L s'écrit comme somme, produit et quotient d'éléments de K et de $x_1, \ldots, x_n$. On note alors

$$L = K(x_1, \ldots, x_n). \tag{39}$$

Si L/K est une extension finie, alors L a une structure de K-espace vectoriel. On note $[L : K] = \dim_K L$, on l'appelle le *degré de l'extension*.

Proposition 3.3 (Multiplicativité des degrés)**.** *Soit $K \hookrightarrow L \hookrightarrow M$ une tour d'extensions, alors*

$$[M : K] = [M : L][L : K]. \tag{40}$$

Proposition 3.4. *Soit L/K une extension finie et $\alpha \in L$. Il existe un unique polynôme unitaire $P_\alpha \in K[X]$ tel que*

$$P_\alpha(\alpha) = 0 \tag{41}$$

et pour tout $Q \in K[X]$ tel que $Q(\alpha) = 0$ on a que P_α divise Q dans $K[X]$.

Proof. On considère le morphisme d'évaluations $ev_\alpha : K[X] \to L$. Ce morphisme a un noyau non-trivial car L est de dimension finie sur K alors que $\dim_K K[X] = +\infty$. Or tout idéal de $K[X]$ est principal, i.e engendré par un seul élément. On peut choisir ce générateur unitaire c'est le polynôme P_α qu'on cherche. □

Proposition 3.5. *Soit K un corps et $P \in K[X]$ un polynôme irréductible. Il existe un unique corps L (à isomorphisme près) tel que L contient une racine α de P et*

$$L = K(\alpha). \tag{42}$$

En particulier, L/K est une extension finie de degré $\deg P$*. On appelle L un* corps de rupture *de P sur K.*

Proof. On donne ici une esquisse de preuve. Considérons l'anneau des polynômes $K[X]$. On peut effectuer la division euclidienne de n'importe quel polynôme par P. En particulier, on peut faire le quotient $K[X]/P$ et c'est le corps L. En effet, si on note α l'image de X dans le quotient, alors il est clair que α est une racine de P et $L = K(\alpha)$. □

Proposition 3.6. *Soit K un corps et $P \in K[X]$ un polynôme, il existe un unique corps (à K-isomorphisme près) K_P tel que P soit scindé dans K_P et $K_P = K(\text{racines de } P)$.*

Proof. On prouve le résultat par récurrence sur le degré de P. Si $\deg P = 1$, alors $K_P = K$ et il est bien unique. Supposons maintenant que P soit de degré $d \geqslant 2$. Par la proposition 3.5, en considérant le corps de rupture d'un facteur irréductible de P on construit $L = K(x)$ de P où x est une racine de

P. On a alors dans L que $P = (X-x)Q(X)$ avec $\deg Q < \deg P$. Par récurrence, il existe un corps de décomposition L_Q de Q sur L et on a

$$L_Q = K(x, \mathrm{Rac}(Q)) = K(\mathrm{Rac}(P)). \tag{43}$$

Montrons maintenant l'uncité. Si K_1, K_2 sont deux corps de décompositions de $P \in K[X]$. Soit $R \in K[X]$ un facteur irréductible de P et soit x_i une racine de R dans K_i. Alors $K(x_i) \subset K_i$ sont deux corps de ruptures de R sur K. On a donc un K-isomorphisme $\sigma : K(x_1) \xrightarrow{\sim} K(x_2)$. On peut donc considérer les extensions $K(x_1) \hookrightarrow K_1$ et $K(x_1) \xrightarrow{\sigma} K(x_2) \hookrightarrow K_2$. On écrit $P = (X-x_1)Q(x)$ avec $\deg Q < \deg P$. On a que K_1 et K_2 sont des corps de décompositions de Q sur $K(x_1)$. Ils sont donc $K(x_1)$-isomorphes par hypothèse de récurrence et donc en particulier K-isomorphes. □

Proposition 3.7. *Soit K un corps et L le corps de décomposition d'un polynôme $P \in K[X]$, alors tout polynôme $Q \in K[X]$ qui a une racine dans L est scindé sur L.*

