Théorie de Galois

Contents

1 Groupes

On ne rappelle pas les définitions et propriétés élémentaires sur les groupes. Une introduction à la théorie des groupes comportant ces notions peut être trouvée en [9].

Théorème 1.0.1 : (*Lagrange*) Soit G un groupe fini et H un sous-groupe de G. Alors le cardinal de H divise celui de G.

Démonstration : On note $\mathcal{R}$ la relation d'équivalence à gauche sur H définie sur G par : $\forall x, y \in G$, $x\mathcal{R}y \Leftrightarrow x^{-1}y \in H$. Si $x \in G$, alors la classe d'équivalence de x est $xH = \{xh,\ h \in H\}$ et est en bijection avec H. Comme ces classes d'équivalence forment une partition de G, on peut écrire $G = \sqcup_{x\in R}[x]$, où R est un système de représentants de $\mathcal{R}$. On a alors :

$$\mathrm{Card}(G) = \sum_{x\in R} \mathrm{Card}([x]) = \mathrm{Card}(R)\mathrm{Card}(H)$$

Figure 1: Joseph-Louis Lagrange, 1736 - 1813

1.1 Groupes distingués et résolubles

Définition 1.1.1 : Soient G un groupe et $g \in G$. L'application $i_g : G \to G$, $g \mapsto gxg^{-1}$ est un automorphisme de G dit **intérieur**. L'ensemble des automorphismes intérieurs de G forme un sous-groupe de $\mathrm{Aut}(G)$.

Définition 1.1.2 : Soit G un groupe. Un sous-groupe H de G est dit **distingué** lorsqu'il est stable par tous les automorphismes intérieurs de G, c'est à dire lorsque pour tout $g \in G$, $i_g(H) \subset H$. On note que si H est distingué, alors pour tout $g \in G$, $i_g(H) = H$. Un sous-groupe de G stable par tous les automorphismes de G est dit **caractéristique**.

Proposition 1.1.1 : Soient G un groupe et H un sous-groupe de G. L'ensemble quotient G/H défini par la relation d'équivalence à gauche sur H peut être muni d'une loi de groupe vérifiant : $\forall x, y \in G$, $[xy] = [x][y]$, si et seulement si H est distingué.

Définition 1.1.3 : Soit G un groupe. Les éléments de G de la forme $xyx^{-1}y^{-1}$, avec $x, y \in G$, sont appelés **commutateurs** de G. Le sous-groupe $D(G)$ engendré par les commutateurs est appelé sous-groupe **dérivé** de G. La suite $(D^n(G))_{n\in\mathbb{N}}$ est appelée **suite dérivée** de G.

Proposition 1.1.2 : Soit G un groupe. Pour tout $n \in \mathbb{N}$, $D^n(G)$ est caractéristique.
Démonstration : Soit $f \in \mathrm{Aut}(G)$. Pour tout $x, y \in G$, $f(xyx^{-1}y^{-1}) = f(x)f(y)f(x)^{-1}f(y)^{-1} \in D(G)$. Il vient donc que $f(D(G)) \subset D(G)$. $D(G)$ est bien caractéristique dans G. Aussi, $f^{-1}(D(G)) \subset D(G)$ donc $f(D(G)) = D(G)$: f induit un automorphisme de $D(G)$. On conclut par récurrence : on suppose que tout élément de $\mathrm{Aut}(G)$ induit un automorphisme de $D^{n-1}(G)$. Alors, $D^n(G)$, qui est caractéristique dans $D^{n-1}(G)$, est caractéristique dans G, et tout élément de $\mathrm{Aut}(G)$ induit un automorphisme de $D^n(G)$.

Proposition 1.1.3 : Soient G un groupe et K un sous-groupe de G. $D(G) \subset K$ si et seulement si K est distingué et G/K est commutatif.
Démonstration : Supposons que $D(G) \subset K$. Soient $k \in K$ et $g \in G$. $gkg^{-1} = gkg^{-1}k^{-1}k \in K$, donc K est distingué. Pour montrer que G/K est commutatif, il suffit de montrer que $ghK = hgK$ pour tout $g, h \in G$. Soit $k \in K$. $ghk = hgg^{-1}h^{-1}ghk = hg(g^{-1}h^{-1}gh)k \in hgK$ donc $ghK \subset hgK$. On montre l'autre inclusion de la même manière. On a bien $ghK = hgK$ et G/K est alors commutatif. Réciproquement, supposons que K est distingué et que G/K est commutatif. Alors, pour tout $x, y \in G$, $[xyx^{-1}y^{-1}] = [x][y][x^{-1}][y^{-1}] = [e]$ car G/K est commutatif. Donc $xyx^{-1}y^{-1} \in K$. Ainsi, $D(G) \subset K$.

Définition 1.1.4 : Soit G un groupe. On dit que G est **résoluble** s'il existe $n \in \mathbb{N}$ tel que $D^n(G) = \{e\}$.

Proposition 1.1.4 : Soient G un groupe et H un sous-groupe de G. Si G est résoluble, alors H aussi. Si H est distingué, alors G/H est résoluble.
Démonstration : Le premier point découle du fait que $D(H) \subset D(G)$. Pour le second, il suffit de remarquer que $D^n(G/H) = \langle [xyx^{-1}y^{-1}],\ x, y \in D^{n-1}(G) \rangle$.

Proposition 1.1.5 : Soient G un groupe et H un sous-groupe distingué de G. Si H et G/H sont résolubles, alors G aussi.
Démonstration : On note π la surjection canonique de $G \to G/H$. On déduit du fait que $\pi(D(G)) = D(G/H)$ que pour tout $n \in \mathbb{N}$, $\pi(D^n(G)) = D^n(G/H)$. Comme G/H est résoluble, on a $n_0 \in \mathbb{N}$ tel quel $D^{n_0}(G/H) = \{e\}$. Mais alors, $D^{n_0}(G) \subset H$ et comme H est résoluble, on en déduit que G aussi.

Définition 1.1.5 : Un groupe **simple** est un groupe qui n'admet que deux sous-groupes distingués : $\{e\}$ et lui-même.

1.2 Groupe symétrique

Définition 1.2.1 : Soit $n \in \mathbb{N}^*$. On rappelle que le **groupe symétrique** d'ordre n, noté S_n (ou $\mathcal{S}_n$) est le groupe des bijections de $\{1, ..., n\}$ dans lui même (appelées **permutations**). Il existe un unique morphisme de groupe non trivial de S_n dans $\{-1, 1\}$, noté ε et appelé **signature**, qui correspond à la parité du nombre de transpositions dans une décomposition d'une permutation. L'ensemble des éléments de S_n dont la signature est 1 est un sous-groupe de S_n : le **sous-groupe alterné** d'ordre n, noté $\mathcal{A}_n$.

Proposition 1.2.1 : Soit $n \geq 3$ et H un sous-groupe distingué de $\mathcal{A}_n$ contenant un 3-cycle. Alors, $H = \mathcal{A}_n$.
Démonstration : La classe de conjugaison d'un 3-cycle est l'ensemble des 3-cycles. Or les 3-cycles engendrent $\mathcal{A}_n$. En effet, ils engendrent les produits de deux transpositions (qui engendrent clairement $\mathcal{A}_n$) :
$(a_1, a_2) \circ (a_2, a_3) = (a_1, a_2, a_3)$ et $(a_1, a_2) \circ (a_3, a_4) = (a_3, a_2, a_4) \circ (a_1, a_3, a_2)$.

Proposition 1.2.2 : Le groupe alterné $\mathcal{A}_n$ est simple si et seulement si $n \notin \{1, 2, 4\}$.
Démonstration : On va d'abord traiter le cas où $n \geq 5$. Soit H un sous-groupe distingué non trivial de $\mathcal{A}_n$. Soit σ un élément de H différent de l'identité. On s'intéresse à la décomposition en cycles **à supports disjoints** de σ.

1. Si σ admet un cycle de longueur $k \geq 4$ dans sa décomposition, disons $\sigma = (a_1, a_2, ..., a_k) \circ s$, avec $s \in \mathcal{S}_n$, alors la permutation $\tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1}$ où $\tau = (a_1, a_2, a_3)$ est un 3-cycle appartenant à H.

2. Si σ admet un 3-cycle et un 2-cycle dans sa décomposition, disons $\sigma = (a_1, a_2, a_3) \circ (a_4, a_5) \circ s$, avec $s \in \mathcal{S}_n$, alors la permutation $\tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1}$ où $\tau = (a_1, a_2) \circ (a_4, a_5)$ est un 3-cycle appartenant à H.

3. Si σ admet un 2-cycle dans sa décomposition et un point fixe, disons $\sigma = (a_1, a_2) \circ s$, avec $s \in \mathcal{S}_n$ et a_3 un point fixe de σ, alors la permutation $\tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1}$ où $\tau = (a_1, a_2, a_3)$ est un 3-cycle appartenant à H.

4. Si σ admet deux 3-cycle dans sa décomposition, disons $\sigma = (a_1, a_2, a_3) \circ (a_4, a_5, a_6) \circ s$, avec $s \in \mathcal{S}_n$, alors la permutation $\tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1}$ où $\tau = (a_1, a_2, a_4)$ est un 5-cycle appartenant à H.

5. Si σ admet trois 2-cycle dans sa décomposition, disons $\sigma = (a_1, a_2) \circ (a_3, a_4) \circ (a_5, a_6) \circ s$, avec $s \in \mathcal{S}_n$, alors la permutation $\tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1}$ où $\tau = (a_1, a_3, a_5)$ est un produit de deux 3-cycles appartenant à H.

On en déduit que H contient un 3-cycle. En effet, si σ contient un cycle de taille supérieure à 4 alors H contient un 3-cycle selon 1). Sinon, tous ses cycles sont des 3-cycles ou des 2-cycles. Si σ contient un 3-cycle alors soit σ est un 3-cycle, soit σ contient un deuxième 3-cycle et dans ce cas H contient un 5-cycle selon 4) et donc un 3-cycle selon 1), soit σ contient un 2-cycle et dans ce cas H contient un 3-cycle selon 2). Sinon, σ ne contient pas de 3-cycles et, étant non triviale, σ contient au moins deux 2-cycle. Comme $n \geq 5$, si σ ne contient que deux 2-cycles, σ admet un point fixe et H un 3-cycle selon 3). Sinon, σ contient au moins trois 2-cycles et H contient une permutation de deux 3-cycles selon 5) et donc H contient un 3-cycle selon 4) et 1). On déduit de la proposition précédente que $H = \mathcal{A}_n$ et donc que $\mathcal{A}_n$ est simple si $n \geq 5$. $\mathcal{A}_3$ est simple car c'est $\mathbb{Z}/3\mathbb{Z}$. $\mathcal{A}_1$ et $\mathcal{A}_2$ sont triviaux, et $\mathcal{A}_4$ n'est pas simple car le sous-groupe à quatre éléments engendré par les doubles-transpositions est distingué.

Proposition 1.2.3 : Pour tout $n \geq 5$, $D(\mathcal{A}_n) = \mathcal{A}_n$.
Démonstration : $D(\mathcal{A}_n)$ est dinstingué dans $\mathcal{A}_n$ donc c'est $\mathcal{A}_n$ ($D(\mathcal{A}_n)$ n'est clairement pas le groupe trivial pour $n \geq 5$).

Proposition 1.2.4 : Pour tout $n \in \mathbb{N}^*$, $D(\mathcal{S}_n) = \mathcal{A}_n$.
Démonstration : Si $n \leq 2$, c'est vrai. Si $n \geq 3$, $D(\mathcal{S}_n) \subset \mathcal{A}_n$ et comme tout 3-cycle s'écrit comme un commutateur de deux transpositions on a $\mathcal{A}_n = D(\mathcal{S}_n)$.

Théorème 1.2.1 : $\mathcal{S}_n$ est résoluble si et seulement si $n \leq 4$.
Démonstration : Si $n \geq 5$, alors $\mathcal{S}_n$ n'est pas résoluble car $D(\mathcal{A}_n) = \mathcal{A}_n$. Si $n \leq 2$, $\mathcal{S}_n$ est résoluble. Si $n = 3$, $\mathcal{A}_n = \mathbb{Z}/3\mathbb{Z}$ est résoluble car commutatif. Si $n = 4$, $D(\mathcal{A}_n)$ est le sous-groupe engendré par les doubles permutations (vérifier à la main !), qui est commutatif donc résoluble.

1.3 Actions de groupe

Définition 1.3.1 : Soient G un groupe et E un ensemble. Une **action** de G sur E est une application $(\cdot)$: $G \times E \to E$ vérifiant :

1. $\forall x \in E,\ 1 \cdot x = x$
2. $\forall g, h \in G,\ \forall x \in E,\ g \cdot (h \cdot x) = gh \cdot x$

Remarque : Si G est un groupe, l'application $G^2 \to G,\ (x, y) \mapsto xyx^{-1}$ est une action de groupe : c'est l'action par conjugaison.

Définition 1.3.2 : Soient G un groupe, E un ensemble non vide et $(\cdot)$ une action de G sur E. Soit $x \in E$. $\omega_x = \{g \cdot x,\ g \in G\}$ est l'**orbite** de x et $S_x = \{g \in G,\ g \cdot x = x\}$ est un sous-groupe de G appelé **stabilisateur** de x.
Remarque : L'ensemble des orbites forme une partition de E.

Proposition 1.3.1 : Soient G un groupe fini, E un ensemble non vide et $(\cdot)$ une action de G sur E. Soit $x \in E$. Alors, $\mathrm{Card}(G) = \mathrm{Card}(S_x)\mathrm{Card}(\omega_x)$.
Démonstration : On note $\mathcal{R}_x$ la relation d'équivalence sur G définie par : $\forall g, h \in G,\ g\mathcal{R}_x h \ \Leftrightarrow\ g \cdot x = h \cdot x$. On remarque que les classes d'équivalence de cette relation sont de la forme gS_x, elles sont donc toutes du même cardinal que S_x. Comme il y a autant de classes d'équivalence que d'éléments dans l'orbite de x, on en déduit l'égalité recherchée.

Théorème 1.3.1 : (*Équation aux classes*) Soient G un groupe fini, X un ensemble non vide et $(\cdot)$ une action de G sur X. Soit R un système de représentants des orbites de cette action. Alors,

$$\mathrm{Card}(X) = \sum_{x \in R} \frac{\mathrm{Card}(G)}{\mathrm{Card}(S_x)}$$

Démonstration : C'est immédiat d'après la proposition précédente.

Théorème 1.3.2 : (*Équation aux classes et centre du groupe*) Soit G un groupe fini. Il existe un ensemble S de sous-groupes stricts de G tels que :

$$\mathrm{Card}(G) = \mathrm{Card}(\mathcal{Z}(G)) + \sum_{H \in S} \frac{\mathrm{Card}(G)}{\mathrm{Card}(H)}$$

où $\mathcal{Z}(G) = \{x \in G,\ \forall y \in G,\ xy = yx\}$ est le **centre** de G.
Démonstration : Il suffit d'appliquer le théorème précédent à l'action par conjugaison et de remarquer que $\mathcal{Z}(G)$ est l'orbite de l'élément neutre de G.

Théorème 1.3.3 : *(Cauchy)* Soit G un groupe fini d'ordre $n > 1$ et p un diviseur premier de n. Il existe un élément de G d'ordre p.
Démonstration : Pour tout $k \in \{1, ..., p\}$, on note $X_k = \{(g_1, ..., g_k) \in G^k,\ g_1...g_k = 1\}$. Il est clair que $\mathrm{Card}(X_1) = 1$. Pour tout $k \in \{1, ..., p-1\}$, $\mathrm{Card}(X_{k+1}) = n\mathrm{Card}(X_k)$ car

$$(g_1, ..., g_k, g) \in X_{k+1} \ \Leftrightarrow\ (g_1, ..., g_k g) \in X_k$$

On a donc $\mathrm{Card}(X_p) = n^{p-1}$.
On vérifie que l'application $m : \mathbb{Z}/p\mathbb{Z} \times X_p \to G^p$, $([k], (g_1, ..., g_p)) \mapsto (g_k, ..., g_p, g_1, ..., g_{k-1})$ définit une action de groupe de $\mathbb{Z}/p\mathbb{Z}$ dans X_p. On a donc, pour tout $(g_1, ..., g_p) \in X_p$, $\ p = \mathrm{Card}(\omega_{(g_1,...,g_p)})\mathrm{Card}(S_{(g_1,...,g_p)})$.

Supposons qu'il n'existe pas d'éléments de G d'ordre p. Alors pour tout $(g_1, ..., g_p) \neq (1, ..., 1)$, on a $\text{Card}(\omega_{(g_1,...,g_p)}) = p$ (sinon $S_{(g_1,...,g_p)}$ est de cardinal p, ce qui veut dire que les $g_1, ..., g_p$ sont égaux deux à deux). On déduit de l'équation aux classes que $\text{Card}(X_p) = 1$ mod p, ce qui est absurde car $p \mid n^{p-1}$.

Figure 2: Augustin Louis Cauchy, 1789 - 1857

2 Anneaux, corps et polynômes

2.1 Anneaux

Définition 2.1.1 : Un **anneau** est un ensemble non vide A muni de deux lois de composition internes notées $+$ et $\times$ telles que :

1. $(A, +)$ est un groupe commutatif
2. $\times$ est distributive sur $+$
3. A possède un élément neutre pour $\times$

Si $(A, +, \times)$ est un anneau, pour tout $a, b \in A$ on note ab le produit $a \times b$. On note 0 l'élément neutre pour la loi $+$ (élément nul) et 1 l'élément neutre pour la loi $\times$ (unité). Pour tout $x \in A$, $a0 = a(1-1) = a - a = 0$ $(= 0a)$. On dit que A est **nul** lorsque $A = \{0\} = \{1\}$ et que $(A, +, \times)$ est **commutatif** lorsque la loi $\times$ est commutative sur A.

Définition 2.1.2 : Un anneau A est dit **intègre** lorsque pour tout $a, b \in A$, $ab = 0$ implique $a = 0$ ou $b = 0$.

Définition 2.1.3 : Soit $(A, +, \times)$ un anneau et I un sous-ensemble de A. On dit que I est un **idéal** (bilatère) de A lorsque :

1. $(I, +)$ est un sous-groupe de $(A, +)$
2. I est **absorbant** pour $\times$, $i.e$ pour tout $i \in I$, pour tout $a \in A$, $ia \in I$ et $ai \in I$.

En fait, on distingue les idéaux (bilatère) des idéaux **à droite** et des idéaux **à gauche** lorsque la loi $\times$ n'est pas commutative.

Définition 2.1.4 : Soit $(A, +, \times)$ un anneau commutatif et I un idéal de A. On dit que I est **principal** lorsqu'il existe $x \in A$ tel que $I = \{xa,\ a \in A\}$ (I est alors noté (x) ou xA).
Si A est intègre et si tous ses idéaux sont principaux, alors A est dit **principal**.

Définition 2.1.5 : Soit $(A, +, \times)$ un anneau et I un idéal de A. On note $\Re$ la relation d'équivalence sur A définie par : $x \Re y \iff x - y \in I$ et A/I l'**ensemble quotient** défini par cette relation.

Proposition 2.1.1 : Soit $(A, +, \times)$ un anneau et I un idéal de A. L'ensemble quotient A/I muni des lois naturellement induites par A est un anneau.

À partir d'ici, on va alléger les notations et noter A l'anneau $(A, +, \times)$.

Définition 2.1.6 : Soient A_1 et A_2 des anneaux et $f : A_1 \to A_2$ une application. On dit que f est un **morphisme** d'anneaux lorsque :

1. f est un morphisme de groupes de $(A_1, +)$ dans $(A_2, +)$.
2. $\forall x, y \in A,\ f(xy) = f(x)f(y)$
3. $f(1) = 1$

Le **noyau** d'un morphisme d'anneau $f : A_1 \to A_2$ est un idéal de A_1.

Définition 2.1.7 : Soit A un anneau. L'application $f : \mathbb{Z} \to A$, $k \mapsto k \cdot 1 = 1 + ... + 1$ (k fois) est un morphisme d'anneau. Son noyau est un idéal de $\mathbb{Z}$: il est de la forme $c\mathbb{Z}$ pour un certain $c \in \mathbb{N}$. L'entier c est la **caractéristique** de A.

Définition 2.1.8 : Soit A un anneau et soit $x \in A$. On dit que x est **inversible** lorsqu'il existe $y \in A$ tel que $xy = yx = 1$. Si x est inversible, il existe un unique **inverse** noté x^{-1}.

Remarque : 0 n'est pas inversible lorsque A est non nul. L'ensemble des inversibles de A est un groupe pour la loi $\times$.

2.2 Corps

Définition 2.2.1 : Soit A un anneau non nul. On dit que A est un **corps** lorsque tous les éléments non nuls de A sont inversibles.

Proposition 2.2.1 : Soit $\mathbb{K}$ un corps. $\mathbb{K}$ est un anneau intègre.
Démonstration : Soit $a, b \in \mathbb{K}$ tels que $ab = 0$. Supposons que a et b soient non nuls. Alors, $a = abb^{-1} = 0 \times b^{-1} = 0$, ce qui est absurde.

Proposition 2.2.2 : Soit $p \in \mathbb{N}$. $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier.
Démonstration : Supposons que p soit premier. Soit $[a] \in \mathbb{Z}/p\mathbb{Z}$ non nul. a est premier avec p donc on a $u, v \in \mathbb{Z}$ tels que $au + pv = 1$. En passant cette égalité *modulo* p, on obtient $[au + pv] = [au] = [a][u] = [1]$ donc $[a]$ est inversible. Réciproquement, supposons que $\mathbb{Z}/p\mathbb{Z}$ est un corps. Soient $q, r \in \mathbb{Z}$ tels que $p = qr$. Alors $[qr] = [q][r] = 0$ donc $q \in p\mathbb{Z}$ ou $r \in p\mathbb{Z}$ (car $\mathbb{Z}/p\mathbb{Z}$ est intègre) et donc $q = p$ ou $r = p$. On en déduit que p est premier.

Proposition 2.2.3 : Soit $\mathbb{K}$ un corps. La caractéristique c de $\mathbb{K}$ est 0 ou un nombre premier.
Démonstration : Supposons que $c > 0$. Alors $c \geq 2$ car $\mathbb{K}$ est non nul. Soient $p, q \in \mathbb{N}$ tels que $c = pq$. Alors, $c \cdot 1 = pq \cdot 1 = (p \cdot 1)(q \cdot 1) = 0$ donc $p \cdot 1 = 0$ ou $q \cdot 1 = 0$, et donc $p = c$ ou $q = c$ car $p, q \in c\mathbb{N}$ et $p, q \leq c$. Les seuls diviseurs positifs de c sont c et 1 donc c est premier. On vérifie que $\mathbb{R}$ a pour caractéristique 0 et que $\mathbb{Z}/p\mathbb{Z}$ a pour caractéristique p pour tout p premier.

Remarque : Ce résultat est en fait vrai pour tout anneau intègre non nul.

Proposition 2.2.4 : Soit $\mathbb{K}$ un corps, A un anneau non nul et $f : \mathbb{K} \to A$ un morphisme d'anneau. Alors f est injectif.
Démonstration : Soit $x \in \mathrm{Ker}(f)$. Si $x \neq 0$, $1 = f(1) = f(xx^{-1}) = f(x)f(x^{-1}) = 0f(x^{-1}) = 0$, ce qui est absurde. Bref, $\mathrm{Ker}(f) = \{0\}$.

Définition 2.2.2 : Soit $\mathbb{K}$ un corps et $\Bbbk \subseteq \mathbb{K}$. On dit que $\Bbbk$ est un **sous-corps** de $\mathbb{K}$ lorsque c'est un corps pour les lois induites par $\mathbb{K}$. Si $\Bbbk$ est un sous-corps de $\mathbb{K}$, on dit que $\mathbb{K}$ est une **extension** de corps de $\Bbbk$. Plus généralement, si $\Bbbk$ est un corps pas forcément contenu dans $\mathbb{K}$ mais qu'il existe un morphisme de $\Bbbk$ dans $\mathbb{K}$, on dira aussi que $\mathbb{K}$ est une extension de corps de $\Bbbk$ car, ce morphisme étant injectif (**P2.2.4**), $\Bbbk$ est isomorphe à un sous-corps de $\mathbb{K}$.

Définition 2.2.3 : Un corps est dit **premier** lorsque son seul sous-corps est lui-même.

Proposition 2.2.5 : Soit $\mathbb{K}$ un corps de caractéristique c. Si $c = 0$, $\mathbb{K}$ contient un sous-corps isomorphe à $\mathbb{Q}$, sinon, il contient un sous-corps isomorphe à $\mathbb{Z}/c\mathbb{Z}$.
Démonstration :

1. Si $c = 0$, on peut considérer l'application $f : \mathbb{Q} \in \mathbb{K},\ \frac{a}{b} \mapsto (a \cdot 1)(b \cdot 1)^{-1}$. Cette application est bien **définie** (*i.e.*, l'image d'un élément de $\mathbb{Q}$ par f ne dépend pas des représentants du rationnel) car $\{(k \cdot 1),\ k \in \mathbb{Z}\}$ est un sous-anneau **commutatif** de $\mathbb{K}$. On vérifie sans problème que c'est un morphisme, donc f est injective, et $f(\mathbb{Q})$ est un sous-corps de $\mathbb{K}$.

2. Sinon, c est un nombre premier. On note $\Bbbk = \{0,\ 1 \cdot 1,\ 2 \cdot 1,\ ...,\ (c-1) \cdot 1\}$. $\Bbbk$ est un corps pour les lois induites par $\mathbb{K}$. Il est clairement isomorphe à $\mathbb{Z}/c\mathbb{Z}$.

Remarque : On déduit de cette proposition que $\mathbb{Q}$ et les $\mathbb{Z}/p\mathbb{Z}$ sont des corps premiers et que ce sont les seuls à isomorphisme près.

2.3 Polynômes

Définition 2.3.1 : Soit A un anneau commutatif. On appelle **polynôme** (à une indéterminée) à coefficient dans A toute suite **presque nulle** (*i.e.*, nulle à partir d'un certain rang) à valeurs dans A. On note $A[X]$ l'ensemble des polynômes à coefficients dans A. Les lois de A confèrent naturellement une structure d'anneau à $A[X]$. On appelle **degré** de $P \in A[X]$ l'indice du plus grand coefficient non nul de P. Par convention, $\deg(0) = -\infty$.

Théorème 2.3.1 : Soit $\mathbb{K}$ un corps commutatif. Pour tout $A, B \in \mathbb{K}[X]$ avec B non nul, il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tels que $A = BQ + R$ et $\deg(R) < \deg(B)$.

Théorème 2.3.2 : Soit A un anneau commutatif intègre. Alors $A[X]$ est principal si et seulement si A est un corps.
Démonstration : Supposons que A soit un corps. Soit I un idéal (bilatère) de A. On note P un polynôme unitaire de degré minimal dans $I\backslash\{0\}$. Pour tout $Q \in I$, on a $U, V \in A[X]$ tels que $Q = UP + V$ et $\deg(V) < \deg(P)$. $V \in I$ mais P est de degré minimal donc $V = 0$ et P divise Q.
Réciproquement, supposons que $A[X]$ soit principal. Soit $a \in A$ non nul. On note $I = \{aQ + XR,\ Q, R \in A[X]\}$. I est un idéal de $A[X]$ donc on a $P \in A[X]$ tel que $I = (P)$. $a \in I$ donc on a $R \in A[X]$ tel que $a = PR$. Mais A est intègre donc $\deg(R) = \deg(P) = 0$, on peut donc écrire $P = p$ et $R = r$ avec $p, r \in A$. De plus, I contient X donc on a $Q \in A[X]$ de coefficient dominant q tel que $X = pQ$. Alors $Q = qX$ car A est intègre et donc $1 = pq$. Comme $p = ar$, on obtient que $1 = arq$ et donc que $a^{-1} = rq$.

Définition 2.3.2 : Soit A un anneau commutatif. Un polynôme $P \in A[X]$ est **irréductible** sur A *(ou dans A[X])* s'il n'est ni inversible, ni produit de deux polynômes non inversibles.

Exemple : Le polynôme $2X + 2$ est irréductible sur $\mathbb{Q}$ mais pas sur $\mathbb{Z}$.

Proposition 2.3.1 : Si $\mathbb{K}$ est un corps, alors $P \in \mathbb{K}[X]$ est irréductible si, et seulement si, il est de degré ≥ 1 et n'admet que ses polynômes associés comme diviseurs non constants.

