Éléments de Théorie de Galois

Arthur Garnier

13 juillet 2015

Table des matières

I Compléments de théorie des groupes et extensions de corps **5**

1 Groupes résolubles **5**
1.1 Sous-groupes caractéristiques et groupe dérivé 5
1.2 Suites de composition et groupes résolubles 7

2 Extensions de corps **11**
2.1 Extensions algébriques et transcendantes 11
2.2 Constructions à la règle et au compas 16
2.3 Corps de rupture, corps de décomposition et clôture algébrique 20
2.4 Racines de l'unité et polynômes cyclotomiques 26
2.5 Corps finis 36
2.6 Extensions normales et extensions séparables 41

II Théorie de Galois et Applications **51**

3 Introduction à la Théorie de Galois **51**
3.1 Extensions galoisiennes et groupes de Galois 51
3.2 Lemme d'Artin et Correspondance de Galois 58
3.3 Théorème de Kummer 62

4 Applications aux polygones et aux équations algébriques **64**
4.1 Polygones constructibles 64
4.2 Equations résolubles par radicaux 66

Annexe **73**

Introduction

Dans ce cours, nous proposons une initiation à la Théorie de Galois qui fût introduite par Évariste Galois en 1829 dans son
Mémoire sur les conditions de résolubilité des équations par radicaux.
Elle est issue de l'idée géniale de Galois qui consiste à analyser les racines d'un polynôme en les faisant permuter. L'ensemble des permutations de ces racines possède une structure particulière : celle de groupe. C'est alors que sont nées la théorie des corps ainsi que la théorie des groupes. Galois énonce également des conditions de résolubilité des équations algébriques, c'est-à-dire du type $P(X) = 0$ avec P un polynôme, au travers du groupe de permutations des racines de P. Nous proposons ici une formulation moderne et abstraite des idées de Galois.

Avant toute chose, nous introduisons la notion de groupes résolubles dont nous aurons besoin. Notons que ces groupes doivent justement leur nom à la relation qu'il ont avec les équations algébriques dites elles aussi "résolubles". Nous supposons connues du lecteur les bases de la théorie des groupes, en particulier les notions de sous-groupes distingués, de groupes quotients et d'action de groupes.

On se propose, par la suite, de familiariser le lecteur avec le concept d'extension de corps, que nous étudions en détail. Nous y prouvons notamment le théorème de Steinitz sur les clotûres algébriques. Là encore, on suppose que le lecteur a déjà étudié la théorie des anneaux commutatifs, ainsi que la théorie des anneaux de polynômes.

Ensuite, après avoir présenté un apreçu de la Théorie de Galois pure, nous nous intéresserons à deux de ses applications les plus spectaculaires dont la deuxième constitue même la raison d'être de ladite théorie. Nous étudierons entre autres le lemme d'Artin, la correspondance de Galois ainsi que les théorèmes de Galois et d'Abel-Galois concernant les équations algébriques.

Afin d'être le plus autonome possible, ce cours possède une Annexe dans laquelle on démontre des résultats indispensables, mais qui ne font pas nécessairement partie des cours "canoniques" sur les notions utilisées. On y prouve en particulier le théorème fondamental sur les polynômes symétriques.

Enfin, le lecteur intéressé par la vie passionnante d'Évariste Galois pourra lire, par exemple, le livre Évariste de François-Henri Désérable.

Notations

Pour un groupe $(G, \cdot)$, on notera :

1. $\mathrm{Aut}(G)$ le groupe des automorphismes de G.
2. Si H est un sous-groupe de G, on écrit $H \leq G$ et $H < G$ si H est propre.
3. Si, de plus, H est distingué dans G (ie $\forall g \in G,\ gHg^{-1} = H$), on notera $H \trianglelefteq G$.
4. Le groupe cyclique d'ordre $n \in \mathbb{N}^*$ sera noté $C_n \simeq \mathbb{Z}/n\mathbb{Z}$.
5. Pour un élément $x \in G$, on note $o(x)$ l'ordre de x (ie le plus petit entier n tel que $x^n = e$).
6. Si $E \subseteq G$, on note $\langle E \rangle$ le sous-groupe de G engendré par E.
7. Pour $n \in \mathbb{N}^*$, le groupe des perumations de l'ensemble $\{1, \ldots, n\}$ sera noté $\mathfrak{S}_n$ et le sous-groupe (distingué) des permutations paires (ie de signature positive) sera noté $\mathfrak{A}_n$.

Sauf mention contraire, tout anneau et tout corps sera commutatif. De plus, pour un anneau A et un corps k, on écrira :

1. $\mathrm{Frac}(A)$ le corps des fractions de A (voir Annexe).
2. $k[X]$ l'anneau des polynômes à coefficients dans k.
3. $k(X)$ le corps des fractions rationnelles à coefficients dans k et on a $k(X) = \mathrm{Frac}(k[X])$.

Première partie
Compléments de théorie des groupes et extensions de corps

1 Groupes résolubles

1.1 Sous-groupes caractéristiques et groupe dérivé

Dans cette section, on se donne un groupe $(G, \cdot)$ fixé.

Définition 1. Soit $H \leq G$. On dit que H est caractéristique dans G et on note $H \sqsubseteq G$ si :

$$\forall \alpha \in \mathrm{Aut}(G),\ \alpha(H) = H.$$

Proposition 1. *Soient $H, K \leq G$. On a :*

1. $H \sqsubseteq G \ \Rightarrow\ H \trianglelefteq G$,
2. $K \sqsubseteq H \sqsubseteq G \ \Rightarrow\ K \sqsubseteq G$.
3. $K \sqsubseteq H \trianglelefteq G \ \Rightarrow\ K \trianglelefteq G$.

Démonstration. 1. Soit $g \in G$. L'application

$$\begin{array}{rccc} \gamma_g & : & G & \to & G \\ & & x & \mapsto & gxg^{-1} \end{array}$$

est un automorphisme de G et comme H est caractéristique, on a $\gamma_g(H) = H$, soit $gHg^{-1} = H$ et ce, pour tout $g \in G$, donc H est distingué dans G.

2. Soit $\alpha \in \mathrm{Aut}(G)$. Comme $\alpha(H) = H$, $\alpha_{|H}$ est un automorphisme de H et donc $\alpha_{|H}(K) = K = \alpha(K)$, donc K est caractéristique.

3. Soit $\sigma \in \mathrm{Aut}(G)$ un automorphisme intérieur de G. On a $\sigma_{|H} \in \mathrm{Aut}(H)$, donc $\sigma_{|H}(K) = K$, donc $K \trianglelefteq G$.

□

Proposition-Définition 1. *Dans G, il existe un unique sous-groupe normal G' minimal parmis les $N \trianglelefteq G$ tels que G/N soit abélien. On l'appelle le groupe dérivé de G.*

Démonstration. L'unicité étant évident par définition, montrons l'existence. On pose

$$E := \{N \trianglelefteq G \ ; \ G/N \ \textit{abélien}\}$$

On a $G \in E \neq \emptyset$. Soit $(N_i)_{i\in I}$ une chaîne de E (ie un sous-ensemble totalement ordonné de E). Posons encore

$$N_0 := \bigcap_{i\in I} N_i.$$

Alors N_0 est distingué dans G et $G/\bigcap_{i\in I} N_i$ est abélien. Donc N_0 est un minorant de $(N_i)_{i\in I}$, donc E est inductif. On en déduit l'existence de G' d'après le lemme de Zorn. □

Définition 2. Pour $x, y \in G$, on appelle commutateur de x et y l'élément de G défini par $[x, y] := xyx^{-1}y^{-1}$.

Théorème 1. $G' = \left\langle \ [x, y]_{x,y\in G} \ \right\rangle$

Démonstration. On note $D(G) := \left\langle \ [x, y]_{x,y\in G} \ \right\rangle$, il s'agit de montrer que $D(G)$ est le sous-groupe normal minimal tel que le quotient soit abélien. Soient $x, y, z \in G$. On a

$$z[x, y]z^{-1} = zxyx^{-1}y^{-1}z^{-1} = zxz^{-1}zyz^{-1}zx^{-1}z^{-1}zy^{-1}z^{-1} = [zxz^{-1}, zyz^{-1}]$$

donc $D(G) \trianglelefteq G$. Soit $N \trianglelefteq G$. Dire que G/N est abélien signifie que

$$\forall \overline{x}, \overline{y} \in G/N, \ \overline{xy} = \overline{yx} \ \Leftrightarrow \ [x, y] = xyx^{-1}y^{-1} \in N.$$

D'où G/N abélien si et seulement si $D(G) \in N$. Par unicité, $G' = D(G)$. □

Définition 3. On note $(G^{(n)})_{n\in\mathbb{N}}$ la suite des groupes dérivés de G définie par

$$\begin{cases} G^{(0)} := G, \\ G^{(1)} := G', \\ \forall n \in \mathbb{N}, \quad G^{(n+1)} := (G^{(n)})'. \end{cases}$$

Remarque 1. On obtient ainsi une suite décroissante de sous-groupes :

$$G = G^{(0)} \trianglerighteq G' \trianglerighteq G'' \trianglerighteq \cdots \trianglerighteq G^{(n)} \trianglerighteq G^{(n+1)} \trianglerighteq \cdots$$

Lemme 1.

$$\forall n \in \mathbb{N},\ G^{(n)} \sqsubseteq G.$$

Démonstration. On procède par récurrence :

Initialisation Montrons que G' est caractéristique dans G. Soit donc $\alpha \in \mathrm{Aut}(G)$. On a

$$\forall x, y \in G,\ \alpha([x,y]) = \alpha(xyx^{-1}y^{-1}) = \alpha(x)\alpha(y)\alpha(x)^{-1}\alpha(y)^{-1} = [\alpha(x), \alpha(y)],$$

d'où $\alpha(G') \subseteq G'$. On obtient l'inclusion réciproque en considérant $\alpha^{-1} \in \mathrm{Aut}(G)$. Par suite, $\alpha(G') = G'$, et G' est caractéristique.

Hérédité Supposons que $G^{(n)}$ est caractéristique dans G et montrons que $G^{(n+1)}$ l'est aussi. D'après l'initialisation, $G^{(n+1)} \sqsubseteq G^{(n)}$ et par hypothèse de récurrence, $G^{(n)} \sqsubseteq G$, donc d'après la Proposition 1-2), $G^{(n+1)} \sqsubseteq G$, d'où le résultat. □

1.2 Suites de composition et groupes résolubles

Définition 4. Soit $(G, \cdot)$ un groupe. On appelle suite de composition de G toute famille finie de sous-groupes $(G_i)_{0\leq i\leq n}$ telle que :

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_i \trianglerighteq G_{i+1} \trianglerighteq \cdots \trianglerighteq G_{n-1} \trianglerighteq G_n = \{e\}.$$

Les groupes $(G_i/G_{i+1})_{0\leq i\leq n-1}$ sont appelés les quotients de la suite et n sa longueur. De plus, on dit que la suite est normale si $\forall 0 \leq i \leq n,\ G_i \trianglelefteq G$ et qu'elle est abélienne si tous les quotients sont abéliens.

Définition 5. On dit qu'un groupe G est résoluble s'il admet une suite de composition abélienne.

Remarque 2.
1. Si G est un groupe abélien, la suite de composition $G \trianglerighteq \{e\}$ est abélienne, donc tout groupe abélien est résoluble. En particulier, tout groupe monogène ou cyclique est résoluble.
2. La suite $(G^{(n)})_{n\in\mathbb{N}}$ étant décroissante, elle est stationnaire à $\{e\}$ si et seulement si $G^{(m)} = \{e\}$ pour au moins un $m \in \mathbb{N}$.

On dispose du résultat pratique suivant :

Théorème 2. *Un groupe G est résoluble si et seulement s'il existe $n \in \mathbb{N}$ tel que $G^{(n)} = \{e\}$.*

Démonstration. Supposons que G est résoluble et soit $(G_i)_{0\leq i\leq n}$ une suite de composition abélienne de G. Quitte à supprimer des termes, on peut la supposer strictement décroissante. On a que G/G_1 est abélien, donc $G' \leq G_1$ ce qui implique $G'' \leq G_1'$. Ensuite G_1/G_2 abélien entraîne $G_1' \leq G_2$ donc $G'' \leq G_2$. On voit, par récurrence, que $G^{(i)} \leq G_i,\ \forall 0 \leq i \leq n$, d'où $G^{(n)} \leq G_n = \{e\}$. Réciproquement, si $n \in \mathbb{N}$ est le plus petit entier tel que $G^{(n)} = \{e\}$ alors la suite $(G^{(i)})_{0\leq i\leq n}$ est une suite de composition et elle est abélienne par définition du groupe dérivé. G est donc résoluble. □

Théorème 3. *Tout sous-groupe et tout quotient d'un groupe résoluble est résoluble.*

Démonstration. Soit H un sous-groupe de G. On a $H \leq G \ \Rightarrow\ H' \leq G' \ \Rightarrow\ H^{(i)} \leq G^{(i)},\ \forall i \in \mathbb{N}$. Donc si G est résoluble, H l'est aussi d'après le Théorème précédent. Soit maintenant $N \trianglelefteq G$ et montrons que G/N est résoluble. On note $\pi : G \twoheadrightarrow G/N$ la surjection canonique (ie $\forall x \in G, \pi(x) = \overline{x}$). On a

$$\forall \overline{x}, \overline{y} \in G/N,\ [\overline{x}, \overline{y}] = \overline{x}\ \overline{y}\ \overline{x}^{-1}\overline{y}^{-1} = \overline{xyx^{-1}y^{-1}} = \overline{[x, y]},$$

donc

$$(G/N)' = \pi(G') \ \Rightarrow\ \forall i \in \mathbb{N},\ (G/N)^{(i)} = \pi(G^{(i)}).$$

Donc, si G est résoluble, G/N l'est aussi d'après le Théorème précédent. □

Théorème 4. *Les assertions suivantes sont équivalentes :*

1. *G est résoluble*
2. *G admet une suite de compostition abélienne et normale*

Démonstration. L'implication 2. $\Rightarrow$ 1. étant claire, montrons que 1. $\Rightarrow$ 2.. Si G est résoluble, la suite des groupes dérivés est une suite de composition abélienne et comme chaque dérivé est caractéristique dans G (Lemme 1), il est distingué (Proposition 1-1.), la suite est donc normale. □

Corollaire 1. *Les seuls groupes simples résolubles sont les groupes cycliques d'ordre premier.*

Pour démontrer ceci, nous avons besoin du :

Lemme 2. *Les seuls groupes simples abéliens sont les $C_p,\ p \in \mathbb{P}$.*

Démonstration. Les C_p sont clairement simples et abéliens pour p premier. Soit donc un groupe H simple et abélien. Comme H est simple, $H \neq \{e\}$ et $\exists x \in H \setminus \{e\}$ et $\langle x \rangle \trianglelefteq H \ \Rightarrow\ H = \langle x \rangle$ donc H est monogène et comme il est simple, il est cyclique : $H \simeq C_n$ pour un $n \in \mathbb{N}$. Enfin, H étant simple, n est premier. □

Nous pouvons démontrer le corollaire :

Démonstration. Si G est simple, sa seule suite de composition strictement décroissante est $G \trianglerighteq \{e\}$ et comme G est résoluble, il est abélien. G est donc un groupe simple abélien, c'est un C_p pour un certain $p \in \mathbb{P}$ d'après le Lemme précédent. □

Théorème 5. *Soit G un groupe non trivial. Alors G est résoluble si et seulement s'il existe un sous-groupe distingué propre $N \triangleleft G$ tel que N et G/N soient résolubles.*

Démonstration. Si G est résoluble, alors $G' \lhd G$ est résoluble comme sous-groups d'un groupe résoluble et G/G' étant abélien, il est aussi résoluble et $N := G'$ convient. Réciproquement, on suppose qu'il existe $N \lhd G$ résoluble tel que G/N soit résoluble. Il existe donc deux suites de compositions :

$$N = N_0 \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_n = \{e\},$$

$$G/N = G_0/N \trianglerighteq G_1/N \trianglerighteq \cdots \trianglerighteq G_m/N = \{\overline{e}\},$$

telles que N_i/N_{i+1} et $(G_j/N)/(G_{j+1}/N)$ soient abéliens. Or, d'après le théorème d'isomorphie, on a $(G_j/N)/(G_{j+1}/N) \simeq G_j/G_{j+1}$, donc la suite de composition

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_{m-1} \trianglerighteq N = N_0 \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_n = \{e\}$$

est une suite de composition abélienne pour G, qui est donc résoluble. □

Proposition 2. *Le groupe symétrique $\mathfrak{S}_n$ est résoluble pour $1 \leq n \leq 4$.*

Démonstration. Si $n = 1$, il n'y a rien à montrer. Si $n = 2$, $\mathfrak{S}_2 \simeq C_2$ est résoluble. Si $n = 3$, la suite de composition $\mathfrak{S}_3 \trianglerighteq \mathfrak{A}_3 \trianglerighteq \{id\}$ est abélienne car $\mathfrak{S}_3/\mathfrak{A}_3 \simeq C_2$ et $\mathfrak{A}_3 \simeq C_3$. Si $n = 4$, soient $V := \{id, (12)(34), (13)(24), (14)(23)\}$ et $W \leq V$ un sous-groupe de V d'ordre 2. On vérifie aisément que $V \trianglelefteq \mathfrak{S}_4$, donc $V \trianglelefteq \mathfrak{A}_4$, on obtient ainsi un suite de composition :

$$\mathfrak{S}_4 \trianglerighteq \mathfrak{A}_4 \trianglerighteq V \trianglerighteq W \trianglerighteq \{id\}$$

dont tous les quotients sont d'ordre 2 ou 3, donc abéliens, $\mathfrak{S}_4$ est donc résoluble. □

Proposition 3. *$\mathfrak{A}_n$ n'est pas résoluble pour $n \geq 5$.*

Démonstration. Soit un 3-cycle $(abc) \in \mathfrak{A}_n$. Comme $n \geq 5$, il existe $d, e \in \{1, \ldots, n\}$ distincts de a, b, c. On a

$$(abc) = (adc)(bec)(acd)(bce) = (adc)(bec)(adc)^{-1}(bec)^{-1} = [(adc), (bec)] \in \mathfrak{A}'_n.$$

Or, $\mathfrak{A}_n = \langle ((abc))_{1 \leq a,b,c \leq n} \rangle$, donc $\mathfrak{A}_n \leq \mathfrak{A}'_n$ et donc $\mathfrak{A}'_n = \mathfrak{A}_n$. On en déduit que pour tout $i \in \mathbb{N}$, $\mathfrak{A}_n^{(i)} = \mathfrak{A}_n$ et ainsi que $\mathfrak{A}_n$ n'est pas résoluble d'après le Théorème 2. □

Théorème 6. *Le groupe symétrique $\mathfrak{S}_n$ est résoluble si et seulement si $n \leq 4$.*

Démonstration. Si $1 \leq n \leq 4$, $\mathfrak{S}_n$ est résoluble d'après la Proposition 2. Si $n \geq 5$, $\mathfrak{S}_n$ n'est pas résoluble car s'il l'était, $\mathfrak{A}_n \leq \mathfrak{S}_n$ le serait également en vertu du Théorème 3, or la Proposition 3 montre que ce n'est pas le cas. □

2 Extensions de corps

2.1 Extensions algébriques et transcendantes

Définition 6. Soient k et K deux corps. On dit que K est une extension de k et on note K/k s'il existe un plongement (ie un monomorphisme) $\varphi : k \hookrightarrow K$ tel que $k \simeq \mathrm{Im}(\varphi)$ et on notera parfois abusivement $k \subseteq K$.
De plus, si K/k et L/k sont deux extensions, on dit que L/k est une sous-extension de K/k si $L \subseteq K$.
Enfin, une suite d'extensions emboîtées $k \subseteq k_1 \subseteq \cdots \subseteq k_n \subseteq \cdots$ sera appelée une tour de corps.

Définition 7. Soient K/k une extension de corps et $\emptyset \neq E \subseteq K$. On notera

$$k[E] := \bigcap_{\substack{A \subseteq K \text{ anneau} \\ E \subseteq A}} A, \quad k(E) := \bigcap_{\substack{L/k \subseteq K/k \\ E \subseteq L}} L.$$

$k[E]$ (resp. $k(E)$) est alors le plus petit sous-anneau (resp. sous-corps) de K contenant k et E et $k(E)$. Par ailleurs, si $E = \{\alpha_1, \ldots, \alpha_n\}$ on écrit $k[E] = k[\alpha_1, \ldots, \alpha_n]$ et $k(E) = k(\alpha_1, \ldots, \alpha_n)$ et on dit alors que l'extension $k(E)/k$ est de type fini. Enfin, si $E = \{\alpha\}$, on dit que $k(\alpha)/k$ est une extension simple.

Une simple récurrence nous conduit immédiatement à :

Proposition 4. *Pour tout $n \in \mathbb{N}^*$ et tous $\alpha_1, \ldots, \alpha_n \in K$, on a $k(\alpha_1, \ldots, \alpha_n) = k(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$.*

Proposition 5. *Soient K/k une extension et $\alpha \in K$. On a*

$$k(\alpha) = \left\{ \frac{P(\alpha)}{Q(\alpha)},\ P, Q \in k[X],\ Q(\alpha) \neq 0 \right\}.$$

Démonstration. Le membre de droite est un sous-corps de K contenant k et α inclus dans $k(\alpha)$, d'où le résultat. □

Définition 8. Soit K/k une extension de corps. On peut voir K comme un espace vectoriel sur k et ainsi considérer sa dimension sur k. On définit alors le degré de l'extension K/k et on note $[K : k]$ le nombre (éventuellement infini) :

$$[K : k] := \dim_k K,$$

et on dit que l'extension K/k est finie si $[K : k] < \infty$.

Proposition 6. *Soient L/K et K/k deux extensions finies. Alors L/k est finie et on a*

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

Démonstration. On pose $n := [K : k]$ et $m := [L : K]$ et soient $(u_i)_{1 \leq i \leq n}$ une base de K sur k et $(v_j)_{1 \leq j \leq m}$ une base de L sur K. Soit $x \in L$. Il existe $(a_j)_{1 \leq j \leq m}$ dans K tels que $x = \sum_{j=1}^{m} a_j v_j$ et $a_j \in K$ donc pour tout $1 \leq j \leq m$, il existe $(a_{i,j})_{1 \leq i \leq n}$ dans k tels que $a_j = \sum_{i=1}^{n} a_{i,j} u_i$, donc

$$x = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} a_{i,j} u_i v_j,$$

et donc $L = \mathrm{Vect}_k(u_i v_j)_{i,j}$. Ensuite, s'il existe $x_{i,j} \in k$ tels que

$$\sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} x_{i,j} u_i v_j = 0 \ \Rightarrow \ \sum_{1 \leq j \leq m} \left(\sum_{1 \leq i \leq n} x_{i,j} u_i \right) v_j = 0 \ \Rightarrow \ \sum_{1 \leq i \leq n} x_{i,j} u_i = 0$$

$$\Rightarrow \ x_{i,j} = 0, \ \forall i, j.$$

Donc $(u_i v_j)_{i,j}$ est une base de L sur k. On en déduit que

$$[L : k] = \dim_k L = \text{card}((u_i v_j)_{(i,j)\in\{1,\dots,n\}\times\{1,\dots,m\}}) = nm = [L : K][K : k] < \infty.$$

□

Proposition 7. *Toute extension finie est de type finie.*

Démonstration. Soit K/k une extension finie. Il existe $\alpha_1, \dots, \alpha_n \in K$ tels que $K = \text{Vect}_k(\alpha_1, \dots, \alpha_n)$ et on a alors $K = k(\alpha_1, \dots, \alpha_n)$ est bien de type finie. □

Définition 9. Soient K/k et L/k deux extensions et $\varphi : K \to L$ un morphisme de corps. On dit que φ est un k-homomorphisme si $\varphi_{|k} = id_k$. Un k-isomorphisme est par définition un k-homomorphisme qui est aussi un isomorphisme de corps. De plus, s'il existe un k-isomorphisme entre K et L, on dit que les deux extensions sont k-isomorphes et on note $K \simeq_k L$.