Proof. Il suffit de montrer le résultat pour tout polynôme Q irréductible. Soit $x \in L$ une racine de Q. Supposons que Q ne soit pas scindé sur L, en considérant un des facteurs irréductibles de Q, on obtient $L(y)$ le corps de rupture d'un de ces facteurs. Considérons également les extensions $K(y)$ et $K(x)$, ce sont deux corps de rupture de Q au-dessus de K. Il existe donc un K-isomorphisme $\sigma : K(x) \xrightarrow{\sim} K(y)$. Maintenant, $L(y)$ est un corps de décomposition de P au-dessus de $K(y)$ et $L = L(x)$ est un corps de décomposition de P au-dessus de $K(x)$. On a donc que $L(y)$ est un corps de décomposition de P au-dessus de $K(x)$ donné par les extensions

$$K(x) \to K(y) \hookrightarrow L(y). \tag{44}$$

Donc $L(y)$ est $K(x)$ isomorphe à $L = L(x)$. En comparant les degrés de ces extensions on a que $L = L(y)$ donc $y \in L$. □

Théorème 3.8 (Théorème de l'élément primitif)**.** *On rappelle que ici un corps contient toujours* **Q**. *Soit L/K une extension finie, alors il existe $\alpha \in L$ tel que*

$$L = K(\alpha). \tag{45}$$

Proof. Il est clair que $L = K(\alpha_1, \ldots, \alpha_n)$ pour certains α_i. Par récurrence il suffit de montrer le résultat lorsque $L = K(x,y)$.

Soient P, Q les polynômes minimaux de x et y sur K. On a que P, Q s'écrivent

$$P = \prod_i (t - x_i) \quad Q = \prod_j (t - y_j) \tag{46}$$

avec $x_1 = x$ et $y_1 = y$. Comme P, Q sont irréductibles on a que les x_i et les y_j sont deux à deux distincts. Comme K est infini, il existe $\lambda \in K$ tels que

$$\lambda \neq \frac{x - x_i}{y - y_j} \tag{47}$$

pour tout i et pour tout $j \neq 1$. On considère $z := x + \lambda y$. On a

$$P(z - \lambda y) = 0, \quad P(z - \lambda y_j) \neq 0, \forall\, j \geqslant 2. \tag{48}$$

Considérons alors les polynômes

$$P(z - \lambda X), Q(X) \tag{49}$$

sur le corps $K(z)$. Ils ont une unique racine en commun qui est $y = y_1$. Par invariance du PGCD on a que le PGCD de ces deux polynômes dans $K(z)[X]$ est $X - y$ et donc $y \in K(z)$. Comme $z = x + \lambda y$ on a également que $x \in K(z)$. □

3.1. **Théorie de Galois.** Soit L/K une extension finie. On définit le *groupe de Galois* de L/K par

$$\mathrm{Gal}(L/K) = \{\sigma \in \mathrm{Aut}(L) : \forall \lambda \in K, \sigma(\lambda) = \lambda\}. \tag{50}$$

Proposition 3.9. *Si L/K est une extension finie, alors*

$$|\mathrm{Gal}(L/K)| \leqslant [L : K] \tag{51}$$

Proof. Par le théorème de l'élément primitif on a que $L = K(\alpha)$. Soit P_α le polynôme minimal de α sur K. On a pour tout $\sigma \in \mathrm{Gal}(L/K)$ que $\sigma(\alpha)$ est également une racine de P. Comme $L = K(\alpha)$, σ est entièrement caractérisé par $\sigma(\alpha)$ et on a autant de choix pour $\sigma(\alpha)$ que de racines de P dans L c'est à dire au plus $[L : K]$ choix. □

Définition 3.10. On dit qu'une extension est *Galoisienne* si $|\mathrm{Gal}(L/K)| = [L : K]$.

Lemme 3.11. *Soit L/K une extension finie, alors L/K est Galoisienne si et seulement si c'est le corps de décomposition d'un polynôme de K.*

Proof. On a que $L = K(\alpha)$ par le théorème de l'élément primitif. Soit P le polynôme minimal de α sur K. Il y a une bijection entre $\mathrm{Gal}(L/K)$ et $\mathrm{Rac}_L(P)$ l'ensemble des racines de P contenues dans L qui est donné par $\sigma \mapsto \sigma(\alpha)$. Si $|\mathrm{Gal}(L/K)| = [L : K] = \deg P$ cela signifie que L contient $\deg(P)$ racines de P et donc que P est scindé sur L. Réciproquement, par la proposition 3.7, P est scindé sur L. On va montrer que pour tout $\beta \in \mathrm{Rac}(P)$, il existe un K-automorphisme de L qui envoie α sur β. On a $L = K(\alpha) = K(\beta)$. En effet, $K(\beta) \subset K(\alpha) = L$ mais $K(\alpha)$ et $K(\beta)$ sont tous les deux des corps de rupture de P, ils sont donc K-isomorphe ce qui implique l'égalité $K(\alpha) = K(\beta)$. On a donc un K-automorphisme $L \to L$ qui envoie α sur β donné par

$$\begin{array}{ccc} L = K(\alpha) & \dashrightarrow & L = K(\beta) \\ & \overset{\sim}{\nwarrow} \quad \overset{\sim}{\nearrow} & \\ & K[X]/(P) & \end{array} \tag{52}$$