Définition 2.3.3 : Soit $\Bbbk$ un corps, $\mathbb{K}$ une extension de $\Bbbk$ et $P \in \Bbbk[X]$ de degré ≥ 1. On dit que $x \in \mathbb{K}$ est une **racine** de P lorsque $P(x) = 0$. On remarque que $x \in \mathbb{K}$ est racine de P si et seulement si $X - x$ divise P. On en déduit que le nombre de racines (comptées avec leur **multiplicité**, *i.e., l'unique entier* $n \in \mathbb{N}^*$ *tel que* $(X - x)^n$ *divise* P *et* $(X - x)^{n+1}$ *ne divise pas* P) de P est inférieur ou égal au degré de P.

Définition 2.3.4 : Un polynôme $P \in \mathbb{K}[X]$ de degré $n \geq 1$ est **scindé** lorsqu'il peut s'écrire comme produit de n polynômes de degré 1. Si $\mathbb{K}$ est un corps, P est scindé si et seulement s'il a n racines (comptées avec leur multiplicité).

Définition 2.3.5 : Soit $\mathbb{K}$ un corps. Une $\mathbb{K}$-algèbre est un anneau non vide A muni d'une structure de $\mathbb{K}$-espace vectoriel.

Définition 2.3.6 : Soit $P \in \mathbb{K}[X]$ irréductible de degré $n > 0$. (P) est un idéal de $\mathbb{K}$ et l'ensemble-quotient $\mathbb{K}/(P)$ est une $\mathbb{K}$-algèbre de dimension n et $\{[1], [X], ..., [X^{n-1}]\}$ en est une base.

Proposition 2.3.2 : $\mathbb{K}[X]/(P)$ est un corps si et seulement si P est irréductible sur $\mathbb{K}$.
Démonstration : C'est exactement la même démonstration que pour **(P2.2.2)** mais adaptée aux polynômes.

Exemple : On peut donner une construction formelle du corps $\mathbb{C}$ à partir de ce résultat. En effet, $X^2 + 1$ est irréductible sur $\mathbb{R}$ donc $\mathbb{K} = \mathbb{R}[X]/(X^2 + 1)$ est une extension de $\mathbb{R}$. On peut construire un isomorphisme de corps de $\mathbb{K} \to \mathbb{C}$ en envoyant $[A] \mapsto A(i)$.

Proposition 2.3.3 : Soit P irréductible dans $\mathbb{K}[X]$. Il existe une extension simple de $\mathbb{K}$ dans laquelle P a une racine. Un telle extension est appelée **corps de rupture** et est unique à isomorphisme près.
Démonstration : En effet, $[X]$ est racine de P dans $\mathbb{K}[X]/(P)$, qui est bien une extension de $\mathbb{K}$ car $x \mapsto [x]$ est un morphisme de $\mathbb{K}$ dans $\mathbb{K}[X]/(P)$. L'unicité découle du fait que si $\mathbb{L}$ est un corps de rupture de P et que $a \in \mathbb{L}$ est une racine de P, alors $\mathbb{K}[X]/(P) \to \mathbb{L},\ [A] \mapsto A(a)$ est un isomorphisme car P est associé au polynôme minimal de a (voir **(P4.0.3)**).

Proposition 2.3.4 : Soit $P \in \mathbb{K}[X]$ de degré supérieur à 1. Il existe une extension dans laquelle P est scindé.
Démonstration : On le démontre sans problème par récurrence sur le degré de P.

Définition 2.3.7 : Un corps $\mathbb{K}$ est **algébriquement clos** lorsque tout polynôme à coefficients dans $\mathbb{K}$ de degré non nul admet une racine dans $\mathbb{K}$.

Théorème 2.3.3 : (*D'Alembert-Gauss*) $\mathbb{C}$ est algébriquement clos.
Démonstration : Soit $P \in \mathbb{C}[X]$ de degré $n \geq 1$. On a $r \in \mathbb{R}_+$ tel que pour tout $z \in \mathbb{C}$, si $|z| > r$ alors $|P(z)| > |P(0)|$. La fonction polynomiale associée à P est continue sur $B(0, r)$ qui est une partie compacte de $\mathbb{C}$, donc il existe $x_0 \in B(0, r)$ tel que $|P(x_0)| = \inf \{|P(x)|,\ x \in B(0, r)\}$. Le développement de Taylor de P en x_0 nous donne $a \in \mathbb{C}^*$, $Q \in \mathbb{C}[X]$ et $k \in \mathbb{N}^*$ tels que pour tout $x \in \mathbb{C}$,

$$P(x) = P(x_0) + a(x - x_0)^k + Q(x)(x - x_0)^{k+1}$$

Supposons que $P(x_0) \neq 0$ et introduisons u une racine k-ième de $\frac{-P(x_0)}{a}$. Alors, pour tout $t \in [0, 1]$,

$$|P(x_0 + tu)| = |P(x_0)(1 - t^k - t^{k+1}\frac{u}{a}Q(x_0 + tu))| \leq |P(x_0)|(|1 - t^k| + t^{k+1}|\frac{u}{a}Q(x_0 + tu)|) \leq |P(x_0)|(1 - t^k + t^{k+1}M)$$

où M est un majorant de $\{|Q(x_0 + tu)|,\ t \in [0, 1]\}$. Il est clair que $\{1 - t^k + t^{k+1}M,\ t \in [0, 1]$ contient un élément strictement inférieur à 1 et donc que $\{x_0 + tu,\ t \in [0, 1]\}$ contient un élément x_1 tel que $|P(x_1)| < |P(x_0)|$ ce qui est absurde. On en déduit que $P(x_0) = 0$ et donc que P a une racine.

(a) Jean Le Rond d'Alembert, 1717 - 1783

(b) Carl Friedrich Gauss, 1777 - 1855

3 Corps finis

Dans toute la suite, on va souvent noter $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$. Il est conseillé de voir les plans de preuves de cette partie qui sont parfois plus détaillés que les démonstrations proposées ici.

Proposition 3.0.1 : Soit $\mathbb{K}$ un corps fini. La caractéristique de $\mathbb{K}$ est un nombre premier.
Démonstration : Oui, sinon l'application de $\mathbb{Z}$ dans $\mathbb{K}$, $k \mapsto k \cdot 1$ serait injective et $\mathbb{K}$ infini.

Théorème 3.0.1 : Soit $\mathbb{K}$ un corps fini de cardinal r. Alors, il existe $p \in \mathbb{N}$ premier et $n \in \mathbb{N}^*$ tels que $r = p^n$.
Démonstration : En effet, en notant p la caractéristique de $\mathbb{K}$, on a un sous-corps $\mathbb{k}$ de $\mathbb{K}$ isomorphe à $\mathbb{F}_p$ (donc de cardinal p). $\mathbb{K}$ est un $\mathbb{k}$-espace vectoriel de dimension finie n (sinon on pourrait trouver une famille $\mathbb{k}$-libre de $\mathbb{K}$ infinie). $\mathbb{K}$ est alors isomorphe (en tant qu'espace vectoriel) à $(\mathbb{F}_p)^n$ qui est de cardinal p^n.

Théorème 3.0.2 : (*Wedderburn*) Soit $\mathbb{K}$ un anneau fini (*a priori* non commutatif) dans lequel tout élément non nul est inversible (un corps sans l'hypothèse de commutativité quoi !). Alors $\mathbb{K}$ est commutatif.
Démonstration : On va raisonner par récurrence sur le cardinal de $\mathbb{K}$.
On note $\mathcal{Z}(\mathbb{K}) = \{x \in \mathbb{K},\ \forall y \in \mathbb{K},\ xy = yx\}$ le centre de $\mathbb{K}$, et pour tout $x \in \mathbb{K}$, on note $\mathbb{K}_x = \{y \in \mathbb{K},\ xy = yx\}$. On note $q = \mathrm{Card}(\mathcal{Z}(\mathbb{K}))$. $\mathcal{Z}(\mathbb{K})$ est un sous-corps commutatif de $\mathbb{K}$ donc $\mathbb{K}$ est un $\mathcal{Z}(\mathbb{K})$-espace vectoriel de dimension finie n et donc $\mathrm{Card}(\mathbb{K}) = q^n$. Si $n = 1$, alors $\mathbb{K} = \mathcal{Z}(\mathbb{K})$, donc $\mathbb{K}$ est commutatif. On suppose que $n > 1$. Pour tout $x \in \mathbb{K} \setminus \mathcal{Z}(\mathbb{K})$, $\mathbb{K}_x$ est un sous-corps (commutatif par hypothèse) de $\mathbb{K}$ qui contient $\mathcal{Z}(\mathbb{K})$, donc $\mathrm{Card}(\mathbb{K}_x) = q^{d_x}$ avec $d_x \mid n$ **(T4.0.1)**. Le groupe $\mathbb{K}^*$ agit sur lui même par conjugaison et les stabilisateurs de cette action sont les $\mathbb{K}_x$. On en déduit que

$$q^n - 1 = q - 1 + \sum_{x \in \omega} \frac{q^n - 1}{q^{d_x} - 1}$$

où ω est système de représentants de l'action **(T1.3.2)**. On a donc une famille d'entiers (λ_d) indéxée par les diviseurs stricts de n telle que

$$q^n - 1 = q - 1 + \sum_{d<n,\ d|n} \lambda_d \frac{q^n - 1}{q^d - 1}$$

Notons, pour tout $k \in \mathbb{N}^*$,

$$\phi_k = \prod_{r \in \mathbb{V}_k} (X - r)$$

(où $\mathbb{V}_k$ est l'ensemble des racines k-ième **primitives** de l'unité) le polynôme cyclotomique d'ordre k. En remarquant que $\mathbb{U}_n = \sqcup_{d|n} \mathbb{V}_d$, on obtient l'égalité $X^n - 1 = \prod_{d|n} \phi_d$. On déduit d'une récurrence que pour tout $n \in \mathbb{N}$, $\phi_n \in \mathbb{Z}[X]$. Mais on peut aussi remarquer que si d divise n, alors ϕ_d divise le polynôme $\frac{X^n-1}{X^d-1}$ dans $\mathbb{Z}[X]$.

En effet, il suffit d'appliquer la décomposition précédente à $X^d - 1$ et de voir qu'elle est contenue dans la décomposition de $X^n - 1$. En notant P le polynôme

$$P = X^n - 1 - \sum_{d|n,\ d<n} \lambda_d \frac{X^n - 1}{X^d - 1}$$

on a $\phi_n(q) \mid P(q) = q - 1$ (car ϕ_n divise P dans $\mathbb{Z}[X]$). Ainsi, $\phi_n(q) \leq q - 1$. Mais comme $\phi_n(q) = \prod_{r\in\mathbb{V}_n}(q - r)$, on a

$$|\phi_n(q)| = |\prod_{r\in\mathbb{V}_n}(q - r)| > \prod_{r\in\mathbb{V}_n}|(q - 1)| = (q - 1)^{\varphi(n)}$$

Comme $n > 1$, $\varphi(n) \geq 1$, ce qui est absurde.

Figure 4: Joseph Wedderburn, 1882 - 1948

Théorème 3.0.3 : Soit $\mathbb{K}$ un corps fini. Alors le groupe $\mathbb{K}^*$ des éléments inversibles de $\mathbb{K}$ est cyclique.
Démonstration : On note n le cardinal de $\mathbb{K}^*$. Les ordres des éléments de $\mathbb{K}^*$ sont des diviseurs de n. Mais $\mathbb{K}$ est un corps donc pour tout d qui divise n, le polynôme $X^d - 1$ admet au plus d racines, il y a au plus d éléments x de $\mathbb{K}^*$ tels que $x^d = 1$. Soit d un diviseur de n, on note $c(d)$ le nombre d'éléments d'ordre d dans $\mathbb{K}^*$. Si $c(d)$ est non nul, on a $x \in \mathbb{K}^*$ d'ordre d. Le groupe $\langle x\rangle$ contient tous les éléments z de $\mathbb{K}^*$ tels que $z^d = 1$. Mais on sait qu'exactement $\varphi(d)$ éléments de $\langle x\rangle$ sont d'ordre d donc $c(d) \leq \varphi(d)$. Comme $n = \sum_{d|n} c(d)$ et $n = \sum_{d|n} \varphi(d)$, on déduit de ce qui précède que si $c(n) = 0$, alors $n = \sum_{d|n,\ d<n} c(d) < \sum_{d|n} \varphi(n) = n$, ce qui est absurde. On en déduit que $c(n) > 0$ et que $\mathbb{K}^*$ est cyclique.

Remarque : En fait, même si $\mathbb{K}$ n'est pas fini, tout sous-groupe fini de $\mathbb{K}^*$ est cyclique.

Proposition 3.0.2 : Soit $p \in \mathbb{N}$ premier et $n \in \mathbb{N}^*$. S'il existe un polynôme $P \in \mathbb{F}_p[X]$ irréductible de degré n, alors le corps $\mathbb{F}_p[X]/(P)$ est de cardinal p^n.
Démonstration : On vérifie que la famille $(\{[1], [X], ..., [X^{n-1}]\})$ est une base de $\mathbb{F}_p[X]$, qui est donc un $\mathbb{F}_p$-espace vectoriel de dimension n, et donc de cardinal p^n.

Théorème 3.0.4 : (*Lemme de Dedekind*) Soit $\mathbb{K}$ un corps. Soit $n \in \mathbb{N}^*$ et $f_1, ..., f_n$ des morphismes distincts de $\mathbb{K} \to \mathbb{K}$. Les $(f_1, ..., f_n)$ forment une famille libre de l'espace des fonctions de $\mathbb{K} \to \mathbb{K}$.
Démonstration : Procédons par récurrence. Pour $n = 1$, tout va bien. Supposons que ce soit vrai pour $n - 1$. Soient $\alpha_1, ..., \alpha_n \in \mathbb{K}$ tels que $\alpha_1 f_1 + ... + \alpha_n f_n = 0$. Pour tout $x, y \in \mathbb{K}$,

$$\alpha_1 f_1(xy) + ... + \alpha_n f_n(xy) = \alpha_1 f_1(x) f_1(y) + ... + \alpha_n f_n(x) f_n(y) = 0$$

et

$$\alpha_1 f_1(x) f_n(y) + ... + \alpha_n f_n(x) f_n(y) = 0$$

donc

$$\alpha_1 f_1(x)(f_n(y) - f_1(y)) + ... + \alpha_{n-1} f_{n-1}(x)(f_n(y) - f_{n-1}(y)) = 0$$

Or les $(f_1, ..., f_{n-1})$ forment une famille libre donc pour tout $y \in \mathbb{K}$, $i \in [\![1, n-1]\!]$, $\alpha_i(f_n(y) - f_i(y)) = 0$. On déduit de l'intégrité de $\mathbb{K}$ et du fait que ces applications sont distinctes que les α_i sont nuls. Le fait que α_n est nul est alors immédiat. $(f_1, ..., f_n)$ est bien une famille libre.

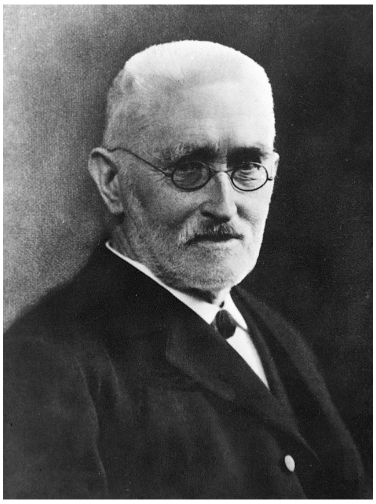


Figure 5: Richard Dedekind, 1831 - 1916

Théorème 3.0.5 : (*Morphisme de Frobenius*) Soit $\mathbb{K}$ un corps fini de caractéristique p et de cardinal p^n avec $n > 0$. Le groupe $\mathrm{Aut}(\mathbb{K})$ est cyclique d'ordre n et l'application de $\mathbb{K}$ dans $\mathbb{K}$, $x \mapsto x^p$ est un automorphisme de corps de $\mathbb{K}$ qui engendre $\mathrm{Aut}(\mathbb{K})$.
Démonstration : Notons $f : x \mapsto x^p$. Pour tout $x, y \in \mathbb{K}$, $f(xy) = x^p y^p$ et

$$f(x+y) = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p$$

car p divise $\binom{p}{k}$ pour tout $k \in [\![1, p-1]\!]$, donc f est bien un morphisme. f est injective car $\mathbb{K}$ est intègre, c'est bien un automorphisme. Ensuite, on remarque que pour tout $x \in \mathbb{K}^*$, $f^n(x) = x^{p^n} = x$ car $\mathbb{K}^*$ est un groupe de cardinal $p^n - 1$ (ce qui donne $x^{p^n-1} = 1$ par le théorème de Lagrange). On en déduit que $f^n = \mathrm{id}$ et que l'ordre de f est inférieur à n. Mais l'ordre de f est aussi supérieur à n car si pour tout $x \in \mathbb{K}$, $f^k(x) = x$, alors pour tout $x \in \mathbb{K}$, $x^{p^k-1} = 1$ donc le polynôme $X^{p^k-1} - 1$ admet p^n racines, ce qui force k à être supérieur à n. Bref, f est d'ordre n dans $\mathrm{Aut}(\mathbb{K})$.
Enfin, supposons qu'on puisse trouver $n+1$ éléments distincts dans $\mathrm{Aut}(\mathbb{K})$ que l'on note $f_1, ..., f_{n+1}$, et notons $e_1, ..., e_n$ une base de $\mathbb{K}$. On s'intéresse à la matrice à n ligne et $n+1$ colonnes formée des $f_i(e_j)$. Les $n+1$ colonnes sont identifiables à des vecteurs de $\mathbb{K}^n$ et forment une famille liée. Les (f_i) vérifient alors exactement la même relation de liaison que ces vecteurs, ce qui est impossible selon **(T3.0.4)**. $\mathrm{Aut}(\mathbb{K})$ est de cardinal inférieur à n, donc exactement n et engendré par f.

Théorème 3.0.6 : Soit $p \in \mathbb{N}$ premier et $n \in \mathbb{N}^*$. Il existe un polynôme $P \in \mathbb{F}_p[X]$ irréductible et de degré n. De plus, le corps $\mathbb{F}_p[X]/(P)$ est, à isomorphisme près, l'unique corps de cardinal p^n.
Démonstration : On note $P = X^{p^n} - X$ et, pour tout $d \in \{1, ..., n\}$, I_d l'ensemble des polynômes irréductibles sur $\mathbb{F}_p$ unitaires de degré d.

1. $Q \in I_d$ divise P si et seulement si d divise n. En effet, si $n = dr$, on se place dans le corps $\mathbb{F}_p[X]/(Q)$ et on remarque que $[P] = [X]^{p^n} - [X] = [X]^{p^{dr}} - [X] = ((([X]^{p^d})^{p^d}) \; ... \;)^{p^d} - [X]$. Mais $\mathbb{F}_p[X]/(Q)$ est de cardinal p^d donc l'application $\mathcal{F} : x \to x^p$ est un automorphisme d'ordre d, ce qui donne $[X]^{p^d} = [X]$ et $[P] = 0$.

Figure 6: Georg Frobenius, 1849 - 1917

Autrement dit, Q divise P. Réciproquement, si Q divise P, alors dans $\mathbb{F}_p/(Q)$ on a $[P]=0$ donc $[X]^{p^n}=[X]$ et donc $\mathcal{F}^n([X])=[X]$. On en déduit que pour tout $R\in\mathbb{F}_p[X]$, $\mathcal{F}^n([R])=[R]$ donc $\mathcal{F}^n=id$. Comme $\mathcal{F}$ est d'ordre d dans $\mathrm{Aut}(\mathbb{F}_p[X]/(Q))$, d divise n.

2. Par le lemme de Gauss, pour tout d qui divise n, pour tout $Q\in I_d$, Q apparait au moins une fois dans la décomposition en facteurs irréductibles de P, donc $\prod_{d|n}(\prod_{Q\in I_d}Q)$ divise P. Supposons maintenant que pour un certain d diviseur de n, on ait $Q\in I_d$ tel que Q^2 divise P. Alors Q divise aussi le polynôme dérivé $p^nX^{p^n-1}-1$. Dans $\mathbb{F}_p[X]/(Q)$, on a $p^n[X]^{p^n-1}=[1]$, mais $\mathbb{F}_p[X]/(Q)$ est de caractéristique p donc $[0]=[1]$ ce qui est absurde. Ainsi, Q^2 ne divise pas P, et donc la décomposition en facteurs irréductibles de P comporte chaque élément de I_d exactement une fois : $P=\prod_{d|n}(\prod_{Q\in I_d}Q)$.

3. La nouvelle écriture de P nous permet de trouver une expression pour son degré : $p^n=\sum_{d|n}d\mathrm{Card}(I_d)$. On veut montrer que $\mathrm{Card}(I_n)>0$. On peut commencer par écrire que

$$\mathrm{Card}(I_n)=\frac{1}{n}(p^n-\sum_{d|n,d<n}d\mathrm{Card}(I_d))$$

Or,

$$\sum_{d|n,d<n}d\mathrm{Card}(I_d)\leq\sum_{d|n,d<n}dp^d\leq\sum_{d=1}^{n-1}dp^{d-1}$$

car construire un polynôme unitaire de degré d sur $\mathbb{F}_p$ c'est choisir $d-1$ coefficients avec p choix à chaque fois. On montre par récurrence que pour tout entier $m\leq 2$,

$$\sum_{d=1}^{n-1}dm^{d-1}=\frac{1+(n-1)m^n-nm^{n-1}}{(1-m)^2}$$

donc

$$p^n-\sum_{d=1}^{n-1}dp^{d-1}=\frac{n(p^n-p^{n-1})+p^n((1-p^2)-1)-1}{(1-p)^2}$$

$p\geq 2$ car p est premier donc $n(p^n-p^{n-1})\geq 1$ et $p^n((1-p)^2-1)\geq 1$ (ce sont des entier strictement positifs). Alors, $\frac{1}{n}(p^n-\sum_{d=1}^{n}dp^{d-1})>0$ et donc I_n est non-vide. Il existe bien un polynôme irréductible sur $\mathbb{F}_p$ de degré n et, *a fortiori*, un corps de cardinal p^n.

4. Il ne reste plus qu'à montrer que ce corps est unique à isomorphisme près. Soit $\mathbb{K}$ un corps de cardinal p^n et $Q \in I_n$. P est scindé sur $\mathbb{K}$ car pour tout $x \in \mathbb{K}$, $x^{p^n} = x$. Or Q divise P donc Q est aussi scindé sur $\mathbb{K}$. En particulier, on peut trouver $r \in \mathbb{K}$ tel que $Q(r) = 0$. La famille $(1, r, ..., r^{n-1})$ est donc une base de $\mathbb{K}$ en tant que $\mathbb{F}_p$-algèbre (elle est libre car si on avait un polynôme non nul $R \in \mathbb{F}_p[X]$ de degré strictement inférieur à n tel que $R(r) = 0$, on aurait $U, V \in \mathbb{F}_p[X]$ tels que $QU + RV = 1$ et alors $r = 0$ ce qui contredit l'hypothèse d'irréductibilité de Q). On peut donc définir un isomorphisme (de corps) de $\mathbb{F}_p[X]/(Q) \to \mathbb{K}$ en envoyant $[A]$ sur $A(r)$.

Exemple : On a vu dans cette partie qu'il n'existait pas de corps à 6 éléments mais qu'il suffisait de trouver un polynôme irréductible sur $\mathbb{F}_2$ de degré 3 pour construire un corps à 8 éléments. En notant 0 et 1 les éléments de $\mathbb{F}_2$, on peut trouver facilement les seuls polynômes qui fonctionnent : $X^3 + X + 1$ et $X^3 + X^2 + 1$. Comme $\mathbb{F}_8^*$ est cyclique, on peut montrer que $\mathbb{F}_8 = \{0,\ 1,\ a,\ a^2,\ a+1,\ a^2+a,\ a^2+a+1,\ a^2+1\}$ où a est racine de $X^3 + X + 1$.

4 Extensions de corps

Pour désigner les extensions de corps, on va utiliser la notation suivante : $\Bbbk \subset \mathbb{K}$ signifie que $\mathbb{K}$ est une extension de $\Bbbk$ et $\Bbbk \subset \mathbb{K} \subset \mathbb{L}$ signifie que $\mathbb{K}$ et $\mathbb{L}$ sont des extensions de $\Bbbk$ et que $\mathbb{L}$ est une extension de $\mathbb{K}$. Le symbole $\subset$ désigne une simple inclusion (sauf mention contraire) pour des ensembles notés sans lettres ajourées.

Définition 4.0.1 : Soient $\Bbbk \subset \mathbb{K}$ et $\Bbbk \subset \mathbb{L}$ des extensions. Un morphisme ϕ de $\mathbb{K}$ dans $\mathbb{L}$ tel que pour tout $x \in \Bbbk$, $\phi(x) = x$ est appelé **$\Bbbk$-morphisme**. On note $\mathrm{Hom}_{\Bbbk}(\mathbb{K}, \mathbb{L})$ l'ensemble des $\Bbbk$-morphismes de $\mathbb{K}$ dans $\mathbb{L}$. L'ensemble des éléments bijectifs de $\mathrm{Hom}_{\Bbbk}(\mathbb{K})$ ($\Bbbk$-automorphismes de $\mathbb{K}$) est appelé **groupe de Galois** de $\mathbb{K}$ sur $\Bbbk$ et est noté $\mathrm{Gal}(\mathbb{K}/\Bbbk)$. C'est un sous-groupe de $\mathrm{Aut}(\mathbb{K})$.

Proposition 4.0.1 : Soit $\mathbb{K}$ un corps et $\Bbbk$ son sous-corps premier. Alors, $\mathrm{Aut}(\mathbb{K}) = \mathrm{Gal}(\mathbb{K}/\Bbbk)$.
Démonstration : En effet, $\Bbbk$ est le sous-corps de $\mathbb{K}$ engendré par 1. Un automorphisme de $\mathbb{K}$ y est donc forcément invariant. L'autre inclusion est claire.

Exemple : L'identité $\mathrm{id}_{\mathbb{R}}$ est le seul $\mathbb{Q}$-automorphisme de $\mathbb{R}$. Soit $\phi \in \mathrm{Gal}(\mathbb{R}/\mathbb{Q})$. Soient $x, y \in \mathbb{R}$ tels que $y \leq x$. $\phi(x-y) = \phi(\sqrt{x-y}^2) = \phi(\sqrt{x-y})^2 \geq 0$ donc ϕ est croissante. $\mathbb{Q}$ est dense dans $\mathbb{R}$ donc on a deux suites (α_n) et (β_n) convergeant vers x et telles que pour tout $n \in \mathbb{N}$, $\alpha_n \leq x \leq \beta_n$. Alors, pour tout $n \in \mathbb{N}$, $\alpha_n = \phi(\alpha_n) \leq \phi(x) \leq \phi(\beta_n) = \beta_n$. On en déduit que $\phi(x) = x$. Ainsi, ϕ est l'identité.

Définition 4.0.2 : On a vu que si $\Bbbk \subset \mathbb{K}$ est une extension de corps, alors $\mathbb{K}$ est un $\Bbbk$-espace vectoriel. La dimension de cet espace est appelée **degré** de l'extension et noté $[\mathbb{K} : \Bbbk]$. L'extension est dite **finie** quand $[\mathbb{K} : \Bbbk]$ est fini.

Exemple : $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{C} : \mathbb{Q}]$ est infini car la famille $(\sqrt{p},\ p \in \mathbb{P})$, où $\mathbb{P}$ est l'ensemble des entiers premiers, est libre (sur $\mathbb{Q}$).

Théorème 4.0.1 : Soit $\Bbbk \subset \mathbb{K} \subset \mathbb{L}$ des extensions. Soient $(e_i)_I$ une $\Bbbk$-base de $\mathbb{K}$ et $(f_j)_J$ une $\mathbb{K}$-base de $\mathbb{L}$. Alors $(e_i f_j)_{I \times J}$ est une $\Bbbk$-base de $\mathbb{L}$.
Démonstration : Soit $x \in \mathbb{L}$. $x = \sum_{j \in J} \alpha_j f_j$ où la famille $(\alpha_j)_J$ est à support fini. Pour tout $j \in J$, $\alpha_j \in \mathbb{K}$ donc on peut trouver une famille $(\beta_{i,j})_I$ à support fini telle que $\alpha_j = \sum_{i \in I} \beta_{i,j} e_i$. Alors, $x = \sum_{j \in J} (\sum_{i \in I} \beta_{i,j} e_i) f_j$ $= \sum_{(i,j) \in I \times J} \beta_{i,j} e_i f_j$. On en déduit que la famille $(e_i f_j)_{I \times J}$ est génératrice du $\Bbbk$-espace vectoriel $\mathbb{L}$. Elle est libre car si $\sum_{(i,j) \in I \times J} \beta_{i,j} e_i f_j = 0$, alors $\sum_{j \in J} (\sum_{i \in I} \beta_{i,j} e_i) f_j = 0$ et donc, comme les $(f_j)_J$ forment une $\mathbb{K}$-base de $\mathbb{L}$, pour tout $j \in J$, $\sum_{i \in I} \beta_{i,j} e_i = 0$. Mais les $(e_i)_I$ forment une $\Bbbk$-base de $\mathbb{K}$, donc pour tout $j \in J$, les $(\beta_{i,j})_I$ sont nuls.