Définition 10. Soient K/k une extension, $\alpha \in K$ et φ_α le morphisme

$$\begin{array}{rccc} \varphi_\alpha & : & k[X] & \to & K \\ & & P & \mapsto & P(\alpha) \end{array}$$

Si φ_α est injectif, on dit que α est transcendant sur k et qu'il est algébrique sinon. De plus, on dit que l'extension K/k est algébrique si tout $\alpha \in K$ est algébrique sur k et transcendante sinon.

Lemme 3. *Toute extension finie est algébrique.*

Démonstration. Soient K/k une extension finie et $\alpha \in K \setminus \{0\}$. K/k étant finie, la famille $\{\alpha^n, \ n \in \mathbb{N}\}$ est liée, donc il existe $P \in k[X] \setminus \{0\}$ tel que $P(\alpha) = 0$, donc $\text{Ker}(\varphi_\alpha) \neq \{0\}$ et α est donc algébrique et 0 étant aussi algébrique sur k, l'extension K/k est bien algébrique. □

Lemme 4. *Si $\alpha \in K$ est algébrique, alors $k(\alpha)$ est une extension algébrique.*

Démonstration. Si α est algébrique, il existe $a_1, \ldots, a_n \in k$ non tous nuls tels que $\sum_{i=1}^{n} a_i \alpha^i = 0$, alors $k(\alpha) = \mathrm{Vect}_k(1, \alpha, \ldots, \alpha^{n-1})$ est une extension finie, donc algébrique d'après le Lemme 3. □

Lemme 5. *$\alpha_1, \ldots, \alpha_n \in K$ sont algébriques si et seulement si $k(\alpha_1, \ldots, \alpha_n)$ est finie.*

Démonstration. La condition suffisante est claire d'après le Lemme 3 et la condition nécessaire s'obtient en effectuant une récurrence à partir du Lemme 4. □

Proposition 8. *Soient K/k une extension et $\alpha \in K$. Les essertions suivantes sont équivalentes :*

1. *α est transcendant sur k,*
2. *On a $k(\alpha) \simeq_k k(X)$ et $k[\alpha] \simeq_k k[X]$.*

Démonstration. Supposons que α est transcendant sur k. φ_α est donc injectif et on a bien $k[\alpha] \simeq_k k[X]$. De plus, d'après la Proposition 5 on a

$$k(\alpha) = \left\{ \frac{P(\alpha)}{Q(\alpha)},\ Q(\alpha) \neq 0 \right\} = \{R(\alpha),\ R \in k[X]\},$$

donc l'application $\psi_\alpha : k(X) \to k(\alpha),\ R \mapsto R(\alpha)$ est un k-isomorphisme. Inversement, comme la famille $\{X^n,\ n \in \mathbb{N}\}$ étant libre dans $k[X] \hookrightarrow k(X)$, l'extension $k(X)$ est infinie, donc $k(\alpha) \simeq_k k(X)$ est une extension infinie. Or, si α était algébrique, $k(\alpha)$ serait finie d'après le Lemme 4, ce qui n'est pas le cas ; α est donc transcendant. □

Corollaire 2. *Deux extensions simples transcendantes d'un corps k sont k-isomorphes.*

Corollaire 3. *Si $\alpha \in K$ est transcendant, alors $k(\alpha) = Frac(k[\alpha])$.*

Démonstration. D'après la Proposition 8 on a

$$k(\alpha) \simeq k(X) = \mathrm{Frac}(k[X]) \simeq \mathrm{Frac}(k[\alpha]),$$

d'où le résultat. □

Théorème 7. *Soient K/k une extension et $\alpha \in K$. Les assertions suivantes sont équivalentes :*

1. *α est algébrique sur k,*
2. *Il existe un unique polynôme $P \in k[X] \setminus \{0\}$ unitaire irréductible tel que $P(\alpha) = 0$ et vérifiant :*

$$\forall Q \in k[X] \setminus \{0\},\ Q(\alpha) = 0 \ \Leftrightarrow\ P|Q,$$

3. *$[k(\alpha) : k] = \deg P < \infty$,*
4. *$k[\alpha] = k(\alpha)$*

Démonstration. 1. $\Rightarrow$ 2. On a $\{0\} \neq \mathrm{Ker}(\varphi_\alpha)$ est un idéal propre de l'anneau principal $k[X]$ donc il existe un polynôme $P \in k[X] \setminus \{0\}$ que l'on peut supposer unitaire (il est alors unique) tel que $\mathrm{Ker}(\varphi_\alpha) = (P)$ et le théorème d'isomorphie implique que $k[X]/(P) \simeq k[\alpha]$ et comme $k[\alpha]$ est intègre, l'idéal (P) est premier et donc P est irréductible et on a bien $P(\alpha) = 0$.
2. $\Rightarrow$ 1. C'est clair.
1. $\Rightarrow$ 4. Si α est algébrique, soit $P \in k[X]$ le polynôme du 2. et $Q \in k[X]$ tel que $Q(\alpha) \neq 0$. P ne divise pas Q et P étant irréductible, on a $P \wedge Q = 1$, donc il existe $U, V \in k[X]$ tels que $PU + QV = 1$ d'après le théorème de Bézout appliqué dans l'anneau principal $k[X]$. On a alors $Q(\alpha)V(\alpha) = 1$ et $Q(\alpha) \in k[\alpha]^*$ et donc $k[\alpha] = k(\alpha)$.
4. $\Rightarrow$ 1. Supposons, par l'absurde, que α soit transcendant. Alors, d'après la Proposition 8, on a $k[X] \simeq k[\alpha] = k(\alpha) \simeq k(X)$, donc $k[X] \simeq k(X)$, ce qui est absurde ; donc α est algébrique.
1. $\Rightarrow$ 3. On considère le polynôme P du 2. et on pose $d := \deg P$. La famille $\{1, \alpha, \ldots, \alpha_{d-1}\}$ est libre car sinon il existe $a_i \in k$ tels que $a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} = 0$ et si $g(X) := a_0 + a_1X + \cdots + a_{d-1}X^{d-1} \neq 0$, alors $g(\alpha) = 0$ et

donc $P|g$, ce qui est absurde. Soit ensuite $f(\alpha) \in k[\alpha]$, $(f \in k[X])$, et il existe $Q, R \in k[X]$ tels que $\deg R < \deg P = d$ et $f(X) = P(X)Q(X) + R(X)$ donc $f(\alpha) = R(\alpha)$ et $k[\alpha] = \mathrm{Vect}_k(1, \alpha, \ldots, \alpha^{d-1})$ et $k[\alpha] = k(\alpha)$ d'après 4. donc $[k(\alpha) : k] = d$.
3. $\Rightarrow$ 1. C'est le Lemme 3. □

Définition 11. Soient K/k une extension de corps et $\alpha \in K$ algébrique sur k. Alors le polynôme irréductible unitaire $P \in k[X] \setminus \{0\}$ du Théorème 7 sera appelé le polynôme minimal de α sur k et sera noté $\mu_{\alpha,k}$. De plus, on appelera le degré de α sur k le nombre $\deg_k \alpha := \deg \mu_{\alpha,k} = [k(\alpha) : k]$.

2.2 Constructions à la règle et au compas

Nous allons ici donner une première application des extensions de corps : les problèmes de constructibilité à la règle et au compas avec, entre autres, pour but de démontrer l'impossibilité de la trisection de l'angle, la duplication du cube et la quadrature du cercle. On commence par définir ce qu'est un "point constructible".

Définition 12. Soit Σ un sous-ensemble de $\mathbb{R}^2$ contenant $(0,0)$ et $(1,0)$. On dit qu'un point $P \in \mathbb{R}^2$ est constructible à partir de Σ s'il peut être obtenu par une suite finie d'opérations du type :

1. Intersection de deux droites non parallèles passant chacune par deux points déjà construits,
2. Intersection de deux cercles de centre distincts construits et passant chacun par un point construit,
3. Intersection d'une droite passant par deux points construits et d'un cercle dont le centre est construit et passant par un point construit.

De plus, on dit qu'une droite est constructible à partir de Σ si elle passe par deux points constructibles et qu'un cercle est constructible à partir de Σ si il est de centre constructible et s'il passe par un point constructible. De plus, on dit qu'un point (resp. une droite, un cercle) est constructible s'il est constructible à partir de $\Sigma = \{(0,0), (1,0)\}$. Enfin, on dit que $x \in \mathbb{R}$ est constructible si le point $(x, 0)$ est constructible.

Proposition 9. *Sont constructibles ;*

1. *Tout $n \in \mathbb{Z}$,*
2. *Tout rationnel,*
3. *Le milieu de deux points constructibles,*
4. *La médiatrice de deux points constructibles,*
5. *La bissectrice de deux droites constructibles non parallèles,*
6. *La droite perpendiculaire à une droite constructible et passant par un point constructible,*
7. *La parallèle à une droite constructible et passant par un point constructible.*

De plus, si $x \in \mathbb{R}_+$ est constructible, alors $\sqrt{x}$ l'est aussi.

Démonstration. Il s'agit simplement de contructions géométriques faciles mais qui sont fastidueuses à décrire proprement, nous laissons donc ces vérifications au lecteur. □

On en déduit :

Théorème 8. *L'ensemble des réels constructibles est un sous-corps de $\mathbb{R}$.*

Remarque 3. Le Théorème 8 montre qu'il revient au même de dire qu'un point est constructible à partir de Σ et qu'il est constructible à partir du sous-corps engendré par Σ. En particulier, il est équivalent de dire qu'un point est constructible à partir de $\{0, 1\}$ et qu'il est constructible à partir de $\mathbb{Q}$.

Lemme 6. *Soient K un corps de caractéristique différente de 2 et L/K une extension de degré 2. Il existe $x \in L \setminus K$ tel que $x^2 \in K$ et $L = K(x)$.*

Démonstration. Si $y \in L \setminus K$, la famille $\{1, y\}$ est libre et c'est donc une base du K-espace vectoriel L, donc il existe $a, b \in K$ tels que

$$y^2 = ay + b.$$

Or K est de caractéristique différente de 2 donc on peut poser $x := y - \frac{a}{2}$ et on a alors

$$x^2 = \left(y - \frac{a}{2}\right)^2 = y^2 + \frac{a^2}{4} - ay = b + \frac{a^2}{4} \in K$$

et $L = K(y) = K(x)$. □

Théorème 9. *(Wantzel)*
Soit $K \subseteq \mathbb{R}$ un sous-corps. Alors $x \in \mathbb{R}$ est constructible à partir de K si et seulement s'il existe un tour de corps

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \mathbb{R}$$

telle que $x \in K_n$ et $\forall 0 \leq i \leq n-1,\ [K_{i+1} : K_i] = 2$.

Démonstration. Soit L un sous-corps de $\mathbb{R}$. On vérifie immédiatement que :

1. Les coordonnées du point d'intersection de deux droites non parallèles construites à partir de points de coordonnées dans L sont dans L,
2. Les coordonnées d'un point d'intersection de deux cercles de rayons joignant deux points de coordonnées dans L sont solutions d'une équation de degré 2 à coefficients dans L,
3. Les coordonnées d'un point d'intersection d'une droite joignant deux points de coordonnées dans L et d'un cercle de rayon joignant deux points de coordonnées dans L sont solutions d'une équation de degré 2 à coefficients dans L.

Il vient alors par récurrence que les coordonnées de tout point constructible à partir de K sont dans un corps du type K_n décrit dans l'énoncé.
Réciproquement, pout montrer que tout point dans un corps du type K_n est constructible à partir de K, il suffit de montrer que tout point dans une extension quadratique (de degré 2) d'un corps $L \subseteq \mathbb{R}$ est constructible à partir de L. Or, d'après le Lemme 6, une telle extension est engendrée par un $x \in \mathbb{R}$ tel que $x^2 \in L$, donc $x = \pm\sqrt{x^2}$ est constructible à partir de L d'après la Proposition 9. □

Corollaire 4. *Soit un réel x constructible à partir d'un sous-corps $K \subseteq \mathbb{R}$. Alors x est algébrique sur K, de degré une puissance de 2.*

Démonstration. Si x est constructible à partir de K, d'après le Théorme de Wantzel, il est dans une extension K_n de K telle que $[K_n : K] = 2^n$ en vertu de la Proposition 6. En considérant donc la tour finie $K \subseteq K(x) \subseteq K_n$, on en déduit que $[K(x) : K]$ est une puissance de 2 et donc en particulier que x est algébrique sur K. □

Définition 13. On dit qu'un angle α est constructile à partir d'un angle θ si $(\cos\alpha, \sin\alpha)$ est constructible à partir de $\{(0,0),(1,0),(\cos\theta,\sin\theta)\}$. De plus, comme $\sin\alpha$ est constructible à partir de $\cos\alpha$, cela revient au même de dire que $\cos\alpha$ est constructible à partir de $\{0, 1, \cos\theta\}$.

Corollaire 5. *Le réel $\sqrt[3]{2}$ n'est pas constructible.*

Démonstration. Le polynôme $P(X) = X^3 - 2$ est irréductible d'après le critère d'Eisenstein et annule $\sqrt[3]{2}$, c'est donc son polynôme minimal et on a $\deg_{\mathbb{Q}} \sqrt[3]{2} = 3$ qui n'est pas une puissance de 2. Ce réel n'est donc pas constructible d'aprè le Corollaire 4. □

Corollaire 6. *L'angle $\theta/3$ est constructible à partir de θ si et seulement si le polynôme $X^3 - 3X - 2\cos\theta$ s'annule dans $\mathbb{Q}(\cos\theta)$.*
En particulier, l'angle $\pi/9$ n'est pas constructible.

Démonstration. On a $\cos 3u = 4\cos^3 u - 3\cos u$, le réel $\cos(\theta/3)$ est racine du polynôme $P(X) = 4X^3 - 3X - \cos\theta$.
Si P est irréductible sur $\mathbb{Q}(\cos\theta)$, $\cos(\theta/3)$ est de degré 3 sur ce corps et n'est donc pas constructible d'après le Corollaire 4.
Si P est réductible sur $\mathbb{Q}(\cos\theta)$, comme il est de degré 3, il a une racine dans ce corps et doit alors se factoriser sur ce corps en un produit d'un polynôme de degré 1 et d'un polynôme de degré 2. Le réel $\cos(\theta/3)$ est racine d'un de ces deux polynômes et il est donc constructible sur $\mathbb{Q}(\cos\theta)$ d'après le Lemme 6 et le Théorème de Wantzel. Or $2P(X/2) = X^3 - 3X - 2\cos\theta$, la première partie de l'énoncé est démontrée.
On vérifie aisément que le polynôme $X^3 - 3X - 1$ n'a pas de racine dans $\mathbb{Q}$, donc l'angle $\pi/9$ n'est pas constructible car $\mathbb{Q}(\cos(\pi/3)) = \mathbb{Q}$. □

Corollaire 7. *Le réel $\sqrt{\pi}$ n'est pas constructible.*

Démonstration. Le réel π étant transcendant sur $\mathbb{Q}$ (voir par exemple [3], Appendice B.), le réel $\sqrt{\pi}$ n'est pas non plus constructible d'après la Proposition 9. □

On déduit des trois Corollaires précédents que :

Corollaire 8. *La duplication du cube, la trisection de l'angle et la quadrature du cercle sont impossibles à la règle et au compas.*

2.3 Corps de rupture, corps de décomposition et clôture algébrique

Nous allons voir ici quelques exemples fondamentaux d'extensions de corps qui nous seront grandement utiles pour la suite de nôtre étude.

Définition 14. Soient k un corps et $P \in k[X$ un polynôme non nul. On appelle corps de rupture de P sur k toute extension K/k telle que :

1. $\exists \alpha \in K \ ; \ P(\alpha) = 0$,
2. $K = k(\alpha)$.

Théorème 10. *Soient k un corps et $P \in k[X]$ un polynôme irréductible. Alors P admet un corps de rupture sur k, unique à k-isomorphisme près. On le note $\mathcal{R}_k(P)$.*

Démonstration. Existence : L'anneau $k[X]$ est euclidien (donc principal) et P est irréductible donc l'idéal (P) est maximal dans $k[X]$ donc l'anneau quotient $k[X]/(P)$ est un corps, extension de k et si l'on note $\alpha := \overline{X}$ la classe de X dans $k[X]/(P)$, on a $P(\alpha) = P(\overline{X}) = \overline{P(X)} = \overline{0}$. De plus, comme α est algébrique sur k, le Théorème 7-4. et le théorème d'isomorphie

permettent d'affirmer que $k[X]/(P) \simeq k[\alpha] = k(\alpha)$ est un corps de rupture de P sur k.
Unicité : Soient $k(\alpha)$ et $k(\beta)$ deux corps de rupture de P sur k. $k(\beta)$ étant une extension de k dans laquelle P a une racine β, on peut considérer le k-homomorphisme $\psi_\beta : k[X] \to k(\beta)$ tel que $\psi_\beta(X) = \beta$. Comme $P(\beta) = 0$, on a $(P) \subseteq \mathrm{Ker}(\psi_\beta)$ et donc ψ_β passe au quotient $\overline{\psi_\beta} : k[X]/(P) \to k(\beta)$. Comme $k[X]/(P)$ est un corps, ce morphisme est injectif. Or $k(\beta)$ est simple engendrée par β, donc $\overline{\psi_\beta}$ est aussi surjectif ; c'est donc un isomorphisme. De même, il existe un k-isomorphisme $\overline{\psi_\alpha} : k[X]/(P) \to k(\alpha)$ et donc

$$k(\beta) \simeq_k k[X]/(P) \simeq_k k(\alpha).$$

□

Exemple 1. $\mathbb{C}$ est un corps de rupture de $X^2 + 1 : \mathbb{C} \simeq \mathbb{R}[X]/(X^2 + 1)$.

Définition 15. Soient k un corps et $P \in k[X]$ un polynôme non nul. On appelle corps de décomposition de P sur k toute extension K/k telle que :

1. P est scindé sur K,
2. Si $\alpha_1, \ldots, \alpha_n$ sont les racines de P, alors $K = k(\alpha_1, \ldots, \alpha_n)$.

Théorème 11. *Soient k un corps et $P \in k[X]$ un polynôme non constant. Alors P admet un corps de décomposition sur k, unique à k-isomorphisme près. On le note $\mathcal{D}_k(P)$.*

Démonstration. On procède par récurrence sur $n := \deg P$.
Initialisation : $n = 1$, donc k convient et c'est le seul.
Hérédité : Si P n'a que des facteurs de degré 1, k convient et c'est aussi le seul. Sinon, soit Q un facteur irréductible de P de degré supérieur ou égal à 2. Q admet alors un corps de rupture $k(\alpha)$ sur k et il existe $R \in k(\alpha)[X]$ tel que $P = (X - \alpha)R$. Par hypothèse de récurrence, R admet un corps de décomposition $k(\alpha_1, \ldots, \alpha_r)$ et alors $k(\alpha, \alpha_1 \ldots, \alpha_r)$ est un corps de décompostition de P sur k. De plus, si L et M sont deux corps de décomposition de P sur k, soient $\alpha \in L$ et $\beta \in M$ deux racines de Q. On a $P = (X - \alpha)R,\ R \in k(\alpha)[X]$.

Par unicité du corps de rupture, il existe un k-isomorphisme $\sigma : k(\alpha) \to k(\beta)$ tel que $\sigma(\alpha) = \beta$ et $\sigma_{|k} = id_k$. On a donc $k(\alpha) \simeq k(\beta) \hookrightarrow M$ et donc L et M sont deux corps de décomposition de R sur $k(\alpha)$, ils sont donc $k(\alpha)$-isomorphes par hypothèse de récurrence et sont alors k-isomorphes. □

Proposition 10. *Soient k un corps, $P \in k[X]$ un polynôme non constant de degré $n \in \mathbb{N}^*$ et $K \simeq \mathcal{D}_k(P)$ un corps de décomposition de P sur k. Alors*

$$[K : k] \leq n!$$

Démonstration. On procède encore par récurrence sur $n = \deg P$.
Initialisation : Si $n = 1$, alors $K \simeq k$ et il n'y a rien à démontrer.
Hérédité : Si P n'est composé que de facteurs de degré 1, alors $K \simeq k$ et $[K : k] = 1 \leq n!$. Sinon, soit Q un facteur irréductible de P de degré supérieur ou égale à 2. Soit $k(\alpha)$ un corps de rupture de Q sur k. Comme $\deg Q \leq \deg P$, on a $[k(\alpha) : k] = \deg_k(\alpha) = \deg Q \leq n$. Il existe $R \in k(\alpha)[X]$ tel que $P = (X - \alpha)R$ et on a $\deg R < \deg P$ et soit $k(\alpha_1, \ldots, \alpha_r)$ un corps de décomposition de R sur $k(\alpha)$. Alors $K \simeq k(\alpha_1, \ldots, \alpha_r, \alpha)$ et, en utilisant la multiplicativité des degrés, on a, par hypothèse de récurrence :

$$[K : k] = [k(\alpha_1, \ldots, \alpha_r, \alpha) : k] = [k(\alpha_1, \ldots, \alpha_r)(\alpha) : k]$$

$$= [k(\alpha_1, \ldots, \alpha_r)(\alpha) : k(\alpha)][k(\alpha) : k] \leq (\deg R)! \deg Q \leq (n-1)! \times n = n!,$$

d'où le résultat. □

Définition 16. On dit d'un corps k qu'il est algébriquement clos si

$$\forall P \in k[X] \setminus k,\ \exists \alpha \in k\ ;\ P(\alpha) = 0.$$

Proposition 11. *Soit k un corps. Les assertions suivantes sont équivalentes :*

1. *k est algébriquement clos,*
2. *Tout polynôme non constant de $k[X]$ est scindé sur k,*
3. *Tout polynôme irréductible de $k[X]$ est de degré 1.*

Démonstration. 1. $\Rightarrow$ 2. Il s'agit d'effectuer une récurrence sur le degré de P.
2. $\Rightarrow$ 3. Supposons que P soit un polynôme irréductible de $k[X]$, de degré $n > 1$. Alors P est scindé sur k d'après 2, ce qui est absurde, donc P est de degré 1.
3. $\Rightarrow$ 1. Comme l'anneau $k[X]$ est factoriel, tout polynôme non constant P a au moins un diviseur irréductible et d'après 2., ce dernier est de degré 1, donc P a au moins une racine dans k, qui est donc algébriquement clos. □

On va montrer que $\mathbb{C}$ est algébriquement clos. Pour ce faire, on rappelle le théorème de Liouville en analyse complexe, dont on trouvera une démonstration dans [9]-4.7 :

Théorème 12. *(Liouville)*
Toute fonction entière $f : \mathbb{C} \to \mathbb{C}$ bornée en module est constante.