Comme L contient les $\deg P$ racines de P on a bien $|\mathrm{Gal}(L/K)| = \deg P = [L : K]$. □

Proposition 3.12 (lemme d'Artin)**.** *Soit L un corps et $H \subset \mathrm{Aut}(L)$ un sous-groupe fini. Soit*

$$L^H := \{\lambda \in L : h(l) = l, \forall h \in H\} \tag{53}$$

le corps fixe de H, alors l'extension $[L : L^H]$ est une extension Galoisienne de degré $|H|$ et de groupe de Galois $\mathrm{Gal}(L/L^H) = H$.

Proof. Soit $x \in L$, posons

$$P(x) = \prod_{h \in H} (X - h(x)). \tag{54}$$

On a que $h(P) = P$ donc $P \in L^H(X)$ et x est une racine de P. Ainsi, tout élément dans L est racine d'un polynôme de degré $\leqslant |H|$. Soit $x \in L$ de degré maximal, on va montrer que $L = L^H(x)$. Soit $y \in L$. On a que $L^H(x,y)$ est finie sur L^H et par le théorème de l'élément primitif on a que

$$L^H(x,y) = L^H(z) \tag{55}$$

pour un certain $z \in L^H(x,y)$. Mais comme $L^H(x)$ est de degré maximal, on a que $L^H(z) = L^H(x)$ donc $y \in L^H(x)$. Comme $y \in L$ est quelconque, on a le résultat.

Ainsi, on a que $[L : L^H] \leqslant |H|$ mais il est clair que $H \subset \mathrm{Gal}(L/L^H)$ de sorte qu'on a $[L : L^H] = |H|$ et $\mathrm{Gal}(L/L^H) = H$. □

Théorème 3.13 (Correspondance de Galois)**.** *Soit L/K une extension Galoisienne de groupe de Galois $G = \mathrm{Gal}(L/K)$, alors on a une bijection*

$$\{\textit{Sous-groupes de } G\} \leftrightarrow \{\textit{Extensions intermédiaires de } L/K\} \tag{56}$$

$$H \subseteq G \quad \mapsto \quad L^H \tag{57}$$

$$\mathrm{Gal}(L/M) \quad \leftarrow \quad L/M/K. \tag{58}$$

De plus, l'extension L^H/K est Galoisienne si et seulement si H est distingué dans G et alors

$$\mathrm{Gal}(L^H/K) = G/H. \tag{59}$$

4. Preuve du théorème

Définition 4.1. Une extension de corps L/K est dite *radicale* s'il existe une suite d'extensions

$$K = K_0 \subset K_1 \subset \cdots \subset K_n = L \tag{60}$$

telle que pour tout i, il existe $x_i \in K_i$ tel que $K_{i+1} = K_i(\sqrt[q_i]{x_i})$.

Définition 4.2. Soit K un corps et $P \in K[X]$, on dit que P est *résoluble par radicaux* s'il est scindé dans une extension radicale de K.

Proposition 4.3. *Soit K un corps et $n \geqslant 1$. Le corps de décomposition de $X^n - 1$ est une extension Galoisienne de groupe de Galois isomorphe à un sous-groupe de $(\mathbf{Z}/n\mathbf{Z})^\times$ et en particulier abélien.*

Proof. Soit L un corps de décomposition de $X^n - 1$. L'extension L/K est alors Galoisienne. Soit $\zeta \in \mu_n(L)$ une racine primitive n-ième de l'unité. Alors $\mu_n(K) = \langle \zeta \rangle$ et $L = K(\zeta)$. Tout $\sigma \in \mathrm{Gal}(L/K)$ est caractérisé par $\sigma(\zeta)$ et on a donc un morphisme de groupe injectif

$$\mathrm{Gal}(L/K) \mapsto \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) = (\mathbf{Z}/n\mathbf{Z})^{\times}. \tag{61}$$

Donc le groupe $\mathrm{Gal}(L/K)$ est abélien. □

Remarque 4.4. Une telle extension est appelée extension *cyclotomique*. Le théorème de Kronecker-Weber affirme que la réciproque est vraie. Toute extension finie de $\mathbf{Q}$ de groupe de Galois abélien est contenue dans une extension cyclotomique.