Remarque : On déduit du théorème précédent que $[\mathbb{K} : \Bbbk]$ et $[\mathbb{L} : \mathbb{K}]$ sont finis si et seulement si $[\mathbb{L} : \Bbbk]$ est fini. Dans ce cas, on a $[\mathbb{L} : \Bbbk] = [\mathbb{K} : \Bbbk] \times [\mathbb{L} : \mathbb{K}]$.

Définition 4.0.3 : Soient $\Bbbk \subset \mathbb{K}$ une extension et E une partie quelconque de $\mathbb{K}$.

1. On note $\Bbbk[E]$ le plus petit sous-anneau de $\mathbb{K}$ contenant $\Bbbk$ et E. On remarque que $\Bbbk[E] = \{P(e_1, ..., e_n),\ (e_1, ..., e_n) \in E^n,\ P \in \Bbbk[X_1, ..., X_n],\ n \in \mathbb{N}\}$.
2. On note $\Bbbk(E)$ le plus petit sous-corps de $\mathbb{K}$ contenant $\Bbbk$ et E. On remarque que $\Bbbk(E) = \{P(e_1, ..., e_n) Q(e_1, ..., e_n)^{-1},\ (e_1, ..., e_n) \in E^n,\ Q(e_1, ..., e_n) \neq 0,\ P, Q \in \Bbbk[X_1, ..., X_n],\ n \in \mathbb{N}\}$.

Proposition 4.0.2 : Soient E, F des parties de $\mathbb{K}$. On a $\Bbbk(E \cup F) = \Bbbk(E)(F)$.

Définition 4.0.4 : Soient $\Bbbk \subset \mathbb{K}$ une extension et $x \in \mathbb{K}$. On dit que x est **algébrique** sur $\Bbbk$ s'il existe un polynôme non nul $P \in \Bbbk[X]$ tel que $P(x) = 0$. Si ce n'est pas le cas, on dit que x est **transcendant**.

Exemple : $\sqrt{2}$ et $\frac{1+\sqrt{5}}{2}$ sont algébriques sur $\mathbb{Q}$. e et π sont transcendants.

Proposition 4.0.3 : Soit $x \in \mathbb{K}$ algébrique sur $\Bbbk$. L'ensemble $I = \{P \in \Bbbk[X],\ P(x) = 0\}$ est un idéal principal de $\Bbbk[X]$. On a un donc un unique polynôme unitaire μ_x appelé **polynôme minimal** de x tel que $I = (\mu_x)$. Le degré de μ_x est appelé **degré** de x et est noté d_x. De plus, μ_x est irréductible sur $\Bbbk$.
Démonstration : On vérifie sans problème que I est un idéal principal de $\Bbbk[X]$. Supposons que $\mu_x = PQ$. Alors, $P(x)Q(x) = 0$ donc $P(x) = 0$ ou $Q(x) = 0$ et donc $P \in (\mu_x)$ ou $Q \in (\mu_x)$. On en déduit que P ou Q est associé à μ_x. Ainsi, μ_x est bien irréductible.

Exemple : $X^2 - 2$ est le polynôme minimal de $\sqrt{2}$ et $X^2 - X - 1$ est le polynôme minimal de $\frac{1+\sqrt{5}}{2}$.

Théorème 4.0.2 : Soient $\Bbbk \subset \mathbb{K}$ une extension et $x \in \mathbb{K}$. x est algébrique sur $\Bbbk$ si et seulement si la $\Bbbk$-algèbre $\Bbbk[x]$ est de dimension finie.
Démonstration : Supposons x algébrique. Alors, pour tout $P \in \Bbbk[X]$, on a $A, B \in \Bbbk[X]$ tels que $\deg(B) < \deg(\mu_x)$ et $P = A\mu_x + B$. Alors, $P(x) = B(x) \in \mathrm{Vect}(1, x, ..., x^{d_x - 1})$. On a montré que la famille $(1, x, ..., x^{d_x-1})$ est génératrice (c'est même une base car elle est clairement libre) et donc que $\Bbbk[x]$ est de dimension finie. Réciproquement, si $\Bbbk[x]$ est de dimension finie n, alors la famille $(1, x, ..., x^n)$ est liée donc x est algébrique.

Théorème 4.0.3 : x est algébrique si et seulement si $\Bbbk[x] = \Bbbk(x)$.
Démonstration : Supposons x algébrique. On rappelle que $\Bbbk(x) = \{P(x)Q(x)^{-1},\ P, Q \in \Bbbk[X],\ Q(x) \neq 0\}$. Il est clair que $\Bbbk[x] \subset \Bbbk(x)$. Soit $y = P(x)Q(x)^{-1} \in \Bbbk(x)$. μ_x est irréductible et $Q \notin (\mu_x)$ donc Q et μ_x sont premiers entre eux. Selon le théorème de Bézout, on a $U, V \in \Bbbk[X]$ tels que $1 = U\mu_x + VQ$. En évaluant en x, on a $1 = V(x)Q(x)$ donc $y = P(x)V(x) \in \Bbbk[x]$. On a alors $\Bbbk(x) \subset \Bbbk[x]$ ce qui donne l'égalité. Réciproquement, si $\Bbbk[x] = \Bbbk(x)$ et $x \neq 0$, alors on a $P \in \Bbbk[X]$ tel que $x^{-1} = P(x)$. Alors le polynôme $XP - 1$ annule x.

Théorème 4.0.4 : x est algébrique si et seulement si l'extension $\Bbbk \subset \Bbbk(x)$ est finie.
Démonstration : Si x est algébrique, $\Bbbk[x] = \Bbbk(x)$ donc $\Bbbk \subset \Bbbk[x]$ est une extension de corps, finie selon **(T4.2)**. Si $\Bbbk \subset \Bbbk(x)$ est finie, alors $\Bbbk[x]$ est aussi de dimension finie car inclus dans $\Bbbk(x)$. On conclus avec **(T4.2)**.

Définition 4.0.5 : Une extension $\Bbbk \subset \mathbb{K}$ est dite **algébrique** lorsque tous les éléments de $\mathbb{K}$ sont algébriques.

Théorème 4.0.5 : Soit $\Bbbk \subset \mathbb{K}$ une extension. $\mathbb{K}$ est algébrique si et seulement si toutes les sous-algèbres de $\mathbb{K}$ sont des corps.
Démonstration : Supposons que $\mathbb{K}$ soit algébrique. Soit A une sous-algèbre de $\mathbb{K}$ et $x \in A$ non nul. Il est clair que $\Bbbk[x] \subset A$, mais x est algébrique donc $\Bbbk[x] = \Bbbk(x)$ et donc $x^{-1} \in A$. Réciproquement, si toute sous-algèbre de $\mathbb{K}$ est un corps, alors, en particulier, les $\Bbbk[x]$ sont des corps donc pour tout $x \in \mathbb{K}$, $\Bbbk[x] = \Bbbk(x)$.

Théorème 4.0.6 : Si $[\Bbbk : \mathbb{K}]$ est fini, alors $\mathbb{K}$ est algébrique.
Démonstration : Oui car pour tout $x \in \mathbb{K}$, $\Bbbk[x]$ est une sous-algèbre de $\mathbb{K}$ donc est de dimension finie.

Remarque : En fait, pour tout $x \in \mathbb{K}$, le degré de x divise $[\mathbb{K} : \Bbbk]$ en vertu du **(T4.1)**.

Remarque : La réciproque est complètement fausse. On verra plus tard que l'ensemble $\hat{\mathbb{Q}}$ des complexes algébriques sur $\mathbb{Q}$ est un corps, mais que l'extension $\mathbb{Q} \subset \hat{\mathbb{Q}}$ n'est pas finie.

Proposition 4.0.4 : Soit $E \subset \mathbb{K}$ tel que tout élément de E est algébrique. Alors l'extension $\Bbbk \subset \Bbbk(E)$ est algébrique.

Démonstration : En effet, soit $x \in E$. On a $n \in \mathbb{N}^*$ et $e_1, ..., e_n \in E$ tels que $x \in \Bbbk(e_1, ..., e_n)$ (c'est comme cela que sont construit tous les éléments de $\Bbbk(E)$). Alors $\Bbbk[x]$ est de dimension finie car
$\Bbbk[x] \subset \Bbbk(e_1, ..., e_n) = \Bbbk(e_1)(...)(e_n)$, qui est de dimension finie sur $\Bbbk$ ($\Bbbk(e_1)$ est de dimension finie car e_1 est algébrique sur $\Bbbk$ mais e_2 est aussi algébrique sur $\Bbbk$ donc sur $\Bbbk(e_1)$ et donc $\Bbbk(e_1)(e_2)$ est de dimension finie, etc...).

Remarque : D'ailleurs, si E est fini, alors $\Bbbk \subset \Bbbk(E)$ est finie.

Théorème 4.0.7 : Soient $\Bbbk \subset \mathbb{K} \subset \mathbb{L}$ des extensions. $\Bbbk \subset \mathbb{L}$ est algébrique si et seulement si $\Bbbk \subset \mathbb{K}$ et $\mathbb{K} \subset \mathbb{L}$ le sont.
Démonstration : Si $\Bbbk \subset \mathbb{L}$ est algébrique alors clairement $\Bbbk \subset \mathbb{K}$ et $\mathbb{K} \subset \mathbb{L}$ aussi. Réciproquement, soit $x \in \mathbb{L}$. x est algébrique sur $\mathbb{K}$ donc on a $\alpha_0, ..., \alpha_n \in \mathbb{K}$ tels que $\alpha_0 + \alpha_1 x + ... + \alpha_n x^n = 0$. x est algébrique sur $\Bbbk(\alpha_0, ..., \alpha_n)$ donc $\Bbbk(\alpha_0, ..., \alpha_n) \subset \Bbbk(\alpha_0, ..., \alpha_n)(x)$ est finie. Mais comme $\Bbbk \subset \Bbbk(\alpha_0, ..., \alpha_n)$ est finie,
$\Bbbk \subset \Bbbk(\alpha_0, ..., \alpha_n)(x)$ est finie. $\Bbbk[x] \subset \Bbbk(\alpha_0, ..., \alpha_n)(x)$ donc x est algébrique.

Théorème 4.0.8 : Soit $\Bbbk \subset \mathbb{K}$ une extension. L'ensemble $\hat{\mathbb{K}}$ des éléments de $\mathbb{K}$ algébriques sur $\Bbbk$ est un corps.
Démonstration : Soient $x, y \in \hat{\mathbb{K}}$ avec x non nul. xy et $x + y$ sont algébriques car $\Bbbk[xy]$ et $\Bbbk[x + y]$ sont inclus dans $\Bbbk(x)(y)$ qui est de dimension finie. x^{-1} est algébrique car $\Bbbk[x^{-1}] \subset \Bbbk(x)$.

Définition 4.0.6 : L'ensemble $\hat{\mathbb{K}}$ est la **fermeture algébrique** de $\Bbbk$ dans $\mathbb{K}$.

Évidemment, la fermeture algébrique dépend de l'extension choisie. La fermeture algébrique de $\mathbb{C}$ pour l'extension $\mathbb{R} \subset \mathbb{C}$ est $\mathbb{C}$, ce n'est pas le cas pour l'extension $\mathbb{Q} \subset \mathbb{C}$.
Définition 4.0.7 : On dit que $\Bbbk$ est **algébriquement fermé** dans $\mathbb{K}$ si $\hat{\mathbb{K}} = \Bbbk$.

Attention, cette définition n'a rien à voir avec le fait d'être *algébriquement clos* (et encore moins avec le fait d'être un *fermé* en topologie). On a cependant le théorème suivant :

Théorème 4.0.9 : Soit $\Bbbk$ un corps. $\Bbbk$ est algébriquement clos si et seulement si il est algébriquement fermé dans toutes ses extensions.
Démonstration : Si $\Bbbk$ est algébriquement clos, on se donne une extension non triviale $\Bbbk \subset \mathbb{K}$ et $x \in \mathbb{K} \setminus \Bbbk$. Tout polynôme $P \in \Bbbk[X]$ est scindé dans $\Bbbk$ donc y admet toutes ses racines, x ne peut donc être racine d'aucun polynôme, il est transcendant sur $\Bbbk$. Réciproquement, soit $P \in \Bbbk[X]$ irréductible. $\Bbbk[X]/(P)$ est un corps et $\Bbbk$ est algébriquement fermé dans l'extension $\Bbbk \subset \Bbbk[X]/(P)$. P admet une racine x dans $\Bbbk[X]/(P)$, on a forcément $x \in \Bbbk$. Ainsi, P est de degré 1 et donc $\Bbbk$ est algébriquement clos.

Proposition 4.0.5 : Soit $\Bbbk \subset \mathbb{K}$ une extension. Si $\mathbb{K}$ est algébriquement clos, la fermeture algébrique $\hat{\mathbb{K}}$ sur $\Bbbk$ est algébriquement close.
Démonstration : Soit $P \in \hat{\mathbb{K}}[X]$. P admet une racine $x \in \mathbb{K}$. x est algébrique sur $\hat{\mathbb{K}}$ donc sur $\Bbbk$ **(T4.7)**. P admet donc une racine dans $\hat{\mathbb{K}}$.

Définition 4.0.8 : Soit $\Bbbk$ un corps et $P \in \Bbbk[X]$ irréductible. Une extension $\Bbbk \subset \mathbb{K}$ dans laquelle P a une racine α telle que $\mathbb{K} = \Bbbk(\alpha)$ est appelée **corps de rupture** de P. L'existence d'un corps de rupture découle du fait que $\Bbbk \subset \Bbbk[X]/(P)$ est une extension dans laquelle P admet une
racine. Il suffit de prendre le sous-corps contenant $\Bbbk$ engendré par cette racine pour avoir un corps de rupture de P.

Théorème 4.0.10 : Soit $\Bbbk$ un corps, $P \in \Bbbk[X]$ irréductible, $\Bbbk(\alpha)$ et $\Bbbk(\beta)$ des corps de rupture de P. Alors $\Bbbk(\alpha)$ et $\Bbbk(\beta)$ sont isomorphes, et il existe un unique $\Bbbk$-isomorphisme $\phi : \Bbbk(\alpha) \to \Bbbk(\beta)$ tel que $\phi(\alpha) = \beta$.
Démonstration : α et β sont tous deux algébriques sur $\Bbbk$ et leur polynôme minimal est l'unique polynôme

unitaire associé à P. $\Bbbk(\alpha)$ et $\Bbbk(\beta)$ sont alors isomorphes à $\Bbbk[X]/(P)$ et donc isomorphes entre eux. De plus, $\Bbbk(\alpha) = \Bbbk[\alpha]$ et $\Bbbk(\beta) = \Bbbk[\beta]$ donc l'application $\phi : \Bbbk(\alpha) \to \Bbbk(\beta)$, $Q(\alpha) \mapsto Q(\beta)$ est un $\Bbbk$-isomorphisme qui envoie α sur β. C'est le seul puisqu'il est entièrement déterminé par l'image de α et des éléments de $\Bbbk$.

Théorème 4.0.11 : Soient $P \in \Bbbk[X]$ irréductible de degré n et $\Bbbk \subset \mathbb{K}$ une extension finie de degré m premier avec n. Alors P est irréductible dans $\mathbb{K}[X]$.
Démonstration : Supposons que P admette un facteur $Q \in \mathbb{K}[X]$ irréductible. Soit $\mathbb{K}_Q$ un corps de rupture de Q. Alors $[\mathbb{K}_Q : \Bbbk] = m \times \deg(Q)$. Mais $\mathbb{K}_Q$ est un corps dans lequel P a une racine, notée α. Alors $[\Bbbk(\alpha) : \Bbbk] = n$, donc n divise $m \times \deg(Q)$, et donc $\deg(Q)$, ce qui est absurde.

5 Théorèmes de Steinitz

Définition 5.0.1 : Soit $\Bbbk$ un corps. Une extension algébrique et algébriquement close sur $\Bbbk$ est appelée **clôture algébrique** de $\Bbbk$. On va montrer que $\Bbbk$ admet une clôture algébrique mais on donne d'abord les définitions et résultats suivants :

Définition 5.0.2 : Un ensemble ordonné $(E, \leq)$ est dit **inductif** lorsque toute partie totalement ordonnée de E admet un majorant.

Théorème 5.0.1 : *(Zorn)* Tout ensemble inductif admet un élément maximal.

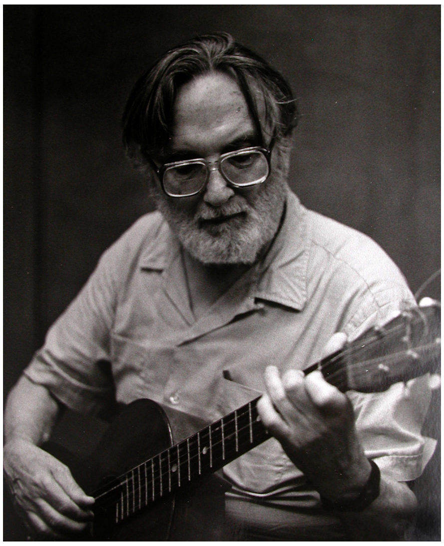


Figure 7: Max Zorn, 1906 - 1993

Définition 5.0.3 : On a vu que si A est un anneau, on peut définir $A[X]$ l'anneau des polynômes à une indéterminée à coefficients dans A. En fait, il n'y a pas de contraintes sur le nombre d'indéterminées. On peut définir par récurrence sur n l'anneau $A[X_1, ..., X_n]$ des polynômes à n indéterminées en disant que c'est $A[X_1, ..., X_{n-1}][X_n]$. On peut même définir $A[(X_i)_I]$ où $(X_i)_I$ est une famille infinie d'indéterminées en prenant la réunion des $A[(X_j)_J]$ où J parcours l'ensemble des parties finie de I.

Exemple : Un polynôme à deux indéterminées $P \in \Bbbk[X, Y]$ peut être vu comme un élément de $\Bbbk[X][Y]$, un polynôme à coefficients dans $\Bbbk[X]$.

Définition 5.0.4 : Soit A un anneau et E une partie de A. L'idéal **engendré** par E (noté $A(E)$) est le plus petit idéal de A contenant E : c'est l'intersection de tous les idéaux de A contenant E. On remarque que $A(E) = \{a_1e_1 + ... + a_ne_n,\ n \in \mathbb{N}^*,\ (a_1, ..., a_n) \in A^n,\ (e_1, ..., e_n) \in E^n\}$. Si E contient 1, alors $A(E) = A$.

Exemple : L'idéal de $\mathbb{Z}$ engendré par $\{3, 6\}$ est $3\mathbb{Z}$ et celui engendré par $\{4, 5\}$ est $\mathbb{Z}$ car 4 et 5 sont premiers entre eux. En général, $\mathbb{Z}(\{a, b\}) = \mathrm{PGCD}(a, b)\mathbb{Z}$.

Définition 5.0.5 : Soit A un anneau et I un idéal strict de A. On dit que I est **maximal** lorsqu'il n'existe pas d'idéal J tel que $I \subset J \subset A$ (avec les inclusions **strictes**).

Proposition 5.0.1 : Soit A un anneau et I un idéal maximal de A. Alors le quotient A/I est un corps.
Démonstration : On sait déjà que A/I peut être muni naturellement d'une structure d'anneau. Soit $\bar{a} \in A/I$ non nul. L'idéal de A engendré par I et a est différent de I, donc égal à A. On a donc $1 = xi + ya$ avec $x, y \in A$.

En passant au quotient, on trouve $\bar{1} = \bar{y}\bar{a}$, donc $\bar{a}$ est inversible.

Théorème 5.0.2 : Soit A un anneau et I un idéal strict de A. Il existe un idéal maximal M de A dans lequel I est inclus.
Démonstration : On note E l'ensemble des idéaux stricts de A dans lesquels I est inclus. E n'est pas vide puisqu'il contient I. On va vérifier que la relation d'inclusion (large), que l'on note $\subset$, fait de $(E, \subset)$ un ensemble inductif. Soit F une partie de E totalement ordonnée. $F = \{J_k,\ k \in K\}$ où K est un ensemble quelconque. On note $J = \cup_K J_k$. J est un idéal de A car si $x, y \in J$ et $a \in A$, disons $x \in J_{k_1}$ et $y \in J_{k_2}$, alors
$x - y,\ ax,\ xa \in \max(J_{k_1}, J_{k_2})$. $J \neq A$ car sinon il contiendrait 1 et un des J_k serait égal à A. J est clairement un majorant de F.

Théorème 5.0.3 : *(Steinitz)* Tout corps $\Bbbk$ admet une extension algébriquement close.
Démonstration : On note E l'ensemble des polynômes de degré supérieur à 1 à coefficients dans $\Bbbk$ et on se donne une famille $(X_P)_E$ d'indéterminées indexée par E. On note A l'anneau $\Bbbk[(X_P)_E]$ et I l'idéal engendré par les $(P(X_P))_E$. Supposons que $I = A$. Alors on a $P_1, ..., P_n \in E$ et $Q_1, ..., Q_n \in A$ tels que
$1 = Q_1P_1(X_{P_1}) + ... + Q_nP_n(X_{P_n})$. On peut trouver une extension $\Bbbk \subset \mathbb{K}$ dans laquelle chaque $P_i,\ 1 \leq i \leq n$ a une racine α_i. En substituant les X_{P_i} par α_i et les autres indéterminées par 0, on a $1 = 0$, ce qui est absurde. On a donc un idéal M de A maximal contenant I. On note $\mathbb{K}_1$ le corps A/M. On remarque que tous les éléments de E ont une racine dans $\mathbb{K}_1$: en effet, soit $P \in E$, $P(\bar{X_P}) = 0$. Par le même procédé, on peut construire par récurrence une suite $\mathbb{K}_1 \subset ... \subset \mathbb{K}_n \subset ...$ de corps tels que tout élément de $\mathbb{K}_n[X] \setminus \mathbb{K}_n$ admet une racine dans $\mathbb{K}_{n+1}$. On note $\mathbb{K}$ la réunion des $(\mathbb{K}_n)_{\mathbb{N}}$, et on remarque que $\mathbb{K}$ est un corps algébriquement clos contentant $\Bbbk$.

Théorème 5.0.4 : *(Steinitz)* Tout corps $\Bbbk$ admet une clôture algébrique.
Démonstration : On peut trouver une extension $\Bbbk \subset \mathbb{K}$ algébriquement close. En prenant la fermeture algébrique de $\mathbb{K}$ dans $\Bbbk$, on a bien trouvé une clôture algébrique pour $\Bbbk$. (La fermeture algébrique $\hat{\mathbb{K}}$ de $\Bbbk$ dans $\mathbb{K}$ est algébriquement fermée dans toutes ses extensions, donc algébriquement close **(T4.9)**.)

Théorème 5.0.5 : *(Steinitz)* "La" clôture algébrique d'un corps $\Bbbk$ est unique à isomorphisme près.
Démonstration : Soient $\Bbbk \subset \mathbb{K}$ et $\Bbbk \subset \mathbb{L}$ deux clôtures algébriques de $\Bbbk$. On note E l'ensemble des couples $(\mathbb{M}, \phi)$ où $\mathbb{M}$ est un sous-corps de $\mathbb{K}$ contenant $\Bbbk$ et ϕ un morphisme de $\mathbb{M} \to \mathbb{L}$ prolongeant $id_{\Bbbk}$. E n'est pas vide puisqu'il contient $(\Bbbk, id_{\Bbbk})$. On peut ordonner E en définissant $\leq$: $(\mathbb{M}_1, \phi_1) \leq (\mathbb{M}_2, \phi_2) \Leftrightarrow$
$\mathbb{M}_1 \subset \mathbb{M}_2\ \wedge \phi_2\ |_{\mathbb{M}_1} = \phi_1$. E est inductif : on peut trouver un majorant d'une partie totalement ordonnée de E en prenant la réunion de tous les sous-corps des couples constituant cette partie. On a donc $(\mathbb{M}, \phi)$ un élément maximal de E. Supposons que $\mathbb{M} \neq \mathbb{K}$ et donnons nous $x \in \mathbb{K} \setminus \mathbb{M}$. x est algébrique sur $\mathbb{M}$, son polynôme minimal μ_x est à coefficients dans $\mathbb{M}$, on note Q le polynôme de $\mathbb{L}[X]$ dont les coefficients sont les images des coefficients de μ_x par ϕ. Q admet une racine $\alpha \in \mathbb{L}$ car $\mathbb{L}$ est algébriquement clos. ϕ se prolonge donc en un morphisme $\phi' : \mathbb{M}(x) \to \mathbb{L}$ tel que $\phi'(x) = \alpha$. Alors, $(\mathbb{M}, \phi) \leq (\mathbb{M}(x), \phi')$ ce qui contredit la maximalité de $(\mathbb{M}, \phi)$. On en déduit qu'il existe un $\Bbbk$-morphisme ϕ de $\mathbb{K}$ dans $\mathbb{L}$. ϕ est injectif et $\phi(\mathbb{K})$ est un sous-corps de $\mathbb{L}$ contenant $\Bbbk$. $\mathbb{K}$ est algébriquement clos donc $\phi(\mathbb{K})$ aussi, $\phi(\mathbb{K})$ est donc algébriquement fermé dans toutes ses extensions, en particulier dans $\phi(\mathbb{K}) \subset \mathbb{L}$. On en déduit que $\phi(\mathbb{K}) = \mathbb{L}$ ce qui permet de conclure.

La preuve du **(T5.5)** utilise une idée très importante, qui donne le théorème suivant :
Théorème 5.0.6 : Soient $\Bbbk \subset \mathbb{K}$ une extension algébrique, $\mathbb{L}$ un corps algébriquement clos et σ un morphisme de $\Bbbk$ dans $\mathbb{L}$. Alors, il existe un morphisme θ de $\mathbb{K}$ dans $\mathbb{L}$ tel que $\theta|_{\Bbbk} = \sigma$.
Démonstration : Même preuve qu'en **5.5**.

Proposition 5.0.2 : Soient $\Bbbk \subset \mathbb{K}$ une extension algébrique et $\Bbbk \subset \mathbb{L}$ la clôture algébrique de $\Bbbk$. Selon **(T5.6)**, on peut plonger $\mathbb{K}$ dans $\mathbb{L}$ et considérer que $\Bbbk \subset \mathbb{K} \subset \mathbb{L}$. Soit $\sigma \in \mathrm{Hom}_{\Bbbk}(\mathbb{K}, \mathbb{L})$ tel que $\sigma(\mathbb{K}) \subset \mathbb{K}$. Alors $\sigma(\mathbb{K}) = \mathbb{K}$ et il existe $\theta \in \mathrm{Gal}(\mathbb{L}/\Bbbk)$ tel que $\theta|_{\mathbb{K}} = \sigma$.

Démonstration : On veut montrer que σ est surjectif sur $\mathbb{K}$. Soit $x \in \mathbb{K}$. x est algébrique, on note R l'ensemble des racines de μ_x dans $\mathbb{K}$ et $\hat{\sigma}$ le morphisme de $\mathbb{K}[X] \to \mathbb{L}[X]$ naturellement induit par σ. Alors $\sigma(R) = R$ car σ est injectif et car les $\sigma(r)$ où $r \in R$ sont racines de $\hat{\sigma}(\mu_x)$ (et $\hat{\sigma}(\mu_x) = \mu_x$ car σ est invariant sur $\mathbb{k}$). On en déduit que x est l'image par σ d'une racine dans $\mathbb{K}$ de μ_x. Ainsi, $\sigma(\mathbb{K}) = \mathbb{K}$ et l'application $\mathbb{K} \to \mathbb{K},\ x \mapsto \sigma(x)$ est un élement de $\mathrm{Gal}(\mathbb{K}/\mathbb{k})$ qui, selon **(T5.6)**, peut être prolongé en un élément $\theta \in \mathrm{Hom}_{\mathbb{k}}(\mathbb{L})$. Il est alors clair que $\theta(\mathbb{L}) \subset \mathbb{L}$ et, en appliquant le même raisonnement, on trouve que $\theta \in \mathrm{Gal}(\mathbb{L}/\mathbb{k})$.

Figure 8: Ernst Steinitz, 1871 - 1928

6 Extensions séparables

Définition 6.0.1 : On dit que deux polynômes sont **premiers entre eux** lorsqu'ils ont un plus grand diviseur commun constant.