Corollaire 9. *Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.*

Démonstration. Soit $P \in \mathbb{C}[X]$ un polynôme non constant. Supposons, par l'absurde qu'il n'ait pas de racine dans $\mathbb{C}$ et notons $\widetilde{P}$ la fonction polynômiale associée à P. Comme P est non constant, on a $\lim_{|z|\to+\infty} \frac{1}{\widetilde{P}} = 0$, donc $\frac{1}{\widetilde{P}}$ est bornée en module sur $\mathbb{C}$. De plus, $\widetilde{P}$ est holomorphe sur $\mathbb{C}$ (ie est entière), donc $\frac{1}{\widetilde{P}}$ est entière car P ne s'annule pas. Donc, $\frac{1}{\widetilde{P}}$ est une fonction constante d'après le théorème de Liouville, donc P est constant, ce qui est absurde. P admet donc une racine danc $\mathbb{C}$. □

Définition 17. Soit k un corps. On dit qu'un corps K est une clôture algébrique de k si

1. K/k est une extension algébrique,
2. K est algébriquement clos.

Théorème 13. *(Steinitz)*
Tout corps k admet une clôture algébrique unique à k-isomorphisme près, notée k^a.

La démonstration que nous allons donner de ce résultat est dûe à Emil Artin. Elle se fait en plusieurs étapes :

Lemme 7. *(Krull)*
Soient A un anneau commutatif et I un idéal propre de A. Alors il existe un idéal maximal $\mathfrak{m}$ contenant I.

Démonstration. Soit l'ensemble $E := \{J \subseteq A \text{ idéal de } A \ ; \ I \subseteq J\}$. On a $I \in E \neq \emptyset$ et si $(J_i)_{i\in\Lambda}$ est une chaîne de E, alors $\bigcup_{j\in\Lambda} J_i$ est un majorant de la famille $(J_i)_i$ et on a $\bigcup_i J_i \in E$ car $1 \notin \bigcup_i J_i$. Donc E est inductif et il admet un élément maximal $\mathfrak{m}$ d'après le lemme de Zorn. □

Lemme 8. *Soient k un corps et $\{P_\lambda, \ \lambda \in \Lambda\}$ l'ensemble des polynômes irréductibles et unitaires de $k[X]$. On considère l'anneau $A := k[X_\lambda]_{\lambda\in\Lambda}$ des polynômes à une infinité d'indéterminées X_λ et on note $P_\lambda(X_\lambda)$ l'image de P_λ par le morphisme $k[X] \to A$, $P(X) \mapsto P(X_\lambda)$. On pose encore $I := ((P_\lambda(X_\lambda))_{\lambda\in\Lambda}$. Alors I est un idéal propre de A.*

Démonstration. Par l'absurde, on suppose qu'il existe $Q_{\lambda_i} \in A$ tels que

$$\sum_{i=1}^{n} Q_{\lambda_i} P_{\lambda_i}(X_{\lambda_i}) = 1, \tag{1}$$

où $\lambda_i \in \Lambda_0 := \{\lambda_1, \ldots, \lambda_n\}$. Posons $\Lambda_1 := \{\lambda \in \Lambda \ ; \ X_\lambda \text{ apparaisse dans } Q_{\lambda_i}\} \cup \Lambda_0$. La relation (1) a lieu dans $k[X_\lambda]_{\lambda\in\Lambda_1}$. P_{λ_1} est irréductible donc il existe k_1/k un corps de rupture de P_{λ_1} et $\alpha_1 \in k_1$ tel que $P_{\lambda_1}(\alpha_1) = 0$. Soient P_2 un facteur irréductible de P_{λ_2} dans $k_1[X]$, k_2/k_1 un corps de rupture de P_2 sur k_1 et $\alpha_2 \in k_2$ tel que $P_2(\alpha_2) = P_{\lambda_2}(\alpha_2) = 0$. On construit alors par récurrence une tour de corps $k \subseteq k_1 \subseteq k_2 \subseteq \cdots \subseteq k_n$ et il existe $\alpha_1, \ldots, \alpha_n \in k_n$ tels que $P_{\lambda_i}(\alpha_i) = 0$. La relation (1) a donc lieu dans $k_n[X_\lambda]_{\lambda\in\Lambda_1}$ et soit le morphisme $\varphi : k_n[X_\lambda]_{\lambda\in\Lambda_1} \to k_n$ tel que $\varphi(Q) = Q(\alpha_1, \ldots, \alpha_n, 0 \ldots, 0)$. En appliquant φ à (1), on obtient alors $1 = 0$, ce qui est absurde. Donc l'idéal I est propre. □

Lemme 9. *Le Lemme de Krull implique qu'il existe $\mathfrak{m}$ un idéal maximal de A contenant I et on pose $K_0 := k$ et $K_1 := A/\mathfrak{m}$. Alors K_1 est un corps et soit x_λ l'image (quotient) de X_λ dans K_1. Alors tout polynôme P_λ irréductible de $k[X]$ a une racine x_λ dans $K_1 = A/\mathfrak{m}$ et K_1/K_0 est algébrique.*

Démonstration. Si $y \in K_1$, $y = \pi_{A/\mathfrak{m}}(Q)$, $Q \in A$ et il existe $s \in \mathbb{N}^*$ tel que Q ne contienne que les indéterminées $(X_{\lambda_i})_{1\leq i\leq s}$ et $y \in k[x_{\lambda_i}]_{1\leq i\leq s}$. Tout x_{λ_i} étant algébrique sur k, l'extension $k[x_{\lambda_i}]_i/k$ est algébrique et donc y est algébrique sur k. □

Lemme 10. *Soient K/k une extension algébrique et Ω un cors algébriquement clos. Alors tout plongement $\tau : k \hookrightarrow \Omega$ se prolonge en $K \hookrightarrow \Omega$.*

Démonstration. On pose $E := \{(k', \tau') \ ; \ k'/k \subseteq K/k, \ \tau'_{|k} = \tau\}$. On définit sur E la relation binaire :

$$\forall (k_1, \tau_1), (k_2, \tau_2) \in E, \ (k_1, \tau_1) \preceq (k_2, \tau_2) \ \Leftrightarrow \ k_1 \subseteq k_2 \text{ et } \tau_{2|k_1} = \tau_1.$$

Alors $(E, \preceq)$ est un ensemble ordonné non vide. Soit ensuite $(k_i, \tau_i)_{i \in I}$ est une chaîne de E. Posons $\widetilde{k} := \bigcup_{i \in I} k_i$ et $\widetilde{\tau} : \widetilde{k} \hookrightarrow \Omega$ le plongement défini par $\widetilde{\tau} = \tau_i(x)$ si $x \in k_i$. Ceci est bien défini car si $x \in k_i, k_j$, il existe $l \in I$ tel que $k_i, k_j \subseteq k_l$ et alors $\tau_i(x) = \tau_l(x) = \tau_j(x)$. $(\widetilde{k}, \widetilde{\tau})$ est donc un majorant de $(k_i, \tau_i)_i$. Ainsi E est un ensemble inductif et il admet un élément maximal (k_0, τ_0) d'après le lemme de Zorn. Montrons alors que $k_0 = K$. On a $k_0 \subseteq K$. Soit $x \in K$. x est algébrique sur k, donc sur k_0 et soit $P := \mu_{x,k_0}$. Il existe $\alpha \in \Omega$ tel que $\tau_0(P)(\alpha) = 0$ et $k_0 \simeq \tau_0(k_0)$ donc $k_0(x) \simeq k_0[X]/(P) \simeq k_0(\alpha)$ et τ_0 se prolonge $k_0(x) \simeq k_0(\alpha) \hookrightarrow \Omega$. Donc, par maximalité, $k_0(x) = k_0 \ \Rightarrow \ x \in k_0 \ \Rightarrow \ K = k_0$ et τ se prolonge en $\tau_0 : k_0 \hookrightarrow \Omega$. □

Lemme 11. *Si L est une clôture algébrique de k, alors L/k est une extension algébrique maximale.*

Démonstration. Soit $L'/k \supseteq L/k$ une autre extension algébrique et soit $x \in L'$. x est algébrique sur k donc x est algébrique sur L et soit $P := \mu_{x,L}$. Alors, $\deg P = 1$ car L est algébriquement clos, donc $x \in L$ et $L' \subseteq L$ donc $L = L'$. □

Démonstration. (du théorème de Steinitz)
Existence : En reprenant les notations du Lemme 9, si $K_1 = A/\mathfrak{m}$ est algébriquement clos, $k^a = K_1$ convient, sinon on reproduit le procédé des Lemmes 8 et 9 et on construit une extension algébrique K_2/K_1. Alors K_2/K_0 est algébrique et par récurrence, on construit une tour de corps

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots$$

et on pose

$$K := \bigcup_{i \in \mathbb{N}} K_i.$$

Alors tout polynôme de $K[X]$ a ses coefficients dans un K_i, donc a une racine dans K_{i+1}, donc dans K et comme K_i/K est algébrique pour tout $i \in \mathbb{N}$, K/k est aussi algébrique et on peut poser $k^a := K$.
Unicité : Si Ω et Ω' sont deux clôtures algébriques de k, alors en appliquant le Lemme 10 à $K := \Omega'$ et à $\tau : k \hookrightarrow \Omega$ l'injection canonique, on obtient un plongement $k \hookrightarrow \Omega' \overset{\tau'}{\hookrightarrow} \Omega$ et en appliquant le Lemme 11 à $L := \Omega'$ et $L' := \Omega$, on obtient que τ' est surjective. Donc $\Omega \overset{\tau'}{\simeq} \Omega'$ et $\tau'_{|k} = id_k$, ce qui achève la démonstration. □

Exemple 2.
1. $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$, ($\mathbb{C} \simeq \mathbb{R}^a$)
2. $\{x \in \mathbb{C} \ ; \ x \textit{ est algébrique sur } \mathbb{Q}\}$ est un sous-corps de $\mathbb{C}$ et est une clôture algébrique de $\mathbb{Q}$.

2.4 Racines de l'unité et polynômes cyclotomiques

Définition 18. Soient k un corps. Pour $n \in \mathbb{Z}$, on définit $n.1_k$ par

$$n.1_k := \begin{cases} 1_k + \cdots + 1_k & \text{si} \quad n \in \mathbb{N}^* \\ 0 & \text{si} \quad n = 0 \\ -(1_k + \cdots + 1_k) & \text{si} \quad n \in \mathbb{Z} \setminus \mathbb{N} \end{cases}$$

et σ_k le morphisme

$$\begin{array}{rccc} \sigma_k & : & \mathbb{Z} & \to & k \\ & & n & \mapsto & n.1_k \end{array}$$

On appelle caractéristique de k et on note $\mathrm{car}(k)$ l'unique entier engendrant $\mathrm{Ker}(\sigma_k)$. Plus précisément, si σ_k est injectif, $\mathrm{car}(k) := 0$ et sinon, il existe un unique $c \in \mathbb{N}^*$ tel que $\mathrm{Ker}(\sigma_k) = c\mathbb{Z}$ et alors $\mathrm{car}(k) := c$.

Proposition 12. *La caractéristique d'un corps est soit nulle, soit un nombre premier.*

Démonstration. Soit k un corps pour lequel on suppose que $\mathrm{car}(k) \neq 0$ et soit $c \in \mathbb{N}^*$ sa caractéristique. Supposons de plus qu'il existe deux entiers $a, b \in \mathbb{N} \setminus \{1, c\}$ tels que $c = ab$. Alors $\sigma_k(a)\sigma_k(b) = \sigma_k(ab) = \sigma_k(c) = 0_k$ et k étant en particulier un anneau intègre, cela implique que $\sigma_k(a) = 0$ ou $\sigma_k(b) = 0$ ce qui est absurde car on a $2 \leq a, b < c$. Donc c est un nombre premier. □

Proposition-Définition 2. *Pour tout $n \in \mathbb{N}$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier. De plus, pour tout $p \in \mathbb{P}$, on note*

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}.$$

Démonstration. Si $p \in \mathbb{P}$, tout $1 \leq k \leq p-1$ est premier avec p et d'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $pu + kv = 1$. En considérant la classe modulo p, on obtient $\overline{k}\ \overline{v} = 1$ et donc $\overline{k}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$. On en déduit que toute classe non nulle est inversible et donc que $\mathbb{Z}/p\mathbb{Z}$ est un corps. Ensuite, si n n'est pas premier, il existe $1 \leq k_0 \leq n-1$ divisant n et on a $\overline{k_0} \neq \overline{0}$. Mais, si $m := \frac{n}{k_0}$, alors $\overline{m} \neq \overline{0}$ et pourtant $\overline{k_0}\ \overline{m} = \overline{k_0 m} = \overline{n} = \overline{0}$. Donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre et n'est donc pas un corps. □

Remarque 4. On a $\mathrm{car}(\mathbb{F}_p) = p$.

Dans la suite, sauf mention contraire, on fixe un corps k et un entier $n \in \mathbb{N}^*$ tels qu'une des deux conditions suivantes (*) soit réalisée :

1. $\mathrm{car}(k) = 0$,
2. $\mathrm{car}(k) = p$ et p ne divise pas n.

Définition 19. On appelle groupe des racines $n^{\text{ièmes}}$ de l'unité le groupe $\mu_n(k)$ défini par :

$$\mu_n(k) := \{x \in \mathcal{D}_k(X^n - 1)\ ;\ x^n = 1\}.$$

De plus, on définit l'ensemble des racines primitives $n^{\text{ièmes}}$ de l'unité, noté $\mu_n^*(k)$, par :

$$\mu_n^*(k) := \{x \in \mu_n(k)\ ;\ \forall 0 \leq k \leq n-1,\ x^k \neq 1\}$$

Remarque 5. On voit immédiatement que pour tout $x \in \mu_n(k)$, $x \in \mu_n^*(k)$ tel que $o(x) = n$.

Définition 20. Pour $n \in \mathbb{N}^*$ on note $\varphi(n) := \text{card}(\{1 \leq k \leq n \ ; \ k \wedge n = 1\})$ et on l'appelle la fonction indicatrice d'Euler.

Propriété 1.

$$\forall n, m \in \mathbb{N}^*, \ n \wedge m = 1 \ \Rightarrow \ \varphi(nm) = \varphi(n)\varphi(m).$$

Démonstration. On a clairement $\varphi(k) = |(\mathbb{Z}/k\mathbb{Z})^\times|$ pout tout $k \in \mathbb{N}^*$. Comme $n \wedge m = 1$, on peut appliquer le lemme chinois (Annexe) pour obtenir :

$$\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

et le résultat suit. □

Proposition 13. *On a*

1. $|\mu_n(k)| = n$,
2. $|\mu_n^*(k)| = \varphi(n)$.

Démonstration. 1. On a $(X^n - 1)' = nX^{n-1} \neq 0$ donc $(X^n - 1) \wedge (nX^{n-1}) = 1$ et donc $X^n - 1$ est à racines simples, on en déduit que $|\mu_n(k)| = n$.
2. Pour tout $x \in \mu_n(k)$, on a $\mu_n^*(k) = \{x^k \in \mu_n(k) \ ; \ k \wedge n = 1\}$, d'où le résultat. □

Lemme 12. *Soient G un groupe abélien, $a, b \in G$ et $p := o(a)$, $q := o(b)$. On a*

$$p \wedge q = 1 \ \Rightarrow \ o(ab) = pq.$$

Démonstration. Si $x \in \langle a \rangle \cap \langle b \rangle$, alors l'ordre de x divise p et q, donc $o(x) = 1 \Rightarrow x = e \Rightarrow \langle a \rangle \cap \langle b \rangle = \{e\}$. D'autre part, $(ab)^{pq} = a^{pq}b^{pq} = e$ et si $d = o(ab)$, alors $(ab)^d = a^d b^d = e \Rightarrow a^d = (b^{-1})^d \in \langle a \rangle \cap \langle b \rangle = \{e\}$ d'où $a^d = b^d = e$. On en déduit que d est le ppcm de p et q et c'est donc leur produit car ces deux derniers sont premiers entre eux. Donc $d = pq$. □

On en déduit par récurrence le

Lemme 13. *Si $a_1, \ldots, a_m \in G$ sont des élément d'ordres deux à deux premiers entre eux, alors l'ordre du produit est le produit des ordres.*

Théorème 14. *Le groupe $\mu_n(k)$ est cyclique.*

Démonstration. On décompose n en produit de nombres premiers : $n = p_1^{n_1} \cdots p_r^{n_r}$. Le polynôme $X^{\frac{n}{p_i}} - 1$ possède au plus $\frac{n}{p_i}$ racines donc il existe au plus $\frac{n}{p_i}$ éléments $\alpha \in \mathcal{D}_k(X^n - 1)$ tels que $\alpha^{\frac{n}{p_i}} = 1$. Pour tout $1 \leq i \leq r$, on peut choisir $a_i \in \mathcal{D}_k(X^n - 1)$ tel que $a_i^{\frac{n}{p_i}} \neq 1$. Posons ensuite $m_i := \frac{n}{p_i^{n_i}}$ et $b_i := a_i^{m_i}$. On a $o(b_i) = p_i^{n_i}$ car $b_i^{p_i^{n_i}} = 1$ et $b_i^{p_i^{n_i - 1}} \neq 1$. Or $\forall i \neq j,\ o(b_i) \wedge o(b_j) = p_i^{n_i} \wedge p_j^{n_j} = 1$ donc en posant $b := b_1 \cdots b_r$, on obtient $o(b) = o(b_1 \cdots b_r) = o(b_1) \cdots o(b_r) = p_1^{n_1} \cdots p_r^{n_r} = n$. Donc $\mu_n(k)$ admet un élément d'ordre n, il est donc cyclique. □

Remarque 6. Notons que dans la preuve précédente, nous n'avons pas utilisé les conditions (*).

Théorème 15. *Si k est un corps quelconque et si $(G, \cdot) \leq (k^*, \cdot)$ est un sous-groupe fini, alors G est cyclique.*

Démonstration. Pour tout $x \in G$, on a $x^{|G|} = 1$ d'après le Théorème de Lagrange, donc $G \leq \mu_{|G|}(k)$ qui est cyclique d'ordre au plus $|G|$. G est donc cyclique comme sous-groupe d'un groupe cyclique. □

Corollaire 10.

$$\mu_n(k) = \bigsqcup_{d|n} \mu_d^*(k).$$

Démonstration. $\mu_n(k)$ est cyclique d'ordre n et pour tout $d|n$, il existe $\varphi(d)$ éléments d'ordre d dans $\mu_n(k)$. □

Définition 21. Soit k un corps et $n \in \mathbb{N}^*$ vérifiant la condition (*).

1. On appelle $n^{\text{ième}}$ polynôme cyclotomique et on note $\Phi_{n,k}(X)$ le polynôme :
$$\Phi_{n,k}(X) := \prod_{\zeta \in \mu_n^*(k)} (X - \zeta).$$
2. On appelle $n^{\text{ième}}$ extension cyclotomique de k toute extension K/k telle qu'il existe $\omega \in \mu_n^*(k)$ tel que $K = k(\omega)$.

Proposition 14. *On a :*

1. $\deg \Phi_{n,k} = \varphi(n)$,
2. $\forall x \in \mu_n(k),\ \Phi_{n,k}(x) = 0 \ \Leftrightarrow\ o(x) = n$,
3. $X^n - 1 = \prod_{d|n} \Phi_{d,k}(X)$,
4. $\sum_{d|n} \varphi(d) = n$.

Démonstration. 1. et 2. sont évidentes. Pour 3., on a

$$\mu_n(k) = \bigsqcup_{d|n} \mu_d^*(k) \ \Rightarrow\ X^n - 14 = \prod_{d|n} \Phi_{d,k}(X).$$

Enfin, pour 4., on a $\deg \Phi, d, k = \varphi(d)$ donc

$$n = \deg(X^n - 1) = \deg\left(\prod_{d|n} \Phi_{d,k}\right) = \sum_{d|n} \deg \Phi_{d,k} = \sum_{d|n} \varphi(d).$$

□

Définition 22. La fonction de Möbius l'application

$$\begin{array}{rccc} \mu & : & \mathbb{N}^* & \to & \mathbb{N} \\ & & d & \mapsto & \mu(d) \end{array}$$

telle que :

1. $\mu(1) = 1$,
2. $\mu(d) = (-1)^k$ si d est le produit de k nombres premiers distincts,
3. $\mu(d) = 0$ si d est divisible par le carré d'un nombre premier.