Proposition 4.5. *Soit K un corps tel que $\mu_n(K)$ est de taille n. Soit L/K une extension Galoisienne, alors* $\mathrm{Gal}(L/K) = \mathbf{Z}/n\mathbf{Z}$ *si et seulement si L est de la forme*

$$L = K(\sqrt[n]{a}) \tag{62}$$

pour un certain $a \in K$ tel que $a \notin K^d$ pour tout $d|n$ et $d > 1$. Le corps L est alors le corps de décomposition de $X^n - a$, ce polynôme est irréductible sur K et L est également son corps de rupture.

Proof. Supposons que $L = K(\sqrt[n]{a})$ avec a vérifiant les hypothèses du théorème. Comme L est le corps de décomposition de $P := X^n - a$, l'extension L/K est Galoisienne par le lemme 3.11. On note $x = \sqrt[n]{a}$, on a alors

$$P = \prod_{\zeta \in \mu_n(K)} (X - \zeta x). \tag{63}$$

Pour montrer le résultat, il suffit de montrer que P est irréductible sur K. Supposons que ce n'est pas le cas. Soit Q une facteur unitaire de P de degré $e > 0$. Son coefficient constant est un produit de e facteurs de la forme ζx avec $\zeta \in K$ donc on a que $x^e \in K$. Maintenant on a également que $x^n = a \in K$ donc par le théorème de Bézout, on a $x^d \in K$ avec $d = pgcd(n, e)$ mais cela contredit l'hypothèse sur a. Ainsi P est irréductible et L est un corps de rupture de P ainsi que son corps de décomposition. On a alors que $\mathrm{Gal}(L/K) = \mathbf{Z}/n\mathbf{Z} = \mu_n(K)$ où $\zeta \mapsto \sigma_\zeta$ est donné par

$$\sigma_\zeta(x) = \zeta x. \tag{64}$$

Réciproquement, si L/K est cyclique d'ordre n, soit $\sigma \in \mathrm{Gal}(L/K)$ un générateur. On a $\sigma^n = \mathrm{id}_L$, comme $X^n - 1$ est scindé à racines simples, l'endomorphisme linéaire induit par σ est diagonalisable. Ses valeurs propres sont des racines n-ièmes de l'unité. Maintenant l'ensemble des valeurs propres de σ est un sous-groupe de $\mu_n(K)$. En effet, si $\sigma(x) = \mu x$ et $\sigma(y) = \zeta y$, alors

$$\sigma(xy^{-1}) = \mu\zeta^{-1}xy^{-1} \tag{65}$$

et $\sigma(1) = 1$. Ce groupe est alors cyclique d'ordre d avec d divisant n. Comme σ est d'ordre n, on a que $d = n$. Donc il existe $x \in L$ tel que $\sigma(x) = \zeta x$ avec ζ une racine primitive de l'unité. Considérons le polynôme

$$P = \prod_i (X - \zeta^i x) = X^n - a \tag{66}$$

avec $a = x^n$. Ce polynôme est invariant par l'action de $\mathrm{Gal}(L/K)$ donc il est à coefficient dans K. En particulier, $a = x^n \in K$ car c'est le coefficient constant de P. Comme $\mathrm{Gal}(L/K)$ agit transitivement sur les racines de P, on a que P est irréductible sur K. Donc son corps de décomposition est une extension de degré $\geqslant n$ contenue dans L donc c'est L. Enfin, si $d > 1$ divise n et $a = b^d$, on a que

$$X^n - a = (X^{n/d})^d - b^d \tag{67}$$

est divisible par $X^{n/d} - b$ donc $b \notin K$. □

Théorème 4.6 (Galois)**.** *Soit K un corps et $P \in K[X]$, on a que P est résoluble par radicaux si et seulement si* $\mathrm{Gal}(P)$ *est résoluble.*