On rappelle les théorèmes de Bézout pour les polynômes :
Théorème 6.0.1 : Soient $\mathbb{K}$ un corps et $P, Q \in \mathbb{K}[X]$. $D \in \mathbb{K}[X]$ est un pgcd de P et Q si, et seulement si, D divise P et Q et il existe $U, V \in \mathbb{K}[X]$ premiers entre eux tels que $UP + VQ = D$.
Théorème 6.0.2 : Soient $\mathbb{K}$ un corps et $P, Q \in \mathbb{K}[X]$. P et Q sont premiers entre eux si, et seulement si, il existe $U, V \in \mathbb{K}[X]$ tels que $UP + VQ = 1$.

Proposition 6.0.1 : Soient $\Bbbk \subset \mathbb{K}$ une extension, et $P, Q \in \Bbbk[X]$. Si P et Q sont premiers entre eux dans $\Bbbk[X]$, ils le sont aussi dans $\mathbb{K}[X]$.
Démonstration : Selon le théorème de Bézout, on peut trouver $U, V \in \Bbbk[X]$ tels que $UP + VQ = 1$. Comme $\Bbbk[X] \subset \mathbb{K}[X]$, on peut appliquer le théorème **(T6.2)** dans l'autre sens et en déduire que P et Q sont premiers entre eux dans $\mathbb{K}[X]$.

Proposition 6.0.2 : Avec les mêmes notations, si D est un pgcd de P et de Q dans $\Bbbk[X]$, alors c'en est un aussi dans $\mathbb{K}[X]$.
Démonstration : Si D est un pgcd de P et de Q dans $\Bbbk[X]$, on a $A, B \in \Bbbk[X]$ premiers entre eux dans $\Bbbk[X]$ tels que $AP + BQ = D$. Alors A et B sont premiers entre eux dans $\mathbb{K}[X]$, donc D est un pgcd de P et Q dans $\mathbb{K}[X]$.

Remarque : Il est clair que si D est un pgcd de P et Q dans $\mathbb{K}[X]$ et que $D \in \Bbbk[X]$, alors D est un pgcd de P et Q dans $\Bbbk[X]$.

Proposition 6.0.3 : Soient $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$. $\alpha \in \mathbb{K}$ est une racine simple de P *(i.e., $X - \alpha$ divise P et $(X - \alpha)^2$ ne divise pas P)* si et seulement si $P(\alpha) = 0$ et $P'(\alpha) \neq 0$.

Définition 6.0.2 : Soit $P \in \Bbbk[X]$ de degré ≥ 1. On dit que P est **séparable** lorsque les racines de P dans la clôture algébrique de $\Bbbk$ sont simples.

Théorème 6.0.3 : Soient $P \in \Bbbk[X]$ non constant. TFAE :

1. P est séparable.
2. Dans toute extension de $\Bbbk$, P n'a que des racines simples.
3. P et P' sont premiers entre eux.
4. Dans toute extension de $\Bbbk$, P et P' n'ont pas de racine commune.

Démonstration : (1) $\Rightarrow$ (2) : Soit $\mathbb{K}$ une extension dans laquelle P a une racine α et $\mathbb{L}$ la clôture algébrique de la fermeture algébrique de $\mathbb{K}$. Alors $\mathbb{L}$ est aussi la clôture algébrique de $\Bbbk$. On en déduit que $P'(\alpha) \neq 0$.
(2) $\Rightarrow$ (3) : Soit $\mathbb{L}$ la clôture algébrique de $\Bbbk$. P est scindé à racines simples dans $\mathbb{L}$ donc P et P' sont premiers entre eux.
(3) $\Rightarrow$ (4) : P et P' sont premiers entre eux dans $\Bbbk[X]$ donc dans toute extension, donc P n'a jamais de racine multiple.
(4) $\Rightarrow$ (1) : P est scindé dans la clôture algébrique de $\Bbbk$ et n'a pas de racine commune avec P' donc ses racines sont simples, et donc P est séparable.

Remarque : On notera qu'une autre condition (5) parfaitement équivalente à ces dernières est l'existence d'une extension dans laquelle P est scindé à racines simples. (1) implique clairement (5) et (5) implique (3).

Exemple : Le polynôme $X^2 + X + 1 \in \mathbb{Q}[X]$ est séparable car il se décompose en $(X - j)(X + j)$ dans $\mathbb{C}[X]$. En revanche, $X^2 + X + 1 \in \mathbb{F}_3[X]$ n'est pas séparable car il admet 1 comme racine et son polynôme dérivé $2X + 1$ aussi.

Théorème 6.0.4 : Soient $P \in \Bbbk[X]$ irréductible. TFAE :

1. P est séparable.

2. Il existe une extension dans laquelle P a une racine simple.

3. $P' \neq 0$.

Démonstration : (1) $\Rightarrow$ (2) : Pas de problème.
(2) $\Rightarrow$ (3) : Si α est racine simple de P alors $P'(\alpha) \neq 0$ donc $P' \neq 0$.
(3) $\Rightarrow$ (1) : On peut supposer P unitaire. Soient $\Bbbk \subset \mathbb{L}$ la clôture algébrique de $\Bbbk$ et $x \in \mathbb{L}$ une racine de P. P est le polynôme minimal de x donc x n'est pas racine de P' car $\deg(P') < \deg(P)$. On en déduit que x est racine simple de P. C'est le cas de toutes les racines de P, qui est donc séparable.

Définition 6.0.3 : Soit $\Bbbk$ un corps. On dit que $\Bbbk$ est **parfait** s'il est de caractéristique nulle ou si $\Bbbk = \{x^c,\ x \in \Bbbk\}$ où $c > 0$ est la caractéristique de $\Bbbk$.

Proposition 6.0.4 : Si $\Bbbk$ est fini, alors il est parfait.
Démonstration : La caractéristique p de $\Bbbk$ est un nombre premier. On a vu en **(T3.4)** que l'application $x \mapsto x^p$ est un automorphisme (donc une application surjective).

Proposition 6.0.5 : Si $\Bbbk$ est algébriquement clos, alors il est parfait.
Démonstration : On peut supposer $\Bbbk$ de caractéristique p non nulle. Soit $a \in \Bbbk$. Le polynôme $X^p - a$ admet une racine donc on a $\alpha \in \Bbbk$ tel que $\alpha^p = a$. L'application $x \mapsto x^p$ est surjective donc $\Bbbk$ est parfait.

Définition 6.0.4 : Soit $\Bbbk \subset \mathbb{K}$ une extension. On dit que l'extension est **séparable** lorsque tous les éléments de $\mathbb{K}$ sont séparables *(i.e, ils sont algébriques et leurs polynômes minimaux sont séparables).*

Théorème 6.0.5 : Soit $\Bbbk$ un corps. TFAE :

1. $\Bbbk$ est parfait.

2. Tout polynôme irréductible dans $\Bbbk[X]$ est séparable.

3. Toute extension algébrique de $\Bbbk$ est séparable.

4. La clôture algébrique de $\Bbbk$ est séparable.

Démonstration : (1) $\Rightarrow$ (2) : Soit $P \in \Bbbk[X]$ irréductible. Si $\Bbbk$ est de caractéristique nulle, alors $P' \neq 0$. Sinon, en notant p sa caractéristique, on peut écrire que

$$\{Q \in \Bbbk[X],\ Q' = 0\} = \{Q(X^p),\ Q \in \Bbbk[X]\} = \{Q^p,\ Q \in \Bbbk[X]\}$$

La première égalité est claire et la seconde découle du fait que si $Q = a_0 + a_1X^p + ... + a_nX^{pn}$, alors comme $\Bbbk$ est parfait, on a $b_0, ..., b_n \in \Bbbk$ tels que $Q = b_0^p + b_1^pX^p + ... + b_n^pX^{pn}$, et donc $Q = (b_0 + b_1X + ... + b_nX^n)^p$ (car $x \mapsto x^p$ est un morphisme). Si on avait $P' = 0$, alors P s'écrirait Q^p pour un certain $Q \in \Bbbk[X]$, ce qui est absurde car P est irréductible. On en déduit que $P' \neq 0$ et donc que P est séparable.

$(2) \Rightarrow (3)$: Si $\Bbbk \subset \mathbb{K}$ est une extension algébrique, alors tout élément de $\mathbb{K}$ est séparable car son polynôme minimal est irréductible, donc séparable par hypothèse. $\mathbb{K}$ est bien séparable.
$(3) \Rightarrow (4)$: Oui.
$(4) \Rightarrow (1)$: On peut supposer $\Bbbk$ de caractéristique $p > 0$. Soit $a \in \Bbbk$. $P = X^p - a$ admet une racine b dans $\mathbb{L}$ la clôture algébrique de $\Bbbk$. μ_b divise P et est séparable donc $P = \mu_b^r$ pour $r \neq 0$. En effet, si $P = \mu_b D$, alors $0 = P' = \mu_b' D + \mu_b D'$, donc $-\mu_b D' = \mu_b' D$ donc μ_b divise D. On peut itérer le raisonnement pour montrer que μ_b est le seul facteur irréductible de $\Bbbk[X]$ de P. Comme $P' = r\mu_b'\mu_b^{r-1} = 0$ et μ_b séparable, on a p qui divise r, donc $p = r$. On en déduit que μ_b est de degré 1 et donc que $b \in \Bbbk$. $x \mapsto x^p$ est donc surjectif et $\Bbbk$ parfait.

Théorème 6.0.6 : Soient $\Bbbk \subset \mathbb{K}$ une extension séparable de degré fini n et $\Bbbk \subset \mathbb{L}$ une extension algébriquement close. Alors, $\mathrm{Card}(\mathrm{Hom}_{\Bbbk}(\mathbb{K}, \mathbb{L})) = n$.
Démonstration : Traitons d'abord le cas où $\mathbb{K}$ est simple : $\mathbb{K} = \Bbbk(a)$. Dans $\mathbb{L}[X]$, on peut écrire $\mu_a = (X - a_1)...(X - a_n)$ avec les a_i distincts deux à deux. Alors, pour tout i, $\sigma_i : \mathbb{K} \to \mathbb{L},\ P(a) \mapsto P(a_i)$ est bien défini et est un élément de $\mathrm{Hom}_{\Bbbk}(\mathbb{K}, \mathbb{L})$. Les σ_i sont clairement distincts. Si $\sigma \in \mathrm{Hom}_{\Bbbk}(\mathbb{K}, \mathbb{L})$, alors $\sigma(a)$ est racine de μ_a donc est un des a_i. On en déduit que σ est un des σ_i et que $\mathrm{Card}(\mathrm{Hom}_{\Bbbk}(\mathbb{K}, \mathbb{L})) = n$.
On va maintenant raisonner par récurrence et supposer que $\mathbb{K}$ n'est pas simple. Soit $(e_1, ..., e_r)$ une famille minimale telle que $\mathbb{K} = \Bbbk(e_1)...(e_r)$. Alors, $p = [\mathbb{K} : \Bbbk(e_1)...(e_{r-1})] > 1$ et $q = [\Bbbk(e_1)...(e_{r-1}) : \Bbbk] > 1$ et $n = pq$. $\Bbbk \subset \mathbb{K}$ est séparable donc $\Bbbk \subset \Bbbk(e_1)...(e_{r-1})$ aussi et donc $\mathrm{Card}(\mathrm{Hom}_{\Bbbk}(\Bbbk(e_1)...(e_{r-1}), \mathbb{L})) = q$ selon notre hypothèse de récurrence.
Soit $\sigma \in \mathrm{Hom}_{\Bbbk}(\Bbbk(e_1)...(e_{r-1}), \mathbb{L})$. σ induit un morphisme $\hat{\sigma}$ de $\Bbbk(e_1, ..., e_{r-1})[X] \to \mathbb{L}[X]$ qui envoie un polynôme $b_0 + ... + b_m X^m$ sur $\sigma(b_0) + ... + \sigma(b_m)X^m$. e_r est séparable donc son polynôme minimal **sur** $\Bbbk(e_1, ..., e_{r-1})$ (que l'on note μ_r) est de degré p et scindé à racines simples dans $\mathbb{L}$: $\mu_r = (X - a_1)...(X - a_p)$. Les $\sigma(a_i)$ on tous le même polynôme minimal $\hat{\sigma}(\mu_r)$. Pour tout i, on peut définir un élément de $\mathrm{Hom}_{\Bbbk}(\mathbb{K}, \mathbb{L})$,

$$\sigma_i : \Bbbk(e_1, ..., e_{r-1})(e_r) \to \mathbb{L},\ Q(e_r) \mapsto \hat{\sigma}(Q)(a_i)$$

Il est clair que les éléments de la famille des $(\sigma_i,\ 1 \leq i \leq p,\ \sigma \in \mathrm{Hom}_{\Bbbk}(\Bbbk(e_1)...(e_{r-1}), \mathbb{L}))$ sont distincts deux à deux et donc que $\mathrm{Card}(\mathrm{Hom}_{\Bbbk}(\mathbb{K}, \mathbb{L})) \leq n$.
Par ailleurs, si $\sigma \in \mathrm{Hom}_{\Bbbk}(\mathbb{K}, \mathbb{L})$, alors

$$\theta = \sigma_{|\Bbbk(e_1, ..., e_{r-1})} \in \mathrm{Hom}_{\Bbbk}(\Bbbk(e_1)...(e_{r-1}), \mathbb{L})$$

et $\sigma(e_r)$ est racine de $\hat{\theta}(\mu_r)$, donc σ est un des σ_i construits plus tôt. On en déduit que $\mathrm{Card}(\mathrm{Hom}_{\Bbbk}(\mathbb{K}, \mathbb{L})) = n$.

Théorème 6.0.7 : *(de l'élément primitif)* Toute extension finie et séparable est simple.
Démonstration : Soient $\Bbbk \subset \mathbb{K}$ de degré n et séparable, et $\Bbbk \subset \mathbb{L}$ la clôture algébrique de $\Bbbk$.
Si $\Bbbk$ est fini, alors $\mathbb{K}$ est aussi fini (car isomorphe à $\Bbbk^n$ en tant que $\Bbbk$-espace vectoriel). $\mathbb{K}^*$ est alors cyclique **(T3.2)** et donc $\mathbb{K}$ est simple.
On peut maintenant supposer $\Bbbk$ infini. On note $\sigma_1, ..., \sigma_n$ les éléments de $\mathrm{Hom}_{\Bbbk}(\mathbb{K}, \mathbb{L})$ et pour tout $(i, j) \in \mathcal{F} = \{(i, j),\ 1 \leq i < j \leq n\}$ on note

$$\mathcal{Z}_{i,j} = \{x \in \mathbb{K},\ \sigma_i(x) = \sigma_j(x)\}$$

On remarque d'abord que ce sont des sous-$\Bbbk$-espaces vectoriels de $\mathbb{K}$.
Pour toute partie $\mathcal{G}$ de $\mathcal{F}$, on note $U_{\mathcal{G}} = \cup_{a \in \mathcal{G}} \mathcal{Z}_a$. On veut montrer que $U_{\mathcal{F}} \neq \mathbb{K}$. Procédons par récurrence sur le cardinal de $\mathcal{G}$. Il est clair que si $\mathcal{G}$ est un singleton alors $U_{\mathcal{G}} \neq \mathbb{K}$.
Supposons maintenant que $U_{\mathcal{G}} \neq \mathbb{K}$ pour toute partie stricte $\mathcal{G}$ de $\mathcal{F}$ et que $U_{\mathcal{F}} = \mathbb{K}$. On peut écrire $U_{\mathcal{F}} = \mathcal{Z}_{1,2} \cup U_{\mathcal{F} \setminus \{1,2\}}$. Si $\mathcal{Z}_{1,2} \subset U_{\mathcal{F} \setminus \{1,2\}}$, alors $\mathbb{K} = U_{\mathcal{F}} = U_{\mathcal{F} \setminus \{1,2\}} \neq \mathbb{K}$ ce qui est absurde. Sinon, soient $x \in \mathcal{Z}_{1,2} \setminus U_{\mathcal{F} \setminus \{1,2\}}$ et $y \in \mathbb{K} \setminus \mathcal{Z}_{1,2}$. Alors, $\{x + \alpha y,\ \alpha \in \Bbbk\} \subset U_{\mathcal{F} \setminus \{1,2\}}$ car s'il existait $\alpha \in \Bbbk$ tel que $x + \alpha y \in \mathcal{Z}_{1,2}$, on aurait $y \in \mathcal{Z}_{1,2}$.

Comme $\Bbbk$ est infini, on a $\alpha, \beta \in \Bbbk$ et $(i, j) \in \mathcal{F}$ tels que $\alpha \neq \beta$ et $x + \alpha y \in \mathcal{Z}_{i,j}$ et $x + \beta y \in \mathcal{Z}_{i,j}$. On trouve alors que $x, y \in \mathcal{Z}_{i,j}$, ce qui est absurde. On a donc $U_{\mathcal{F}} \neq \mathbb{K}$, ce qui achève la récurrence.
On peut alors trouver $x \in \mathbb{K} \setminus U_{\mathcal{F}}$. Pour tout i, $\sigma_{i\,|\Bbbk(x)} \in \mathrm{Hom}_{\Bbbk}(\Bbbk(x), \mathbb{L})$, et si $j \neq i$ alors $\sigma_{i\,|\Bbbk(x)} \neq \sigma_{j\,|\Bbbk(x)}$ par définition de x. Or, le théorème précédent **(T6.6)** nous affirme que $\mathrm{Card}(\mathrm{Hom}_{\Bbbk}(\Bbbk(x), \mathbb{L})) = [\Bbbk(x) : \Bbbk]$. On en déduit que $n = [\Bbbk(x) : \Bbbk]$ et que $\mathbb{K} = \Bbbk(x)$.

Théorème 6.0.8 : Soient $\Bbbk \subset \mathbb{K} \subset \mathbb{L}$ des extensions algébriques. Alors l'extension $\Bbbk \subset \mathbb{L}$ est séparable si, et seulement si, les extensions $\Bbbk \subset \mathbb{K}$ et $\mathbb{K} \subset \mathbb{L}$ sont séparables.

Théorème 6.0.9 : Soit $\Bbbk \subset \mathbb{K}$ une extension telle que $\mathbb{K}$ est le corps de décomposition d'une famille $\mathcal{F}$ de polynômes séparables. Alors $\Bbbk \subset \mathbb{K}$ est séparable.
Démonstration : On note $\mathcal{F} = (P_i)_I$ les éléments de $\mathcal{F}$ et R l'ensemble de leurs racines. Soit $x \in \mathbb{K}$. On a $P \in \Bbbk[X_1, ..., X_m]$ et $r_1, ..., r_m \in R$ tels que $x = P(r_1, ..., r_m)$. L'extension $\Bbbk \subset \Bbbk(r_1, ..., r_m)$ est séparable :
$\Bbbk \subset \Bbbk(r_1)$ et $\Bbbk(r_1) \subset \Bbbk(r_1, r_2)$ sont séparables donc $\Bbbk \subset \Bbbk(r_1, r_2)$ aussi. On conclut par récurrence.

7 Groupe de Galois d'un corps fini

Théorème 7.0.1 : Le groupe de Galois de l'extension $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ est cyclique d'ordre n.
Démonstration : On a vu en **(T3.4)** que $\mathrm{Aut}(\mathbb{F}_{p^n})$ est cyclique d'ordre n engendré par le morphisme $\mathcal{F} : x \mapsto x^p$. On veut donc montrer que $\mathrm{Aut}(\mathbb{F}_{p^n}) = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Soit $x \in \mathbb{F}_p$ et $\sigma \in \mathrm{Aut}(\mathbb{F}_{p^n})$. On a $k \geq 0$ tel que $\sigma = \mathcal{F}^k$. Alors, $\sigma(x) = \mathcal{F}^k(x) = x^{p^k}$. Comme $p-1$ divise $p^k - 1$, et $\mathbb{F}_p^*$ est d'ordre $p-1$, on trouve $x^{p^k-1} = 1$, et donc $\sigma(x) = x$. On a montré que σ est invariant sur $\mathbb{F}_p$, et donc que $\mathrm{Aut}(\mathbb{F}_{p^n}) = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Bref, $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \sim \mathbb{Z}/n\mathbb{Z}$.
Sinon, on voit facilement par le même argument que $\mathcal{F}$ laisse invariant $\mathbb{F}_p$, donc le groupe qu'il engendre est inclu dans $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. On a le résultat par double inclusion.

8 Extensions normales

Définition 8.0.1 : Soit $\Bbbk \subset \mathbb{K}$ une extension algébrique. On dit qu'elle est **normale** si tout polynôme irréductible sur $\Bbbk$ ayant une racine dans $\mathbb{K}$ est scindé sur $\mathbb{K}$. Autrement dit, si tous les μ_x sont scindés dans $\mathbb{K}$.

Définition 8.0.2 : Soient $\Bbbk \subset \mathbb{K}$ algébrique et $x, y \in \mathbb{K}$. On dit que x et y sont conjugués s'ils ont le même polynôme minimal. Si x est de degré n, alors il existe au plus n éléments de $\mathbb{K}$ conjugués à x. Si x est séparable, alors il admet exactement n conjugués dans la clôture algébrique de $\Bbbk$.

Proposition 8.0.1 : Soient $\Bbbk \subset \mathbb{K}$ algébrique et $x, y \in \mathbb{K}$. Selon **(T5.6)**, on peut plonger $\mathbb{K}$ dans la clôture algébrique $\mathbb{L}$ de $\Bbbk$. TFAE :

1. x, y sont conjugués
2. Il existe $\sigma \in \mathrm{Gal}(\mathbb{L}/\Bbbk)$ tel que $\sigma(x) = y$.

Démonstration : (1) $\Rightarrow$ (2) : On définit l'application $\sigma : \Bbbk(x) \to \mathbb{L},\ P(x) \mapsto P(y)$. Cette application est bien définie et est un élément de $\mathrm{Hom}_{\Bbbk}(\Bbbk(x), \mathbb{L})$ donc on peut le prolonger en un élement $\theta \in \mathrm{Gal}(\mathbb{L}/\Bbbk)$ **(P5.2)**. Il est clair que $\theta(x) = y$.
(2) $\Rightarrow$ (1) : On vérifie sans problème que $\sigma(x)$ est racine de μ_x, donc que y est algébrique et que μ_y divise μ_x. Comme μ_x est irréductible unitaire, on en déduit que $\mu_x = \mu_y$.

Définition 8.0.3 : Soient $\Bbbk$ un corps et $(P_i)_I$ une famille de polynômes à coefficients dans $\Bbbk$ de degrés ≥ 1. Une extension $\Bbbk \subset \mathbb{K}$ dans laquelle tous les P_i sont scindés et telle que $\mathbb{K} = \Bbbk(R)$, où R est l'ensemble des racines des P_i dans $\mathbb{K}$, est appelée **corps de décomposition** des $(P_i)_I$. C'est la plus petite extension dans laquelle tous les P_i sont scindés.

Théorème 8.0.1 : Soit $\Bbbk \subset \mathbb{K}$ une extension algébrique, que l'on peut considérer plongée dans la clôture algébrique $\mathbb{L}$ de $\Bbbk$. TFAE :

1. $\mathbb{K}$ est normale
2. Il existe une famille $(P_i)_I$ de polynômes tels que $\mathbb{K}$ est un corps de décomposition des (P_i).
3. Pour tout $\sigma \in \mathrm{Hom}_{\Bbbk}(\mathbb{K}, \mathbb{L})$, $\sigma(\mathbb{K}) \subset \mathbb{K}$.

Démonstration : (1) $\Rightarrow$ (2) : $\mathbb{K}$ est algébrique donc en prenant la famille $(\mu_x)_{x \in \mathbb{K}}$, on a bien $\mathbb{K} = \Bbbk(R)$.
(2) $\Rightarrow$ (3) : Soit $\sigma \in \mathrm{Hom}_{\Bbbk}(\mathbb{K}, \mathbb{L})$. Soit $x \in \mathbb{K}$. x peut s'écrire $x = P(r_1, ..., r_m)$ où $P \in \Bbbk[X_1, ..., X_m]$ et les r_i sont des racines des P_i. Alors, $\sigma(x) = P(\sigma(r_1), ..., \sigma(r_m))$. Or, pour tout i, $\sigma(r_i)$ est racine du même polynôme que r_i, donc $\sigma(x) \in \mathbb{K}$. On en déduit que $\sigma(\mathbb{K}) \subset \mathbb{K}$.
(3) $\Rightarrow$ (1) : Soit $P \in \Bbbk[X]$ irréductible de degré $n \geq 1$ et ayant une racine a_1 dans $\mathbb{K}$. P est scindé sur $\mathbb{L}$ donc on peut écrire $P = \lambda(X - a_1)...(X - a_n)$. Alors, tous les a_i sont conjugués à a_1, donc sont l'image de a_1 par un morphisme $\sigma_i \in \mathrm{Gal}(\mathbb{L}/\Bbbk)$ et donc sont dans $\mathbb{K}$ par hypothèse. P est alors scindé sur $\mathbb{K}$.

Remarque : Il est important de noter que (3) est parfaitement équivalente à une assertion *a priori* plus forte : Pour tout $\sigma \in \mathrm{Gal}(\mathbb{L}/\Bbbk)$, $\sigma(\mathbb{K}) = \mathbb{K}$ (justifié en **(P5.2)**).

Théorème 8.0.2 : Soit $\Bbbk \subset \mathbb{K}$ une extension algébrique finie. TFAE :

1. $\mathbb{K}$ est normale.
2. Il existe un polynôme P tel que $\mathbb{K}$ est un corps de décomposition de P.

Démonstration : (1) $\Rightarrow$ (2) : Soit $\mathcal{F}$ une famille de polynômes telle que $\mathbb{K}$ est un corps de décomposition de $\mathcal{F}$, on note R l'ensemble des racines des éléments de $\mathcal{F}$. Alors $\mathbb{K} = \Bbbk(R)$. Mais $[\mathbb{K} : \Bbbk]$ est fini, donc on peut trouver une partie finie $R' \subset R$ telle que $\mathbb{K} = \Bbbk(R')$. Alors, à chaque élément de R', on peut associer un élement P_r de $\mathcal{F}$ tel que $P_r(r) = 0$. $\mathbb{K}$ est un corps de décomposition du produit des P_r.
(2) $\Rightarrow$ (1) : **(T8.1)**.

Définition 8.0.4 : Soit $\Bbbk$ un corps et E une partie de $\mathbb{L}$, la clôture algébrique de $\Bbbk$. L'extension $\Bbbk \subset \mathbb{K} = \Bbbk(\cup\, \sigma(E))$, où les $\sigma \in \mathrm{Gal}(\mathbb{L}/\Bbbk)$, est normale. En effet, soient $\sigma \in \mathrm{Gal}(\mathbb{L}/\Bbbk)$ et $x \in \mathbb{K}$. On peut écrire

$$x = P(\sigma_1(e_1), ..., \sigma_m(e_m))$$

avec $P \in \Bbbk[X_1, ..., X_m]$, les $\sigma_i \in \mathrm{Gal}(\mathbb{L}/\Bbbk)$ et les $e_i \in E$. Alors, $\sigma(x) = P(\sigma(\sigma_1(e_1)), ..., \sigma(\sigma_m(e_m)))$ est toujours un élément de $\mathbb{K}$ car pour tout i, $\sigma \circ \sigma_i \in \mathrm{Gal}(\mathbb{L}/\Bbbk)$. On a donc $\sigma(\mathbb{K}) \subset \mathbb{K}$ pour tout $\sigma \in \mathrm{Gal}(\mathbb{L}/\Bbbk)$. $\mathbb{K}$ est l'extension de $\Bbbk$ **normale engendrée par** E. C'est la plus petite extension normale de $\Bbbk$ qui contient E.

Définition 8.0.5 : Soit $\Bbbk \subset \mathbb{K} \subset \mathbb{L}$ des extensions. On dit que $\mathbb{L}$ est une **clôture normale** de $\Bbbk \subset \mathbb{K}$ si $\Bbbk \subset \mathbb{L}$ est normale et si pour toute extension normale $\Bbbk \subset \mathbb{M}$ telle que $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$ on a $\mathbb{M} = \mathbb{L}$. Autrement dit, c'est la plus petite extension normale de $\Bbbk$ contenant $\mathbb{K}$.

Théorème 8.0.3 : Soit $\Bbbk \subset \mathbb{K}$ une extension algébrique. Il existe une clôture normale de $\Bbbk \subset \mathbb{K}$, qui est unique à isomorphisme près.
Démonstration : L'extension normale de $\Bbbk$ engendrée par $\mathbb{K}$ est une clôture normale. Si $\Bbbk \subset \mathbb{K} \subset \mathbb{K}_1$ et $\Bbbk \subset \mathbb{K} \subset \mathbb{K}_2$ sont des clôtures normales, elles sont "contenues" dans la clôture algébrique $\mathbb{L}$ de $\Bbbk$. On peut donc identifier $\mathbb{K}_1$ et $\mathbb{K}_2$ à l'extension normale engendrée par $\mathbb{K}$.