Lemme 14.

$$\forall n \in \mathbb{N}^*,\ \sum_{d|n} \mu(d) = \begin{cases} 1 & si \quad n = 1 \\ 0 & si \quad n \geq 2 \end{cases}.$$

Démonstration. Si $n = 1$, il n'y a rien à vérifier. Si $n \geq 2$, et si $p_1, \ldots, p_r$ sont les nombres premiers distincts divisant n, alors

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{1 \leq i \leq r} \mu(p_i) + \sum_{1 \leq i < j \leq r} \mu(p_i p_j) + \cdots + \mu(p_1 \cdots p_r)$$

$$= 1 + (-1)\binom{k}{1} + (-1)^2\binom{k}{2} + \cdots + (-1)^k = (1 + (-1))^k = 0.$$

□

Théorème 16. *On a :*

$$\Phi_{n,k}(X) = \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)}.$$

Démonstration. Pour $d|n$, on note $d' := \frac{n}{d}$. D'après la Proposition 14-3. et le Lemme 14 et en posant

$$A := \{(d, c) \in (\mathbb{N}^*)^2 \ ;\ d|n \text{ et } c|d'\} = \{(d, c) \in (\mathbb{N}^*)^2 \ ;\ c|n \text{ et } d|c'\},$$

on obtient

$$\prod_{d|n}(X^{d'}-1)^{\mu(d)} = \prod_{d|n}\prod_{c|d'}(\Phi_{c,k}(X))^{\mu(d)} = \prod_{(d,c)\in A}(\Phi_{c,k}(X))^{\mu(d)}$$

$$= \prod_{c|n}\prod_{d|c'}(\Phi_{c,k}(X))^{\mu(d)} = \prod_{c|n}(\Phi_{c,k})^{\sum_{d|c'}\mu(d)} = \Phi_{n,k}(X).$$

□

Exemple 3. Ce résultat permet de calculer facilement des polynômes cyclotomiques, par exemple :

$$\Phi_8(X) = (X^8-1)^{\mu(1)}(X^4-1)^{\mu(2)}(X^2-1)^{\mu(4)}(X-1)^{\mu(8)}$$

$$= (X^8-1)(X^4-1)^{-1} = X^4+1.$$

Lemme 15. *Soient $P, Q \in \mathbb{Z}[X]$ avec Q unitaire. Alors le quotient et le reste de la division euclidienne de P par Q sont à coefficients entiers.*

Démonstration. Il suffit de poser proprement la division euclidienne et le résultat vient. □

Théorème 17. *Si $car(k) = 0$ (resp. $car(k) = p \neq 0$) alors $\Phi_{n,k}$ est unitaire dans $\mathbb{Z}[X]$ (resp. dans $\mathbb{F}_p[X]$).*

Démonstration. On raisonne par récurrence sur $n \in \mathbb{N}^*$.
Initialisation : Pour $n = 1$, quelle que soit la caractéristique du corps k, on a $\Phi_1(X) = X - 1$, qui est bien unitaire.
Hérédité : Par hypothèse de récurrence, pour tout diviseur d de n tel que $1 \leq d < n$, $\Phi_{d,k}$ est unitaire dans $\mathbb{Z}[X]$ si $\mathrm{car}(k) = 0$ et unitaire dans $\mathbb{F}_p[X]$ si $\mathrm{car}(k) = p$. On pose

$$\phi_k(X) := \prod_{d|n,\ d<n}\Phi_{d,k}(X).$$

Le polynôme φ_k est unitaire dans $\mathbb{Z}[X]$ si $\mathrm{car}(k) = 0$ (resp. unitaire dans $\mathbb{F}_p[X]$ si $\mathrm{car}(k) = p \neq 0$). D'après la Proposition 14-3., on a

$$X^n - 1 = \phi_k(X)\Phi_{n,k}(X). \tag{2}$$

Si $\mathrm{car}(k) = 0$, le Lemme 15 donne

$$X^n - 1 = \phi_k(X)Q(X) + R(X),\ \deg R < \deg \phi_k \text{ ou } R = 0. \tag{3}$$

Si $\mathrm{car}(k) = p \neq 0$, on obtient (3) en effectuant la division euclidienne de $X^n - 1$ par ϕ_k dans $\mathbb{F}_p[X]$. Les relations (2) et (3) montrent que dans $k^a[X]$

$$\phi_k(X)(\Phi_{n,k}(X) - Q(X)) = R(X).$$

Si $R(X) \neq 0$, le premier membre de l'égalité précédente est un polynôme de degré supérieur ou égal au degré de ϕ_k alors que le second membre est de degré strictement inférieur à celui de ϕ_k, ce qui est absurde. Donc $R = 0$ et par suite, $\Phi_{n,k}(X) = Q(X)$. Enfin, la relation (2) a lieu dans $\mathbb{Z}[X]$ (resp. dans $\mathbb{F}_p[X]$) et les polynômes $\phi_k(X)$ et $X^n - 1$ étant unitaires, $\Phi_{n,k}$ est aussi unitaire, d'où le résultat. □

Théorème 18. *Pour tout $n \in \mathbb{N}^*$ le polynôme $\Phi_n := \Phi_{n,\mathbb{Q}}$ est irréductible sur $\mathbb{Q}$.*

Démonstration. Le résultat étant évident pour $n = 1$, on supposera $n \geq 2$. D'après le Théorème 17, $\Phi_n \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$ et donc, pour tout $\omega \in \mu_n^*(\mathbb{Q})$, on a

$$\Phi_n(\omega) = 0 \ \Rightarrow\ \mu_{\omega,\mathbb{Q}} | \Phi_n \text{ dans } \mathbb{Q}[X]. \tag{4}$$

Posons $P_\omega := \mu_{\mathbb{Q}}(\omega)$. Il existe $Q \in \mathbb{Q}[X]$ tel que

$$\Phi_n(X) = P_\omega(X)Q(X). \tag{5}$$

Or, Φ_n est unitaire dans $\mathbb{Z}[X]$ d'après le Théorème 17, donc P_ω et Q sont unitaires dans $\mathbb{Q}[X]$. Il existe alors $\gamma, \delta \in \mathbb{Q}^*$ tels que

$$P_\omega(X) = \gamma R(X),\ Q(X) = \delta S(X), \tag{6}$$

où $R, S \in \mathbb{Z}[X]$ sont des polynômes primitifs. Notons a (resp. b) le coefficient dominant de R (resp. S) ; les relations (6) montrent que $\gamma a = \delta b = 1$. De plus, d'après la relation (5),

$$ab\Phi_n(X) = R(X)S(X) \in \mathbb{Z}[X].$$

Dans $\mathbb{Z}[X]$, les polynômes R et S sont primitifs et Φ_n est unitaire, on peut donc supposer $ab = 1$ et $a = b = 1$, d'où $P_\omega(X) = R(X)$. Ensuite, le polynôme unitaire P_ω est primitif dans $\mathbb{Z}[X]$ et irréductible dans $\mathbb{Q}[X]$ et on en déduit que P_ω est unitaire et irréductible dans $\mathbb{Z}[X]$. Il reste à vérifier que pour tout $\omega' \neq \omega$ dans $\mu_n^*(\mathbb{Q})$, on a $P_{\omega'} = P_\omega$. Pour ce faire, il suffit de montrer que tout $\omega' \in \mu_n^*(\mathbb{Q})$ est racine de P_ω. On sait que $\mu_n^*(\mathbb{Q}) = \{\omega^k,\ 1 \leq k \leq n,\ k \wedge n = 1\}$.
1. Supposons que $\omega' = \omega^r,\ 1 \leq r \leq n,\ r$ ne divise pas n et $r \in \mathbb{P}$. On pose

$$P_{\omega^r}(X) := \mu_{\omega^r,\mathbb{Q}},$$

alors $P_{\omega^r}(\omega^r) = 0 \ \Rightarrow \ P_\omega(X)$ et $P_{\omega^r}(X^r)$ ont une racine commune : ω. Supposons que $P_{\omega^r}(X) \wedge P_\omega(X) = 1$. Les polynômes $P_{\omega^r}(X)$ et $P_\omega(X)$ sont alors deux diviseurs unitaires irréductibles de $X^n - 1$ dans $\mathbb{Z}[X]$, donc il existe $Q \in \mathbb{Z}[X]$ tel que

$$X^n - 1 = P_\omega(X)P_{\omega^r}(X)Q(X) \tag{7}$$

On note $\pi : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/r\mathbb{Z}$ la surjection canonique et $\widehat{\pi} : \mathbb{Z}[X] \twoheadrightarrow (\mathbb{Z}/r\mathbb{Z})[X]$ le prolongement canonique de π. Pour tout $P \in \mathbb{Z}[X]$, on pose $\widehat{\pi}(P(X)) =: \overline{P}(X)$, en particulier, $\widehat{\pi}(X^n - 1) = X^n - \overline{1}$. Le nombre premier r ne divise pas n, donc $X^n - \overline{1}$ n'a que des racines simples dans un corps de décomposition sur $\mathbb{Z}/r\mathbb{Z}$. D'autre part, la relation (7) implique

$$X^n - \overline{1} = \overline{P_\omega}(X)\overline{P_{\omega^r}}(X)\overline{Q}(X) \in \mathbb{Z}/r\mathbb{Z}[X]. \tag{8}$$

Or, $P_\omega(X)$ et $P_{\omega^r}(X^r)$ ont une racine commune, donc ils ne sont pas premiers entre eux et $P_\omega(X)$ étant irréductible dans $\mathbb{Z}[X]$, on a nécessairement

$$P_\omega(X) | P_{\omega^r}(X^r) \in \mathbb{Z}[X].$$

Il existe donc $U \in \mathbb{Z}[X]$ tel que $P_{\omega^r}(X^r) = P_\omega(X)U(X)$ et r étant premier,

$$\overline{P_\omega}(X)\overline{U}(X) = \overline{P_{\omega^r}}(X^r) = (\overline{P_{\omega^r}}(X))^r \in \mathbb{Z}/r\mathbb{Z}[X].$$

On en déduit que, dans l'anneau factoriel $(\mathbb{Z}/r\mathbb{Z})[X]$, les polynômes $\overline{P_\omega}(X)$ et $\overline{P_{\omega^r}}(X)$ ont au moins un diviseur irréductible en commun, que nous noterons $\overline{T}(X)$. La relation (8) implique alors

$$(\overline{T}(X))^2 | X^n - \overline{1} \in (\mathbb{Z}/r\mathbb{Z})[X].$$

Mais $\overline{T}(X)$ étant irréductible, on a $\deg \overline{T} \geq 1$, donc le polynôme $X^n - \overline{1}$ a au moins une racine double dans un corps de décomposition sur $\mathbb{Z}/r\mathbb{Z}$, ce qui est absurde d'après la Proposition 13-1.. On en conclut que, dans $\mathbb{Z}[X]$, les polynômes irréductibles et unitaires $P_{\omega^r}(X)$ et $P_\omega(X)$ ne sont pas premiers entre eux, par suite,

$$P_{\omega^r}(X) = P_\omega(X). \tag{9}$$

2. Supposons $\omega' = \omega^s$, avec $1 < s < n,\ s \wedge n = 1$. Soit $s = r_1 \cdots r_i$ la factorisation de s en nombres premiers (non nécessairement distincts) dans $\mathbb{N}$. En utilisant la relation (9), on obtient :

$$P_\omega(X) = P_{\omega^{r_1}}(X) = P_{\omega^{r_1 r_2}}(X) = \ldots = P_{\omega^{r_1 \cdots r_i}}(X) = P_{\omega'}(X).$$

Donc, pour tout $\omega \in \mu_n^*(\mathbb{Q})$, $P_\omega = \mu_{\omega,\mathbb{Q}}$ admet pour racines les $\varphi(n)$ racines primitives $n^{\text{ièmes}}$ de l'unité contenues dans $\mathbb{Q}^a$, donc

$$\Phi_n | \mu_{\omega,\mathbb{Q}} \in \mathbb{Q}[X]. \tag{10}$$

Finalement, en combinant les relations (4) et (10), on obtient que $\Phi_n = \mu_{\omega,\mathbb{Q}}$ est bien irréductible sur $\mathbb{Q}$, ce qui termine la démonstration. □

Corollaire 11. *On a*

1. *Pour tout $n \in \mathbb{N}$, Φ_n est irréductible sur $\mathbb{Z}$,*
2. *$\forall \omega \in \mu_n^*(\mathbb{Q}),\ \Phi_n = \mu_{\omega,\mathbb{Q}}$. En particulier $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$.*

Démonstration. 1. Φ_n est irréductible sur $\mathbb{Q}$ et primitif car unitaire. On en déduit que Φ_n est irréductible sur $\mathbb{Z}$.
2. Φ_n est irréductible sur $\mathbb{Q}$ d'après le Théorème précédent et $\Phi_n(\omega) = 0$ donc $\mu_{\omega,\mathbb{Q}} = \Phi_n$ et $\deg \Phi_n = \varphi(n)$. Ainsi, $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg_{\mathbb{Q}}(\omega) = \deg \Phi_n = \varphi(n)$, d'où le résultat. □

2.5 Corps finis

Avant de parler des corps finis (encore appelés corps de Galois) nous nous permettons une petite digression sur les corps premiers.

Définition 23.
1. On dit qu'un corps est premier s'il n'a pas de sous-corps propre.
2. Pour un corps k, on note $(k_i)_{i\in I}$ l'ensemble des sous-corps de k (qui est non vide car k est un sous-corps de lui-même).
   On appelle sous-corps premier de k et on note Δ_k le sous-corps

$$\Delta_k := \bigcap_{i\in I} k_i.$$

   On remarque que ce corps est automatiquement premier et que c'est le plus petit sous-corps de k. De plus, un corps k est premier si et seulement si $\Delta_k = k$.

Proposition 15. *Les corps $\mathbb{Q}$ et $\mathbb{F}_p$ sont premiers.*

Démonstration. Soit K un sous-corps de $\mathbb{Q}$. K contient 0 et 1, donc contient $\mathbb{Z}$ et donc contient le corps des fractions de $\mathbb{Z}$ qui est $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$, et donc $K = \mathbb{Q}$. On en déduit que $\mathbb{Q}$ est un corps premier.
Soit $p \in \mathbb{P}$. Si $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ avait un sous-corps, celui-ci serait de la forme $m\mathbb{Z}/p\mathbb{Z},\ m > 1$ et $p\mathbb{Z} \subset m\mathbb{Z} \subset \mathbb{Z}$. Donc $m|p,\ m \neq p$ et $m \neq 1$, ce qui est absurde car p est premier. Ainsi $\mathbb{F}_p$ n'admet pas de sous-corps propre, il est donc premier. □

Théorème 19. *Pour tout corps k, on a*

$$\Delta_k \simeq \mathbb{Q},$$

ou

$$\exists! p \in \mathbb{P}\ ;\ \Delta_k \simeq \mathbb{F}_p.$$

Démonstration. Soit $\sigma_k : \mathbb{Z} \to k$ le morphisme de la définition 18. Δ_k contient $0, 1 \in k$, donc contient $\mathrm{Im}(\sigma_k) = \{n.1,\ n \in \mathbb{Z}\}$. Si $\mathrm{car}(k) = 0$, alors σ_k est injectif d'où $\mathrm{Im}(\sigma_k) \simeq \mathbb{Z}$. Ainsi, Δ_k contient un sous-corps isomorphe à $\mathbb{Q}$, mais Δ_k étant le plus petit sous-corps de k, on en déduit $\Delta_k \simeq \mathbb{Q}$. Si $\mathrm{car}(k) = p \neq 0$, alors $\mathrm{Im}(\sigma_k) \simeq \mathbb{F}_p$, donc $\mathrm{Im}(\sigma_k)$ est un sous-corps de δ_k, mais ce dernier étant le plus petit sous-corps de k, $\Delta_k \simeq \mathrm{Im}(\sigma_k) \simeq \mathbb{F}_p$. □

Corollaire 12. *Un corps premier est isomorphe à $\mathbb{Q}$ ou à un certain $\mathbb{F}_p$.*

Passons à l'étude des corps finis.

Lemme 16. *Soit k un corps fini de cardinal $q \in \mathbb{N}^*$. Alors il existe $p \in \mathbb{P}$ et $n \in \mathbb{N}^*$ tels que $q = p^n$. En outre, k est de caractéristique p.*

Démonstration. Comme k est fini, le morphisme $\sigma_k : \mathbb{Z} \to k$ ne peut être injectif et il existe $p \in \mathbb{P}$ tel que $\mathrm{Ker}(\sigma_k) = p\mathbb{Z}$ et ainsi $\mathrm{car}(k) = p \neq 0$. On a $q \geq p$ et soit φ_k l'application

$$\begin{array}{rccc} \varphi_k & : & \mathbb{F}_p & \to & k \\ & & \overline{x} & \mapsto & x.1_k \end{array}$$

Alors φ_k est bien définie et c'est un plongement. $k/\mathbb{F}_p$ est donc une extension finie car k est fini et si $n := [k : \mathbb{F}_p] \in \mathbb{N}^*$, alors $q = |k| = p^n$. □

Remarque 7. La preuve précédente montre que tout corps fini (de caractéristique $p \neq 0$) est une extension finie (donc algébrique) de $\mathbb{F}_p$. De plus, un corps fini n'est pas algébriquement clos. En effet si $k = \{x_1, \ldots, x_n\}$ est un corps fini, alors le polynôme $1 + \prod_{x \in k}(X - x)$ ne s'annule pas sur k.

Lemme 17. *On a*

$$\forall p \in \mathbb{P},\ \forall 1 \leq k \leq p-1,\ p \left| \binom{p}{k} \right. .$$

Démonstration. Soit $p \in \mathbb{P}$. Pour tout $1 \leq k \leq p-1$ on a

$$p\binom{p-1}{k-1} = p\frac{(p-1)!}{(k-1)!(p-k)!} = \frac{p!}{(k-1)!(p-k)!} = k\frac{p!}{k!(p-k)!} = k\binom{p}{k},$$

ce qui donne

$$p\binom{p-1}{k-1} = k\binom{p}{k}.$$

Donc p divise $k\binom{p}{k}$ et comme p est premier et ne divise pas k, le lemme d'Euclide implique que p divise $\binom{p}{k}$. □

Proposition-Définition 3. *Pour un corps k de caractéristique $p \in \mathbb{P}$ non nulle, si on note $\mathcal{F}_p$ l'application*

$$\begin{array}{rccc} \mathcal{F}_p & : & k & \to & k \\ & & x & \mapsto & x^p \end{array},$$

alors $\mathcal{F}_p$ est un endomorphisme de corps appelé endomorphisme de Frobenius. De plus, si k est fini alors $\mathcal{F}_p$ est un automorphisme de corps induisant l'identité sur $\mathbb{F}_p \hookrightarrow k$.

Démonstration. L'application $\mathcal{F}_p$ est bien définie et vérifie $\mathcal{F}_p(1_k) = 1_k$. De plus

$$\forall x, y \in k,\ \mathcal{F}_p(xy) = (xy)^p = x^p y^p = \mathcal{F}_p(x)\mathcal{F}_p(y).$$

Soient ensuite $x, y \in k$. On a :

$$\mathcal{F}_p(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}.$$

Or, d'après le Lemme 17, pour tout $1 \leq k \leq p-1$, $\binom{p}{k} = 0$ car $\mathrm{car}(k) = p$. Alors

$$\mathcal{F}_p(x+y) = y^p + x^p = \mathcal{F}_p(x) + \mathcal{F}_p(y).$$

Donc $\mathcal{F}_p$ est bien un endomorphisme de corps.
Supposons à présent que k est fini. Comme $\mathcal{F}_p$ est un morphisme de corps, il est injectif et k étant fini, cet endomorphisme est aussi surjectif, c'est donc un automorphisme. De plus, d'après le théorème de Fermat, pour tout $a \in \mathbb{N}$ non multiple de p

$$a^{p-1} \equiv 1[p],\ \Rightarrow\ a^p \equiv a[p].$$

Donc, pour tout $x \in \mathbb{F}_p \supset k$, on a $\mathcal{F}_p(x) = x^p = x$, d'où le résultat. □

Théorème 20. *Soient $p \in \mathbb{P}$, $n \in \mathbb{N}^*$ et $q := p^n$. Alors il existe un corps fini à q éléments, unique à $\mathbb{F}_p$-isomorphisme près. Ce corps sera noté $\mathbb{F}_q$.*

Démonstration. Unicité : Si $\mathbb{F}_q$ et $\mathbb{F}'_q$ sont deux corps à q éléments, d'après le théorème de Lagrange, pour tout $x \in \mathbb{F}_q^*$ (resp. $x \in \mathbb{F}_q'^*$), alors $x^{q-1} - 1 = 0$ donc tout $x \in \mathbb{F}_q$ (resp. $x \in \mathbb{F}'_q$) vérifie $x^q = x$ et comme $(X^q - X)' = qX^{q-1} - 1 = -1 \neq 0$, le polynôme $X^q - X$ est à racines simples et donc $\mathbb{F}_q$ et $\mathbb{F}'_q$ sont deux corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. On en déduit $\mathbb{F}_q \simeq_{\mathbb{F}_p} \mathbb{F}'_q$.
Existence : Soit K un corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$. On pose

$$k := \{x \in K \ ; \ x^q = x\}.$$

On a $0, 1 \in k$ et soient $x, y \in k$. On a, par récurrence sur la Proposition-définition 3,

$$(x+y)^q = x^q + y^q = x + y,$$

et

$$(-x)^q = (-1)^q x^q = -x.$$

En effet, si $\mathrm{car}(K) \neq 2$ l'égalité est vraie et si $\mathrm{car}(K) = 2$, alors $2x = 0 \ \Rightarrow \ x = -x$ et l'égalité est encore vraie. De plus,

$$(xy)^q = x^q y^q = xy \text{ et } (x^{-1})^q = (x^q)^{-1} = x^{-1}.$$

On a alors

$$\forall x, y \in k, \ -x, x^{-1}, x+y, xy \in k$$

et donc k est un corps et le polynôme $X^q - X$ étant à racines simples, on a $|k| = q$ et $\mathbb{F}_q := k$ convient. □

Théorème 21. *Soit $\mathbb{F}_q$ un corps fini à $q = p^n$ éléments. Alors*

1. *$(\mathbb{F}_q^*, \cdot)$ est un groupe cyclique,*
2. *$\exists \alpha \in \mathbb{F}_q \ ; \ \mathbb{F}_q = \mathbb{F}_p(\alpha)$.*
3. *$\forall \beta \in \mathbb{F}_q, \ \mathbb{F}_q^* = \langle \beta \rangle \ \Leftrightarrow \ \Phi_{q-1,\mathbb{F}_p}(\beta) = 0$,*

Démonstration. 1. C'est une conséquence directe du Théorème 15 car $\mathbb{F}_q^*$ est un sous-groupe fini dans lui-même.
2. D'après le point 1., il existe $\alpha \in \mathbb{F}_q^*$ tel que $\mathbb{F}_q^* = \langle \alpha \rangle$. Clairement,

$$\mathbb{F}_p(\alpha) \subset \mathbb{F}_q. \tag{11}$$

Si $x \in \mathbb{F}_q$, soit $x = 0 \in \mathbb{F}_p \subset \mathbb{F}_p(\alpha)$, soit $x \in \mathbb{F}_q^*$ et alors il existe $i \in \mathbb{Z}$ tel que $x = \alpha^i \in \mathbb{F}_p(\alpha)$ donc

$$\mathbb{F}_q \subseteq \mathbb{F}_p(\alpha). \tag{12}$$

Les relations (11) et (12) impliquent que

$$\mathbb{F}_q = \mathbb{F}_p(\alpha).$$

3. On écrit

$$X^q - X = X(X^{q-1} - 1) = X \prod_{d|(q-1)} \Phi_{d,\mathbb{F}_p}(X)$$

$$= X(X-1)\Phi_{q-1,\mathbb{F}_p}(X) \prod_{\substack{1 \neq d \neq q-1 \\ d|(q-1)}} \Phi_{d,\mathbb{F}_p}(X) = \prod_{\zeta \in \mathbb{F}_q} (X - \zeta),$$

donc $\Phi_{q-1,\mathbb{F}_p}$ divise $X^q - X$ et comme ce dernier est à racines simples, il existe $x \in \mathbb{F}_q$ tel que $\Phi_{q-1,\mathbb{F}_p}(x) = 0$. De plus, quel que soit $\beta \in \mathbb{F}_q$, β engendre $\mathbb{F}_q^*$ si et seulement s'il est d'ordre $q-1$, si et seulement s'il annule $\Phi_{q-1,\mathbb{F}_p}$. □

Proposition 16. *Soient $p \in \mathbb{P}$, $n, m \in \mathbb{N}^*$ et $q := p^n$, $r := q^m$. Alors $\mathbb{F}_r$ est une extension de $\mathbb{F}_q$ si et seulement si n divise m.*

Démonstration. Si $\mathbb{F}_r$ est une extension de $\mathbb{F}_q$ alors $\mathbb{F}_r$ est un $\mathbb{F}_q$-espace vectoriel de dimension finie $k > 0$. Donc $r = q^k \Rightarrow m = kn$.
Réciproquement, supposons qu'il existe $k \in \mathbb{N}^*$ tel que $m = kn$. Tout $x \in \mathbb{F}_q$ vérifie $x^q = x$ donc, par récurrence, $x^{q^k} = x$, ie $x^r = x$, donc $x \in \mathbb{F}_r$. □

On peut résumer les résultats du Lemme 16 et des Théorèmes 20 et 21 par :

Théorème 22. *Tout corps de Galois est de cardinal une puissance d'un nombre premier et réciproquement, toute puissance d'un nombre premier est le cardinal d'un corps de Galois unique à isomorphisme près. De plus, tout corps de Galois $\mathbb{F}_{p^n}$ est une extension finie et simple de $\mathbb{F}_p$.*

2.6 Extensions normales et extensions séparables

Nous allons à présent nous intéresser aux extensions normales et séparables qui sont centrales dans l'étude de la théorie de Galois. Nous terminerons cette section en disant quelques mots sur les corps parfaits et nous y démontrerons le théorème de l'élément primitif.