Proof. Supposons tout d'abord que P est résoluble par radicaux. On a alors une suite d'extensions

$$K = K_0 \subset K_1 \subset \cdots \subset K_r = K_P \tag{68}$$

telle que $K_{i+1} = K_i(x_i)$ et $x_i^{d_i} \in K_i$. On souhaiterait appliquer la proposition 4.5 mais on n'a pas forcément que K (ou K_i) contiennent les racines de l'unité nécessaire. Considérons l'extension $K \subset K'$ où on a rajouté toutes les racines $d_1 \cdots d_r$-ièmes de l'unité. C'est une extension Galoisienne de groupe de Galois abélien par la proposition 4.3. On considère de même $K_i \subset K_i'$ l'extension $K_i' \subset K_{i+1}'$ est encore Galoisienne car si $K_{i+1} = K_i(x_i)$, alors $K_{i+1}' = K_i'(x_i)$ avec $x_i^{d_i} \in K_i'$ est c'est une extension Galoisienne de groupe de Galois cyclique par la proposition 4.5. De plus, l'extension $K \subset K_P' = K_r'$ est encore Galoisienne. En effet c'est le corps de décomposition de

$$P \cdot (X^{d_1 \cdots d_r} - 1). \tag{69}$$

Par le théorème de correspondance de Galois, on a que $\mathrm{Gal}(K_P/K)$ est un quotient de $\mathrm{Gal}(K_P'/K)$ donc il suffit de montrer que $\mathrm{Gal}(K_P'/K)$ est résoluble. Or la suite d'extensions

$$K = K_0 \subset K_0' \subset K_1' \subset \cdots \subset K_r' = K_P' \tag{70}$$

donne par le théorème de correspondance de Galois si on note $G_i = \mathrm{Gal}(K_r'/K_i')$

$$\mathrm{Gal}(K_P'/K) \rhd G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{\mathrm{id}\}. \tag{71}$$

Et on a

$$\mathrm{Gal}(K_P'/K)/G_0 = \mathrm{Gal}(K'/K) \tag{72}$$

qui est abélien car c'est une extension cyclotomique et on a

$$G_i/G_{i+1} = \mathrm{Gal}(K_{i+1}'/K_i') \tag{73}$$

qui est cyclique donc abélien par la proposition 4.5. Donc $\mathrm{Gal}(K_P'/K)$ est résoluble.

Réciproquement, supposons que $\mathrm{Gal}(P) = \mathrm{Gal}(K_P/K)$ soit résoluble. On note K' le corps K auquel on a adjoint les racines $[K_P : K]!$ de l'unité et de même pour K_P'. Les extensions $K \subset K', K \subset K_P'$ et $K_P \subset K_P'$ sont Galoisiennes. Par le théorème de correspondance de Galois on a que $\mathrm{Gal}(K_P/K)$ est le quotient de $\mathrm{Gal}(K_P'/K)$ par $\mathrm{Gal}(K_P'/K_P)$. Par la proposition 4.3, on a que $\mathrm{Gal}(K_P'/K_P)$ est abélien et comme $\mathrm{Gal}(K_P/K)$ est résoluble on a que $\mathrm{Gal}(K_P'/K)$ est résoluble. Et donc $\mathrm{Gal}(K_P'/K')$

est également résoluble. On montre que K'_P/K' est une extension radicale ce qui suffira pour conclure car il est claire que $K \subset K'$ est une extension radicale.

On a $[K'_P : K'] \leqslant [K_P : K]$. En effet, si $K_P = K(a)$, alors $K'_P = K'(a)$ et le polynôme minimal de a sur K' divise le polynôme minimal de a sur K. Soit $G = \mathrm{Gal}(K'_P/K')$. Comme G est résoluble, on a une suite de sous-groupes

$$G_0 = G \rhd G_1 \rhd \cdots \rhd G_r = \{1\} \tag{74}$$

telle que G_i/G_{i+1} est abélien. Or un groupe fini abélien est un produit de groupes cycliques donc quitte à raffiner la suite on peut supposer que chaque G_i/G_{i+1} est cyclique. Soit $K_i := K'^{G_i}_P$, on a par la formule de multiplication des degrés que

$$[K'_P : K'] = [K_r : K_{r-1}] \cdots [K_1 : K_0]. \tag{75}$$

Donc si $d_i = [K_i : K_{i-1}]$, alors K_{i-1} contient les racines d_i-ièmes de l'unité et est cyclique d'ordre d_i. On a donc par la proposition 4.5 que $K_i = K_{i-1}(x_{i-1})$ avec $x_{i-1}^{d_i} \in K_{i-1}$ et le théorème est démontré. □

4.1. **Fin de la preuve.** Soit K un corps. On considère le corps $K(t_1, \ldots, t_n)$ des fractions rationnelles à n indéterminées. On définit $\Sigma_1, \ldots, \Sigma_n \in K(t_1, \ldots, t_n)$ de la façon suivante.

$$P_n := (X - t_1) \cdots (X - t_n) = X^n - \Sigma_1 X^{n-1} + \Sigma_2 X^{n-2} + \cdots + (-1)^n \Sigma_n. \tag{76}$$

On a en fait

$$\Sigma_k = \sum_{i_1 < i_2 < \cdots < i_k} t_{i_1} \cdots t_{i_k}. \tag{77}$$

Considérons le sous-corps $K(\Sigma_1, \ldots, \Sigma_n) =: K(\Sigma)$.