Théorème 8.0.4 : Soit $\Bbbk \subset \mathbb{K}$ une extension séparable finie de degré n. TFAE :

1. $\mathbb{K}$ est normale.
2. $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ a n éléments.

Démonstration : (1) $\Rightarrow$ (2) : $\mathbb{K}$ est séparable finie de degré n donc $\mathrm{Hom}_{\Bbbk}(\mathbb{K},\ \mathbb{L})$ a n éléments **(T6.6)**. Comme $\mathbb{K}$ est normale, tout élément de $\mathrm{Hom}_{\Bbbk}(\mathbb{K},\ \mathbb{L})$ est un élément de $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ et donc $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ a bien n éléments.
(2) $\Rightarrow$ (1) : $\mathrm{Gal}(\mathbb{K}/\Bbbk) \subset \mathrm{Hom}_{\Bbbk}(\mathbb{K},\ \mathbb{L})$ donc ils sont égaux (de même cardinal n). On en déduit que pour tout $\sigma \in \mathrm{Hom}_{\Bbbk}(\mathbb{K},\ \mathbb{L})$, $\sigma(\mathbb{K}) \in \mathbb{K}$, donc $\mathbb{K}$ est normale.

Théorème 8.0.5 : Soit G un sous-groupe fini de $\mathrm{Aut}(\Bbbk)$ de cardinal n. On note $\Bbbk^G$ le **corps des invariants** de G : l'ensemble des éléments de $\Bbbk$ qui sont invariants par tous les éléments de G. Alors, l'extension $\Bbbk^G \subset \Bbbk$ est séparable, normale et de degré fini $\leq n$.
Démonstration : Soit $x \in \Bbbk$. On note $\{x_1, ..., x_m\}$ les éléments distincts de l'orbite de x par G, et $P = (X - x_1)...(X - x_m)$. On peut exprimer P en utilisant les relations coefficients-racines :

$$P = X^m + \sum_{1}^{m} (-1)^k \theta_k(x_1, ..., x_m) X^{n-k} \quad \text{où } \theta_k(x_1, ..., x_m) = \sum_{1 \leq i_1 < ... < i_k \leq r} x_{i_1}...x_{i_k}$$

On vérifie sans problème que pour tout k, $\theta_k(x_1, ..., x_m) \in \Bbbk^G$. Alors, x est algébrique sur $\Bbbk^G$, et son polynôme minimal, qui divise P, est scindé à racines simples. On en déduit que l'extension $\Bbbk^G \subset \Bbbk$ est algébrique, séparable et normale. Pour montrer le reste, on peut supposer que $\Bbbk^G \neq \Bbbk$ et prendre $y \in \Bbbk \setminus \Bbbk^G$. Comme l'orbite de y par G a moins de n éléments, le degré de y est inférieur à n. Si l'extension est simple, on a le résultat. Sinon (cela veut dire qu'elle est de degré infini car elle est séparable), on peut choisir y de plus haut ($\geq$) degré que tous les autres éléments de $\Bbbk$. Comme l'extension n'est pas simple, on a $z \in \Bbbk \setminus \Bbbk^G(y)$. Le degré de $\Bbbk \subset \Bbbk^G(y, z)$ est $>$ à celui de $\Bbbk \subset \Bbbk^G(y)$, mais $\Bbbk \subset \Bbbk^G(y,z)$ est séparable de degré fini donc simple **(T6.7)**. Ceci contredit la maximalité du degré de y. On en déduit que $\Bbbk^G \subset \Bbbk$ est finie de degré $\leq n$.

Théorème 8.0.6 : Soit $\Bbbk \subset \mathbb{K}$ une extension séparable et finie de degré n. TFAE :

1. $\mathbb{K}$ est normale.
2. $\Bbbk = \mathbb{K}^G$ où $G = \text{Gal}(\mathbb{K}/\Bbbk)$.

Démonstration : (1) $\Rightarrow$ (2) : Si $\mathbb{K}$ est normale, soit $x \in \mathbb{K}^G$. μ_x est scindé dans $\mathbb{K}$ et les autres racines de μ_x sont conjuguées à x. Elles sont donc dans l'orbite de x par G, qui est $\{x\}$ par définition. x est la seule racine de μ_x, mais μ_x est séparable, donc μ_x est de degré 1. On a bien $x \in \Bbbk$, et donc $\Bbbk = \mathbb{K}^G$.
(2) $\Rightarrow$ (1) : $\text{Gal}(\mathbb{K}/\Bbbk)$ est fini car l'extension est séparable et finie, donc on peut utiliser **(T8.5)**.

Théorème 8.0.7 : *(Lemme d'Artin)* Soit G un sous-groupe fini de $\text{Aut}(\Bbbk)$ de cardinal n. Alors n est le degré de l'extension $\Bbbk^G \subset \Bbbk$ et G est $\text{Gal}(\Bbbk/\Bbbk^G)$.
Démonstration : $[\Bbbk : \Bbbk^G] \leq n \leq \text{Card}(\text{Gal}(\Bbbk/\Bbbk^G)) = [\Bbbk : \Bbbk^G]$. La première inégalité est **(T8.5)**, la seconde est due au fait que $G \subset \text{Gal}(\Bbbk/\Bbbk^G)$, et l'égalité est **(T8.4)**.

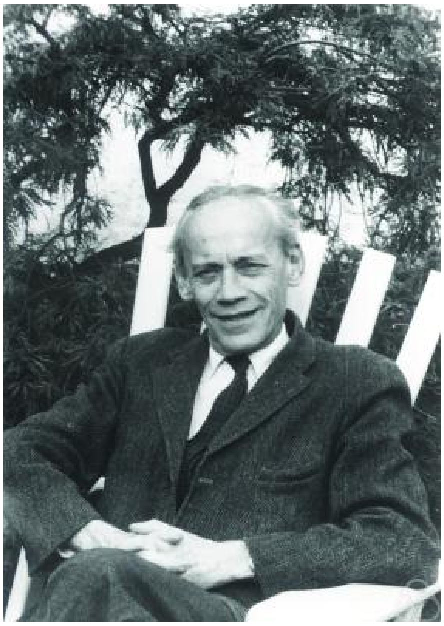


Figure 9: Emil Artin, 1898 - 1962

9 Extensions galoisiennes et correspondance de Galois

Ce chapitre est très inspiré de l'excellent *Chapitre 9 - Théorie de Galois* de [1].

9.1 Extensions galoisiennes

Définition 9.1.1 : Une extension $\Bbbk \subset \mathbb{K}$ normale et séparable est dite **galoisienne**.

Théorème 9.1.1 : Soit $\Bbbk \subset \mathbb{K}$ une extension algébrique. TFAE :

1. $\Bbbk \subset \mathbb{K}$ est galoisienne.
2. Pour tout $x \in \mathbb{K}$, μ_x est scindé à racines simples sur $\mathbb{K}$.
3. $\Bbbk = \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\Bbbk)}$.

Démonstration : (1) $\Rightarrow$ (2) : $\mathbb{K}$ est normale donc μ_x est scindé. Ses racines sont simples car x est séparable.
(2) $\Rightarrow$ (3) : Il est clair que $\Bbbk \subset \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\Bbbk)}$. Soit $x \in \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\Bbbk)}$. μ_x est scindé à racines simples, disons
$\mu_x = (X-x)(X-a_1)...(X-a_n)$. Pour tout i, x et a_i sont conjugués, donc on a $\sigma \in Gal(\mathbb{K}/\Bbbk)$ tel que $\sigma(x) = a_i$.
Par définition de x, on a $a_i = x$. On en déduit que μ_x est de degré 1 et que $x \in \Bbbk$.
(3) $\Rightarrow$ (1) : Soit $x \in \mathbb{K}$. On note $\{a_1, ..., a_r\}$ l'orbite de x par $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ où les a_i sont distincts deux à deux. Alors le polynôme $P = (X-a_1)...(X-a_r)$ est annulateur de x. Comme en **(T8.5)**, en s'intéréssant aux relations coefficients-racines, on voit que $P \in \mathrm{Gal}(\mathbb{K}/\Bbbk)[X] = \Bbbk[X]$ et donc que μ_x, qui divise P, est scindé à racines simples. On en déduit que x est séparable, que $\Bbbk \subset \mathbb{K}$ est normale et séparable.

Théorème 9.1.2 : Soit $\Bbbk \subset \mathbb{K}$ une extension algébrique. TFAE :

1. $\Bbbk \subset \mathbb{K}$ est galoisienne.
2. Il existe une famille $\mathcal{F}$ de polynômes non constants et séparables telle que $\mathbb{K}$ est un corps de décomposition de $\mathcal{F}$.

Démonstration : (1) $\Rightarrow$ (2) : En prenant $\mathcal{F} = (\mu_x)_{x\in\mathbb{K}}$ on a bien le résultat. (2) $\Rightarrow$ (1) : $\Bbbk \subset \mathbb{K}$ est séparable selon **(T6.9)** et normale selon **(T8.1)**.

Théorème 9.1.3 : Soient $\Bbbk$ un corps et G un sous-groupe de $\mathrm{Aut}(\Bbbk)$. Si l'extension $\Bbbk^G \subset \Bbbk$ est algébrique, alors elle est galoisienne.
Démonstration : C'est l'assertion (2) de **(T9.1)**.

9.2 Correspondance de Galois

Dans toute la suite, on se fixe une extension $\Bbbk \subset \mathbb{M}$. On note $\mathcal{F}$ l'ensemble des sous-extensions de $\Bbbk \subset \mathbb{M}$ et $\mathcal{G}$ l'ensemble des sous-groupes de $\mathrm{Gal}(\mathbb{M}/\Bbbk)$. L'idée de cette partie est d'établir, dans le cas où $\Bbbk \subset \mathbb{M}$ est galoisienne, une bijection naturelle entre $\mathcal{F}$ et $\mathcal{G}$.

Définition 9.2.1 : *(Correspondance de Galois)* On note $\gamma : \mathcal{F} \to \mathcal{G},\ \mathbb{K} \mapsto Gal(\mathbb{M}/\mathbb{K})$ et $\phi : \mathcal{G} \to \mathcal{F},\ G \mapsto \mathbb{M}^G$.

Proposition 9.2.1 : Soient $\mathbb{K}, \mathbb{L} \in \mathcal{F}$ et $G, H \in \mathcal{G}$. On vérifie sans problème que $K \subset \phi(\gamma(\mathbb{K}))$ et que $G \subset \gamma(\phi(G))$. Aussi, si $\mathbb{K} \subset \mathbb{L}$ alors $\gamma(\mathbb{L}) \subset \gamma(\mathbb{K})$ et si $G \subset H$, alors $\phi(H) \subset \phi(G)$.

Proposition 9.2.2 : $\gamma \circ \phi \circ \gamma = \gamma$ et $\phi \circ \gamma \circ \phi = \phi$.
Démonstration : Ces deux égalités sont parfaitement symétriques, on ne montre donc que celle de gauche. Soit

$\mathbb{K} \in \mathcal{F}$. La première inclusion de **(P9.1)** donne $\gamma(\mathbb{K}) \subset \gamma(\phi(\gamma(\mathbb{K})))$. $\mathbb{K} \subset \phi(\gamma(\mathbb{K}))$ donc la troisième inclusion de **(P9.1)** donne $\gamma(\phi(\gamma(\mathbb{K}))) \subset \gamma(\mathbb{K})$. On a bien l'égalité.

Proposition 9.2.3 : Soit $\sigma \in \mathrm{Gal}(\mathbb{M}/\mathbb{k})$. $\gamma(\sigma(\mathbb{K})) = \sigma\gamma(\mathbb{K})\sigma^{-1}$ et $\phi(\sigma G \sigma^{-1}) = \sigma(\phi(G))$.
Démonstration : On peut rédiger une preuve mais c'est assez illisible donc je conseille de la faire avec une feuille et un crayon...

Proposition 9.2.4 : Soit $\mathbb{K} \in \mathcal{F}$. $\phi(\gamma(\mathbb{K})) = \mathbb{K}$ si, et seulement si, il existe $G \in \mathcal{G}$ tel que $\mathbb{K} = \phi(G)$.
Démonstration : C'est immédiat avec ce qui précède.

Proposition 9.2.5 : On a l'équivalence analogue pour un élément de $\mathcal{G}$. Soit $G \in \mathcal{G}$. $\gamma(\phi(G)) = G$ si, et seulement si, il existe $\mathbb{K} \in \mathcal{F}$ tel que $G = \gamma(\mathbb{K})$.

Définition 9.2.2 : Un élement de $\mathcal{F}$ ou de $\mathcal{G}$ qui vérifie les conditions équivalentes des deux propositions précédentes est dit **stationnaire**.

Théorème 9.2.1 : On suppose ici que $\mathbb{k} \subset \mathbb{M}$ est algébrique. Soit $\mathbb{K} \in \mathcal{F}$. $\mathbb{K}$ est stationnaire si, et seulement si, $\mathbb{K} \subset \mathbb{M}$ est galoisienne.
Démonstration : Si $\mathbb{K}$ est stationnaire, alors $\phi(\gamma(\mathbb{K})) = \mathbb{K}$. Autrement dit, $\mathbb{M}^{Gal(\mathbb{M}/\mathbb{K})} = \mathbb{K}$ donc $\mathbb{K} \subset \mathbb{M}$ est galoisienne selon **(T9.1)**. Si $\mathbb{K} \subset \mathbb{M}$ est galoisienne, alors $\mathbb{M}^{Gal(\mathbb{M}/\mathbb{K})} = \mathbb{K}$ donc $\phi(\gamma(\mathbb{K})) = \mathbb{K}$ et $\mathbb{K}$ est stationnaire.

Théorème 9.2.2 : Soient $\mathbb{K}, \mathbb{L} \in \mathcal{F}$ tels que $\mathbb{K} \subset \mathbb{L}$ et $[\mathbb{L} : \mathbb{K}]$ est fini (noté n). Alors l'indice $(\gamma(\mathbb{K}) : \gamma(\mathbb{L}))$ est inférieur à n.
Démonstration : Le cas où $n = 1$ est trivial. On peut donc supposer $n \geq 2$. On va distinguer le cas où on peut trouver une extension (strictement) intermédiaire à $\mathbb{K}$ et $\mathbb{L}$ et le cas où c'est impossible. Dans le premier, on note $\mathbb{E}$ une telle extension et on raisonne par récurrence. $n = [\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{E}] \times [\mathbb{E} : \mathbb{K}] := pq$ avec $p, q > 1$. Comme $(\gamma(\mathbb{K}) : \gamma(\mathbb{L})) = (\gamma(\mathbb{K}) : \gamma(\mathbb{E})) \times (\gamma(\mathbb{E}) : \gamma(\mathbb{L}))$ on a bien le résultat. Supposons maintenant qu'une telle extension n'existe pas. Soit $x \in \mathbb{L} \setminus \mathbb{K}$. $\mathbb{K}(x) \neq \mathbb{K}$ donc $\mathbb{K}(x) = \mathbb{L}$. Si $\sigma, \tau \in \gamma(\mathbb{K})$, alors $\sigma(x) = \tau(x)$ si, et seulement si $\sigma(\tau^{-1}(x)) = x$, c'est à dire que $\sigma \circ \tau^{-1} \in \gamma(\mathbb{L})$ (σ et τ appartiennent à la même classe dans $\gamma(\mathbb{K})/\gamma(\mathbb{L})$). Par ailleurs, l'ensemble R des racines de μ_x (le polynôme minimal de x sur $\mathbb{K}$) dans $\mathbb{M}$ est fini de cardinal $\leq n$ et $R = \{\sigma(x),\ \sigma \in \gamma(\mathbb{K})\}$. On peut donc construire une injection $\pi : \gamma(\mathbb{K})/\gamma(\mathbb{L}) \to R$ qui associe à une classe, l'image de x par un représentant de cette classe. On en déduit que $(\gamma(\mathbb{K}) : \gamma(\mathbb{L})) \leq \mathrm{Card}(R) \leq n$.

On a un théorème analogue pour les sous-groupes de $Gal(\mathbb{M}/\mathbb{k})$.
Théorème 9.2.3 : Soient $G, H \in \mathcal{G}$ tels que $H \subset G$ et $(G : H)$ est fini (noté n). Alors, $[\phi(H) : \phi(G)] \leq n$.
Démonstration : On note $C_1, ..., C_n$ les éléments de G/H avec $C_1 = H$. On remarque d'abord que si $x \in \phi(H)$ et si $C_i \in G/H$, alors $\{\sigma(x),\ \sigma \in C_i\}$ contient un seul élement que l'on note $C_{i,x}$. On suppose que $[\phi(H) : \phi(G)] > n$ et on se donne $x_1, ..., x_{n+1}$ une famille d'élements de $\phi(H)$ libre sur $\phi(G)$. On s'intéresse à la matrice A dont les coefficients sont les C_{i,x_j} pour $1 \leq i \leq n$ et $1 \leq j \leq n+1$. A est un élément de $M_{n,n+1}(\mathbb{M})$ donc ses colonnes sont liées. On a donc une famille $a_1, ..., a_{n+1}$ tels que pour tout i, $a_1 C_{i,x_1} + ... + a_{n+1} C_{i,x_{n+1}} = 0$. On choisit cette famille de façon à ce qu'elle ait le plus petit nombre possible d'éléments non nuls (au moins 1) et, quitte à réordonner les colonnes de A, on peut supposer que cette famille est de la forme $a_1, a_2, ..., a_r, 0, ..., 0$ avec les a_j non nuls. Aussi, quitte à multiplier par a_1^{-1}, on peut supposer que $a_1 = 1$. Pour $i = 1$, $C_{1,x_1} + a_2 C_{1,x_2} + ... + a_{n+1} C_{1,x_{n+1}} = x_1 + a_2 x_2 + ... + a_{n+1} x_{n+1} = 0$. Soit $\theta \in G$. Pour tout i, $\theta(C_{i,x_1}) + \theta(a_2)\theta(C_{i,x_2}) + ... + \theta(a_{n+1})\theta(C_{i,x_{n+1}}) = 0$. Mais l'application $C_i \mapsto \theta C_i$ est une permutation de G/H, que l'on note τ. Alors, pour tout i, $C_{\tau(i),x_1} + \theta(a_2) C_{\tau(i),x_2} + ... + \theta(a_{n+1}) C_{\tau(i),x_{n+1}} = 0$. On en déduit que la famille $1, \theta(a_2), ..., \theta(a_{n+1})$ lie les $x_1, ..., x_{n+1}$ et donc, par linearité, que la famille $1 - 1, \theta(a_2) - a_2, ..., \theta(a_{n+1}) - a_{n+1}$ aussi. Les x_j sont libres sur $\phi(G)$ donc les a_j ne sont pas tous dans $\phi(G)$, disons que a_2 n'est pas dans $\phi(G)$. Alors, on aurait pu choisir $\theta \in G$ pour que $\theta(a_2) \neq a_2$. La famille

$0, \theta(a_2) - a_2, ..., \theta(a_{n+1}) - a_{n+1}$ contient au moins un élément non nul et au moins un 0 de plus que $1, a_2, ..., a_{n+1}$ ce qui est absurde. On obtient donc une contradiction sur le fait que $[\phi(H) : \phi(G)] > n$.

Théorème 9.2.4 : Soient $\mathbb{K}, \mathbb{L} \in \mathcal{F}$ tels que $\mathbb{K} \subset \mathbb{L}$ et $[\mathbb{L} : \mathbb{K}]$ est fini (noté n). On suppose que $\mathbb{K}$ est stationnaire. Alors $\mathbb{L}$ aussi et $(\gamma(\mathbb{K} : \gamma(\mathbb{L})) = n$.
Démonstration : On note $m = (\gamma(\mathbb{K} : \gamma(\mathbb{L}))$. Alors $n \leq [\phi(\gamma(\mathbb{L})) : \mathbb{K}] = [\phi(\gamma(\mathbb{L})) : \phi(\gamma(\mathbb{K}))] \leq m \leq n$. La première inégalité découle du fait que $\mathbb{L} \subset \phi(\gamma(\mathbb{L}))$. La deuxième de **(T9.6)** et la troisième de **(T9.5)**.

Encore une fois, on dispose d'un théorème analogue pour les sous-groupes de Gal($\mathbb{M}/\mathbb{k}$).
Théorème 9.2.5 : Soient $G, H \in \mathcal{G}$ tels que $H \subset G$ et $(G : H)$ est fini (noté n). On suppose que H est stationnaire. Alors G aussi et $[\phi(H) : \phi(G)] = n$.
Démonstration : On note $m = [\phi(H) : \phi(G)]$. Alors, $n \leq (\gamma(\phi(G)) : H) = (\gamma(\phi(G)) : \gamma(\phi(H))) \leq m \leq n$. La première inégalité découle du fait que $G \subset \gamma(\phi(G))$. La deuxième de **(T9.5)** et la troisième de **(T9.6)**.

Théorème 9.2.6 : On suppose que $\mathbb{k} \subset \mathbb{M}$ est galoisienne. Alors toute sous-extension finie de $\mathbb{M}$ est stationnaire.
Démonstration : Soit $\mathbb{K} \in \mathcal{F}$ de degré fini sur $\mathbb{k}$. Alors, comme $\mathbb{k} \subset \mathbb{M}$ est galoisienne, $\mathbb{k}$ est stationnaire. $\mathbb{k} \subset \mathbb{K}$ est finie donc selon **(T9.7)**, $\mathbb{K}$ est stationnaire.

Théorème 9.2.7 : On suppose que l'extension $\mathbb{k} \subset \mathbb{M}$ est finie. Alors tout sous-groupe de $Gal(\mathbb{M}/\mathbb{k})$ est stationnaire.
Démonstration : Gal($\mathbb{M}/\mathbb{k}$) est fini (c'est une conséquence du Lemme de Dedekind). Soit $G \in \mathcal{G}$. On pose $H = \{\text{id}\}$. G/H est fini car G est fini et H est stationnaire, donc selon **(T9.8)** G est stationnaire.

On énonce maintenant le théorème le plus important du chapitre, et probablement du texte : le **théorème fondamental de la théorie de Galois**.
Théorème 9.2.8 : *(Galois)* On suppose que $\mathbb{k} \subset \mathbb{M}$ est galoisienne finie. Alors γ et ϕ sont bijections réciproques entre $\mathcal{F}$ et $\mathcal{G}$. De plus, pour tout $G \in \mathcal{G}$, $G = \text{Gal}(\mathbb{M}/\phi(G))$, $\text{Card}(G) = [\mathbb{M} : \phi(G)]$ et $(\text{Gal}(\mathbb{M}/\mathbb{k}) : G) = [\phi(G) : \mathbb{k}]$.
Démonstration : Toutes les sous-extensions de $\mathbb{M}$ et tous les sous-groupes de $Gal(\mathbb{M}/\mathbb{k})$ sont stationnaires, donc γ et ϕ sont surjectifs **(P9.4), (P9.5)**. Si $\phi(G) = \phi(H)$, alors $\gamma(\phi(G)) = \gamma(\phi(H))$ et donc $G = H$, donc ϕ est injectif. On en déduit que ϕ est bijectif et donc que γ aussi (surjection entre deux ensembles de même taille). Soit $G \in \mathcal{G}$. $G = \text{Gal}(\mathbb{M}/\phi(G))$ car G est stationnaire. Si on note $H = \{id\}$, alors $(G : H)$ est $\text{Card}(G)$ et donc $\text{Card}(G) = [\mathbb{M} : \phi(G)]$. Si on note maintenant $H = \text{Gal}(\mathbb{M}/\mathbb{k}) = \gamma(\mathbb{k})$, alors $(H : G) = [\phi(G) : \phi(H)]$.

Théorème 9.2.9 : On suppose $\mathbb{k} \subset \mathbb{M}$ finie. Alors l'extension est galoisienne si, et seulement si, $\text{Card}(\text{Gal}(\mathbb{M}/\mathbb{k})) = [\mathbb{M} : \mathbb{k}]$.
Démonstration : Si elle est galoisienne, on applique le théorème **(T9.11)** à $G = \{id\}$. Si $\text{Card}(Gal(\mathbb{M}/\mathbb{k})) = [\mathbb{M} : \mathbb{k}]$, on veut montrer que $\mathbb{k} = \phi(\gamma(\mathbb{k}))$. On note $n = [\mathbb{M} : \mathbb{k}]$. $n = (Gal(\mathbb{M}/\mathbb{k}) : \{id\}) = [\mathbb{M} : \phi(\gamma(\mathbb{k}))] \leq n$. La deuxième égalité vient de **(T9.8)**.

Théorème 9.2.10 : On suppose que $\mathbb{k} \subset \mathbb{M}$ est galoisienne finie. Soit $\mathbb{K} \in \mathcal{F}$. TFAE :

1. $\mathbb{K}$ est normale.
2. $\mathbb{K}$ est galoisienne.
3. $\gamma(\mathbb{K})$ est un sous-groupe distingué de Gal($\mathbb{M}/\mathbb{k}$).
4. Pour tout $\sigma \in \text{Gal}(\mathbb{M}/\mathbb{k})$, on a $\sigma(\mathbb{K}) = \mathbb{K}$.

Démonstration : (1) $\Rightarrow$ (2) : $\mathbb{K}$ est normale et séparable (car $\mathbb{k} \subset \mathbb{M}$ est séparable). (2) $\Rightarrow$ (3) : Soit $\sigma \in \text{Gal}(\mathbb{M}/\mathbb{k})$ et $\theta \in \gamma(\mathbb{K})$. Pour tout $x \in \mathbb{K}$, $\sigma(\theta(\sigma^{-1}(x))) = x$ car $\sigma(x) \in \mathbb{K}$ car $\mathbb{K}$ est galoisienne. (3) $\Rightarrow$ (4) :

Figure 10: Évariste Galois, 1811 - 1832

Soit $\sigma \in \mathrm{Gal}(\mathbb{M}/\Bbbk)$. $\sigma(\mathbb{K}) = \phi(\sigma\gamma(\mathbb{K})\sigma^{-1}) = \phi(\gamma(\mathbb{K})) = \mathbb{K}$. (4) $\Rightarrow$ (1) : On pose $G = \mathrm{Gal}(\mathbb{M}/\Bbbk)$, $H = \mathrm{Gal}(\mathbb{K}/\Bbbk)$ et $G' = \gamma(\mathbb{K})$. On va montrer que $[\mathbb{K} : \Bbbk] = \mathrm{Card}(\mathrm{Gal}(\mathbb{K}/\Bbbk))$. Alors $\mathrm{Card}(H) \leq [\mathbb{K} : \Bbbk]$ (Lemme de Dedekind). Par ailleurs, $(G : G') = [\phi(G') : \Bbbk] = [\mathbb{K} : \Bbbk]$ et l'application $G/G' \to H$ qui associe à un élément de G/G' la restriction à $\mathbb{K}$ d'un représentant de cette classe est injective, donc $\mathrm{Card}(H) \geq \mathrm{Card}(G/G')$. On en déduit le résultat.

Remarque : En fait, le morphisme défini en (4) $\Rightarrow$ (1) est surjectif (car les cardinaux de H et G/G' sont égaux), donc H est isomorphe à G/G'.

On a donné en **(T2.3)** une preuve du théorème fondamental de l'algèbre faisant appel à des outils d'analyse réelle. La théorie de Galois nous permet d'avoir la satisfaction de proposer une preuve bien plus "algébrique" de ce résultat, qui n'utilise *que* le théorème des valeurs intermédiaires.

Théorème 9.2.11 : *(D'Alembert-Gauss - Deuxième preuve)* $\mathbb{C}$ est algébriquement clos.

Démonstration :

10 Radicaux et résolubilité

Dans cette partie, on suppose que $\Bbbk$ est de caractéristique nulle et on note $\hat{\Bbbk}$ sa clôture algébrique.

Définition 10.0.1 : Une extension $\Bbbk \subset \mathbb{M}$ est dite **abélienne** si elle est galoisienne et si son groupe de Galois est commutatif. On dit qu'elle est **cyclique** si son groupe de Galois est cyclique.