Définition 24. Soit K/k une extension algébrique de corps. On dit que K/k est normale (ou quasi-galoisienne) si tout polynôme irréductible de $k[X]$ qui a une racine dans K y est scindé.

Théorème 23. *Soit K/k une extension de corps. Les assertions suivantes sont équivalentes :*

1. *L'extension K/k est finie et normale,*
2. *K est le corps de décomposition d'un polynôme à coefficients dans k.*

Démonstration. Supposons que K/k soit une extension normale et finie et soit $(x_1, \ldots, x_n)$ une base de K comme k-espace vectoriel. Pour $1 \leq i \leq n$, on note $P_i := \mu_{x_i,k}$ et $Q := P_1 \cdots P_n$. Alors $K = k(x_1, \ldots, x_n)$ et Q est scindé sur K car K/k est normale et on a $K \simeq \mathcal{D}_k(Q)$.
Réciproquement, soient $Q \in k[X]$ un polynôme non constant et supposons que $K \simeq \mathcal{D}_k(Q)$ (K/k est alors finie). Soient $P \in k[X]$ un polynôme irréductible tel qu'il existe $x_1 \in K$ tel que $P(x_1) = 0$, L un corps de décomposition de P sur K et $x_2 \in L$ une racine de P. Il s'agit de montrer que $x_2 \in K$. Pour $i = 1, 2$, on a $K(x_i) \simeq \mathcal{D}_{k(x_i)}(Q)$ et $k(x_i) \simeq \mathcal{R}_k(P)$ donc, d'après le Théorème 10, il existe un k-isomorphisme σ entre $k(x_1)$ et $k(x_2)$. On a alors

$$k(x_1) \hookrightarrow K(x_1) = K \text{ et } k(x_1) \xrightarrow{\sigma} k(x_2) \hookrightarrow K(x_2).$$

Donc K et $K(x_2)$ sont deux corps de décomposition de Q sur $k(x_1)$, ils sont donc $k(x_1)$-isomorphes d'après le Théorème 11 et on a $[K(x_2) : k(x_1)] = [K : k(x_1)]$, donc $K = K(x_2)$ et alors $x_2 \in K$. Donc P a toutes ses racines dans K et K/k est donc normale. □

Corollaire 13. *Soient $L/K/k$ trois extensions finies. Si L/k est normale alors il en est de même de L/K.*

Corollaire 14. *Soient K/k une extension finie et Ω un corps algébriquement clos contenant k. Alors K/k est normale si et seulement si tout les k morphismes $K \hookrightarrow \Omega$ ont la même image.*
En particulier, si Ω est un corps algébriquement clos contenant K, l'extension finie K/k est normale si et seulement si tout k-morphismes $K \to \Omega$ induit un automorphisme de K.

Démonstration. Supposons que l'extension K/k soit normale. D'après le Théorème 23, il existe $Q \in k[X]$ tel que $K \simeq \mathcal{D}_k(Q)$. Alors, pour tout k-morphisme $\sigma : K \to \Omega$, l'image de σ est l'extension de k engendrée par les racines de Q dans Ω et ne dépend donc pas de σ.
Inversement, pour tout k-morphisme $\sigma : K \to \Omega$, on note $K' := \sigma(K)$. Soit $P \in k[X]$ un polynôme irréductible ayant une racine $x \in K$ et soit $y \in \Omega$ une racine de P. $k(x) \subseteq K$ et $k(y) \subseteq \Omega$ sont deux corps de rupture de P d'où $k(x) \simeq_k k(y)$. Il existe donc un k-homomorphisme $k(x) \xrightarrow{\sim} k(y) \hookrightarrow \Omega$ qu'on peut étendre en $\tau : K \hookrightarrow \Omega$ d'après le Lemme 10 donc $\tau(K) = K'$ et on a $y \in K'$ donc P est scindé sur K' et donc P est scindé sur K car $K \simeq_k K'$ et donc l'extension K/k est normale. □

Corollaire 15. *Soient $L/K/k$ trois extensions finies telles que L/k est normale. Alors K/k est normale si et seulement si pour tout $g \in Aut_k(L)$ (groupe des automorphismes de L induisant l'identité sur k) on a $g(K) = K$.*

Démonstration. Il existe un corps algébriquement clos contenant L d'après le Théorème de Steinitz. D'après le Lemme 10, tout k-morphisme $\tau : K \hookrightarrow \Omega$ se prolonge en $\tau' : L \to \Omega$ et $\tau'(L) = L$ car L/k est normale et donc $\tau' \in \mathrm{Aut}_k(L)$.
Réciproquement, tout $g \in \mathrm{Aut}_k(L)$ induit un k-morphisme $L \hookrightarrow \Omega$. D'après le Corollaire 14, K/k est normale si et seulement si tous les $g(K)$ sont égaux à K. □

Corollaire 16. *Soit K/k une extension finie et normale. Alors tout $\sigma \in Aut(k)$ se prolonge en $\sigma' \in Aut(K)$.*

Démonstration. Soit $\sigma \in \mathrm{Aut}(k)$ et soit Ω un corps algébriquement clos contenant K. D'après le Lemme 10, le morphisme $k \overset{\sigma}{\simeq} k \hookrightarrow K \hookrightarrow \Omega$ se prolonge en $\sigma' : K \hookrightarrow \Omega$ et le Corollaire 14 implique que l'image de ce plongement est K, c'est donc un automorphisme du corps K. □

Proposition-Définition 4. *Soient K/k une extension finie et Ω un corps algébriquement clos contenant K. Il existe une plus petite extension L/K dans Ω telle que L/k soit normale. On appelle cette extension la clôture normale de K dans Ω et on la note $\mathcal{N}_K^\Omega$. Cette extension est, de plus, finie sur k.*

Démonstration. Soient $(x_1, \ldots, x_n)$ une base de$K$ comme k-espace vectoriel et $P_i := \mu_{x_i,k}$. Soit L le sous-corps de Ω engendré par les racines de $Q := P_1 \cdots P_n$. $L \simeq \mathcal{D}_k(Q)$ est donc une extension normale et finie de k d'après le Théorème 23. Pour toute extension $\Omega/L'/K$ telle que L'/k est normale, le polynôme irréductible P_i a une racine dans L', donc y est scindé et donc Q est également scindé dans L'. D'où $L \subseteq L'$. □

Remarque 8. Un démonstration analogue à celle du Théorme 23 permet de montrer qu'une extension (finie ou non) est normale si et seulement si c'est le corps de décomposition d'une famille de polynômes $(P_i)_{i\in I}$ à coefficients dans k. Les résultats des Corollaires 14, 15 et 16 s'adaptent au cas infini avec des démonstrations analogues. On peut donc énoncer le résultat suivant, dont on trouvera une preuve directe dans [6], théorème 5.3.3.

Théorème 24. *Soit K/k une extension algébrique contenue dans une clôture algébrique k^a de k. Les assertions suivantes sont équivalentes :*

1. *L'extension K/k est normale,*
2. *Tout polynôme irréductible de $k[X]$ ayant une racine dans K y est scindé,*
3. *K est le corps de décomposition d'une famille de polynômes de $k[X]$,*
4. *Tout k-homomorphisme $K \to k^a$ induit un automorphisme de K.*

Définition 25. On dit d'un polynôme à coefficients dans un corps qu'il est séparable s'il n'a que des racines simples dans un corps de décomposition. Si un polynôme n'est pas séparable, il sera dit inséparable.

Lemme 18. *Un polynôme P est séparable si et seulement si $P \wedge P' = 1$.*

Démonstration. Soient k un corps et $P \in k[X]$. D'après l'algorithme d'Euclide, pour toute extension K/k, le pgcd de P et P' est le même qu'il soit calculé dans $k[X]$ ou dans $K[X]$. Donc, si $K \simeq \mathcal{D}_k(P)$, P est à racines simples dans K si et seulement si P et P' n'ont pas de racine commune dans K, ce qui revient à dire que $P \wedge P' = 1$. □

Lemme 19. *Soient k un corps et un polynôme irréductible $P \in k[X]$. On a*

1. *P est séparable si et seulement si $P' \neq 0$.*
2. *P est inséparable si et seulement k est de caractéristique $p \neq 0$ et $P \in k[X^p]$.*

Démonstration. 1. C'est une conséquence immédiate du Lemme 18.
2. On écrit

$$P(X) = a_n X^n + \cdots + a_1 X + a_0.$$

Le polynôme

$$P'(X) = n a_n X^{n-1} + \cdots + 2a_2 X + a_1$$

est nul si et seulement si on a $a_i = 0$ pour tout i non divisible par p, ce qui est équivalent à dire que $\mathrm{car}(k) = p \neq 0$ et $P \in k[X^p]$. □

Lemme 20. *Soient k un corps de caractéristique $p \neq 0$ et $x \in k \setminus k^p$. Alors le polynôme $X^p - x$ est irréductible et inséparable dans $k[X]$.*

Démonstration. Soit P un facteur irréductible de $X^p - x$ et soit y une racine de P dans un corps de rupture. On a $x = y^p$ et donc $X^p - x = X^p - y^p = (X - y)^p$ dans $\mathcal{R}_k(P)[X]$ et ainsi $P(X) = (X - y)^i, 1 \leq i \leq p$. Comme $y \notin k$, on a $i \geq 2$, donc P n'est pas séparable sur k. D'après le Lemme 18, le degré de P est un multiple de p, donc $i = p$ et $X^p - x = P$ est irréductible. De plus, $(X^p - x)' = 0$ donc ce dernier est inséparable. □

Définition 26. Soit K/k une extension de corps.

1. On dit qu'un élément $\alpha \in K$ est séparable sur k s'il est algébrique et si son polynôme minimal $\mu_{\alpha,k}$ est séparable sur k.
2. L'extension K/k est dite séparable si tout élément de K est séparable sur k. En particulier, toute extension séparable est algébrique.
3. Si K/k est une extension algébrique, soit Ω un corps algébriquement clos contenant K. On sait, d'après le Lemme 10, que tout plongement $\sigma : k \hookrightarrow \Omega$ se prolonge en $\sigma' : K \hookrightarrow \Omega$. L'extension $\sigma'(K)/k$ est alors algébrique donc contenue dans une clôture algébrique k^a de k (Lemme 11). Or, d'après le Théorème de Steinitz, deux clôtures algébriques sont k-isomorphes, donc le cardinal de l'ensemble des prolongements de $k \hookrightarrow \Omega$ en $K \hookrightarrow \Omega$ est indépendant du corps algébriquement clos choisi Ω. Ce nombre sera noté $[K : k]_s$ est on l'appelle degré de séparabilité de l'extension K/k. On remarque que $[K : k]_s \geq 1$.

Lemme 21. *Soient K/k et L/K deux extensions algébriques. On a*

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

Démonstration. Soient Ω un corps algébriquement clos contenant L et soit $(\sigma_i)_{i\in I}$ la famille des k-homomorphismes $K \hookrightarrow \Omega$. On a $\mathrm{card}(I) = [K : k]_s$. On considère l'extension $\sigma_i : K \hookrightarrow \Omega$. Comme on l'a remarqué dans la définition 27-3., l'ensemble des prologements à L est indépendant de i et vaut $[L : K]_s$. On peut alors noter cet ensemble $(\tau_{i,j})_{j\in J}$ et on a $\mathrm{card}(J) = [L : K]_s$. On obtient alors une famille de k-morphismes distincts de L dans Ω indexée par $I \times J$. Inversement, étant donné un tel morphisme $L \hookrightarrow \Omega$, il se restreint à K en l'un des σ_i, c'est donc l'un des $\tau_{i,j}$, d'où le résultat. □

Lemme 22. *Soit K/k une extension simple de corps : $K = k(x)$ avec x algébrique sur k, de polynôme minimal P. Alors, toute extension algébriquement close $k \hookrightarrow \Omega$ se prolonge en $K \hookrightarrow \Omega$ et le nombre de ces prolongements est égal au nombre de racines distinctes de P dans son corps de décomposition.*

Démonstration. On a $K \simeq k[X]/(P)$. Ainsi, se donner un k-morphisme $\sigma : K \to \Omega$ est équivalent à se donner un élément $\sigma(x) \in \Omega$ tel que $P(\sigma(x)) = 0$. On en déduit qu'il y a autant de tels morphismes que de racines de P dans Ω, ou encore dans le sous-corps de Ω engendré par ces racines, qui est le corps de décomposition de P, d'où le résultat. □

Théorème 25. *Soit K/k une extension finie. On a*

$$1 \leq [K : k]_s \leq [K : k].$$

De plus, on a $[K : k]_s = [K : k]$ si et seulement si l'extension K/k est séparable.

Démonstration. Si l'extension K/k est simple : $K = k(x)$, alors en notant $P := \mu_{x,k}$, le Lemme 22 montre que $[K : k]_s$ est égal au nombre de racines distinctes de P dans son corps de décomposition. Ainsi, $[K : k]_s \leq [K : k]$ avec égalité si et seulement si x est séparable sur k.
Si K/k est finie quelconque, on l'écrit comme une tour finie de corps :

$$k \hookrightarrow k(x_1) \hookrightarrow k(x_1, x_2) \hookrightarrow \cdots \hookrightarrow k(x_1, \ldots, x_n) = K$$

et on utilise le Lemme 21 pour obtenir

$$[K : k]_s \leq [K : k].$$

Ensuite, si K/k est séparable, ou plus généralement, si K est engendré par des éléments $x_1, \ldots, x_n$ séparables sur k, alors chaque x_i est séparable sur $k(x_1, \ldots, x_{i-1})$ car son polynôme minimal sur ce corps divise son polynôme minimal sur k, donc est aussi séparable et on a

$$[k(x_1, \ldots, x_{i-1})(x_i) : k(x_1, \ldots, x_{i-1})]_s = [k(x_1, \ldots, x_{i-1})(x_i) : k(x_1, \ldots, x_{i-1})],$$

d'où $[K : k]_s = [K : k]$ d'après le Lemme 21.
Réciproquement, on suppose que $[K : k]_s = [K : k]$ et soit $x \in K$. On a

$$[K : k(x)]_s \leq [K : k(x)] \text{ et } [k(x) : k]_s \leq [k(x) : k] \tag{13}$$

et d'après le Lemme 21, il y a égalité dans les relations (13). x est donc séparable sur k et l'extension K/k est alors séparable. □

Corollaire 17. *Toute extension engendrée par des éléments séparables est séparable.*

Théorème 26. *Soient K/k et L/K deux extensions de corps. Si $x \in L$ est séparable sur K et si K/k est séparable, alors x est séparable sur k.*

Démonstration. Si $x \in L$ est séparable sur K, alors il est algébrique et est alors racine d'un polynôme $P \in K[X]$. Si K/k est séparable, alors l'extension finie $K' \subseteq K$ de k engendrée par les coefficients de P est finie et séparable, donc $[K' : k]_s = [K' : k]$ d'après le Théorème 25. Or, x étant séparable sur K, l'extension $K'(x)/K'$ est séparable et on a $[K'(x) : K']_s = [K'(x) : K']$. Avec le Lemme 21, il vient $[K'(x) : k]_s = [K'(x) : k]$. L'extension finie $K'(x)/k$ est alors séparable et donc x est aussi séparable sur k. □

Corollaire 18. *Si $L/K/k$ sont trois extensions, alors L/k est séparable si et seulement si L/K et K/k le sont.*

Démonstration. Si l'extension L/k est séparable, il est évident que l'extension K/k l'est aussi, ainsi que L/K, puisque le polynôme minimal de x sur K divise son polynôme minimal sur k. La réciproque vient de la première partie du théorème. □

Proposition-Définition 5. *Soit K/k une extension. L'ensemble des éléments de K séparables sur k forme un sous-corps de K et une extension séparable de k. On appelle cette extension la clôture séparable de k dans K et on la note $\mathcal{S}_k^K$.*

Démonstration. Soient $x, y \in K$ deux éléments séparables sur k. D'après le Corollaire 17, l'extension $k(x, y)/k$ est séparable. Les éléments $x - y$ et x/y de K sont alors séparables sur k. L'ensemble des éléments de K séparables sur k est donc bien un sou-corps de K. □

Définition 27. Soient k un corps et k^a une clôture algébrique de k. La clôture séparable de k dans k^a est simplement appelée la clôture séparable de k et on la note $k^s := \mathcal{S}_k^{k^a}$.

Nous pouvons maintenant parler de corps parfait :

Définition 28. Un corps k est dit parfait si toute extension algébrique de k est séparable.

Théorème 27. *Un corps k est parfait si et seulement si l'une des deux conditions suivantes est réalisée :*

1. *$car(k) = 0$,*
2. *$car(k) = p$ et $k = k^p$.*

Démonstration. Soit K/k une extension algébrique.
- Si $\text{car}(k) = 0$, alors tout élément de K est séparable sur k d'après le Lemme 19, donc K/k est séparable et k est parfait.
- Si $\text{car}(k) = p \neq 0$, on a $k^p := \{x^p,\ x \in k\}$ et on suppose que $k^p = k$. Soient $\alpha \in K$ et $P := \mu_{\alpha,k}$. Si P est inséparable sur k, alors d'après le Lemme 19, P est de la forme

$$P(X) = \sum_{i=0}^{r} a_i X^{ip},\ r \in \mathbb{N}^*,\ a_i \in k,\ \forall 0 \leq i \leq r.$$

On a

$$k = k^p \ \Rightarrow\ \forall 0 \leq i \leq r,\ \exists b_i \in k\ ;\ a_i = b_i^p,$$

d'où

$$P(X) = \sum_{i=0}^{r} b_i^p (X^i)^p = \left(\sum_{i=0}^{r} b_i X^i \right)^p, \tag{14}$$

car $\text{car}(k) = p$. L'équation (14) est en contradiction avec le fait que P soit irréductible dans $k[X]$, donc P est séparable sur k et donc K/k est une extension séparable. Ainsi, k est parfait.
Inversement, supposons que k soit un corps parfait, alors $\text{car}(k) = 0$ ou $\text{car}(k) = p \neq 0$. Dans ce second cas, montrons que $k = k^p$. Soit donc $a \in k$.

Si $a = 0$, alors $a = 0^p$ et on peut supposer que $a \neq 0$. Par l'absurde, supposons que $a \in k \setminus k^p$. D'après le Lemme 20, le polynôme $X^p - a$ est irréductible et inséparable dans $k[X]$. Alors $\mathcal{R}_k(X^p - a)$ est une extension algébrique de k et inséparable, ce qui est absurde car k est parfait. Donc $a \in k^p$ et $k^p = k$. □

Corollaire 19. *$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ et les corps finis $\mathbb{F}_q$ sont des corps parfaits.*

Démonstration. Comme $\mathrm{car}(\mathbb{Q}) = \mathrm{car}(\mathbb{R}) = \mathrm{car}(\mathbb{C}) = 0$, ces corps sont parfaits en vertu du Théorème 27. Soient ensuite $p \in \mathbb{P}$, $n \in \mathbb{N}^*$ et $q = p^n$. Comme on l'a vu dans la Proposition-définition 3, l'automorphisme de Frobenius montre que

$$\mathbb{F}_q = \mathbb{F}_q^p,$$

et donc $\mathbb{F}_q$ est parfait d'après le Théorème 27. □

Enfin, on termine cette section par un résultat fondamental dans létude des extensions séparables : le théorème de l'élément primitif.

Lemme 23. *Soient k un corps, $K := k(x, y_1, \ldots, y_n)$ une extension finie avec $y_1, \ldots, y_n$ séparables sur k. Alors*

$$\exists \alpha \in K \ ; \ K = k(\alpha).$$

Démonstration. - Si k est fini, le résultat vient directement du Théorème 21-2..
- Si k est infini, on voit par récurrence qu'il suffit de considérer le cas $n = 1$, $y := y_1$ et $K = k(x, y)$. On pose

$$\begin{cases} P := \mu_{x,k} \in k[X] \\ Q := \mu_{y,k} \in k[X] \end{cases}$$

Alors Q est séparable par hypothèse. On écrit

$$P = \prod_{j=1}^{r} (X - \alpha_j) \in \mathcal{D}_k(P)[X]$$

et

$$Q = \prod_{i=1}^{s} (X - \beta_i) \in \mathcal{D}_k(Q)[X],$$

avec $\alpha_1 = x,\ \beta_1 = y$ et $\forall i \neq j,\ \beta_i \neq \beta_j$ car Q est séparable. Comme k est infini, il existe $t \in k$ tel que

$$\forall i \neq 1 \neq j,\ t \neq \frac{x - \alpha_j}{\beta_j - y}.$$

On pose $z := x + ty \in k(x, y)$. On a

$$\forall j \neq 1,\ P(z - t\beta_j) \neq 0 \text{ et } P(z - t\beta_1) = P(z - ty) = P(x) = 0.$$

Donc $Q(X) \in k[X]$ et $P(z - tX) \in k(z)[X]$ ont une racine commune, ainsi $P \wedge Q = X - y$ et comme $P \wedge Q \in k(z)[X]$, on a $y \in k(z)$, donc $x = z - ty \in k(z) \ \Rightarrow\ K = k(x, y) \subset k(z) \ \Rightarrow\ K = k(z)$. □

<u>Théorème</u> 28. *Toute extension séparable finie est simple.*

Démonstration. Si K/k est une extension finie, il existe $\alpha_1, \ldots, \alpha_n \in K$ tels que $K = k(\alpha_1, \ldots, \alpha_n)$ d'après la Proposition 7. Comme K/k est séparable, les $\alpha_1, \ldots, \alpha_n$ sont séparables sur k et d'après le Lemme 23, on peut choisir $z \in K$ tel que $K = k(z)$. L'extension K/k est donc simple, et le théorème est démontré. □

Deuxième partie
Théorie de Galois et Applications

3 Introduction à la Théorie de Galois

3.1 Extensions galoisiennes et groupes de Galois

Dans cette section, nous allons étudier les extensions galoisiennes finies ainsi que des groupes particuliers qui leurs sont liés, appelés groupes de Galois. Cette étude fait le lien entre la théorie de corps et la théorie des groupes et constitue le fondement de la théorie de Galois. Cette approche à été menée par Évariste Galois en 1829 dans le but de répondre à la question des équations résolubles par radicaux ; question à laquelle nous répondrons à la fin de ce cours.
Notons que l'on peut également parler d'extension galoisienne infinie, mais leur étude est plus délicate. A ce sujet, on pourra consulter par exemple [6].

Définition 29. Soit K/k une extension finie de corps. On dit que K/k est une extension galoisienne si elle est normale et séparable.