Proposition 4.7. *L'extension $K(t_1, \ldots, t_n)/K(\Sigma_1, \ldots, \Sigma_n)$ est Galoisienne de degré $n!$ et de groupe de Galois S_n agissant par permutations de $t_1, \ldots, t_n$.*

Proof. L'extension est Galoisienne car c'est le corps de décomposition de P sur $K(\Sigma)$. Il est clair que S_n fixe tous les Σ_i donc $S_n \subset \mathrm{Gal}\,(K(t_1, \ldots, t_n)/K(\Sigma))$. Maintenant, comme P est de degré n, on a que $\{K(t_1, \ldots, t_n) : K(\Sigma)\} \leqslant n!$. Comme S_n est de taille $n!$ on a égalité et également égalité au niveau du groupe de Galois. □

Corollaire 4.8. *Soit K un corps, l'équation polynomiale générale de degré n est résoluble par radicaux si et seulement si $n \leqslant 4$.*

Proof. Par le théorème de Galois P_n est résoluble par radicaux sur K si et seulement si son groupe de Galois est résoluble. Par la proposition 4.7, le groupe de Galois de P_n est S_n et il n'est résoluble seulement si $n \leqslant 4$. □

4.2. **Un exemple.** On donne l'exemple d'un polynôme de degré 5 dont le groupe de Galois sur $\mathbf{Q}$ est S_5.

Théorème 4.9 (Critère d'Eisenstein)**.** *Soit $P = X^n + a_1X^{n-1} + \cdots + a_0 \in \mathbf{Z}[X]$ tel qu'il existe un nombre premier p tel que*

(1) pour $i = 1, \ldots, n$, p divise a_i.
(2) p^2 ne divise pas a_0.

Alors P est irréductible dans $\mathbf{Q}[X]$.

Proof. Si ce n'est pas le cas, alors on peut écrire $P = QR$ avec $Q, R \in \mathbf{Q}[X]$ non constants. Par un argument arithmétique, on peut en fait se ramener à $Q, R \in \mathbf{Z}[X]$. On considère alors la réduction modulo p. On a dans ce cas

$$\overline{P} = \overline{Q} \cdot \overline{R} = X^n. \tag{78}$$

Par unicité de la décomposition en facteurs premiers (on rappelle que $\mathbf{Z}/p\mathbf{Z}$ est un corps), on a qu'il existe $k \geqslant 1$ tel que $\overline{Q} = X^k$ et $\overline{R} = X^{n-k}$. Mais alors les coefficients constants de Q et de R sont divisibles par p et on aurait que p^2 divise a_0. □

Considérons le polynôme $P = X^5 - 40X + 2$. Il est irréductible par le critère d'Eisenstein (avec $p = 2$). Le polynôme dérivé est $P' = 5X^4 - 40$, une étude des variations montrent que P admet 3 racines réelles $x_1 < x_2 < x_3$. Les deux autres racines de P sont donc complexes conjuguées on les note x_4, x_5. On a donc que $\mathrm{Gal}(P)$ contient la conjugaison complexe qui agit comme la transposition (45). De plus, $\mathbf{Q}(x_1)$ est un corps de rupture de P sur $\mathbf{Q}$ de degré 5. Donc le cardinal de $\mathrm{Gal}(P) \subset S_5$ est divisible par 5. Donc $\mathrm{Gal}(P)$ contient un élément d'ordre 5 mais dans S_5 ça ne peut être que un 5-cycle. Donc $\mathrm{Gal}(P) \subset S_5$ contient un 5-cycle et une transposition, c'est tout S_5.

REFERENCES

[Deba] Olivier Debarre. Algèbre 1. https://perso.imj-prg.fr/olivier-debarre/wp-content/uploads/debarre-pub/Algebre1.pdf.

[Debb] Olivier Debarre. Algèbre 2. https://perso.imj-prg.fr/olivier-debarre/wp-content/uploads/debarre-pub/Algebre2.pdf.