Théorème 10.0.1 : Soient $\Bbbk \subset \mathbb{M}$ une extension galoisienne finie et $\mathbb{K} \in \mathcal{F}$. $\mathbb{K}$ est abélienne si et seulement si $\mathbb{K} \subset \mathbb{M}^{D(\mathrm{Gal}(\mathbb{M}/\Bbbk))}$.
Démonstration : $D(\mathrm{Gal}(\mathbb{M}/\Bbbk))$ est distingué dans $\mathrm{Gal}(\mathbb{M}/\Bbbk)$. $\mathbb{K} \subset \mathbb{M}^{D(\mathrm{Gal}(\mathbb{M}/\Bbbk))} \Leftrightarrow \mathbb{K} \subset \phi(D(\mathrm{Gal}(\mathbb{M}/\Bbbk))) \Leftrightarrow \phi(\gamma(\mathbb{K})) \subset \phi(D(\mathrm{Gal}(\mathbb{M}/\Bbbk))) \Leftrightarrow D(\mathrm{Gal}(\mathbb{M}/\Bbbk)) \subset \gamma(\mathbb{K}) \Leftrightarrow \gamma(\mathbb{K})$ est distingué dans $\mathrm{Gal}(\mathbb{M}/\Bbbk)$ et $\mathrm{Gal}(\mathbb{M}/\Bbbk)/\gamma(\mathbb{K})$ est abélien $\Leftrightarrow \Bbbk \subset \mathbb{K}$ est galoisienne et $\mathrm{Gal}(\mathbb{K}/\Bbbk)$ est abélien. La troisième équivalence vient du fait que si $T \subset G$ est un sous-groupe de G, alors $D(G) \subset T$ si et seulement si T est distingué dans G et G/T est abélien **(P1.3)**.

Théorème 10.0.2 : Soient $\Bbbk$ un corps et $n \in \mathbb{N}^*$. L'extension $\Bbbk \subset D_{\Bbbk}(X^n - 1)$ est abélienne et son groupe de Galois est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$ (le groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$).
Démonstration : On note $D = D_{\Bbbk}(X^n - 1)$ une extension de décomposition du polynôme $X^n - 1$ sur $\Bbbk$. $\Bbbk \subset D$ est galoisienne car $X^n - 1$ est séparable en caractéristique nulle. Soit ϵ une racine primitive de $X^n - 1$, c'est-à-dire une racine qui engendre le groupe des racines de $X^n - 1$. Alors $D = \Bbbk(\epsilon)$. L'image de ϵ par un élément $\sigma \in Gal(D/\Bbbk)$ est aussi une racine primitive de $X^n - 1$ donc est de la forme ϵ^{m_σ} avec $0 \leq m_\sigma \leq n-1$ et $m_\sigma \wedge n = 1$. L'application $Gal(D/\Bbbk) \Rightarrow (\mathbb{Z}/n\mathbb{Z})^*$, $\sigma \mapsto m_\sigma$ est un morphisme injectif. On en déduit le théorème.

Définition 10.0.2 : Une extension $\Bbbk \subset \mathbb{K}$ est **radicale** s'il existe $x_1, ..., x_n \in \hat{\Bbbk}$ et des entiers $m_1, ..., m_n$ non nuls tels que $\mathbb{K} = \Bbbk(x_1, ..., x_n)$ et pour tout i, on a $x_i^{m_i} \in \Bbbk(x_1, ..., x_{i-1})$.

Exemple : L'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}, i\sqrt{2})$ est radicale.

Théorème 10.0.3 : Soit $\Bbbk \subset \mathbb{K} \subset \mathbb{L}$ des extensions. Si $\Bbbk \subset \mathbb{K}$ et $\mathbb{K} \subset \mathbb{L}$ sont radicales, alors $\Bbbk \subset \mathbb{L}$ aussi.

Proposition 10.0.1 : Soit $\Bbbk \subset \mathbb{K}$ une extension abélienne finie de degré n. On suppose que $\Bbbk$ contient une racine de $X^n - 1$. Alors il existe une $\Bbbk$-base $(r_1, ..., r_n)$ de $\mathbb{K}$ telle que pour tout i, $r_i^n \in \Bbbk$.
Démonstration : On peut voir les éléments de $Gal(\mathbb{K}/\Bbbk)$ comme des endomorphismes de $\Bbbk$-esapce vectoriel. Ils sont tous annulés par le polynôme $X^n - 1$ (car $Gal(\mathbb{K}/\Bbbk)$ est d'ordre n) qui est scindé à racines simples. Les éléments de $Gal(\mathbb{K}/\Bbbk)$ sont alors diagonalisables, et, mieux que cela, ils commutent donc sont co-diagonalisables. On a donc une base de $\mathbb{K}$ $(r_1, ..., r_n)$ qui diagonalise tous les éléments de $Gal(\mathbb{K}/\Bbbk)$. $\Bbbk \subset \mathbb{K}$ est galoisienne donc $\Bbbk = \phi(\gamma(\Bbbk))$. Pour tout i, pour tout $\sigma \in Gal(\mathbb{K}/\Bbbk)$, $\sigma(r_i^n) = \alpha^n r_i^n$ où α est une valeur propre de σ. C'est aussi une racine n-ème de l'unité donc $\sigma(r_i^n) = r_i^n$. On en déduit que $r_i^n \in \Bbbk$.

Proposition 10.0.2 : Soit $\Bbbk \subset \mathbb{K}$ une extension galoisienne finie de degré n. On suppose que $Gal(\mathbb{K}/\Bbbk)$ est résoluble et que $\Bbbk$ contient une racine non triviale de $X^n - 1$. Alors $\Bbbk \subset \mathbb{K}$ est radicale.
Démonstration : $Gal(\mathbb{K}/\Bbbk)$ est résoluble donc on a $\{\mathrm{id}\} = G_0 \subset ... \subset G_k = Gal(\mathbb{K}/\Bbbk)$ tels que pour tout $i \leq n-1$, G_i est distingué dans G_{i+1} et G_{i+1}/G_i est abélien (et les inclusions sont strictes). On raisonne par récurrence sur la longueur de la chaîne donnée ci-dessus. Si $k = 0$, alors $\Bbbk = \mathbb{K}$ donc l'extension est bien radicale. Sinon, supposons que le résultat soit vrai pour tout $j \leq k-1$. $\Bbbk \subset \mathbb{K}$ est galoisienne finie donc $\phi(G_{k-1}) \subset \mathbb{K}$ est galoisienne finie de groupe de Galois G_{k-1} et $\Bbbk \subset \phi(G_{k-1})$ est galoisienne finie de groupe de Galois isomorphe à $Gal(\mathbb{K}/\Bbbk)/G_{k-1}$ **(T9.13)**. Ces groupes sont résolubles donc par hypothèse de récurrence les extensions $\phi(G_{k-1}) \subset \mathbb{K}$ et $\Bbbk \subset \phi(G_{k-1})$ sont radicales. On en déduit que $\Bbbk \subset \mathbb{K}$ est radicale.

Définition 10.0.3 : On dit qu'une extension $\Bbbk \subset \mathbb{K}$ est **résoluble par radicaux** si elle est contenue dans une extension radicale. On dit qu'un polynôme $P \in \Bbbk[X]$ est **résoluble par radicaux** si son corps de décomposition est résoluble par radicaux.

Définition 10.0.4 : Soit $P \in \Bbbk[X]$. Le **groupe de Galois** de P est le groupe de Galois d'une extension de décomposition de P. Cette définition sous-entend que toutes les extensions de décomposition de P sont isomorphes : c'est le cas.

Proposition 10.0.3 : Soient $\Bbbk$ un corps et p un entier premier. Si $\Bbbk$ contient une racine non triviale de $X^p - 1$, alors toute extension de la forme $\Bbbk \subset \Bbbk(\alpha)$, avec $\alpha^p \in \Bbbk$, est abélienne.
Démonstration : On note $P = X^p - \alpha_p$. Soit ϵ une racine non triviale de $X^p - 1$. Comme p est premier, ϵ engendre le groupe des racines de $X^p - 1$. Les racines de P sont les $\epsilon^k \alpha$ pour $1 \leq k \leq p$. On en déduit que $\Bbbk(\alpha)$ est un corps de décomposition de P, qui est séparable, et donc est galoisienne. Le groupe $Gal(\Bbbk(\alpha)/\Bbbk)$ est alors d'ordre p, isomorphe à $\mathbb{Z}/p\mathbb{Z}$ qui est abélien.

Théorème 10.0.4 : Soient $\Bbbk \subset \mathbb{K}$ et $\Bbbk \subset \mathbb{L}$ des extensions. On suppose que la première est galoisienne et que $\mathbb{K}$ et $\mathbb{L}$ sont inclus dans un même corps $\mathbb{M}$. On note $\mathbb{C}$ le plus petit sous-corps de $\mathbb{M}$ contenant $\mathbb{K}$ et $\mathbb{L}$. Alors, $\mathbb{L} \subset \mathbb{C}$ et $\mathbb{K} \cap \mathbb{L} \subset \mathbb{K}$ sont galoisiennes, et leurs groupes de Galois sont isomorphes.

Théorème 10.0.5 : *(Galois)* Soient $\Bbbk$ un corps et $P \in \Bbbk[X]$. Le polynôme P est résoluble par radicaux si, et seulement si, le groupe de Galois de P est résoluble.
Démonstration : Supposons que le groupe de Galois G d'une extension de décomposition $\Bbbk \subset D$ de P soit résoluble. On note n son degré. Soit $\epsilon \in \hat{\Bbbk}$ une racine non triviale de $X^n - 1$. L'extension $\Bbbk(\epsilon) \subset D(\epsilon)$ est galoisienne finie et $Gal(D(\epsilon)/\Bbbk(\epsilon))$ est isomorphe à $Gal(D/(\mathbb{K} \cap \Bbbk(\epsilon)))$ **(T10.4)** qui est un sous-groupe de G, donc résoluble. On déduit de **P10.2** que $\Bbbk(\epsilon) \subset D(\epsilon)$ est radicale. Comme $\Bbbk \subset \Bbbk(\epsilon)$ est radicale, on a $\Bbbk \subset D(\epsilon)$ radicale et donc $\Bbbk \subset D$ est résoluble par radicaux. Réciproquement, supposons que P soit résoluble par radicaux. On peut trouver une extension de radicale $\Bbbk$ dans laquelle P est scindé. Disons $\Bbbk \subset \Bbbk(\alpha_1, ..., \alpha_n)$ avec, pour tout i, $\alpha_i^{m_i} \in \Bbbk(\alpha_1, ..., \alpha_{i-1})$ pour un certain $n_i \in \mathbb{N}$. Quitte à rajouter des radicaux, on peut supposer les n_i premiers. On peut aussi rajouter une racine ϵ de $X^{\prod n_i} - 1$. On va montrer par récurrence que pour tout $1 \leq i \leq k$, l'extension $\Bbbk \subset \Bbbk(\epsilon, \alpha_1, ..., \alpha_i)$ est galoisienne de groupe de Galois résoluble. On note $F_i = \Bbbk(\epsilon, \alpha_1, ..., \alpha_i)$ et $G_i = Gal(F_i/\Bbbk)$. $\Bbbk \subset F_0 = \Bbbk(\epsilon)$ est abélienne selon **(T10.2)**. Soit $i > 0$. On suppose que $\Bbbk \subset F_{i-1}$ est galoisienne et que G_{i-1} est résoluble. Selon **(P10.3)**, l'extension $F_{i-1} \subset F_i$ est abélienne, donc G_i est résoluble. On en déduit le résultat.

11 Recherche de polynômes à coefficients dans $\mathbb{Q}$ non résolubles par radicaux

11.1 Critères d'irréductiblité sur $\mathbb{Q}$

Proposition 11.1.1 : Soient $A, B \in \mathbb{Z}[X]$. On note $c(A)$ (resp. $c(B)$) le PGCD des coefficients de A (resp. de B). Alors, $c(AB) = c(A)c(B)$.
Démonstration : On note $A = a_0 + ... + a_nX^n$ et $B = b_0 + ... + b_nX^n$ où $n = \max(\deg(A), \deg(B))$. Le degré de AB est inférieur à $2n$ et on peut écrire que $AB = \sum_{k=0}^{n}(\sum_{i=0}^{k} a_ib_{k-i})X^k + \sum_{k=0}^{n-1}(\sum_{i=0}^{k} a_{n-i}b_{n-k+i})X^{2n-k}$. On en déduit que $c(A)c(B)$ divise $c(AB)$ et que si $c(AB) = 1$, alors $c(A) = 1$ et $c(B) = 1$. Sinon, on note $c(AB) = p_1...p_r$ la décomposition de $c(AB)$ en facteurs premiers. On suppose que p_1 ne divise ni $c(A)$, ni $c(B)$. Alors, on peut se donner i (resp. j) le plus petit entier tel que p_1 ne divise pas a_i (resp. b_j), et k (resp. l) le plus grand entier tel que p_1 ne divise pas a_k (resp. b_l). On a $0 \leq i \leq k \leq n$ et $0 \leq j \leq l \leq n$ donc $i + j \leq n$ ou $n \leq k + l$. Si $i + j \leq n$, comme p_1 divise le $(i + j)$-ème coefficient de AB, qui est $\sum_{m=0}^{i+j} a_mb_{i+j-m}$, on trouve que p_1 divise a_ib_j (car il divise tous les autres coefficients de cette somme), et donc p_1 divise a_i ou b_j, ce qui est absurde. Si $n \leq k + l$, on note $\tilde{A} = a_n + ... + a_0X^n$ et $\tilde{B} = b_n + ... + b_0X^n$. On remarque alors que k (resp. l) est le plus petit entier tel que p_1 ne divise pas le k-ème coefficient de $\tilde{A}$ (resp. $\tilde{B}$). Comme A et $\tilde{A}$, et B et $\tilde{B}$ ont les mêmes coefficients, on se retrouve dans le même cas que précédemment, qui est absurde. On en déduit que p_1 divise $c(A)$ ou $c(B)$ (disons p_1 divise $c(A)$). Alors, par le même raisonnement mais sur les polynômes A/p_1 et B, on trouve que p_2, qui divise $c(AB)/p_1$, divise $c(A)/p_1$ ou $c(B)$. Bref, on trouve par récurrence que $c(AB)$ divise $c(A)c(B)$. On a donc bien l'égalité.

Théorème 11.1.1 : Soit $P \in \mathbb{Z}[X]$ de degré ≥ 1. Si P est irréductible dans $\mathbb{Z}[X]$, alors il l'est aussi dans $\mathbb{Q}[X]$.
Démonstration : Supposons que P soit irréductible dans $\mathbb{Z}[X]$ et qu'il s'écrive $P = QR$ dans $\mathbb{Q}[X]$ avec $\deg(Q) \leq \deg(R)$. Déjà, on remarque que $c(P) = 1$, sinon la décomposition $P = c(P) \times P/c(P)$ contredit l'irréductibilité de P. Par ailleurs, on dispose de $q, r \in \mathbb{Z}$ tels que $qQ,\ rR \in \mathbb{Z}[X]$. Alors, $qrP = qQrR$ et on a $qr \times c(P) = c(qQ)c(rR)$, donc $qr = c(qQ)c(rR)$. On en déduit que $P = qQ/c(qQ) \times rR/c(rR)$ est une décomposition dans $\mathbb{Z}[X]$ et donc que $qQ/c(qQ) = 1$ ou $rR/c(rR) = 1$. Alors Q ou R est de degré 0, ce qui prouve l'irréductibilité de P dans $\mathbb{Q}[X]$.

Théorème 11.1.2 : *(Critère d'Eisenstein)* Soit $P = a_0 + ... + a_nX^n \in \mathbb{Z}[X]$. On suppose qu'il existe un nombre p premier tel que : p divise $a_0, ..., a_{n-1}$, p^2 ne divise pas a_0 et p ne divise pas a_n. Alors, P est irréductible sur $\mathbb{Q}$.
Démonstration : On traite d'abord le cas où $c(P) = 1$. On suppose que $P = QR$ dans $\mathbb{Z}[X]$ avec $Q = b_0 + ... + b_nX^n$ et $R = c_0 + ...c_nX^n$. p divise $a_0 = b_0c_0$ donc p divise b_0 ou c_0. Disons que p divise b_0. Soit $0 \leq i < n - 1$, supposons que p divise b_j pour tout $j \leq i$. Alors, comme p divise $a_{i+1} = \sum_{k=0}^{i+1} b_ic_{k-i}$, p divise $b_{i+1}c_0$. Mais p^2 ne divise pas a_0 donc p ne divise pas c_0, donc p divise b_{i+1}. On en déduit que p divise $b_0, ..., b_{n-1}$. p ne divise pas b_n car sinon il diviserait $a_n = \sum_{k=0}^{n} b_ic_{n-i}$. Ainsi $b_n \neq 0$ et $\deg(Q) = n$. Alors, comme $c(R) = 1$ et $\deg(R) = 1$, on a $R = 1$ et donc P est irréductible sur $\mathbb{Z}[X]$. On conclut avec **(T11.1)**. Si $c(P) \neq 1$, p ne divise pas a_n donc pas $c(P)$ non plus. On a $P_0 \in \mathbb{Z}[X]$ tel que $c(P_0) = 1$ et $P = c(P)P_0$, et P_0 vérifie clairement les hypothèses de l'énoncé. P est alors associé à un polynôme irréductible sur $\mathbb{Q}$, donc est aussi irréductible sur $\mathbb{Q}$ (car $\mathbb{Q}$ est un corps).

11.2 Étude du groupe S_n

Proposition 11.2.1 : Soit $P \in \mathbb{k}[X]$ de degré n et $\mathbb{D}$ un corps de décomposition de P. On note R l'ensemble des racines de P dans $\mathbb{D}$. On définit une action de groupe de $\mathrm{Gal}(\mathbb{D}/\mathbb{k})$ sur R avec l'application $(\sigma, \alpha) \mapsto \sigma \cdot \alpha = \sigma(\alpha)$.

Figure 11: Gotthold Eisenstein, 1823 - 1852

Si $\sigma \in \mathrm{Gal}(\mathbb{D}/\Bbbk)$, l'application de $R \to R,\ \alpha \mapsto \sigma(\alpha)$ est un élément de S_R que l'on note $\pi(\sigma)$. On vérifie que π est un morphisme injectif de groupe, et donc que $\mathrm{Gal}(\mathbb{D}/\Bbbk)$ est isomorphe à un sous-groupe de S_r où $r = \mathrm{Card}(R)$.

Remarque : Tous les polynômes de degré $n \leq 4$ sont résolubles par radicaux, car leurs groupes de Galois sont des sous-groupes de S_4 (oui, $S_1 \subset S_2 \subset S_3 \subset S_4$), qui est résoluble.

Proposition 11.2.2 : Soit $n \in \mathbb{N}$.

1. Le groupe S_n est engendré par la famille de permutations $T_1 = ((1,\ 2),\ (1,\ 3),\ ...,\ (1,\ n))$.
2. Le groupe S_n est engendré par la famille de permutations $T_2 = ((1,\ 2),\ (2,\ 3),\ ...,\ (n-1,\ n))$.
3. Le groupe S_n est engendré par la famille de permutations $T_3 = ((1,\ 2)$ et $(1,\ 2,\ ...,\ n))$.

Démonstration : (1) : Toute transposition $(i,\ j)$ s'écrit $(i,\ j) = (1,\ i)(1,\ j)(1,\ i)$. S_n est engendré par les transpositions, qui sont construites à partir des éléments de T_1, donc on a bien le résultat. (2) : On va montrer que pour tout k, on peut construire la transposition $(1,\ k)$. On raisonne par récurrence. Pour $k = 2$, c'est immédiat car $(1,\ 2) \in T_2$. Soit $k < n$, on suppose qu'on peut construire $(1,\ k)$. Alors, $(1,\ k+1) = (1,\ k)(k,\ k+1)(1,\ k)$. On peut construire tous les éléments de T_1 à partir de ceux de T_2 donc T_2 engendre S_n. (3) : On va montrer que pour tout k, on peut construire la transposition $(k,\ k+1)$. On raisonne par récurrence. Pour $k = 1$, c'est immédiat car $(1,\ 2) \in T_3$. Soit $k > 1$, on suppose qu'on peut construire $(k-1,\ k)$. Alors, $(k-1,\ k+1,\ k) = (1,\ 2,\ ...,\ n)(k-1,\ k)(1,\ 2,\ ...,\ n)^{-1}(k-1,\ k)$, et comme $(k,\ k+1) = (k-1,\ k+1,\ k)(k-1,\ k)$ on a bien le résultat. On peut donc construire les éléments de T_2 à partir de ceux de T_3, donc T_3 engendre S_n.

Remarque : On en déduit que si $E = \{a_1,\ ...,\ a_n\}$, alors les familles $((a_1,\ a_2),\ ...,\ (a_1,\ a_n))$, $((a_1,\ a_2),\ ...,\ (a_{n-1},\ a_n))$ et $((a_1,\ a_2),\ (a_1,\ ...,\ a_n))$ engendrent S_E. Cette remarque est très utile car elle permet de considérer les permutations de S_n "à renommage près" des entiers de 1 à n.

Proposition 11.2.3 : Si p est premier, alors S_p est engendré par n'importe quelle famille de la forme (transposition, p-cycle).

Démonstration : Soient τ une transposition et c un p-cycle. Sans perte de généralité, on peut supposer que $\tau = (1,\ 2)$. On note $c = (1,\ a_2,\ ...,\ a_p)$ et j l'entier tel que $a_j = 2$. Si $j = p$, alors $c = (2,\ 1,\ a_2,\ ...,\ a_{p-1})$ et on peut conclure avec **(P11.2)** et la remarque précédente. Sinon, $j < p$. Si $\sigma \in S_p$ est d'ordre p, alors c'est un

p-cycle car son ordre est le PPCM des ordres des éléments de sa décomposition en cycles disjoints et p est premier. On en déduit que c^j, qui est d'ordre p car le groupe engendré par c est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, est un p-cycle de la forme $(1,\ 2,\ b_3,\ ...,\ b_p)$. Encore une fois, on conclut à l'aide de **(P11.2)** et de la remarque précédente.

11.3 Calcul du groupe de Galois de certains polynômes à coefficients dans $\mathbb{Q}$

Proposition 11.3.1 : Soient p un nombre premier supérieur à 5 et $P \in \mathbb{Q}[X]$ un polynôme irréductible de degré p admettant exactement $p-2$ racines réelles. Alors P n'est pas résoluble par radicaux.
Démonstration : On note $\mathbb{D}$ le corps de décomposition de P sur $\mathbb{Q}$ et $G = \mathrm{Gal}(\mathbb{D}/\mathbb{Q})$ le groupe de Galois de P. L'extension $\mathbb{Q} \subset \mathbb{D}$ est galoisienne. La conjugaison complexe (notée σ) induit un élément de G qui laisse invariant les $p-2$ racines réelles de P et qui échange les deux racines qui ne sont pas réelles. L'élément de S_p induit par σ (comme en **(T10.4)**) est une donc une transposition. Si $\alpha \in \mathbb{D}$ est une racine de P, P est son polynôme minimal, donc l'extension $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ est de degré p. On en déduit que p divise le degré de $\mathbb{Q} \subset \mathbb{D}$ qui est l'ordre de G **(T9.12)**, et donc que G contient un élément d'ordre p **(1.4)**. G contient une transposition, un p-cycle et est inclus dans S_p, donc c'est S_p **(P11.5)**. S_p n'est pas résoluble pour $p \geq 5$ donc P n'est pas résoluble par radicaux.

Théorème 11.3.1 : *(Abel)* Les polynômes à coefficients complexes de degré 5 ne sont, *en général*, pas résolubles par radicaux.
Démonstration : Le polynôme $P = X^5 - 6X - 3 \in \mathbb{Q}[X]$ n'est pas résoluble par radicaux. Il est irréductible sur $\mathbb{Q}$ car il vérifie le critère d'Eisenstein **(T11.2)**. $P' = 5X^4 - 6$ admet deux racines réelles : $\pm\sqrt[4]{\frac{6}{5}}$. On en déduit que l'application de $\mathbb{R} \to \mathbb{R},\ x \mapsto P(x)$ est croissante sur $[-\infty,\ -\sqrt[4]{\frac{6}{5}}]$, décroissante sur $[-\sqrt[4]{\frac{6}{5}}],\ \sqrt[4]{\frac{6}{5}}]$ et croissante sur $[\sqrt[4]{\frac{6}{5}},\ +\infty]$. Comme $P(\sqrt[4]{\frac{6}{5}}) = -\frac{24}{5}\sqrt[4]{\frac{6}{5}} - 3 < 0$ et $P(-\sqrt[4]{\frac{6}{5}}) = \frac{24}{5}\sqrt[4]{\frac{6}{5}} - 3 > 0$, on trouve que P a exactement 3 racines réelles. On conclut avec la proposition précédente **(P11.6)**.

Remarque : On vient de montrer que les racines de P ne peuvent être exprimées à partir d'opérations "simples" (addition, multiplication, racine k-ème).

Théorème 11.3.2 : Soient $p \in \mathbb{N}$ premier impair et $m \in \mathbb{N}^*$ pair. Le polynôme $P = (X^2 + m)\prod_{k=1}^{p-2}(X - 2k) - 2$ n'est pas résoluble par radicaux.
Démonstration : On note Q le polynôme $(X^2 + m)\prod_{k=1}^{p-2}(X - 2k)$. Q admet exactement $p-2$ racines réelles qui sont $\{2k,\ 1 \leq k \leq p-2\}$. La courbe de la fonction $x \mapsto P(x)$ est simplement une translation vers le bas de celle de $x \mapsto Q(x)$. Pour montrer que P admet aussi exactement $p-2$ racines réelles, il suffit de montrer que pour tout $1 \leq j < p-2$, il existe $x \in [2j,\ 2(j+1)]$ tel que $|Q(x)| > 2$, et alors en translatant vers le bas de 2 la courbe de $x \mapsto Q(x)$, on ne rajoute ou ne retire pas de racines. Si $p = 3$, le résultat est immédiat. Sinon, pour tout $1 \leq j < p-2$,

$$Q(2j+1) = ((2j+1)^2 + m)\prod_{k=1}^{j}(2(j-k)+1) \times \prod_{k=1}^{p-2-j}(2k-1) \times (-1)^{p-2-j}$$

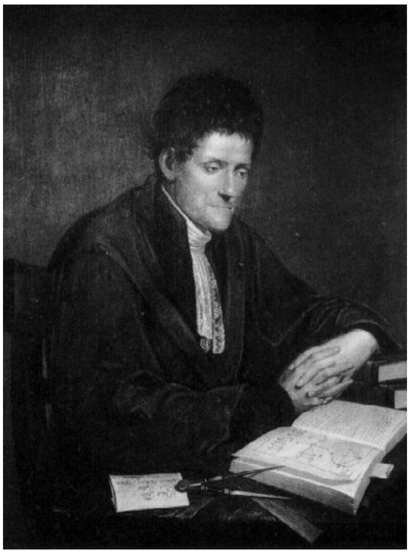
est bien strictement supérieur à 2 en valeur absolue. P admet donc exactement $p-2$ racines réelles. P vérifie le critère d'Eisenstein **(T11.2)** pour le nombre premier 2, donc il est irréductible sur $\mathbb{Q}$. On déduit de **(P11.5)** que P n'est pas résoluble par radicaux.

Figure 12: Courbe de $x \mapsto Q(x)$ pour $m = 2$ et $p = 7$

Théorème 11.3.3 : *(Abel - Ruffini)* Les polynômes à coefficients complexes de degré supérieur ou égal à 5 ne sont, *en général*, pas résolubles par radicaux.

Démonstration : Pour tout $n \in \mathbb{N}$, le polynôme $P = X^n(X^5 - 6X - 3)$ n'est pas résoluble par radicaux. En effet, si on note $\mathbb{D}$ le corps de décomposition de P, et qu'on suppose que $\mathbb{Q} \subset \mathbb{D}$ est une sous-extension d'une extension radicale $\mathbb{Q} \subset \mathbb{K}$, alors, en notant R l'ensemble des racines de $X^5 - 6X - 3$, on a $\mathbb{Q} \subset \mathbb{Q}(R) = \mathbb{D} \subset \mathbb{K}$, et donc $X^5 - 6X - 3$ résoluble par radicaux, ce qui est absurde.

(a) Niels Henrik Abel, 1802 - 1829



(b) Paolo Ruffini, 1765 - 1822

Théorème 11.3.4 : *(Nart - Vila)* Le groupe de Galois de $X^n - X - 1$ est S_n. $X^n - X - 1$ n'est donc pas résoluble par radicaux dès que $n \geq 5$.
Démonstration : Voir [10], ce n'est pas facile du tout !

12 Construction à la règle et au compas

Dans cette partie, on considère le plan euclidien usuel $\mathbb{R}^2$ que l'on identifie à $\mathbb{C}$ par l'isomorphisme de $\mathbb{R}$-espace vectoriel canonique $(x, y) \mapsto x + iy$. On appelle **point** ou **vecteur** les éléments de $\mathbb{C}$.