Lemme 24. *Soit K/k une extension finie. Alors*

$$|Aut_k(K)| \leq [K : k]_s \leq [K : k].$$

De plus, les inégalités ci-dessus sont des égalités si et seulement si K/k est galoisienne.

Démonstration. Soit Ω un corps algébriquement clos contenant K. Ce dernier existe d'après le Théorème de Steinitz. On a une injection canonique

$$\mathrm{Aut}_k(K) \hookrightarrow \mathrm{Hom}_k(K, \Omega),$$

d'où

$$|\mathrm{Aut}_k(K)| \leq |\mathrm{Hom}_k(K,\Omega)| \overset{\text{def}}{=} [K:k]_s \leq [K:k]$$

d'après le Théorème 25. Encore avec le Théorème 25 et le corollaire 13, on voit que l'on a égalité si et seulement si l'extension K/k est simultanément normale et séparable, c'est-à-dire si elle est galoisienne. □

Théorème 29. *Soit K/k une extension finie. Les assertions suivantes sont équivalentes :*

1. *K/k est galoisienne,*
2. *$|Aut_k(K)| = [K:k]$,*
3. *Il existe un polynôme séparable $P \in k[X]$ tel que $K \simeq \mathcal{D}_k(P)$.*

Démonstration. 1. $\Leftrightarrow$ 2. Cela a été établi dans le Lemme précédent.
1. $\Leftrightarrow$ 3. S'il existe $P \in k[X]$ séparable tel $K \simeq \mathcal{D}_k(P)$, K/k est engendrée par des éléments séparables, donc est normale et séparable d'après le Théorème 23 et le Corollaire 17. Inversement, si K/k est galoisienne, on écrit $K = k(\alpha_1, \ldots, \alpha_n)$ et $P_i := \mu_{\alpha_i,k}$. Comme K/k est normale et séparable, chaque P_i est simplement scindé dans K, donc $P := P_1 \vee \cdots \vee P_n$ aussi. Ensuite, K/k étant engendrée par les α_i, racines de P, on a $K \simeq \mathcal{D}_k(P)$. □

Exemple 4.
1. $\mathbb{C}/\mathbb{R}$ est galoisienne car $\mathbb{C} \simeq \mathcal{D}_{\mathbb{R}}(X^2+1)$ et l'on peut appliquer le Théorème 29.
2. De même, comme $\mathbb{F}_q = \mathcal{D}_{\mathbb{F}_p}(X^q - X)$, l'extension $\mathbb{F}_q/\mathbb{F}_p$ est galoisienne.

Définition 30. Soit K/k une extension galoisienne. Le groupe $\mathrm{Aut}_k(K)$ des k-automorphismes de K est appelé le groupe de Galois de l'extension K/k et on le note $\mathrm{Gal}(K/k)$.

Avec le Théorème 29, on a trivialement

Proposition 17. *Pour une extension galoisienne K/k, on a*

$$|Gal(K/k)| = [K:k].$$

Définition 31. Une extension galoisienne est dite abélienne (resp. monogène, cyclique) si son groupe de Galois est abélien (resp. monogène, cyclique).

Exemple 5. $\mathbb{C}/\mathbb{R}$ est cyclique d'ordre 2. En effet, elle est galoisienne (Exemple 4). De plus, si $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ alors

$$\forall z = x + iy \in \mathbb{C},\ \sigma(z) = \sigma(x + iy) = \sigma(x) + \sigma(i)\sigma(y) = x + \sigma(i)y.$$

Donc σ est déterminé par son image en i, qui est soit i soit $-i$. Si $\sigma(i) = i$ alors $\sigma = id_{\mathbb{C}}$. Si $\sigma(i) = -i$, alors σ est la conjugaison complexe

$$\gamma : x + iy \mapsto x - iy.$$

Ainsi $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{id_{\mathbb{C}}, \gamma\}$ est d'ordre 2, donc cyclique.

Théorème 30. *Soient $p \in \mathbb{P},\ n \in \mathbb{N}^*,\ q := p^n$. Alors $\mathbb{F}_q/\mathbb{F}_p$ est galoisienne et*

$$Gal(\mathbb{F}_q/\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}.$$

Autrement dit, l'extension $\mathbb{F}_q/\mathbb{F}_p$ est cyclique d'ordre n.

Démonstration. Nous avons déjà vu dans l'Exemple 4 que $\mathbb{F}_q/\mathbb{F}_p$ est galoisienne. Ensuite, d'après la Proposition-Définition 3, le morphisme de Frobenius $\mathcal{F}_p$ est un automorphisme de $\mathbb{F}_q$ induisant l'identité sur $\mathbb{F}_p$. On a alors $\mathcal{F}_p \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. D'après le Théorème 21-1., il existe $x \in \mathbb{F}_q^*$ tel que $\mathbb{F}_q^* = \langle x \rangle$. On pose $P := \mu_{x,\mathbb{F}_p}$. Alors $\deg P = n$ car $\mathbb{F}_q = \mathbb{F}_p(x)$. Comme $P(x) = 0$, on a

$$\forall 1 \leq i \leq n,\ P(\mathcal{F}_p^i(x)) = \mathcal{F}_p^i(P(x)) = 0$$

car $\mathcal{F}_{p|\mathbb{F}_p} = id_{\mathbb{F}_p}$ et $P \in \mathbb{F}_p[X]$. De plus, $\forall 1 \leq i \neq j \leq n$, on a $\mathcal{F}_p^i(x) \neq \mathcal{F}_p^j(x)$, donc l'ensemble

$$\left\{\mathcal{F}_p^i(x),\ 1 \leq i \leq n\right\}$$

constitue l'ensemble des n racines de P dans $\mathbb{F}_q$. Ainsi, si $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, on a $P \circ \sigma = \sigma \circ P$ donc il existe $j \in \{1, \ldots, n\}$ tel que

$$\sigma(x) = \mathcal{F}_p^j(x).$$

Dans ce cas, on a

$$\sigma(x^i) = \sigma(x)^i = (\mathcal{F}_p^j(x))^i = \mathcal{F}_p^j(x^i) \text{ et } \sigma(0) = 0 = \mathcal{F}_p^j(0)$$

et donc

$$\sigma = \mathcal{F}_p^j,$$

ce qui montre que $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle \mathcal{F}_p \rangle$. Enfin, $i \neq j \ \Rightarrow \ \mathcal{F}_p^i \neq \mathcal{F}_p^j$ et $\mathcal{F}_p^n = id_{\mathbb{F}_q}$, donc $\langle \mathcal{F}_p \rangle$ est cyclique, d'ordre n. D'où $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle \mathcal{F}_p \rangle \simeq \mathbb{Z}/n\mathbb{Z}$, ce qui termine la démonstration. □

Lemme 25. *Soit K/k une extension galoisienne. D'après le Théorème 29, il existe un polynôme séparable $P \in k[X]$ tel que $K \simeq \mathcal{D}_k(P)$. On pose $n := \deg P$. Alors*

$$Gal(K/k) \lesssim \mathfrak{S}_n$$

ie $Gal(K/k)$ est isomorphe à un sous-groupe de $\mathfrak{S}_n$. Autrement dit, $Gal(K/k)$ permute les racines de P dans K.

Démonstration. On écrit

$$P(X) = \prod_{i=1}^{n} (X - \alpha_i), \ i \neq j \ \Rightarrow \ \alpha_i \neq \alpha_j.$$

Alors $K = k(\alpha_1, \ldots, \alpha_n)$. K/k est normale donc le conjugué de $\alpha_i \in K$ (ie un élément $x \in K$ tel que $\mu_{\alpha_i,k}(x) = 0$) est dans K et est l'un des α_j, $j \neq i$ car P est séparable. Si $\sigma \in \mathrm{Gal}(K/k)$, $\sigma \circ P = P \circ \sigma$ car $P \in k[X]$, donc $\sigma(\alpha_i)$ est un conjugué de α_i, d'où $\sigma(\alpha_i) \in \{\alpha_1, \ldots, \alpha_n\}$. Ainsi, l'application

$$\begin{array}{rccc} \omega & : & \mathrm{Gal}(K/k) \times \{\alpha_1, \ldots, \alpha_n\} & \to & \{\alpha_1, \ldots, \alpha_n\} \\ & & (\sigma, \alpha_i) & \mapsto & \sigma(\alpha_i) \end{array}$$

est bien définie et c'est une action de groupe. L'application

$$\begin{array}{rccc} \pi & : & \mathrm{Gal}(K/k) & \to & \mathfrak{S}(\alpha_1, \ldots, \alpha_n) \simeq \mathfrak{S}_n \\ & & \sigma & \mapsto & \omega(\sigma, \cdot) \end{array}$$

est donc un morphisme de groupes. De plus, comme K/k est galoisienne,

$$|\mathrm{Gal}(K/k)| = [K : k] \leq n! = |\mathfrak{S}_n|,$$

d'après la Proposition 10. Enfin, si $\pi(g) = \pi(g')$, alors pour tout i, $g^{-1}g'(\alpha_i) = \alpha_i$ et comme $g^{-1}g'_{|k} = id_k$ on a $g^{-1}g' = id_K$ et donc $g' = g$. π est alors un monomorphisme de groupe, donc un isomorphisme sur son image et on a bien

$$\mathrm{Gal}(K/k) \lesssim \mathfrak{S}_n.$$

□

Lemme 26. *Soient K/k une extension normale finie et $P \in k[X]$ un polynôme séparable et scindé dans K. Alors P est irréductible si et seulement si l'action de $Gal(K/k)$ sur l'ensemble des racines de P dans K est transitive.*

Démonstration. Par contraposée, supposons que P ne soit pas irréductible et écrivons $P = QR$. P étant séparable, Q et R n'ont pas de racine commune. Or, tout $\sigma \in \mathrm{Gal}(K/k)$ envoie une racine de Q sur une racine de Q ; l'action n'est donc pas transitive.
Réciproquement, supposons que P est irréductible et soit $Q \in k[X]$ séparable tel que $K \simeq \mathcal{D}_k(Q)$. Soient encore $x, y \in K$ tels que $P(x) = P(y) = 0$. Comme $k(x)$ et $k(y)$ sont des corps de rupture de P sur k, il existe un k-isomorphisme $\sigma : k(x) \xrightarrow{\sim} k(y)$ tel que $\sigma(x) = y$. Alors

$$i : k(x) \hookrightarrow K$$

et

$$i' : k(x) \xrightarrow{\sim} k(y) \hookrightarrow K$$

sont des corps de décomposition de $Q \in k(x)[X]$, et sont donc $k(x)$-isomorphes. Il existe donc $g \in \mathrm{Aut}(K)$ tel que $g \circ i = i'$. $g_{|k} = id_k \;\Rightarrow\; g \in \mathrm{Gal}(K/k)$ et on a $g(x) = g(i(x)) = i'(x) = y$. L'action est ainsi transitive. □

Théorème 31. *Soient k un corps parfait et K/k une extension finie. Alors K/k est galoisienne si et seulement si l'action de $Aut_k(K)$ sur les conjugués de tout élément de K est transitive.*

Démonstration. Si K/k est galoisienne, le Lemme 26 donne le résultat. Montrons que la condition est suffisante. L'extension K/k étant séparable et finie, le Théorème de l'élément primitif (Théorème 28) montre qu'il existe $x \in K$ tel que $K = k(x)$. $\deg_k(x) = [K : k]$ donc x a exactement $[K : k]$ conjugués dans K et la transitivité de l'action de $\mathrm{Aut}_k(K)$ implique que $|\mathrm{Aut}_k(K)| \geq [K : k]$. Ainsi, $|\mathrm{Aut}_k(K)| = [K : k]$ et l'extension K/k est galoisienne en vertu du Théorème 29. □

Lemme 27. *Soient $n \in \mathbb{N}^*$ et $\omega \in \mu_n^*(\mathbb{Q})$. Alors*

1. *$\mathbb{Q}(\omega)/\mathbb{Q}$ est galoisienne et on note G_ω son groupe de Galois,*
2. *Il existe une application $\chi : G_\omega \to (\mathbb{Z}/n\mathbb{Z})^*$ telle que*
$$\forall(\sigma, \eta) \in G_\omega \times \mu_n(\mathbb{Q}),\ \sigma(\eta) = \eta^{\chi(\sigma)},$$
3. *De plus, χ est un monomorphisme de groupes.*

Démonstration.

1. D'après le Théorème 18, Φ_n est irréductible sur $\mathbb{Q}$ et séparable par définition, et comme $\mathcal{R}_\mathbb{Q}(\Phi_n) \simeq \mathcal{D}_\mathbb{Q}(\Phi_n) \simeq \mathbb{Q}(\omega)$, l'extension $\mathbb{Q}(\omega)/\mathbb{Q}$ est galoisienne d'après le Théorème 29.
2. L'image de $\omega \in \mu_n^*(\mathbb{Q})$ par un $\sigma \in G_\omega = \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ s'écrit
$$\sigma(\omega) = \omega^{\chi(\sigma)},\ \chi(\sigma) \in \mathbb{Z}/n\mathbb{Z}$$
et comme $\sigma(\omega) \in \mu_n^*(\mathbb{Q})$, on a $\chi(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^*$. De plus, si $\eta \in \mu_n(\mathbb{Q})$, on a $\eta = \omega^m$ et alors
$$\sigma(\eta) = \sigma(\omega^m) = \sigma(\omega)^m = \omega^{m\chi(\sigma)} = (\omega^m)^{\chi(\sigma)} = \eta^{\chi(\sigma)}.$$
3. Soient $\sigma, \sigma' \in G_\omega,\ \eta \in \mu_n(\mathbb{Q})$. On a
$$\eta^{\chi(\sigma')\chi(\sigma)} = \eta^{\chi(\sigma)\chi(\sigma')} = \sigma'(\eta^{\chi(\sigma)}) = \sigma'(\sigma(\eta)) = (\sigma' \circ \sigma)(\eta) = \eta^{\chi(\sigma' \circ \sigma)}$$
$$\Rightarrow\ \chi(\sigma')\chi(\sigma) = \chi(\sigma'\sigma)$$
et
$$\eta = (\sigma \circ \sigma^{-1})(\eta) = \sigma(\eta^{\chi(\sigma^{-1})}) = \eta^{\chi(\sigma)\chi(\sigma^{-1})}\ \Rightarrow\ \chi(\sigma^{-1}) = \chi(\sigma)^{-1},$$
donc, χ est un morphisme de groupes. Comme ω engendre $\mathbb{Q}(\omega)$, χ est injectif ; c'est donc un monomorphisme.

□

Théorème 32. *Soient $n \in \mathbb{N}^*$ et $\omega \in \mu_n^*(\mathbb{Q})$. Alors $\mathbb{Q}(\omega)/\mathbb{Q}$ est galoisienne, de groupe de Galois $(\mathbb{Z}/n\mathbb{Z})^*$.*

Démonstration. On a vu au Lemme 27 que $\mathbb{Q}(\omega)/\mathbb{Q}$ est une extension galoisienne. D'après le Corollaire 11 et la Proposition 17, on a

$$|G_\omega| = [\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|.$$

Le monomorphisme $\chi : G_\omega \to (\mathbb{Z}/n\mathbb{Z})^*$ est donc surjectif ; c'est donc un isomorphisme et on a

$$\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = G_\omega \simeq (\mathbb{Z}/n\mathbb{Z})^*.$$

□

Proposition-Définition 6. *Soient K/k une extension finie séparable et Ω un corps algébriquement clos contenant K. La clôture normale $\mathcal{N}_K^\Omega$ de K dans Ω est une extension finie et galoisienne de k. On l'appelle la clôture galoisienne de K dans Ω et on la note $\mathcal{G}_K^\Omega$.*

Démonstration. D'après la preuve de la Proposition-Définition 4, si P_i est séparable, alors $P_1 \vee \ldots \vee P_n$ l'est aussi et donc $\mathcal{N}_K^\Omega$ est séparable sur k. De plus, comme elle est normale et finie, elle est bien galoisienne. □

3.2 Lemme d'Artin et Correspondance de Galois

Proposition 18. *Soient K/k une extension galoisienne et $L/k \subseteq K/k$ une extension intermédiaire. Alors K/L est galoisienne et on a*

$$[L : k] = [Gal(K/k) : Gal(K/L)].$$

Démonstration. Il est clair, d'après les Corollaires 13 et 18, que K/L est galoisienne. On a

$$|\mathrm{Gal}(K/k)| = [K : k] = [K : L][L : k] = |\mathrm{Gal}(K/L)|[L : k],$$

donc

$$[L : k] = \frac{|\mathrm{Gal}(K/k)|}{|\mathrm{Gal}(K/L)|} \overset{\text{def}}{=} [\mathrm{Gal}(K/k) : \mathrm{Gal}(K/L)].$$

□

Définition 32. Soient K/k une extension galoisienne et $G \leq \mathrm{Gal}(K/k)$. On appelle corps des invariants de K par G le sous-corps de K défini par

$$K^G := \{x \in K \ ; \ \sigma(x) = x, \ \forall \sigma \in G\}.$$

Lemme 28. *(Artin) Soient K un corps et $G \leq Aut(K)$ un sous-groupe fini du groupe des automorphismes de K. Alors l'extension K/K^G est galoisienne, de groupe de Galois G.*

Démonstration. Soient $k := K^G$ et $x \in K$. G agit trivialement sur K et si Gx représente l'orbite de x dans K, posons

$$P(X) := \prod_{y \in Gx} (X - y) = \prod_{g \in G} (X - g(x)).$$

On a

$$\forall g \in G, \ gP = P \ \Rightarrow \ P \in k[X],$$

et P séparable donc x est séparable sur k et $\deg_k(x) \leq |G|$. On peut choisir $x_0 \in K$ de degré maximal et montrons que $K = k(x_0)$. Soit donc $y \in K$.

x_0 et y étant séparables sur k, $k(x_0, y)$ est une extension séparable et finie de k. D'après le Théorème de l'élément primitif, il existe $z \in k(x_0, y)$ tel que $k(x_0, y) = k(z)$. Or, $k(z)$ contient $k(x_0)$, ce qui implique que $k(z) = k(x_0)$ par maximalité du degré de x_0. Donc $y \in k(x_0)$ et $K = k(x_0)$ est une extension finie de degré inférieur ou égal à $|G|$. Alors, avec le Lemme 24,

$$|G| \leq |\mathrm{Aut}_k(K)| \leq [K : k] \leq |G|,$$

donc on a égalité partout. En utilisant le Théorème 29, on en déduit que l'extension K/k est galoisienne et

$$\mathrm{Gal}(K/K^G) = \mathrm{Gal}(K/k) = G.$$

□

Lemme 29. *Soit K/k une extension galoisienne, de groupe de Galois G. Alors $k = K^G$.*

Démonstration. On a clairement $k \subseteq K^G$. Soient $x \in K^G$ et $P := \mu_{x,k}$ son polynôme minimal, scindé sur K. Soit ensuite que $y \in K$ une racine de P. L'extension K/k est normale et $P \in k[X]$ est irréductible et séparable, donc d'après le Lemme 26, il existe $g \in G$ tel que $g(x) = y$. Or $x \in K^G$, donc $y = x$. P n'a donc qu'une racine et étant séparable, il est de degré 1 et ainsi $x \in k$, d'où le résultat. □

Définition 33. Soient K/k une extension galoisienne, de groupe de Galois $G := \mathrm{Gal}(K/k)$. On note

$$\mathfrak{K} := \{k \hookrightarrow L \ ; \ L/k \subseteq K/k\}$$

l'ensemble des corps intermédiaires entre k et K et

$$\mathfrak{G} := \{H \subseteq G \ ; \ H \leq G\}$$

l'ensemble des sous-groupes de G. Ces deux ensembles sont partiellement ordonnés par l'inclusion. On pose

$$\begin{array}{rccc} \gamma & : & \mathfrak{K} & \to & \mathfrak{G} \\ & & L & \mapsto & \mathrm{Gal}(K/L) \end{array} \qquad \begin{array}{rccc} \delta & : & \mathfrak{G} & \to & \mathfrak{K} \\ & & H & \mapsto & K^H \end{array}$$

Le couple (γ, δ) est appelé la correspondance de Galois associée à l'extension K/k.

Théorème 33. *(Correspondance de Galois) Si K/k est galoisienne, alors la correspondance de Galois (γ, δ) associée à K/k est un couple de bijections décroissantes et réciproques l'une de l'autre.*

Démonstration. Soient $L \in \mathfrak{K}$ et $H \in \mathfrak{G}$. On a clairement

$$L \subseteq \delta(\gamma(L)) = L^{\mathrm{Gal}(K/L)}$$

et

$$H \subseteq \gamma(\delta(H)) = \mathrm{Gal}(K/K^H),$$

il s'agit donc de montrer les inclusions réciproques. L'extension K/L est galoisienne en vertu des Corollaires 13 et 18. D'après le Lemme 29, on a

$$L = K^{\mathrm{Gal}(K/L)} \ \Rightarrow \ L = \delta(\gamma(L)).$$

Ensuite, d'après le Lemme d'Artin, on a

$$H = \mathrm{Gal}(K/K^H) \ \Rightarrow \ H = \gamma(\delta(H)).$$

Ainsi,

$$\delta \circ \gamma = id_{\mathfrak{K}}, \ \gamma \circ \delta = id_{\mathfrak{G}}.$$

□

Théorème 34. *Soient K/k une extension galoisienne, de groupe de Galois G et $H \leq G$ un sous-groupe. Alors l'extension K^H/k est galoisienne si et seulement si $H \trianglelefteq G$ et dans ce cas on a*

$$Gal(K^H/k) \simeq G/H.$$

Démonstration. Soient $H \leq G$ et $g \in G$. L'extension $g(K^H)/k$ est galoisienne, de groupe de Galois $gHg^{-1} \leq G$ (car $(ghg^{-1})(x) = x \ \Leftrightarrow \ h(g^{-1}(x)) = g^{-1}(x)$). D'après le Corollaire 15 et la Correspondance de Galois, K^H/k est normale (donc galoisienne) si et seulement si $gHg^{-1} = H$, ie si et seulement si $H \trianglelefteq G$. Soit ensuite le morphisme canonique

$$\varphi : G \to \mathrm{Gal}(K^H/k).$$

Alors φ est surjectif d'après le Corollaire 15 et on a

$$\mathrm{Ker}(\varphi) = \{g \in G \ ; \ g_{|K^H} = id_{K^H}\} = H,$$

avec la Correspondance de Galois. Donc, d'après le théorème d'isomorphie, il vient

$$\mathrm{Gal}(K^H/k) = \mathrm{Im}(\varphi) \simeq G/\mathrm{Ker}(\varphi) = G/H.$$

□

Nous pouvons résumer les résultat des Théorèmes 33, 34 et de la Proposition 18 avec

Théorème 35. *(Théorème fondamental de Galois) Soient K/k une extension galoisienne de groupe de Galois G et $k \hookrightarrow L \hookrightarrow K$ un corps intermédiaire. Alors*

1. *La correspondance de Galois (γ, δ) associée à K/k est un couple de bijections décroissantes, réciproques l'une de l'autre.*
2. *L'extension K/L est galoisienne et en notant $H := Gal(K/L)$, on a*

$$[L : k] = [G : H].$$

3. *Les assertions suivantes sont équivalantes :*
   (a) L/k est galoisienne
   (b) L/k est normale
   (c) $H \trianglelefteq G$

   et dans ce cas, on a

$$Gal(L/k) \simeq Gal(K/k)/Gal(K/L) = G/H.$$

4. *En outre, si $H \leq G$, alors K^H/k est galoisienne si et seulement si $H \trianglelefteq G$ et dans ce cas on a*

$$Gal(K^H/k) \simeq G/H.$$

3.3 Théorème de Kummer

Nous terminons cette section par l'impressionnant théorème de Kummer, résultat qui nous sera grandement utile lors de l'étude des équations résolubles par radicaux.

Lemme 30. *Soient k un corps et $n \in \mathbb{N}^*$ tels que $car(k) = 0$ ou $car(k) \nmid n$ et $a \in k$. Si une extension K/k est engendrée par une racine du polynôme $X^n - a$, alors K/k est galoisienne et on a*

$$Gal(K/k) \leq \mu_n(k).$$

En particulier, l'extension K/k est cyclique.

Démonstration. Soit $x \in K$ tel que $K = k(x)$ et $x^n = a$. Les racines de $X^n - a$ sont les ηx, avec $\eta \in \mu_n(k)$ qui sont toutes dans K par hypothèse puisque $|\mu_n(k)| = n$ avec la Proposition 13-1.. L'extension K/k est donc un corps de décomposition de $X^n - a$ et est ainsi galoisienne. Ensuite, tout élément $g \in \mathrm{Gal}(K/k)$ permute les racines de $X^n - a$ et est déterminé par son image $\eta_g x$ en x car les éléments de $\mu_n(k) \subseteq k$ sont fixes. On en déduit l'existence d'un monomorphisme de groupes

$$\begin{array}{ccc} \mathrm{Gal}(K/k) & \to & \mu_n(k) \\ g & \mapsto & \eta_g \end{array},$$

d'où le résultat. □

Théorème 36. *(Kummer) Soient k un corps, $n \in \mathbb{N}^*$ tels que $car(k) = 0$ ou $car(k) \nmid n$. Une extension K/k est cyclique d'ordre n si et seulement s'il existe $a \in k$ tel que, pour tout $1 < d|n$, $a \notin k^d$ et $K \simeq \mathcal{D}_k(X^n - a)$. Ce polynôme est alors irréductible et K est aussi son corps de rupture.*

Démonstration. Supposons que K soit un corps de décomposition sur k de $X^n - a := P(X)$ avec $a \notin k^d$ pour tout $1 < d|n$. Soit $x \in K$ une racine de P. On a

$$P(X) = \prod_{\eta \in \mu_n(k)} (X - \eta x) \in K[X].$$

De plus, K étant engendré par les racines de P et comme tous les $\eta \in k$, on a $K = k(x)$. D'après le Lemme précédent, K/k est galoisienne, cyclique d'ordre $[K : k]$. Il reste à montrer que P est irréductible (ce sera alors le polynôme minimal de x). Soit $Q \in k[X]$ un facteur irréductible et unitaire de P de degré $\deg Q =: e > 0$. Son coefficient constant est produit de e facteurs ηx avec $\eta \in k$, donc $x^e \in k$. On a $x^n = a \in k$, donc d'après le théorème de Bézout, $x^d \in k$ avec $d := n \wedge e$ et ainsi $a = x^n = (x^d)^{n/d}$. Par hypothèse, on a $d = n$, donc $P = Q$ est irréductible.
Réciproquement, on suppose que $\mathrm{Gal}(K/k)$ est cyclique d'ordre n et on en choisit un générateur g que l'on regarde comme étant un endomorphisme de K en tant que k-espace vectoriel. Comme $g^n = id_K$ et que $X^n - 1$ est scindé à racines simples dans k, l'endomorphisme g est diagonalisable. Les valeurs propres de g forment un sous-groupe de $\mu_n(k)$. En effet, si λ, μ sont deux valeurs propres de g et si $g(x) = \lambda x,\ g(y) = \mu y,\ x, y \neq 0$, alors $g(xy^{-1}) = g(x)g(y)^{-1} = \lambda\mu^{-1}(xy^{-1})$ de sorte que $\lambda\mu^{-1}$ est aussi une valeur propre. D'après le Théorème 14, ce sous-groupe est cyclique d'ordre $d|n$. Alors $g^d = id_K$, donc $d = n$ puisque g est d'ordre n. Donc il existe $x \in K \setminus \{0\}$ tel que $g(x) = \omega x$ où $\omega \in \mu_n^*(k)$. Soit le polynôme

$$\prod_{i=1}^{n}(X - \omega^i x) = X^n - a = X^n - x^n.$$

Ce polynôme séparable est scindé dans K et est fixe sous l'action de g, donc de $\mathrm{Gal}(K/k)$. C'est donc un polynôme à coefficients dans k d'après le Lemme d'Artin (Lemme 28). Comme $\mathrm{Gal}(K/k)$ agit transitivement sur ses racines, il est irréductible dans k d'après le Lemme 26. Son corps de décomposition sur k est de degré n et contenu dans K, c'est donc K. Enfin, si $d > 1$ est un diviseur de n et si $a = b^d$, alors le polynôme irréductible $X^n - a = (X^{n/d})^d - b^d$ est divisible par $X^{n/d} - b$, donc $b \notin k$. □

4 Applications aux polygones et aux équations algébriques

4.1 Polygones constructibles

Théorème 37. *Soit $z \in \mathbb{C}$ algébrique sur $\mathbb{Q}$. Alors z est constructible (à la règle et au compas) si et seulement si $[\mathcal{D}_{\mathbb{Q}}(\mu_{z,\mathbb{Q}}) : \mathbb{Q}]$ est une puissance de 2.*

Démonstration. Soient $z \in \mathbb{Q}^a$, $P := \mu_{z,\mathbb{Q}}$ et $K := \mathcal{D}_{\mathbb{Q}}(P)$.
Supposons z constructible. D'après le Théorème de Wantzel (Théorème 9), il existe une tour de corps

$$\mathbb{Q} = K_0 \hookrightarrow K_1 \hookrightarrow \cdots \hookrightarrow K_n$$

avec $[K_{i+1} : K_i] = 2$ et $z \in K_n$. Soit encore $L := \mathcal{N}_{K_n}^{\mathbb{C}}$ une clôture normale de K_n dans $\mathbb{C}$. $L/\mathbb{Q}$ est finie et galoisienne et pour tout conjugué z' de z, il existe $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ tel que $\sigma(z) = z'$ d'après le Lemme 26. Les corps $\sigma(K_i)$ forment une tour de corps de degrés 2 et $z' \in \sigma(K_n)$ est constructible d'après le Théorème de Wantzel. En particulier, tout $\zeta \in K$ est constructible. De plus, $K/\mathbb{Q}$ est finie et séparable, donc elle est engendrée par un élément constructible en vertu du Théorème de l'élément primitif, donc $[K : \mathbb{Q}]$ est une puissance de 2, d'après le Corollaire 4.
Inversement, supposons qu'il existe m tel que $[K : \mathbb{Q}] = 2^m$. On a alors $|\mathrm{Gal}(K/\mathbb{Q})| = 2^m$, donc il existe une suite de sous-groupes

$$\mathrm{Gal}(K/\mathbb{Q}) = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{id_K\}$$

telle que $[G_i : G_{i+1}] = 2$. D'après la Correspondance de Galois, il existe une tour

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K,$$

avec $[K_{i+1} : K_i] = 2$. Ainsi, tout $\zeta \in K$ est constructible, donc en particulier, $z \in K$ est constructible. □

Nous pouvons maintenant énoncer et démontrer le théorème de Gauss-Wantzel. On rappelle qu'un nombre premier de Fermat est un nombre premier de la forme $2^{2^m} + 1$.

Théorème 38. *(Gauss-Wantzel) Le polygone régulier à n côtés est constructible à la règle et au compas si et seulement si n est le produit d'une puissance de 2 et de nombres premiers de Fermat distincts.*

Démonstration. On note P_n le polygone régulier à n côtés. P_n est constructible si et seulement si $z_n := e^{\frac{2i\pi}{n}}$ est constructible. D'après le Corollaire 11, on a $\mu_{z_n,\mathbb{Q}} = \Phi_n$, $\mathcal{D}_{\mathbb{Q}}(\Phi_n) = \mathbb{Q}(z_n)$ et $[\mathbb{Q}(z_n) : \mathbb{Q}] = \deg \Phi_n = \varphi(n)$. D'après le Théorème 37, P_n est constructible si et seulement si $\varphi(n)$ est une puissance de 2.
Supposons qu'il existe m tel que $\varphi(n) = 2^m$. On écrit la décomposition de n en produit de facteurs premiers :

$$n = 2^r \prod_{i=1}^{N} p_i^{n_i},$$

avec $p_i \in \mathbb{P}$ impairs. Le calcul de $\varphi(n)$ donné en Annexe montre que

$$\varphi(n) = 2^{r-1} \prod_{i=1}^{N} (p_i - 1) p_i^{n_i - 1},$$

donc $n_i = 1$ pour tout i et $p_i = 1 + 2^{m_i}$, avec $m_i = \alpha\beta$ où α est une puissance de 2 et β est impair. Donc $(1 + 2^\alpha) | p_i$ et $p_i \in \mathbb{P}$ impliquent que $p_i = 1 + 2^\alpha$; ainsi $m_i = \alpha$ et n est bien de la forme voulue.
Réciproquement, si n est de la forme de l'énoncé, alors $\varphi(n)$ est une puissance de 2, ce qui achève la démonstration. □

Corollaire 20. *(Gauss) Le polygone régulier à 17 côtés est constructible.*

4.2 Equations résolubles par radicaux

Dans la suite, on fixe un corps k de caractéristique nulle.

Définition 34. Soit $P \in k[X]$ un polynôme non constant. On appelle groupe de Galois de P sur k le groupe de Galois de son corps de décomposition :

$$\mathrm{Gal}_k(P) := \mathrm{Gal}(\mathcal{D}_k(P)/k).$$

Notons que ceci est bien défini (Théorèmes 27-1. et 29) et ne dépend que de P.

Proposition 19. *Soient k un corps et $n \in \mathbb{N}^*$ non divisible par car(k). Alors*

$$Gal_k(X^n - 1) \lesssim (\mathbb{Z}/n\mathbb{Z})^*.$$

En particulier, $Gal_k(X^n - 1)$ est abélien.

Démonstration. On pose $K := \mathcal{D}_k(X^n - 1)$. D'après la Proposition 13 et le Théorème 14, $\mu_n(k)$ est cyclique d'ordre n, donc

$$\mu_n(k) \simeq (\mathbb{Z}/n\mathbb{Z}, +).$$

Tout $\sigma \in \mathrm{Gal}(K/k)$ induit un automorphisme du groupe $\mu_n(k)$, donc de $(\mathbb{Z}/n\mathbb{Z}, +)$, qui détermine entièrement σ. Cet automorphisme est déterminé par l'image de 1, qui doit être un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$, donc une unité de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$. D'où un monomorphisme :

$$\mathrm{Gal}(K/k) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*.$$

□

Définition 35. Une extension K/k est dite radicale s'il existe une tour de corps

$$k = k_0 \hookrightarrow k_1 \hookrightarrow \cdots \hookrightarrow k_n = K$$

telle que

$$\forall 1 \leq i \leq n,\ \exists x_i \in k_i\ ;\ k_i = k_{i-1}(x_i) \text{ et } \exists d_i > 0\ ;\ x_i^{d_i} \in k_{i-1}.$$

Remarque 9. 1. Un extension radicale permettra de définir la notion de polynôme résoluble par radicaux.

2. Si L/K et K/k sont radicales, il en est de même de L/k.

Proposition 20. *Si K/k est une extension radicale, alors il en est de même de $\mathcal{G}_K^{K^a}/k$.*

Démonstration. Soit une tour faisant de K/k une extension radicale :

$$k = k_0 \hookrightarrow \cdots \hookrightarrow k_n = K,\ K = k_{n-1}(x),\ x^d \in k_{n-1}.$$

Soit L/k une clôture normale de k_{n-1}/k dans un corps algébriquement clos Ω contenant K. La clôture normale de K/k dans Ω contient L et x, c'est donc la clôture normale L' de $L(x)$ dans Ω. On voit, par récurrence, qu'il suffit de montrer que L'/L est radicale. L' est engendrée par les conjugués de x dans Ω, ou encore par les images de x par les k-morphismes $\sigma : L' \to \Omega$. Or $x^d \in L \ \Rightarrow\ \sigma(x)^d \in \sigma(L)$ et $\sigma(L) = L$ car L/k est normale. Donc L'/L est obtenue en adjoignant successivement les éléments $\sigma(x)$ de Ω, dont la $d^{\text{ième}}$ puissance est dans L. L'/L est donc radicale. □

Définition 36. Soit $P \in k[X] \setminus k$ un polynôme non constant. P est dit résoluble par radicaux s'il existe une extension $K/\mathcal{D}_k(P)$ telle que K/k soit radicale. Autrement dit, P est résoluble par radicaux s'il est scindé dans une extension radicale.

Nous sommes en mesure de démontrer le résultat principal de cette section :

Théorème 39. *(Galois) Un polynôme est résoluble par radicaux si et seulement si son groupe de Galois est résoluble.*

Résultat que nous démontrerons sous la forme équivalente

Théorème 40. *Une extension galoisienne K/k est contenue dans une extension radicale si et seulement si $Gal(K/k)$ est résoluble.*

Démonstration. On rappelle que $\mathrm{car}(k) = 0$.
Supposons que K/k soit contenue dans une extension radicale L/k. D'après la Proposition 20, on peut supposer que L/k est galoisienne. Comme tout quotient d'un groupe résoluble est résoluble (Théorème 3), il suffit, d'après le Théorème 34, de montrer que $\mathrm{Gal}(L/k)$ est résoluble. Par hypothèse, il existe une tour

$$k = k_0 \hookrightarrow \cdots \hookrightarrow k_n = L,\ \forall 1 \leq i \leq n,\ k_i = k_{i-1}(x_i),\ x_i^{d_i} \in k_{i-1}.$$

Soit k'/k l'extension obtenue en adjoignant à k les racines $d_1 \cdots d_n^{\text{ièmes}}$ de l'unité (ie $k' = \mathcal{D}_k(X^{d_1 \cdots d_n} - 1)$). D'après la Proposition 19, k'/k est galoisienne abélienne. En notant k_i'/k_i l'extension analogue pour chaque i, on obtient une tour

$$k \hookrightarrow k' = k_0' \hookrightarrow k_1' \hookrightarrow \cdots \hookrightarrow k_n' = L',\ k_i' = k_{i-1}'(x_i),\ x_i^{d_i} \in k_{i-1}'.$$

En vertu du Théorème 29, il existe $P \in k[X]$ séparable tel que $L = \mathcal{D}_k(P)$ car L/k est galoisienne. Alors

$$L' = \mathcal{D}_k((X^{d_1 \cdots d_n} - 1)P(X)),$$

L'/k est donc galoisienne et avec la Correspondance de Galois, il vient

$$\mathrm{Gal}(L'/k) =: G > G_0 > G_1 > \cdots > G_n = \{id_{L'}\},\ G_i = \mathrm{Gal}(L'/k_i').$$

Soit la tour

$$k_{i-1}' \hookrightarrow k_i' \hookrightarrow L'.$$

Comme k_i'/k_{i-1}' est cyclique (Lemme 30), avec le Théorème 34, on a $G_i \trianglelefteq G_{i-1}$ avec G_{i-1}/G_i cyclique. De même, avec la tour

$$k \hookrightarrow k' \hookrightarrow L'$$

on a

$$G_0 = \mathrm{Gal}(L'/k') \trianglelefteq \mathrm{Gal}(L'/k) = G.$$

De plus, d'après la Proposition 19, $G/G_0 \simeq \mathrm{Gal}(k'/k)$ est abélien, donc G est résoluble et donc $\mathrm{Gal}(L/k)$ aussi.
Réciproquement, supposons que $\mathrm{Gal}(K/k)$ est résoluble et montrons que K est contenue dans une extension radicale de k. On considère l'extension galoisienne radicale k'/k obtenue en adjoignant à k toutes les racines d'ordre

$[K : k]!$ de l'unité ainsi que l'extension analogue K'/K, galoisienne et abélienne (Proposition 19). Comme K'/k est galoisienne, il existe un polynôme $P \in k[X]$ tel que $K' = \mathcal{D}_k(P)$ et le sous-groupe $\mathrm{Gal}(K'/K)$ de $\mathrm{Gal}(K'/k)$ est distingué et on a

$$\mathrm{Gal}(K'/k)/\mathrm{Gal}(K'/K) \simeq \mathrm{Gal}(K/k).$$

$\mathrm{Gal}(K/k)$ est résoluble et $\mathrm{Gal}(K'/K)$ est abélien, donc $\mathrm{Gal}(K'/k)$ est résoluble. Ainsi, en vertu du Théorème 3,

$$G := \mathrm{Gal}(K'/k') \leq \mathrm{Gal}(K'/k)$$

est également résoluble. Comme k'/k est radicale, il suffit de montrer que K'/k' est radicale. On remarque que $[K' : k'] \leq [K : k]$ (en effet, si $K = k(a)$, $Q := \mu_{a,k}$, $\deg Q = [K : k]$, alors $K' = k'(a)$ et $\mu_{a,k'}|Q$). Donc k' contient toutes les racines d'ordre $[K' : k']!$ de l'unité. De plus, G étant résoluble, il admet une suite de composition abélienne

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{id_{K'}\},$$

où l'on peut supposer G_{i-1}/G_i cyclique (voir [4], théorème de Jordan-Hölder). D'après la Correspondance de Galois, il existe une tour de corps

$$k' = k'_0 \hookrightarrow k'_1 \hookrightarrow \cdots \hookrightarrow k'_n = K'$$

avec k'_i/k'_{i-1} galoisienne et cyclique, de degré $n_i := [k'_i : k'_{i-1}]$. En effet, comme plus haut, on considère la tour

$$k'_{i-1} \hookrightarrow k'_i \hookrightarrow K'.$$

Comme $n_i|[K' : k']!$, k'_{i-1} contient les racines $n_i^{\text{ièmes}}$ de l'unité, donc l'extension k'_i/k'_{i-1} est radicale d'après le Théorème de Kummer (Théorème 36). Donc K'/k' est radicale, ce qui achève la démonstration. □

Nous terminons cette étude par le théorème d'Abel-Galois. On rappelle que des éléments $a_1, \ldots, a_n \in K$ dans une extension K/k sont dits algébriquement indépendants sur k si

$$\forall P \in k[X_1, \ldots, X_n],\ P(a_1, \ldots, a_n) = 0 \ \Leftrightarrow\ P = 0$$

Ce qui revient à dire que le morphisme

$$\begin{array}{rccc} \varphi & : & k[X_1,\ldots,X_n] & \to & K \\ & & P & \mapsto & P(a_1,\ldots,a_n) \end{array}$$

est injectif.

Définition 37. 1. On appelle polynôme général de degré n tout polynôme

$$P(X) = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} + X^n$$

où les $a_0,\ldots,a_{n-1}$ sont algébriquement indépendants sur $\mathbb{Q}$.

2. On appelle équation générale de degré n toutes équation du type

$$P(X) = 0$$

avec P un polynôme générale de degré n.

Par la suite, on fixe un polynôme générale (sur $\mathbb{Q}$) :

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$

et on pose

$$K := \mathbb{Q}(a_0,\ldots,a_{n-1}).$$

On a alors

$$P \in K[X], \text{ et } K \simeq \mathbb{Q}(X_1,\ldots,X_n) \simeq \mathrm{Frac}(\mathbb{Q}[X_1,\ldots,X_n]).$$

Soient aussi $x_1,\ldots,x_n$ les racines de P dans un corps de décomposition $K(x_1,\ldots,x_n)$ de P sur K et $\sigma_1,\ldots,\sigma_n$ les fonctions symétriques élémentaires en les $x_1,\ldots,x_n$:

$$\sigma_k = \sum_{1\le i_1<\ldots<i_k\le n} x_{i_1}\cdots x_{i_k}.$$

Proposition 21. *$x_1,\ldots,x_n$ sont algébriquement indépendants sur $\mathbb{Q}$.*
En particulier, $x_1,\ldots,x_n$ sont deux à deux distincts.

Démonstration. Supposons le contraire et soit

$$\sum_{i_1,\dots,i_n\in\mathbb{N}} \alpha_{i_1,\dots,i_n} x_1^{i_1}\cdots x_n^{i_n} = 0$$

où

$$0 \neq Q(X_1,\dots,X_n) := \sum_{i_1,\dots,i_n\in\mathbb{N}} \alpha_{i_1,\dots,i_n} X^{i_1}\cdots X^{i_n} \in \mathbb{Q}[X_1,\dots,X_n].$$

On pose

$$H(X_1,\dots,X_n) := \prod_{\sigma\in\mathfrak{S}_n} Q(X_{\sigma(1)},\dots,X_{\sigma(n)}).$$

H est manifestement symétrique, donc d'après le théorème fondamental sur les polynômes symétriques (voir Annexe), il existe $R \in \mathbb{Q}[X_1,\dots,X_n]$ tel que

$$H(X_1,\dots,X_n) = R(\Sigma_1,\dots,\Sigma_n)$$

où Σ_i est le $i^{\text{ème}}$ polynôme symétrique élémentaire. Or

$$Q(x_1,\dots,x_n) = 0 \;\Rightarrow\; H(x_1,\dots,x_n) = 0 \;\Rightarrow\; R(\sigma_1,\dots,\sigma_n) = 0,$$

mais on a $\forall 1 \leq k \leq n,\ \sigma_k = (-1)^k a_{n-k}$, d'où

$$R(-a_{n-1},\dots,(-1)^n a_0) = 0.$$

Enfin, les $a_0,\dots,a_{n-1}$ étant algébriquement indépendants, on en déduit que $R = 0$, donc $H = 0$ et donc $Q = 0$, d'où le résultat. □

Proposition 22. *On a*

$$\mathbb{Q}(x_1,\dots,x_n) = K(x_1,\dots,x_n).$$

Démonstration.

$$K(x_1,\dots,x_n) = \mathbb{Q}(a_0,\dots,a_{n-1})(x_1,\dots,x_n)$$

$$= \mathbb{Q}(a_0,\dots,a_{n-1},x_1,\dots,x_n) = \mathbb{Q}(x_1,\dots,x_n),$$

car les coefficients a_k s'expriment algébriquement en les racines x_k par le biais des fonctions symétriques élémentaires σ_k. □

Théorème 41. *On a*

$$Gal_K(P) \simeq \mathfrak{S}_n.$$

Démonstration. On pose $A := \{x_1, \ldots, x_n\}$ l'ensemble des racines de P. Comme $\mathfrak{S}(A) \simeq \mathfrak{S}_n$, il suffit de montrer que $\mathrm{Gal}_K(P) \simeq \mathfrak{S}(A)$. Soit donc $g \in \mathrm{Gal}_K(P)$. D'après le Lemme 25, g permute les racines de P, donc il induit un $\sigma \in \mathfrak{S}(A)$.
Réciproquement, soit $\sigma \in \mathfrak{S}(A)$ et posons

$$\begin{array}{rccc} g & : & \mathbb{Q}[x_1, \ldots, x_n] & \to & \mathbb{Q}[x_1, \ldots, x_n] \\ & & f(x_1, \ldots, x_n) & \mapsto & f(\sigma(x_1), \ldots, \sigma(x_n)) \end{array}$$

Alors $g \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[x_1, \ldots, x_n])$ et il se prolonge en un $\mathbb{Q}$-automorphisme du corps $\mathbb{Q}(x_1, \ldots, x_n) = \mathrm{Frac}(\mathbb{Q}[x_1, \ldots, x_n])$ que l'on note $\widetilde{g}$. De plus, a_k étant, au signe près, une fonction symétrique en les $x_1, \ldots, x_n$, $\widetilde{g}$ fixe les a_k, donc

$$\widetilde{g} \in \mathrm{Aut}_K(\mathbb{Q}(x_1, \ldots, x_n)) = \mathrm{Aut}_K(K(x_1, \ldots, x_n)) \overset{\text{def}}{=} \mathrm{Gal}_K(P).$$

□

Remarque 10. Une autre façon de voir ce résultat est de considérer l'extension finie $\mathbb{Q}(x_1, \ldots, x_n)/\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$ et d'utiliser le Lemme d'Artin. En effet, d'après le théorème fondamental des polynômes symétriques

$$\begin{aligned} \mathrm{Gal}_{\mathbb{Q}(a_0,\ldots,a_{n-1})}(P) &= \mathrm{Gal}(\mathbb{Q}(x_1, \ldots, x_n)/\mathbb{Q}(a_0, \ldots, a_{n-1})) \\ &\simeq \mathrm{Gal}(\mathbb{Q}(x_1, \ldots, x_n)/\mathbb{Q}(\sigma_1, \ldots, \sigma_n)) \\ &\simeq \mathrm{Gal}(\mathbb{Q}(x_1, \ldots, x_n)/\mathbb{Q}(x_1, \ldots, x_n)^{\mathfrak{S}_n}) \simeq \mathfrak{S}_n \end{aligned}$$

Théorème 42. *(Abel-Galois) Le polynôme générale de degré n est résoluble par radicaux si et seulement si $n \leq 4$.*
En particulier, l'équation générale de degré $n \geq 5$ n'est pas résoluble par radicaux.