12.1 Rappels de géométrie

Définition 12.1.1 : Une **droite vectorielle** est un sous-espace de $\mathbb{C}$ de dimension 1.

Définition 12.1.2 : Une **droite** (ou **droite affine**) $\mathcal{D}$ est un ensemble de la forme $\{A + X,\ X \in \mathcal{D}_v\}$ où A est un point et $\mathcal{D}_v$ une droite vectorielle. La droite vectorielle $\mathcal{D}_v$ est unique, c'est la **direction** de $\mathcal{D}$. Une droite est caractérisée par la donnée de deux points distincts par lesquels elle passe ou par la donnée de sa direction et d'un point par lequel elle passe.

Définition 12.1.3 : Deux droites sont dites **parallèles** si leurs directions sont égales.
Remarque : En géométrie euclidienne plane, deux droites non parallèles sont toujours sécantes : il existe un unique point appartenant aux deux droites.

Définition 12.1.4 : Deux droites sont dites **perpendiculaires** si leurs directions sont orthogonales.

Définition 12.1.5 : Si A et B sont deux points distincts, l'ensemble $\{A + (B - A)t,\ t \in \mathbb{R}\}$ est une droite de direction $\mathrm{Vect}(B - A)$ qui contient les points A et B. C'est l'unique droite contenant ces deux points, on dit que c'est la **droite passant par** A **et** B et on la note $\mathcal{D}_{A,B}$.

Définition 12.1.6 : Soient A, B deux points distincts. Les **segment** d'extrémités A, B, noté $\mathcal{S}_{A,B}$ est l'ensemble $\{A + (B - A)t,\ t \in [0,\ 1]\}$. Pour tout $X \in \mathcal{S}_{A,B}$, on a $|X - A| + |X - B| = |B - A|$.

Définition 12.1.7 : Un **cercle** est un ensemble de la forme $\{X \in \mathbb{C},\ |X - A| = r\}$ où A est un point et r un réel positif. Le point A est unique, c'est le **centre** du cercle. Le réel r est unique, c'est le **rayon** du cercle. Un cercle est donc caractérisé par son rayon et son centre.

Définition 12.1.8 : Si A et B sont deux points distincts, l'ensemble $\{X \in \mathbb{C},\ |X - A| = |B - A|\}$ est l'unique cercle de centre A contenant B. On dit que c'est le **cercle de centre** A **passant par** B et on le note $\mathcal{C}_{A,B}$.

Proposition 12.1.1 : Soient $\mathcal{C}_1$ et $\mathcal{C}_2$ deux cercles de centres A_1 et A_2 et de rayons r_1 et r_2. L'intersection de $\mathcal{C}_1$ et $\mathcal{C}_2$ est :

1. infinie si $\mathcal{C}_1 = \mathcal{C}_2$ (c'est-à-dire si $A_1 = A_2$ et $r_1 = r_2$).
2. constituée d'un unique point si $|A_1 - A_2| = r_1 + r_2$.
3. vide si $|A_1 - A_2| + r_1 < r_2$ ou si $|A_1 - A_2| + r_2 < r_1$ ou si $r_1 + r_2 < |A_1 - A_2|$.
4. constituée de deux points sinon (c'est à dire si $|r_1 - r_2| \leq |A_1 - A_2| < r_1 + r_2$).

Définition 12.1.9 : Soient $\mathcal{D}$ une droite passant par un point A de direction $\mathcal{D}_v$ et B un point. Il existe une unique droite $\mathcal{D}'$ de direction $\mathcal{D}_v^\perp$ passant par B. Le point d'intersection P de $\mathcal{D}$ et $\mathcal{D}'$ est appelé **projeté orthogonal de** B **sur** $\mathcal{D}$ et noté $P_{B,\mathcal{D}}$. Pour tout $X \in \mathcal{D}$, $|P_{X,\mathcal{D}} - B| \leq |X - B|$.

Proposition 12.1.2 : Soient $\mathcal{D}_1$ et $\mathcal{D}_2$ deux droites parallèles. Pour tout $X, Y \in \mathcal{D}_1$, $|X - P_{X,\mathcal{D}_2}| = |Y - P_{Y,\mathcal{D}_2}|$
Démonstration : Pour simplifier, on note $P_X = P_{X,\mathcal{D}_2}$ et $P_Y = P_{Y,\mathcal{D}_2}$. $Y - P_Y = Y - X + X - P_X + P_X - P_Y$ donc $|Y - P_Y|^2 = |X - P_X|^2 + |P_X - P_Y + Y - X|^2$ donc $|Y - P_Y|^2 - |X - P_X|^2 = |P_X - P_Y + Y - X|^2$ donc

$0 \leq |Y - P_Y|^2 - |X - P_X|^2$. Par symétrie, on trouve aussi $0 \leq |X - P_X|^2 - |Y - P_Y|^2$, ce qui permet de conclure.

Proposition 12.1.3 : Soient $\mathcal{D}$ une droite passant par A de direction $\mathcal{D}_v$ et $\mathcal{C}$ un cercle de centre B et de rayon r. On note P le projeté orthogonal du point B sur $\mathcal{D}$. L'intersection de $\mathcal{D}$ et $\mathcal{C}$ est :

1. vide si $r < |P - B|$.
2. constituée d'un unique point si $r = |P - B|$.
3. constituée de deux points si $r > |P - B|$.

Définition 12.1.10 : Soient $A, B \in \mathbb{C}$ distincts. Le symétrique de A par rapport à B est le point $A + 2(B - A) = 2B - A$.

Définition 12.1.11 : Soient $A \in \mathbb{C}$ et $\mathcal{D}$ une droite. Le **symétrique orthogonal** de A par rapport à $\mathcal{D}$ est le symétrique de A par rapport au projeté orthogonal de A sur $\mathcal{D}$.

12.2 Constructibilité

Définition 12.2.1 : Soit E une partie non vide de $\mathbb{C}$. On dit qu'une droite (resp. un cercle) est **constructible en une étape à partir de** E si elle passe par deux points distincts de E (resp. si son centre est un point de E et qu'il passe par un point de E).

Définition 12.2.2 : Soit E une partie non vide de $\mathbb{C}$. L'ensemble des **points constructibles en une étape à partie de** E, noté $c(E)$, est formé des points suivants :

1. Les points de E.
2. Les points qui sont des intersections de deux droites **distinctes**, deux cercles **distincts** ou d'une droite et d'un cercle constructibles en une étape à partie de E.

Remarque : Si E est un singleton, $c(E) = E$.

Définition 12.2.3 : On pose $K_0 = \{0,\ 1\}$ et pour tout $n \in \mathbb{N}^*$, $K_n = c(K_{n-1})$. L'ensemble des **points constructibles** de $\mathbb{C}$ est $\bigcup_{n=0}^{\infty} K_n$ et noté K. On dit qu'une droite (resp. un cercle) est constructible si elle est constructible en une étape à partir d'un des K_n.

Proposition 12.2.1 : Soient $A, B \in K$. Le symétrique S de A par rapport à B est constructible.
Démonstration : S est clairement un point de $\mathcal{D}_{A,B}$. Mais S vérifie aussi $|S - B| = |A - B|$, donc S est un point de $\mathcal{C}_{B,A}$. Ainsi, $S \in \mathcal{D}_{A,B} \cap \mathcal{C}_{B,A}$.

Proposition 12.2.2 : Soient $A \in \mathbb{K}$ et $\mathcal{D}$ une droite constructible. Le projeté orthogonal de A sur $\mathcal{D}$ est constructible.
Démonstration : $\mathcal{D}$ est constructible donc elle passe par deux points B et C distincts et constructibles. Les cercles $\mathcal{C}_{B,A}$ et $\mathcal{C}_{C,A}$ sont de rayon $|B - A|$ et $|C - A|$ et, par la relation de Chasles, on a $0 \leq |B - C| \leq |B - A| + |C - A|$, donc ils s'intersectent en deux points : A et I. Par ailleurs, $\langle A - I, B - C\rangle = \langle A, B\rangle - \langle I, B\rangle + \langle I, C\rangle - \langle A, C\rangle = 0$ (cela découle des égalités $|A - C| = |I - C|$ et $|A - B| = |I - B|$), donc $\mathcal{D}$ et $\mathcal{D}_{A,I}$ sont perpendiculaires. Le point d'intersection de $\mathcal{D}$ et $\mathcal{D}_{A,I}$ est donc le projeté orthogonal de A par rapport à $\mathcal{D}$. On a montré au passage que la droite perpendiculaire à $\mathcal{D}$ passant par A est constructible.

Proposition 12.2.3 : Soient $A \in K$ et $\mathcal{D}$ une droite constructible. Le symétrique orthogonal de A par rapport $\mathcal{D}$ est constructible.
Démonstration : Le projeté orthogonal P de A sur $\mathcal{D}$ est constructible et le symétrique de A par rapport à P est constructible.

Proposition 12.2.4 : Soient $A, B \in K$ deux points distincts. Le **milieu** de $\mathcal{S}_{A,B}$ (le point $A + (B - A)/2$) est constructible.
Démonstration : On note I_1 et I_2 les points d'intersection des cercles $\mathcal{C}_{A,B}$ et $\mathcal{C}_{B,A}$. Alors, la droite $\mathcal{D}_{I_1,I_2}$ est perpendiculaire à $\mathcal{D}_{A,B}$. Pour tout $X = I_1 + (I_2 - I_1)\alpha \in \mathcal{D}_{I_1,I_2}$, on a $|X - A| = |X - B|$ (c'est le théorème de Pythagore). On en déduit que le point d'intersection M de $\mathcal{D}_{I_1,I_2}$ et $\mathcal{D}_{\mathcal{A},\mathcal{B}}$ vérifie $|M - A| = |M - B|$ et $|M - A| + |M - B| = |B - A|$. On a donc le résultat.

Proposition 12.2.5 : Soit $\mathcal{D}$ une droite constructible passant un point $A \in K$. On peut construire la droite perpendiculaire à $\mathcal{D}$ qui passe par A.
Démonstration : On se donne B un autre point constructible sur la droite $\mathcal{D}$ et on note S le symétrique de B par rapport à A. Alors A est le milieu du segment $\mathcal{S}_{B,S}$. On a vu en **(P1.6)** que A est le point d'intersection de la droite $\mathcal{D}$ avec la droite $\mathcal{D}_{I_1,I_2}$ où I_1, I_2 sont les points d'intersection des cercles $\mathcal{C}_{B,S}$ et $\mathcal{C}_{S,B}$. Bref, $\mathcal{D}_{I_1,I_2}$ est la droite perpendiculaire à $\mathcal{D}$ passant par A et est constructible.

Proposition 12.2.6 : Soit $\mathcal{D}$ une droite constructible passant par un point $A \in K$ et soit $B \in K$. La droite parallèle à $\mathcal{D}$ passant par B est constructible.
Démonstration : On peut construire la droite $\mathcal{D}'$ perpendiculaire à $\mathcal{D}$ passant par B. Selon **(P1.7)**, on peut construire la droite $\mathcal{D}''$ perpendiculaire à $\mathcal{D}'$ passant par B. La direction de $\mathcal{D}''$ est orthogonale à la direction de $\mathcal{D}'$ qui est orthogonale à celle de $\mathcal{D}$, donc celle de $\mathcal{D}''$ et celle de $\mathcal{D}$ sont égales (unicité du supplémentaire orthogonal), $\mathcal{D}$ et $\mathcal{D}''$ sont parallèles.

Proposition 12.2.7 : Soit $A \in K$. Alors $-A$ est constructible.
Démonstration : En effet, il suffit de remarquer que $-A$ est le symétrique de A par rapport à 0.

Proposition 12.2.8 : Soit $A \in K$. Pour tout $k \in \mathbb{Z}$, kA est constructible.
Démonstration : Tenant compte du point précédent, il suffit de prouver que pour tout $n \in \mathbb{N}$, le point nA est constructible. Soit $n \in \mathbb{N}^*$. On suppose que pour tout $k \leq n, kA$ est constructible. Le symétrique de $(n-1)A$ par rapport à nA est $(n+1)A$, et est constructible. 0 est clairement constructible donc on a bien le résultat.

Proposition 12.2.9 : Soient $A, B \in K$. Alors $A + B$ est constructible.
Démonstration :

1. Si $A = B$, alors **(P1.10)**.

2. Sinon, on note $\mathcal{D}$ la droite $\mathcal{D}_{A,B} = \mathcal{D}_{0,A} = \mathcal{D}_{0,B}$. On suppose que 0, A et B sont alignés. On se donne A' un point d'intersection du cercle $\mathcal{C}_{0,A}$ et de la droite perpendiculaire à $\mathcal{D}$. On note $\mathcal{D}'$ la droite parallèle à $\mathcal{D}$ passant par A' et $\mathcal{D}''$ la droite perpendiculaire à $\mathcal{D}$ passant par B et A'' leur point d'intersection. Alors, le rayon de $\mathcal{C}_{B,A''}$ est $|A|$ **(P1.2)**. On en déduit que les deux points d'intersection de $\mathcal{D}$ avec $\mathcal{C}_{B,A''}$ sont $B - A$ et $B + A$.

3. On peut tracer la droite $\mathcal{D}$ parallèle à $\mathcal{D}_{0,A}$ passant par B et la droite $\mathcal{D}'$ parallèle à $\mathcal{D}_{0,B}$ passant par A. Alors, si on note I le point d'intersection de $\mathcal{D}$ et $\mathcal{D}'$, on a $|A - I| = |B|$ **(P1.2)**. La droite $\mathcal{D}'$ est parallèle à $\mathcal{D}_{0,B}$ qui est une droite vectorielle, donc c'est sa direction. Ainsi, I s'écrit $A + X$ avec $X \in \mathcal{D}_{0,B}$ et $|X| = |B|$, donc $X = \pm B$. Si $X = B$, on a bien construit $A + B$. Sinon, $X = -B$, on construit alors $A + B$ en prenant le symétrique de I par rapport à B.

Remarque : La définition qu'on a donné de la constructibilité peut paraître plus restrictive que celle qu'on utilise pour construire des figures géométriques. En effet, si on suppose construits un point A et un réel r, alors, *à priori*, on ne peut pas mesurer la longueur r avec notre compas et la reporter sur A, c'est-à-dire tracer le cercle de centre A et de rayon r. Mais avec la proposition précédente, on voit que le point $A + r$ est constructible, et donc que ce cercle est constructible ! Toute longueur constructible peut être reportée sur n'importe quel point constructible.

Proposition 12.2.10 : Soit $A \in \mathbb{C}$. Alors A est constructible si, et seulement si $\mathrm{Re}(A)$ et $\mathrm{Im}(A)$ sont constructibles.
Démonstration : Déjà, il faut noter que $\mathcal{D}_{0,i}$ est constructible car $\langle i, 1\rangle = 0$ donc la perpendiculaire à $\mathcal{D}_{0,1}$ passant par 0 contient i. Elle est constructible **(P1.8)**. Si A est constructible, les projetés orthogonaux de A sur $\mathcal{D}_{0,1}$ et sur $\mathcal{D}_{0,i}$ sont constructibles. $\mathrm{Re}(A)$ et $i\times\mathrm{Im}(A)$ sont constructibles. $\mathrm{Im}(A)$ est alors une des intersections de $\mathcal{D}_{0,1}$ et $\mathcal{C}_{0,i\times\mathrm{Im}(A)}$. Si $\mathrm{Re}(A)$ et $\mathrm{Im}(A)$ sont constructibles, alors $i\times\mathrm{Im}(A)$ est une des intersections de $\mathcal{D}_{0,i}$ et $\mathcal{C}_{0,\mathrm{Im}(A)}$ donc est constructible. Selon la proposition précédente **(P1.12)**, $A = \mathrm{Re}(A) + i\mathrm{Im}(A)$ est constructible.

Proposition 12.2.11 : Soient $A, B \in K \cap \mathbb{R}^*$. Alors, $1/A$, AB et A/B sont constructibles.
Démonstration : On note $\mathcal{D}$ la droite parallèle à $\mathcal{D}_{A,i}$ passant par 1 et C son point d'intersection avec $\mathcal{D}_{0,i}$. Selon le théorème de Thalès, on a $1/A = |C|/|i| = |C|$. $1/A$ est donc un des points d'intersection de la droite $\mathcal{D}_{0,1}$ avec $\mathcal{C}_{0,C}$. On note maintenant $\mathcal{D}'$ la droite parallèle à $\mathcal{D}_{A,i}$ passant par $1/B$ et D son point d'intersection avec $\mathcal{D}_{0,i}$. Alors, selon le théorème de Thalès, $A/(1/B) = AB = 1/|D|$. D est constructible et non nul, donc $1/D$ est constructible donc AB aussi. On en déduit que AB est aussi constructible.

Proposition 12.2.12 : Soient $A, B \in K$ non nuls. Alors, $1/A$, AB et A/B sont constructibles.
Démonstration : On pose $A = a_1 + ia_2$ et $B = b_1 + ib_2$. Alors $1/A = (a_1 - ia_2)/|A|^2$, $AB = a_1b_1 - a_2b_2 + i(a_1b_2 + a_2b_1)$. Selon **(P1.14)**, les parties réelles et imaginaires de $1/A$ et de AB sont constructibles, donc $1/A$ et AB sont constructibles **(P1.13)**. On en déduit que A/B est constructible.

Théorème 12.2.1 : L'ensemble K des nombres constructibles est un sous-corps de $\mathbb{C}$.

Proposition 12.2.13 : Soit $A \in K \cap \mathbb{R}_+$. Alors $\sqrt{A}$ est constructible.
Démonstration : On note I le point d'intersection de la droite perpendiculaire à $\mathcal{D}_{0,1}$ passant par A et de la droite parallèle à $\mathcal{D}_{0,1}$ passant par i. Alors $|I| = \sqrt{A}$ selon le théorème de Pythagore. On en déduit que $\sqrt{A}$ est un des points d'intersection de la droite $\mathcal{D}_{0,1}$ avec le cercle $\mathcal{C}_{0,I}$.

Proposition 12.2.14 : Soit $A \in K$. Le polynôme $X^2 - A$ admet deux racines dans $\mathbb{C}$ qui sont constructibles.
Démonstration : On suppose que A est de module 1 et que $A \neq -1$. A s'écrit $\cos(\theta) + i\sin(\theta)$ avec $\theta \in]-\pi, \pi]$. Il est clair que le point $\alpha = \cos(\theta/2) + i\sin(\theta/2)$ est racine de $X^2 - A$. On note β le point d'intersection ($\neq 0$) des cercles $\mathcal{C}_{1,0}$ et $\mathcal{C}_{A,0}$ et $\delta = e^{i\theta'}$ un point d'intersection de $\mathcal{D}_{0,\beta}$ avec le cercle $\mathcal{C}_{0,1}$. Alors, on a

$$|e^{i\theta'} - e^{i\theta}| = |e^{i\theta'} - 1|$$

donc

$$\sin(\frac{|\theta'|}{2}) = \sin(\frac{|\theta - \theta'|}{2})$$

et comme $\frac{|\theta'|}{2}$ et $\frac{|\theta-\theta'|}{2} \in [0, \pi]$, on a $|\theta'| = |\theta - \theta'|$ donc $\theta' = \theta/2$. On a donc $\delta = \alpha$, ce qui achève la preuve.

12.3 Caractérisation des nombres constructibles

Définition 12.3.1 : On note $\mathcal{F}$ l'ensemble des sous-extensions $\mathbb{K}$ de $\mathbb{Q} \subset \mathbb{C}$ stables par conjugaison et telles que pour tout $x \in \mathbb{C}$, $x^2 \in \mathbb{K} \Rightarrow x \in \mathbb{K}$.

Définition 12.3.2 : L'intersection de tous les éléments de $\mathcal{F}$ est un élément de $\mathcal{F}$. On le note $\mathbb{T}$. On va montrer que $\mathbb{T} = K$.

Définition 12.3.3 : On peut généraliser la définition **(D1.14)** et considérer, pour toute partie $S \subset \mathbb{C}$ non vide l'ensemble $K(S)$ des éléments constructibles en un nombre fini d'étape à partir de ceux de S. Il est clair que si S contient 0 et 1, alors $K(S)$ est un corps.

Proposition 12.3.1 : Si $z \in \mathbb{T}$, alors $\mathrm{Re}(z) \in \mathbb{T}$ et $\mathrm{Im}(z) \in \mathbb{T}$.
Démonstration : $-1 \in \mathbb{T}$ donc $i \in \mathbb{T}$. Comme $\bar{z} \in \mathbb{T}$ et $\mathrm{Re}(z) = (z+\bar{z})/2$ et $\mathrm{Im}(z) = (z-\bar{z})/2i$, on en déduit le résultat.

Proposition 12.3.2 : $K(\mathbb{T}) = \mathbb{T}$
Démonstration : Avec **(P1.16)**, il est facile de vérifier que les équations des droites constructibles à partir de $\mathbb{T}$ sont de la forme

$$ax + by + c = 0$$

avec $a, b, c \in \mathbb{T} \cap \mathbb{R}$ et que les équations de cercles constructibles à partir de $\mathbb{T}$ sont de la forme

$$x^2 + y^2 + ax + by + c = 0$$

avec $a, b, c \in \mathbb{T} \cap \mathbb{R}$, avec leurs solutions de la forme $x + iy$. Si on cherche l'intersection de deux droites distinctes, on doit résoudre un système linéaire à coefficient dans $\mathbb{T} \cap \mathbb{R}$. Ses solutions sont donc toujours dans $\mathbb{T} \cap \mathbb{R}$. La solution induite par la solution du système est donc dans $\mathbb{T}$. Si on cherche les intersections d'une droite et d'un cercle, on doit exprime x en fonction de y avec l'équation de la droite et on résoud une équation de degré 2 pour trouver y. Alors, connaissant les formules de résolution des équations de degré 2 et sachant que $i \in \mathbb{T}$, on en déduit que $y \in \mathbb{T}$ et $x \in \mathbb{T}$. Si on cherche les intersections de deux cercles, on peut se ramener à un système droite-cercle en soustrayant la deuxième équation de la première. Bref, on a $c(\mathbb{T}) = \mathbb{T}$, et donc $K(\mathbb{T}) = \mathbb{T}$.

Théorème 12.3.1 : $K = \mathbb{T}$
Démonstration : Il est clair que $K \subset \mathbb{T}$. On va montrer que $K \in \mathcal{F}$. K est stable par conjugaison car si z est constructible, alors $\mathrm{Re}(z)$ et $\mathrm{Im}(z)$ aussi, et donc $\mathrm{Re}(z) - i\mathrm{Im}(z)$ aussi. Si $z = a + ib \in \mathbb{C}$ tel que $z^2 = c + id \in K$, alors $a^2 - b^2 = c$ et $2ab = d$, donc

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

donc $(2a^2 - c)^2$ est constructible et donc $2a^2 - c$ aussi. Comme c est constructible, a^2 aussi, et donc a est constructible. On en déduit que b est constructible. Bref, $z \in K$. $K \in \mathcal{F}$ donc $\mathbb{T} \subset K$, ce qui permet de conclure.

Proposition 12.3.3 : Soit $\Bbbk \subset \mathbb{K}$ une extension de degré 2 et de caractéristique nulle. Alors, il existe $x \in \mathbb{K}$ tel que $x^2 \in \Bbbk$ et $\mathbb{K} = \Bbbk(x)$.
Démonstration :

Théorème 12.3.2 : *(Wantzel)* Soit $z \in \mathbb{C}$. z est constructible si, et seulement si, il existe $r \geq 1$ et une tour $\mathbb{Q} = Q_0 \subset ... \subset Q_r$ de sous-extensions de $\mathbb{Q} \subset \mathbb{C}$ telles que $z \in Q_r$ et pour tout $0 \leq k \leq r-1$, $[L_{k+1} : L_k] = 2$.
Démonstration : On note (P) la propriété définie dans l'énoncé. On va montrer que les éléments de $\mathbb{C}$ qui

vérifient (P) sont constructibles, et que l'ensemble de ces éléments est un sous-corps de $\mathbb{C}$ qui appartient à $\mathcal{F}$.
Soit $z \in \mathbb{C}$ vérifiant (P). Alors $[Q_1 : Q_0] = 2$ donc on a $x_1 \in Q_1$ tel que $Q_1 = Q_0(x_1)$ et $x_1^2 \in Q_0$ **(P1.20)**.
$Q_0 = \mathbb{Q} \subset K$ donc x_1^2 est constructible. x_1 est aussi constructible selon **(P1.17)**. Il en découle que $Q_1 \subset K$. De la même manière, on montre que $Q_2, ..., Q_r \subset K$ et donc que $z \in K$. On se donne maintenant $z_1, z_2 \in \mathbb{C}^*$ vérifiant (P) et on note $\mathbb{Q} = Q_0 \subset ... \subset Q_q$ et $\mathbb{Q} = R_0 \subset ... \subset R_r$ des sous-extensions données par (P) ($z_1 \in Q_q$ et $z_2 \in R_r$).
Alors, $Q_q = Q_{q-1}(x_q)$ avec $x_q^2 \in Q_{q-1},\ ...,\ Q_1 = Q_0(x_1)$ avec $x_1^2 \in Q_0$ et $R_r = R_{r-1}(y_r)$ avec
$y_r^2 \in R_{r-1},\ ...,\ R_1 = R_0(y_1)$ avec $y_1^2 \in R_0$. On considère la tour d'extension :
$\mathbb{Q} = Q_0 \subset Q_0(x_1) \subset ... \subset Q_0(x_1, ..., x_q) \subset Q_0(x_1, ..., x_q, y_1) \subset ... \subset Q_0(x_1, ..., x_q, y_1, ..., y_r)$ que l'on note
$S_0 \subset ... \subset S_{q+r}$. Alors, les $[S_{i+1} : S_i]$ sont tous ≤ 2 donc en retirant les extensions "en double" on a une tour d'extension $S_0 \subset ... \subset S_s$ telle que les $[S_{i+1} : S_i] = 2$ et $z_1, z_2 \in S_s$. On en déduit que $z_1 + z_2,\ z_1 z_2,\ z_1^{-1},\ z_2^{-1}$ vérifient (P), et donc que l'ensemble des éléments de $\mathbb{C}$ qui vérifient (P) est un corps. Si $z^2 \in \mathbb{C}$ vérifie (P), on a $\mathbb{Q} = Q_0 \subset ... \subset Q_r$ tels que $z^2 \in Q_r$ et les $[Q_{i+1} : Q_i] = 2$. Mais z est racine du polynôme $X^2 - z^2$ qui est à coefficient dans Q_r, donc z est algébrique sur Q_r de degré ≤ 2. Si $z \in Q_r$, alors la tour $Q_0 \subset ... \subset Q_r$ fait l'affaire, sinon on prend $Q_0 \subset ... \subset Q_r \subset Q_r(z)$. z vérifie bien (P). $\bar{z}$ vérifie aussi (P) car la tour d'extension est de la forme $\mathbb{Q} \subset \mathbb{Q}(x_1) \subset ... \subset \mathbb{Q}(x_1, ..., x_r)$ donc la tour $\mathbb{Q} \subset \mathbb{Q}(\bar{x_1}) \subset ... \subset \mathbb{Q}(\bar{x_1}, ..., \bar{x_r})$ convient. On en déduit que l'ensemble des éléments vérifiant (P) est un élément de $\mathcal{F}$ et donc qu'il contient $\mathbb{T} = K$. Cet ensemble est donc K.

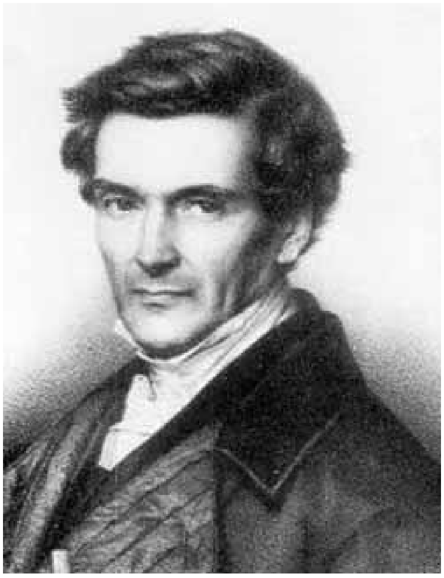


Figure 14: Pierre-Laurent Wantzel, 1814 - 1848

Proposition 12.3.4 : Tout élément de K est algébrique et son degré est une puissance de 2.
Démonstration : Soit $z \in K$. On note $\mathbb{Q} = Q_0 \subset ... \subset Q_r$ comme en **(T1.3)**. Alors,

$$2^r = [Q_r : \mathbb{Q}] = [Q_r : \mathbb{Q}(z)] \times [\mathbb{Q}(z) : \mathbb{Q}]$$

donc $[\mathbb{Q}(z) : \mathbb{Q}]$ est fini et c'est une puissance de 2.

Théorème 12.3.3 : *(Problème de la duplication du cube)* On cherche à savoir si, étant donné un cube C_1 de côté 1 (et donc de volume 1), il est possible de construire un cube C_2 de volume 2. Si c'était possible, C_2 aurait des côtés de longueur $\alpha = \sqrt[3]{2}$ *(constante de Délos)*. Mais α est racine du polynôme $X^3 - 2$, qui est irréductible sur $\mathbb{Q}$ selon le critère d'Eisenstein, donc c'est son polynôme minimal. Le degré de α n'est pas une puissance de 2, donc α n'est pas constructible. On ne peut pas construire C_2.

Théorème 12.3.4 : *(Problème de la trisection de l'angle)* On a vu plus haut qu'étant donné un point constructible $A = e^{i\theta}$, il était possible de construire sa "racine carrée", puisque cela cela revient à construire la bissectrice de l'angle entre la droite réelle et la droite $\mathcal{D}_{0,A}$. On se demande maintenant s'il est possible de construire la "trisectrice" de cet angle. Cela revient à construire les réels $\cos(\theta/3)$ et $\sin(\theta/3)$. Remarquons d'abord que

$$(2\cos(\frac{\theta}{3}))^3 = (e^{i\theta} + e^{-i\theta})^3 = 2\cos(\theta) + 6\cos(\frac{\theta}{3})$$

et donc $2\cos(\frac{\theta}{3})$ est racine de $X^3 - 3X - 2\cos(\theta)$. Prenons $\theta = \frac{\pi}{3}$. Alors $e^{i\theta} = \frac{\sqrt{3}}{2} + \frac{i}{2}$ est constructible et $2\cos(\theta)$ est racine de $X^3 - 3X - 1$ qui est irréductible sur $\mathbb{Q}$ (on montre qu'il est irréductible sur $\mathbb{Z}$, ce n'est pas très compliqué mais un peu long à écrire). On en déduit que $2\cos(\frac{\theta}{3})$ n'est pas constructible, donc $\cos(\frac{\theta}{3})$ non plus. La trisection de l'angle n'est *en général* pas possible.

12.4 Quelques nombres transcendants

Théorème 12.4.1 : L'ensemble $\hat{\mathbb{Q}}$ des nombres complexes algébrique sur $\mathbb{Q}$ est dénombrable.
Démonstration : Pour tout $n \in \mathbb{N}$, l'ensemble des polynômes à coefficients entiers de degré strictement inférieur à n est en bijection avec $\mathbb{Z}^n$, donc dénombrable. $\mathbb{Z}[X]$, qui est l'union de ces ensembles, est alors dénombrable. On note $\sim$ la relation d'équivalence définie sur $\hat{\mathbb{Q}}$ par $x \sim y$ si et seulement si $\mu_x = \mu_y$. Alors, on peut injecter $\hat{\mathbb{Q}}/\sim$ dans $\mathbb{Z}[X]$ en envoyant $\bar{x}$ sur $k\mu_x$ où k un entier tel que $k\mu_x \in \mathbb{Z}[X]$. Comme, $\hat{\mathbb{Q}} = \cup_{C \in \hat{\mathbb{Q}}/\sim} C$, c'est une réunion dénombrable d'ensemble dénombrables (finis), donc $\hat{\mathbb{Q}}$ est dénombrable.

Remarque : $\mathbb{R}$ n'étant pas dénombrable, on en déduit que $\mathbb{R} \setminus \hat{\mathbb{Q}}$ est non vide. Il existe des nombres transcendants.

Théorème 12.4.2 : *(Liouville)* Soit $x \in \mathbb{R} \setminus \mathbb{Q}$.

1. Si x est algébrique de degré n, il existe $\alpha > 0$ tel que pour tout $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$, $|x - \frac{a}{b}| \geq \frac{\alpha}{b^n}$.
2. Si pour tout $k \in \mathbb{N}^*$, il existe $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $b \geq 2$ et $|x - \frac{a}{b}| < \frac{1}{b^k}$, alors x est transcendant.
3. Le nombre *(de Liouville)* $\sum_{k=0}^{\infty} \frac{1}{10^{k!}}$ est transcendant.

Démonstration : (1) : Soit $q\mu_x = (X - x)Q = m_0 + ... + m_n X^n \in \mathbb{Z}[X]$ avec $q \in \mathbb{N}^*$. Pour tout $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $|x - \frac{a}{b}| \geq 1$, on a $|x - \frac{a}{b}| \geq \frac{1}{b^n}$. Par ailleurs, on a un réel $\beta > 0$ tel que pour tout $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $|x - \frac{a}{b}| < 1$, $|Q(\frac{a}{b})| < \alpha$ car Q est borné sur toute partie bornée de $\mathbb{R}$. $b^n q\mu_x(\frac{a}{b}) \in \mathbb{Z}^*$ car μ_x est irréductible sur $\mathbb{Q}$ donc ne s'annule pas sur $\frac{a}{b}$. On a alors $|b^n q(X - \frac{a}{b})Q(\frac{a}{b})| \geq 1$ donc $|x - \frac{a}{b}| \geq \frac{1}{b^n q|Q(\frac{a}{b})|} \geq \frac{1}{b^n q\beta}$. En prenant $\alpha = \min(\frac{1}{q\beta}, 1)$, on a le résultat. (2) : Supposons que x soit algébrique de degré n. Alors, selon (1), on peut trouver $\alpha \leq 1$ tel que pour tout $(c, d) \in \mathbb{Z} \times \mathbb{N}^*$, $|x - \frac{c}{d}| \geq \frac{\alpha}{d^n}$. On peut aussi trouver $m \in \mathbb{N}$ tel que $\frac{1}{2^m} \leq \alpha$. En appliquant notre hypothèse pour $k = n + m$, on a $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $b \geq 2$ et $|x - \frac{a}{b}| < \frac{1}{b^{n+m}}$. Ainsi, $\frac{1}{b^{m+n}} \leq \frac{1}{2^m b^n} \leq \frac{\alpha}{b^n} \leq |x - \frac{a}{b}| < \frac{1}{b^{m+n}}$, ce qui est absurde. x n'est donc pas algébrique. (3) : On va montrer que ce nombre vérifie (2). Soit $n \in \mathbb{N}^*$. Alors,

$$x = \sum_{k=0}^{n} \frac{1}{10^{k!}} + \sum_{k=n+1}^{\infty} \frac{1}{10^{k!}} = \frac{10^{n!} \sum_{k=0}^{n} \frac{1}{10^{k!}}}{10^{n!}} + \sum_{k=n+1}^{\infty} \frac{1}{10^{k!}}$$

donc en posant $a = 10^{n!} \sum_{k=0}^{n} \frac{1}{10^{k!}}$ et $b = 10^{n!}$, on a $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ et

$$|x - \frac{a}{b}| = \sum_{k=1}^{\infty} \frac{1}{10^{(n+k)!}}$$

Or, pour tout $k \geq 1$, $(n + k)! - nn! \geq k$ donc

$$\sum_{k=1}^{\infty} \frac{1}{10^{(n+k)!}} = \frac{1}{10^{nn!}} \sum_{k=1}^{\infty} \frac{1}{10^{(n+k)! - nn!}} \leq \frac{1}{10^{nn!}} \sum_{k=1}^{\infty} \frac{1}{10^k} < \frac{1}{10^{nn!}} \sum_{k=0}^{\infty} \frac{1}{10^k} = \frac{1}{10^{nn!}} \times \frac{9}{10} < \frac{1}{10^{nn!}}$$

On en déduit que $|x - \frac{a}{b}| < \frac{1}{b^n}$. Le nombre $\sum_{k=0}^{\infty} \frac{1}{10^{k!}}$ est donc transcendant.

Figure 15: Joseph Liouville, 1809 - 1882

Lemme (1) : Soit $P \in \mathbb{C}[X]$ de degré n. On note $D(P)$ le polynôme $P + P' + ... + P^{(n)}$. Alors, pour tout $x \in \mathbb{C}$,

$$e^x D(P)(0) - D(P)(x) = xe^x \int_0^1 e^{-xt} P(xt)dt$$

Démonstration : On le montre sans problème par récurrence sur le degré de P et en faisant une intégration par partie.

Lemme (2) : Soient $P = a_0 + ... + a_n X^n \in \mathbb{Z}[X]$ de degré n et $m \geq 2 \in \mathbb{N}$. On pose $Q = \frac{X^{m-1}}{(m-1)!}P$. Alors $D(Q)(0)$ est un entier et $D(Q)(0) = a_0$ $[m]$.
Démonstration : $Q = \frac{1}{(m-1)!}(a_0 X^{m-1} + a_1 X^m + ... + a_n X^{n+m-1})$ donc pour tout $i \in \{0, ..., m-2\}$, $Q^{(i)}(0) = 0$. On remarque que

$$Q^{(m-1)} = \frac{1}{(m-1)!}((m-1)!a_0 + m(m-1)...(m-(m-1)+1)a_1 X + ... + (n+m-1)...(n+1)a_n X^n)$$

et pour tout $k \in \{1, ..., n\}$

$$Q^{(m-1+k)} = \frac{1}{(m-1)!}((m+k-1)!a_k + ... + (n+m-1)...(n-k+1)a_n X^{n-k})$$

Alors,

$$D(Q)(0) = \sum_{k=0}^{n} \frac{(m-1+k)!}{(m-1)!} a_k = a_0 + \sum_{k=1}^{n} (m+1-k)...m \times a_k = a_0 \ [m]$$

Théorème 12.4.3 : *(Hermite)* Le nombre e est transcendant.
Démonstration : On suppose que e est algébrique et on se donne $P = a_0 + ... + a_n X^n \in \mathbb{Z}[X]$ de degré $n > 0$ tel que $P(e) = 0$. Pour nombre premier p, on note $Q_p = \frac{X^{p-1}}{(p-1)!}(X-1)^p...(X-n)^p$. Alors, pour tout $k \in \{1, ..., n\}$,

$$Q_p(X+k) = \frac{X^{p-1}}{(p-1)!} X(X+k)^{p-1} \prod_{i \neq k} (X+k-i)$$

En appliquant le lemme **(2)**, on a $D(Q_p)(k) = D(Q_p(X+k))(0) = 0$ $[p]$ et $D(Q_p)(0) = (-1)^{np}(n!)^p$ $[p]$. En appliquant le lemme **(1)**, on a

$$\sum_{k=0}^{n} a_k(e^k D(Q_p)(0) - D(Q_p)(k)) = \sum_{k=0}^{n} a_k k e^k \int_0^1 e^{-kt} Q_p(kt)dt$$

donc

$$D(Q_p)(0)P(e) - \sum_{k=0}^{n} a_k D(Q_p)(k) = \sum_{k=1}^{n} k e^k \int_0^1 e^{-kt} Q_p(kt)dt$$

et donc

$$-\sum_{k=0}^{n} a_k D(Q_p)(k) = \sum_{k=1}^{n} k e^k \int_0^1 e^{-kt} Q_p(kt)dt$$

La quantité de gauche est congrue à $-a_0(-1)^{np}(n!)^p$ modulo p donc si $p > \max(|a_0|, n)$, elle n'est pas divisible par p. En particulier, pour tout $p > \max(|a_0|, n)$, on a

$$|\sum_{k=0}^{n} a_k D(Q_p)(k)| > 1$$

Or, chaque terme de la quantité de droite tend vers 0 quand p tend vers $+\infty$. En effet, pour tout $k \in \{1, ..., n\}$,

$$|\int_0^1 e^{-kt} Q_p(kt)dt| \leq \int_0^1 |Q_p(kt)|dt \leq \frac{1}{(p-1)!}(n!)^p \underset{p \to +\infty}{\sim} \frac{n!}{\sqrt{2\pi(p-1)}} (\frac{en!}{(p-1)!})^{p-1}$$

On a donc

$$\lim_{p \to +\infty} |\sum_{k=0}^{n} a_k D(Q_p)(k)| \geq 1 \quad \text{et} \quad \lim_{p \to +\infty} |\sum_{k=1}^{n} k e^k \int_0^1 e^{-kt} Q_p(kt)dt| = 0$$

ce qui est absurde. e est donc transcendant.

Figure 16: Charles Hermite, 1822 - 1901

Définition 12.4.1 : Soient $n \in \mathbb{N}^*$ et $P \in \mathbb{Z}[X_1, ..., X_n]$. On dit que P est **symétrique** lorsque pour tout $\sigma \in S_n$, on a $P(X_1, ..., X_n) = P(X_{\sigma(1)}, ..., X_{\sigma(n)})$. Pour tout $k \in \{1, ..., n\}$, on note

$$\theta_k = \sum_{1 \leq i_1 < ... < i_k \leq n} X_{i_1} ... X_{i_k}$$

Il est clair que les θ_k sont symétriques. On les nomme **polynômes symétriques élémentaires**.

Lemme (3) : Soient $n \in \mathbb{N}^*$ et $P \in \mathbb{Z}[X_1, ..., X_n]$ symétrique. Alors, il existe $Q \in \mathbb{Z}[X_1, ..., X_n]$ tel que $P = Q(\theta_1, ..., \theta_k)$.
Démonstration : On admet ce résultat, mais il est démontré en [8].

Lemme (4) : Soit $P = a_0 + ... + a_m X^m \in \mathbb{Z}[X]$. On note $P = a_m(X - r_1)...(X - r_m)$ sa décomposition dans $\mathbb{C}[X]$. Soit $\phi \in \mathbb{Z}[X_1, ..., X_m]$ un polynôme symétrique. Alors $\phi(a_m r_1, ..., a_m r_m)$ est un entier.
Démonstration : Selon **(3)**, on a $\gamma \in \mathbb{Z}[X_1, ..., X_m]$ tel que $\phi = \gamma(\theta_1, ..., \theta_m)$. On peut écrire les relations coefficients-racines de P : pour tout $k \in \{1, ..., m\}$,

$$\theta_k(r_1, ..., r_m) = (-1)^k \frac{a_{m-k}}{a_m}$$

On en déduit que pour tout $k \in \{1, ..., m\}$,

$$\theta_k(a_m r_1, ..., a_m r_m) = (-1)^k a_{m-k} a_m^k \in \mathbb{Z}$$

Alors,

$$\phi(a_m r_1, ..., a_m r_m) = \gamma(\theta_1(a_m r_1, ..., a_m r_m), ..., \theta_m(a_m r_1, ..., a_m r_m)) = \gamma(-a_{m-1} a_m, ..., (-1)^m a_0 a_m^m) \in \mathbb{Z}$$

Théorème 12.4.4 : *(Lindemann)* Le nombre π est transcendant.
Démonstration : On suppose que π est algébrique. Alors $i\pi$ est algébrique. On se donne $P = a_0 + ... + a_m X^m \in \mathbb{Z}[X]$ de degré $m > 0$ tel que $P(i\pi) = 0$. On note $P = a_m(X - r_1)...(X - r_m)$ sa décomposition dans $\mathbb{C}[X]$, $\mathcal{P} = \{J_1, ..., J_{2^m-1}\}$ l'ensemble des parties non vides de $\{1, ..., m\}$ et pour tout $k \in \{1, ..., 2^m - 1\}$, $\alpha_k = \sum_{j \in J_k} r_j$. Alors,

$$\prod_{k=1}^{m}(1 + e^{r_k}) = 1 + \sum_{k=1}^{2^n-1} e^{\alpha_k} = 0$$

car $i\pi \in \{r_1, ..., r_m\}$. Quitte à renuméroter, on suppose que la famille $(\alpha_1, ..., \alpha_{2^m-1})$ est de la forme $(\alpha_1, ..., \alpha_q, 0, ..., 0)$ avec tous les α_k non nuls pour $k \in \{1, ..., q\}$ et $q \in \{1, ..., 2^m - 1\}$. Pour tout p premier, on pose $Q_p = (a_m)^{qp+p-1} \frac{X^{p-1}}{(p-1)!}(X - \alpha_1)^p...(X - \alpha_q)^p$ et $R_p = (p-1)! \sum_{k=1}^{q} Q_p(X + \alpha_k)$. Alors,

$$R_p = (a_m X)^p X^{p-1} \sum_{k=1}^{q}(a_m X - a_m \alpha_k)^{p-1}(\prod_{i \neq k}(a_m X + a_m(\alpha_k - \alpha_i)))^p$$

On remarque que les coefficients de R_p sont de la forme $\phi(a_m \alpha_1, ..., a_m \alpha_q)$ avec $\phi \in \mathbb{Z}[X_1, ..., X_q]$ symétrique. Ils sont donc entiers. En effet, en notant toujours θ_k les polynômes symétriques élémentaires de $\mathbb{Z}[X_1, ..., X_q]$, θ'_k ceux de $\mathbb{Z}[X_1, ..., X_{2^m-1}]$ et $T_J = \sum_{i \in J} X_i$ pour tout $J \in \mathcal{P}$, on remarque que les $S_k = \theta'_k(T_{J_1}, ..., T_{J_{2^m-1}})$ sont symétriques. Comme les $a_m \alpha_i$ sont les $T_J(a_m r_1, ..., a_m r_m)$, on a

$$\theta_k(a_m \alpha_1, ..., a_m \alpha_q) = \theta'_k(a_m \alpha_1, ..., a_m \alpha_{2^m-1}) = S_k(a_m r_1, ..., a_m r_m)$$

Ainsi, selon **(4)**, les $\theta_k(a_m \alpha_1, ..., a_m \alpha_q)$ sont entiers et donc comme tout polynôme symétrique $\phi \in \mathbb{Z}[X_1, ..., X_n]$ s'écrit $\phi = \gamma(\theta_1, ..., \theta_q)$, on a bien que

$$\phi(a_m \alpha_1, ..., a_m \alpha_q) = \gamma(\theta_1(a_m \alpha_1, ..., a_m \alpha_q), ..., \theta_q(a_m \alpha_1, ..., a_m \alpha_q)) \in \mathbb{Z}$$

On peut donc appliquer le lemme **(2)** à $\frac{R_p}{(p-1)!}$ et en déduire que $\sum_{k=1}^{q} D(Q_p)(\alpha_k) = 0$ $[p]$. Alors, selon le lemme **(1)**, on a

$$(1+\sum_{k=1}^{q} e^{\alpha_q} + 2^m - 1 - q)D(Q_p)(0) - \sum_{k=1}^{q} D(Q_p)(\alpha_k) - (2^m - q - 1)D(Q_p)(0) = \sum_{k=1}^{q} \alpha_k e^{\alpha_k} \int_0^1 e^{-\alpha_k t} Q_p(\alpha_k t)dt$$

et donc

$$-(\sum_{k=1}^{q} D(Q_p)(\alpha_k) + (2^m - q - 1)D(Q_p)(0)) = \sum_{k=1}^{q} \alpha_k e^{\alpha_k} \int_0^1 e^{-\alpha_k t} Q_p(\alpha_k t)dt$$

Selon **(2)**, le terme de gauche est congru à $(2^m - 1 - q)(-1)^{qp}(a_m)^{p-1}(\prod_{k=1}^{q} a_m \alpha_k)^p$ $[p]$. Ainsi, pour tout $p > \max(2^m - q - 1, |a_m|^{p-1}, |\prod_{k=1}^{q} a_m \alpha_k|^p)$ p ne divise pas le terme de gauche, qui est donc supérieur à 1 en valeur absolue. On conclut comme en **(T12.8)** en montrant que le terme de droite tend vers 0 lorsque p tend vers $+\infty$, ce qui est absurde.

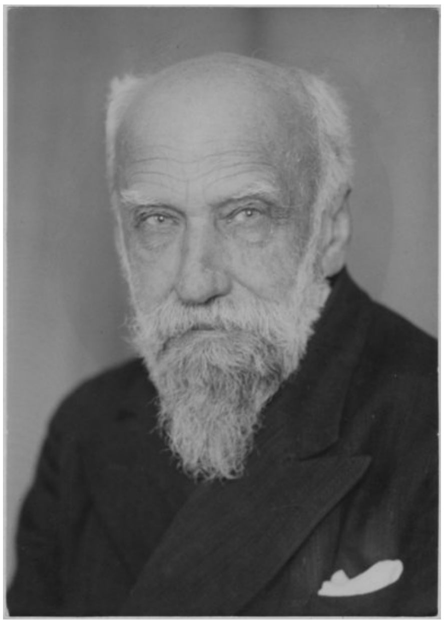


Figure 17: Ferdinand von Lindemann, 1852 - 1939

Théorème 12.4.5 : *(Problème de la quadrature du cercle)* Étant donné un cercle $\mathcal{C}$ de rayon 1, on souhaite construire un carré dont l'aire est celle de $\mathcal{C}$ c'est-à-dire π. Un tel carré est impossible à construire car il serait nécéssairement de côté $\sqrt{\pi}$, qui n'est pas constructible car π est transcendant.

13 Quelques plans de preuve

T1.1 : On note $\mathcal{R}$ la relation d'équivalence à gauche sur H définie sur G par $x\mathcal{R}y \Leftrightarrow x^{-1}y \in H$. Soit $x \in G$.

1. Déterminer la classe $[x]$ de x.
2. Quel est son cardinal ?
3. En déduire le théorème.

T1.4 : Pour tout $k \in \{1, ..., p\}$, on note $X_k = \{(g_1, ..., g_k) \in G^k,\ g_1...g_k = 1\}$.

1. Déterminer le cardinal de X_p.
2. Montrer que l'application $m : \mathbb{Z}/p\mathbb{Z} \times X_p \to G^p,\ [k] \mapsto (g_k, ...g_p, g_1, ...g_{k-1})$ définit une action de groupe de $\mathbb{Z}/p\mathbb{Z}$ sur X_p.
3. On suppose que G ne contient pas d'élément d'ordre p. Montrer que $c = (e, ..., e)$ est le seul élément de X_p tel que $\mathrm{Card}(\omega_c) = 1$. En déduire que $\mathrm{Card}(X_p) = 1 \bmod p$. Conclure.

T2.3 :

1. Montrer qu'il existe $r \in \mathbb{R}_+$ tel que pour tout $z \in \mathbb{C},\ |z| > r \Longrightarrow |P(z)| > |P(0)|$. Une racine de P ne peut donc se trouver ailleurs que dans la boule $B(0, r)$.
2. En utilisant le théorème de Bolzano-Weirestrass, montrer qu'il existe $x_0 \in B(0, r)$ tel que $|P(x_0)| = \inf \{|P(z)|,\ z \in B(0, r)\}$.
3. Montrer qu'il existe $a \in \mathbb{C}^*,\ Q \in \mathbb{C}[X]$ et $k \in \mathbb{N}^*$ tels que pour tout $z \in \mathbb{C},\ P(z) = P(x_0) + (z - x_0) + a(z - x_0)^k + Q(z)(z - x_0)^{k+1}$.
4. On suppose que $P(x_0) \neq 0$. En considérant une racine k-ème u de $\frac{-P(x_0)}{a}$, montrer qu'il existe $t \in [0, 1]$ tel que $|P(x_0 + tu)| < |P(x_0)|$.
5. Conclure.

T3.1 : On va raisonner par récurrence sur le cardinal de $\mathbb{K}$. On suppose que tout sous-corps de $\mathbb{K}$ de cardinal strictement inférieur à celui de $\mathbb{K}$ est commutatif. On note $\mathcal{Z}(\mathbb{K}) = \{x \in \mathbb{K},\ \forall y \in \mathbb{K},\ xy = yx\}$, q le cardinal de $\mathcal{Z}(\mathbb{K})$, et pour tout $x \in \mathbb{K},\ \mathbb{K}_x = \{y \in \mathbb{K},\ yx = xy\}$.

1. Montrer que $\mathbb{K}$ est un $\mathcal{Z}(\mathbb{K})$-espace vectoriel de dimension finie, notée n. En déduire que le cardinal de $\mathbb{K}$ est q^n. Si $n = 1$, le résultat est immédiat, on suppose que $n > 1$.
2. Soit $x \in \mathbb{K} \setminus \mathcal{Z}(\mathbb{K})$. Montrer que le cardinal de $\mathbb{K}_x$ est de la forme q_x^d avec d_x un diviseur strict de n.
3. A l'aide de l'équation aux classes, montrer qu'il existe une famille d'entier $(\lambda_d)_{d<n,\ d|n}$ tels que
$$q^n - 1 = q - 1 + \sum_{d<n,\ d|n} \frac{q^n - 1}{q^d - 1}$$
4. Soit $k \in \mathbb{N}^*$. Montrer que $e^{i\frac{2p\pi}{k}}$ engendre le groupe $\mathbb{U}_k$ si et seulement si $k \wedge p = 1$. On appelle ces éléments les racines **primitives** k-ème de l'unité. On note $\phi_k = \prod_{r\in\mathbb{V}_k}(X - r)$ le polynôme cyclotomique d'ordre k, où $\mathbb{V}_k$ est l'ensemble des racines k-èmes primitives de l'unité. On rappelle que $\varphi(k)$ est le nombre d'entiers positifs et inférieurs à k qui sont premiers avec k (et donc le cardinal de $\mathbb{V}_k$).
5. Montrer que $k = \sum_{d|k} \varphi(k)$. En déduire que $\mathbb{U}_k = \sqcup_{d<k,\ d|k}\mathbb{V}_d$ et que $X^k - 1 = \prod_{d<k,\ d|k} \phi_d$.
6. Par récurrence, montrer que $\phi_k \in \mathbb{Z}[X]$.

7. En déduire que $\phi_n(q)$ divise $q-1$.

8. En montrant que pour tout $r \in \mathbb{U} \setminus \{1\}$, $|q-r| > |q-1|$, obtenir une contradiction.

T3.2 : On note n le cardinal de $\mathbb{K}^*$.

1. Soit G un groupe fini d'ordre n. Montrer que si pour tout diviseur d de n, il y a au plus d éléments x tels que $x^d = 1$, alors G est cyclique. *(Indication : Il va falloir utiliser la formule de Möbius $n = \sum_{d|n} \varphi(d)$.)*

2. En déduire le théorème.

T3.5 : On note $f : x \mapsto x^p$.

1. Montrer que f est un morphisme de $\mathbb{K} \to \mathbb{K}$ et que $f^n = \mathrm{id}$.

2. En déduire que f est d'ordre n dans $\mathrm{Aut}(\mathbb{K})$. *(Indication : Par l'absurde)*

3. On suppose que l'on peut trouver $f_1, ..., f_{n+1}$ éléments distincts dans $\mathrm{Aut}(\mathbb{K})$. Soit $(e_1, ..., e_n)$ une $\mathbb{F}_p$-base de $\mathbb{K}$. En s'intéressant à la matrice dont les coefficients sont les $f_i(e_j)$, obtenir une contradiction avec le *Lemme de Dedekind* **(T3.4)**.

4. Conclure.

T3.6 : On note $P = X^{p^n} - X$ et, pour tout $d \in \{1, ..., n\}$, I_d l'ensemble des polynômes irréductibles sur $\mathbb{F}_p$ unitaires de degré d.

1. Montrer que $Q \in I_d$ divise P si, et seulement si, d divise n.

2. En déduire que $P = \prod_{d|n}(\prod_{Q \in I_d} Q)$.

3. En déduire une expression pour $\mathrm{Card}(I_n)$ et montrer qu'il est strictement positif.

4. Soit $\mathbb{K}$ un corps de cardinal p^n. En prenant $Q \in I_n$, montrer que Q admet une racine dans $\mathbb{K}$. En déduire que $\mathbb{K}$ est isomorphe à $\mathbb{F}_p[X]/(Q)$.

14 Références et bibliographie

1. Tauvel, Patrice. *Corps commutatifs et théorie de Galois - Troisième édition.* Calvage & Mounet, 2021.

2. Laszlo, Yves. *Introduction à la théorie de Galois.* École Polytechnique, CMLS, 2010.

3. Gourdon, Xavier. *Les Maths en tête - Algèbre.* Ellipses, 2009.

4. Perrin, Daniel. *Résolution par radicaux.* –, –.

5. Stewart, Ian. *Galois Theory.* Chapmann-Hall, 1973.

6. Chambert-Loir, Antoine. *Algèbre Corporelle.* École Polytechnique, 2005.

7. Callet, Victoria. *Résolubilité par radicaux - Comparaison de deux moments historiques : Gauss et Galois.* Université de Strasbourg, 2018.

8. Diez, Antoine. *Le théorème de structure des polynômes symétriques.* E.N.S. Rennes, -.

9. Exo7.emath.fr. *Cours de mathématiques - Groupes.*

10. Conrad, Keith. *The Galois group of* $X^n - X - 1$ *over* $\mathbb{Q}$. University of Connecticut, -.