Démonstration. D'après le Théorème de Galois (Théorème 39), P est résoluble par radicaux si et seulement si $\mathrm{Gal}_K(P)$ est résoluble. Or, d'après le Théorème 6, $\mathrm{Gal}_K(P) \simeq \mathfrak{S}_n$ est résoluble si et seulement si $n \leq 4$. □

Annexe

Définition 38. Un ensemble partiellement ordonné $(E, \preccurlyeq)$ est dit inductif si tout sous-ensemble totalement ordonné de E (ie une chaîne) admet un majorant dans E.

Lemme 31. *(Lemme de Zorn) Tout ensemble ordonné inductif admet un élément maximal.*

Remarque 11. Ce résultat peut être vu comme un axiome de la théorie des ensembles et est équivalent à l'axiome du choix.

Proposition-Définition 7. *Soit A un anneau intègre. On définit sur $E := A \times (A \setminus \{0\})$ la relation binaire $\sim$ par*

$$\forall (a,b),(a',b') \in E,\ (a,b) \sim (a',b') \ \Leftrightarrow\ ab' - a'b = 0.$$

On vérifie que c'est une relation d'équivalence et on note $\pi : E \to E/\sim$ la surjection canonique. On définit sur E les lois

$$(a,b) + (a',b') := (ab' + a'b, bb'),$$

et

$$(a,b) \cdot (a',b') := (aa', bb').$$

Comme A est intègre, ces lois sont des LCI sur E. Il est aisé de vérifier qu'elles sont commutatives, associatives et que $\cdot$ est distributive sur $+$.
Alors ces lois passent au quotient, on les note encore $+$ et $\cdot$ et procurent à $K := E/\sim$ une structure de corps commutatif, appelé corps des fractions de A et noté $Frac(A)$. De plus, K admet un sous-anneau isomorphe à A et est minimal pour cette propriété.

Démonstration. Montrons que $+$ et $\cdot$ sont compatibles avec $\sim$. Pour $+$, on a

$$(a,b) \sim (a',b') \;\Leftrightarrow\; ab'-a'b=0 \;\Leftrightarrow\; (ab'-a'b)q^2=0 \;(q\neq 0)$$

$$\Leftrightarrow\; (aq+pb)b'q-(a'q+pb')bq=0 \Leftrightarrow\; (a,b)+(p,q)\sim(a',b')+(p,q).$$

De même, on a

$$(a,b) \sim (a',b') \;\Leftrightarrow\; ab'-a'b=0 \;\Leftrightarrow\; apb'q-a'pbq=(ab'-a'b)pq=0$$

$$\Leftrightarrow\; (a,b)\cdot(p,q)\sim(a',b')\cdot(p,q).$$

Les lois $+$ et $\cdot$ passent donc bien au quotient et on les note encore $+$ et $\cdot$. Elles sont commutatives, associatives et $\cdot$ est distributive sur $+$. De plus, pour l'addition, $\pi(0,1)$ est neutre et $\pi(-a,b)$ est l'opposé de $\pi(a,b)$; $(K,+)$ est donc un groupe abélien. Ensuite, dans la multiplication, $\pi(1,1)$ est neutre et pour tout $\pi(a,b)\neq\pi(0,1)$ (ie $a\neq 0$), $\pi(b,a)$ est l'inverse de $\pi(a,b)$. Ainsi, $(K,+,\cdot)$ est un corps commutatif.
On vérifie facilement que

$$\begin{array}{rccc} \epsilon & : & A & \to & K \\ & & x & \mapsto & \pi(x,1) \end{array}$$

est un monomorphisme d'anneaux, A est donc isomorphe à un sous-anneau de K.
Soit enfin L un corps tel qu'il existe un monomorphisme d'anneaux $\omega : A \to L$. On a

$$(a,b)\sim(a',b') \;\Leftrightarrow\; ab'=a'b \;\Rightarrow\; \omega(a)\omega(b')=\omega(a')\omega(b).$$

Comme $b,b'\neq 0$, $\omega(b),\omega(b')\neq 0$ car ω est injectif et donc $\omega(a)\omega(b)^{-1}$ ne dépend pas du représentant de $\pi(a,b)$ choisi. On a donc une application

$$\begin{array}{rccc} \varphi & : & K & \to & L \\ & & \pi(a,b) & \mapsto & \omega(a)\omega(b)^{-1} \end{array}$$

qui se révèle être un monomorphisme de corps, d'où le résultat. □

Remarque 12.
1. Dans K, on note $\frac{a}{b}$ ou a/b pour désigner $\pi(a,b)$.
2. On a $\mathbb{Q}=\mathrm{Frac}(\mathbb{Z})$.

Théorème 43. *(Lemme chinois) Soient A un anneau et $(I_j)_{1\leq j\leq n}$ des idéaux de A, deux à deux étrangers (ie $\forall i \neq j, I_i + I_j = A$). Alors*

$$A/(I_1 \cap \cdots \cap I_n) \simeq \prod_{1\leq j\leq n} A/I_j.$$

De plus, on a

$$\bigcap_{1\leq j\leq n} I_j = \prod_{1\leq j\leq n} I_j.$$

Démonstration. Il est évident que le noyau du morphisme canonique

$$A \to \prod_{1\leq j\leq n} A/I_j$$

vaut $\bigcap_{1\leq j\leq n} I_j$. Ce morphisme passe au quotient :

$$A/(I_1 \cap \cdots \cap I_n) \to \prod_{1\leq j\leq n} A/I_j.$$

Ce dernier morphisme étant injectif, il s'agit de montrer qu'il est surjectif. On pose

$$I(-j) := \prod_{1\leq k\leq n,\ k\neq j} I_k.$$

On remarque qu'on a

$$\sum_{1\leq j\leq n} I(-j) = A.$$

Pour cela, on procède par récurrence sur n. Si $n = 2$, on a $I_1 + I_2 = A$ par hypothèse. Ensuite, par hypothèse de récurrence, on obtient que la somme des $n-1$ idéaux $I_1 \cdots \widehat{I_j} \cdots I_{n-1}$ vaut A, et en multipliant par I_n on a

$$\sum_{1\leq j\leq n-1} I(-j) = I_n$$

donc la somme $\sum_j I(-j)$ contient I_n. En raisonnant de la même façon pour $I_2 \cdots I_n$, on a que la somme $\sum_j I(-j)$ contient I_1. Ainsi, la somme $\sum_j I(-j)$ contient $I_1 + I_n = A$, donc vaut A.
Il existe alors $a_j \in I(-j)$ tels que

$$\sum_{1\leq j\leq n} a_j = 1.$$

Soit alors $\overline{b_j} \in A/I_j$ des classes quelconques. On pose encore

$$b := \sum_{1 \leq j \leq n} a_j b_j.$$

Alors

$$a_j \equiv \begin{cases} 0 \mod I_i & \text{si } i \neq j, \\ 1 \mod I_i & \text{si } i = j, \end{cases}$$

Ainsi,

$$b \equiv b_j \mod I_j, \ \forall 1 \leq j \leq n,$$

d'où un isomorphisme d'anneaux.
Enfin, le produit des I_j étant clairement contenu dans leur intersection, montrons qu'il lui est égale. Soit donc $a \in \bigcap_{1 \leq j \leq n} I_j$. On a

$$a = \sum_{1 \leq i \leq n} a a_i.$$

Comme $a \in I_i, \ A \in I_i I(-i) = I_1 \cdots I_n$, pour tout $1 \leq i \leq n$, ce que l'on voulait. □

Corollaire 21. *Pour tous $n, m \in \mathbb{N}^*$ premiers entre eux, on a*

$$\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Théorème 44. *(Calcul de $\varphi(n)$)*
Soit $n \geq 2$ un entier naturel dont la décomposition en facteurs irréductibles est

$$n = \prod_{i=1}^{k} p_i^{a_i}.$$

Alors

$$\varphi(n) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Démonstration. Pour tout $1 \leq i \leq k$, on a

$$\varphi(p_i^{a_i}) = p_i^{a_i-1}(p_i - 1).$$

En effet, comme $\varphi(p_i^{a_i})$ est le nombre de nombres premiers à $p_i^{a_i}$, comme p_i est premier, c'est aussi le nombre de non multiples de p_i compris entre 1 et $p_i^{a_i} - 1$. Or, le nombre d'entiers compris entre 1 et p_i qui sont multiples de p_i sont de la forme $p_i q$ avec $1 \leq q \leq p_i^{a_i}$. Il y en a donc $p_i^{a_i-1}$, ainsi

$$\varphi(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i-1} = p_i^{a_i-1}(p_i - 1).$$

Ensuite, comme les $P_i^{a_i}$ sont deux à deux premiers entre eux, la Propriété 1 donne

$$\begin{aligned}\varphi(n) = \varphi\left(\prod_{i=1}^{k} p_i^{a_i}\right) &= \prod_{i=1}^{k} \varphi(p_i^{a_i}) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i - 1) \\ &= \prod_{i=1}^{k} p_i^{a_i}\left(1 - \frac{1}{p_i}\right) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right).\end{aligned}$$

□

Définition 39. Soit A un anneau (commutatif).

1. Soit un monôme $X_1^{i_1} \cdots X_n^{i_n} \in A[X_1, \ldots, X_n]$.
   On appelle poids de $X_1^{i_1} \cdots X_n^{i_n}$ l'entier

$$\pi(X_1^{i_1} \cdots X_n^{i_n}) := \sum_{k=1}^{n} k i_k.$$

2. Si $P = \sum_{i_1,\ldots,i_n \in \mathbb{N}} a_{i,1\ldots,a_i} X_i^{i_1} \cdots X_n^{i_n}$, on appelle poids de P le maximum de l'ensemble

$$\left\{ m \in \mathbb{N} \ ; \ \exists i_1, \ldots, i_n \in \mathbb{N} \ ; \ (a_{i_1,\ldots,i_n} \neq 0) \text{ et } \sum_{k=1}^{n} k i_k = m \right\}$$

   et on le note $\pi(P)$.

On définit de même le degré de P en remplaçant $\sum_k k i_i$ par $\sum_k i_k$.

Définition 40. On dit d'un polynôme $P \in A[X_1, \ldots, X_n]$ qu'il est symétrique si

$$\forall \sigma \in \mathfrak{S}_n,\ P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = P(X_1, \ldots, X_n).$$

Définition 41. Dans $A[X_1, \ldots, X_n]$ et pour tout $1 \leq k \leq n$, on définit le $k^{\text{ième}}$ polynôme symétrique élémentaire Σ_k par

$$\Sigma_k := \sum_{1 \leq i_1 < \ldots < i_k \leq n} X_{i_1} \cdots X_{i_k}.$$

Lemme 32. *Soit $P \in A[X_1, \ldots, X_n]$ un polynôme tel qu'en substituant 0 à l'une quelconques des indéterminées dans $P(X_1, \ldots, X_n)$ on obtient le polynôme nul. Alors P est divisible par Σ_n.*

Démonstration. A tout $1 \leq k \leq n$, on associe l'ensemble

$$I_k := \{(i_1, \ldots, i_n) \in \mathbb{N}^n \ ;\ i_k \neq 0\}.$$

On a

$$P(X_1, \ldots, X_{k-1}, 0, X_{k+1}, \ldots, X_n) = \sum_{(i_1, \ldots, i_n) \in I_k} a_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_{k-1}^{i_{k-1}} X_{k+1}^{i_{k+1}} \cdots X_n^{i_n}.$$

La nullité de $P(X_1, \ldots, X_{k-1}, 0, X_{k+1}, \ldots, X_n)$ implique

$$\forall (i_1, \ldots, i_n) \in I_k,\ a_{i_1, \ldots, i_n} = 0.$$

En faisant successivement $k = 1, \ldots, k = n$, on en déduit que $a_{i_1, \ldots, i_n}$ est nul pour tout n-uplet $(i_1, \ldots, i_n)$ dont l'un des éléments est nul. Autrement it, $a_{i_1, \ldots, i_n} \neq 0$ exige $(i_1, \ldots, i_n) \in (\mathbb{N}^*)^n$ et on peut écrire

$$P = \sum_{(i_1, \ldots, i_n) \in (\mathbb{N}^*)^n} a_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n}$$

$$= X_1 \ldots X_n \left(\sum_{(i_1, \ldots, i_n) \in (\mathbb{N}^*)^n} a_{i_1, \ldots, i_n} X_1^{i_1 - 1} \cdots X_n^{i_n - 1} \right).$$

□

Théorème 45. *Pour tout polynôme symétrique $P \in A[X_1, \ldots, X_n]$ de degré p, il existe un polynôme $Q \in A[Y_1, \ldots, Y_n]$ de poids inférieur ou égale à p tel que*

$$P(X_1, \ldots, X_n) = Q(\Sigma_1, \ldots, \Sigma_n).$$

Démonstration. Si $P = 0$, alors $Q = 0$ convient et on peut donc supposer que P est non nul. Il s'agit de vérifer une assertion du type $\mathcal{A}_{n,p},\ n \in \mathbb{N},\ p \in \mathbb{N}$. Effectuons une récurrence double.
Comme à tout $P(X_1)$ on peut associer $Q(X_1) = P(X_1)$, la propriété $\mathcal{A}_{1,p}$ est vraie pour tout p.
On fixe alors $n \geq 2$. Supposons que $\mathcal{A}_{n-1,p}$ est vraie pour tout p et démontrons que $\mathcal{A}_{n,p}$ est aussi vraie pour tout p, par récurrence sur $p \in \mathbb{N}$.
Il est clair que $\mathcal{A}_{n,0}$ est vraie.
Supposons que $\mathcal{A}_{n,k}$ soit vérifiée pour tout $k < p$ et soit P un polynôme symétrique de degré p de $A[X_1, \ldots, X_n]$. Pour $1 \leq q \leq n-1$, on note $(\Sigma_q)_0$ le polynôme obtenu en substituant 0 à X_n dans Σ_q. On vérifie sans problème que $(\Sigma_q)_0$ est le $q^{\text{ième}}$ polynôme symétrique élémentaire de $A[X_1, \ldots, X_{n-1}]$. Considérons le polynôme $P(X_1, \ldots, X_{n-1}, 0)$; il est manifestement symétrique et de degré au plus p. En utilisant $\mathcal{A}_{n-1,k}$, on peut écrire

$$P(X_1, \ldots, X_{n-1}, 0) = Q_1((\Sigma_1)_0, \ldots, (\Sigma_{n-1})_0)$$

avec $Q_1 \in A[Y_1, \ldots, Y_{n-1}]$ de poids au plus p. On pose

$$P_1(X_1, \ldots, X_n) := P(X_1, \ldots, X_n) - Q_1(\Sigma_1, \ldots, \Sigma_{n-1}).$$

Le polynôme symétrique P_1 est de degré au plus p ; or par construction $P_1(X_1, \ldots, X_{n-1}, 0) = 0$ et, puisque P_1 est symétrique, pour tout $1 \leq k \leq n$

$$P_1(X_1, \ldots, X_{k-1}, 0, X_k, \ldots, X_n) = 0.$$

D'après le Lemme précédent, il existe $P_2 \in A[X_1, \ldots, X_n]$ tel que

$$P_1(X_1, \ldots, X_n) = \Sigma_n P_2(X_1, \ldots, X_n).$$

P_1 et Σ_n étant symétriques, si $\sigma \in \mathfrak{S}_n$,

$$\Sigma_n(P_2(X_1, \ldots, X_n) - P_2(X_{\sigma(1)}, \ldots, X_{\sigma(n)})) = 0.$$

On en déduit (sans hymothèse sur l'intégrité de A) que

$$P_2(X_1, \ldots, X_n) - P_2(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = 0,$$

et on a $\deg(P_2) \leq p - n$. Ainsi, P_2 est symétrique, de degré $k < p$ et on peut lui appliquer l'hypothèse de récurrence :

$$P_2(X_1, \ldots, X_n) = Q_2(\Sigma_1, \ldots, \Sigma_n)$$

où $Q_2 \in A[Y_1, \ldots, Y_n]$ est de poids au plus $p - n$. Il vient alors

$$P(X_1, \ldots, X_n) = Q_1(\Sigma_1, \ldots, \Sigma_{n-1}) + \Sigma_n Q_2(\Sigma_1, \ldots, \Sigma_n).$$

Le polynôme $Q_1(Y_1, \ldots, Y_{n-1}) + Y_n Q_2(Y_1, \ldots, Y_n)$ est de poids au plus p et répond à la question. □

Corollaire 22. *Si l'on note $A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ l'anneau des polynômes symétriques, l'application*

$$\begin{array}{rccc} \Phi & : & A[X_1, \ldots, X_n] & \to & A[X_1, \ldots, X_n]^{\mathfrak{S}_n} \\ & & P(X_1, \ldots, X_n) & \mapsto & P(\Sigma_1, \ldots, \Sigma_n) \end{array}$$

est un isomorphisme d'anneaux.

Enfin, pour la culture, si l'on permet à un corps d'être non commutatif pour la loi $\cdot$ (on parle alors de corps gauche ou d'anneaux à division) alors on a

Théorème 46. *(Wedderburn) Tout corps fini est commutatif.*

Démonstration. Soit K un corps (anneaux à division) fini et soit Z son centre (pour la loi $\cdot$). Z est un corps donc K est un Z-espace vectoriel de dimension $n \in \mathbb{N}^*$. Si $|Z| = q$, alors $|K| = q^n$. Il s'agit de montrer que $n = 1$. On aura alors que $K = Z$ est commutatif.
Par l'absurde, on suppose $n > 1$. Faisons agir le groupe K^* sur lui-même par automorphisme intérieur et notons $\omega(x)$ l'orbite de x dans K^* et $\mathrm{stab}(x)$ son stailisateur. $(\mathrm{stab}(x) \cup \{0\})$ est un sous-corps de K et un sous-corps de Z donc il existe $d(x) \in \mathbb{N}^*$ tel que $|\mathrm{stab}(x) \cup \{0\}| = q^{d(x)}$. Alors

$$|\mathrm{stab}(x)| = q^{d(x)} - 1.$$

Le lemme des orbites donne

$$|\omega(x)| = \frac{|K^*|}{|\mathrm{stab}(x)|} = \frac{q^n - 1}{q^{d(x)} - 1}.$$

De plus, $|K| = |\mathrm{stab}(x) \cup \{0\}|^k$, $k \in \mathbb{N}$ et donc $q^n = q^{kd(x)} \Rightarrow d(x)|n$. D'après la Proposition 3-3., on a

$$|\omega(x)| = \frac{\prod_{m|n} \Phi_n(q)}{\prod_{m|d(x)} \Phi_m(q)} = \prod_{m|n,\ m\nmid d(x)} \Phi_m(q) \ \Rightarrow\ \Phi_n(q)||\omega(x)|$$

pour tout x d'orbite non triviale. De même, on notant T un système de représentants des classes,

$$|K^*| = q^n - 1 = \prod_{m|n} \Phi_n(q) \ \Rightarrow\ \Phi_n(q)||K^*|$$

et avec l'équation aux classes

$$|K^*| = |Z^*| + \sum_{x\in T,\ \omega(x)\neq\{x\}} |\omega(x)|.$$

Or $\omega(x) \neq \{x\} \ \Rightarrow\ d(x) \neq n$ donc

$$\Phi_n(q) \left| \sum_{x\in T,\ \omega(x)\neq\{x\}} |\omega(x)| \right.$$

et donc

$$\Phi_n(q)|(q-1) \ \Rightarrow\ |\Phi_n(q)| \leq q - 1.$$

Cependant,

$$|\Phi_n(q)| = \prod_{\delta\in\mu_n^*(\mathbb{Q})} |q - \delta| < (q - |\delta|^n)^{\varphi(x)} \geq q - 1 \ \Rightarrow\ |\Phi_n(q)| > q - 1$$

ce qui est une contradiction ; et la démonstration est terminée. □

Références

[1] O. Debarre, "Extensions de corps, modules et anneaux," 2012-2013.

[2] E. Hage, "Théorie de galois," 2001.

[3] J. Calais, *Extensions de corps et Théorie de Galois*. Ellipses, 2006.

[4] ——, *Éléments de théorie des groupes*. Presses Universitaires de France, 1984.

[5] Wikipedia.

[6] S. Lang, *Algèbre*. Springer-Verlag, Dunod, 2004.

[7] Y. Palu, "Cours d'algèbre pour la licence 3 : Théorie des anneaux et extensions de corps," 2015.

[8] A. Zimmermann, "Cours d'algèbre pour la licence 3 : Théorie des groupes," 2014.

[9] E. Amar and E. Mathéron, *Analyse complexe*. Cassini, 2004.

[10] B. Deschamps, "Cours de maîtrise : Théorie de galois," 2002-2003.

[11] M. Reversat and B. Zhang, "Cours de théorie des corps," 2013.

[12] Y. Laszlo and D. Hernandez, *Introduction à la Théorie de Galois*, 2012.

[13] E. Ramis, C. Deschamps, and J. Odoux, *Cours de Mathématiques spéciales : Algèbre*. Masson et Cie, 1974.