Corps et Théorie de Galois

Magerin Christophe

Résumé

— équation de degré 2, équation de degré 3(Cardan), équation de degré 4(Ferrari)
(Abel) Il existe une équation de degré 5 non-résoluble par radicaux.
(Galois) L'objet essentiel : sous-groupe du groupe des permutations des racines qui preservent toutes les identités à coefficients rationnels satisfaits par les racines : $\sigma_k(x_1, \cdots, x_n) = (-1)^k a_k$. Si c'est d'autres relations, le groupe de Galois peut être plus petit. Ce groupe conditionne la propriété d'oui ou non résoluble par radicaux. C'est à dire que $Gal(P)$ est résoluble s.s.i. l'équation $P(X) = 0$ est résoluble par radicaux.

— construction à la règle et au compus (extension de corps)
Par exemple, quadrature du cercle est impossible.

— construction de polygones réguliers
Par exemple, 17-gone est constructible(Gauss).

— équations polynômials et équations différentielles linéairs homogènes

— transcendance : π, $e = 2.718\cdots$, $\cdots$
En amont, on sait le théorème fondamental de l'algèbre.

— polynômes et leurs racines
  — corps de rupture
  — corps de décomposition
  — clôture algébrique

— extensions normales

— séparabilité(multiplicité des racines)

— théorie de Galois

Table des matières

Première partie

Rappel

1 Anneaux unitaire et Idéaux

$(A, +, \cdot)$ est un anneau si on suppose que

- $(A, +)$ est un groupe abélien ;
- $(A, \cdot)$ est un monoïde unitaire ;
- $\cdot$ et $+$ sont compatibles, i.e. $a(b + c) = ab + ac$ pour tous a, b, $c \in A$.

Si on suppose plus que

- $(A, \cdot)$ est un monoïde abélien alors on appelle A un anneau commutatif ;
- $1 = 0$ alors $A = \{0\}$ est banal.

On sait bien que 0 est absorbant i.e. $0 \cdot a = 0$ pour tout $a \in A$.

Définition 1.1. Un anneau est dit **réduit** si 0 est le seul élément.

Définition 1.2. $A^* := \{a \in A,\ \exists b \in A,\ ab = 1\}$, on les appelle les unités de A.

Définition 1.3. On appelle A un anneau intègre si a, $b \in A$, $ab = 0 \Rightarrow a = b = 0$. Si on suppose plus que tout élément non nul est inversible i.e. $A^* = A \setminus \{0\}$, alors on appelle A un corps.

Définition 1.4. Soit A un anneau intègre. On définit une relation d'équivalence $\sim$ sur $A \times (A \setminus \{0\})$: $(a, b) \sim (c, d)$ s.s.i. $ad = bc$. On note $K_A = \big(A \times (A \setminus \{0\})\big)/\sim$. On donne l'addition et la multiplication dans K_A comme :

- $[(a, b)] + [(c, d)] = [(ad + bc, bd)]$;
- $[(a, b)] \cdot [(c, d)] = [(ac, bd)]$.

Alors K_A devient un corps.

Lemme 1.5. *Soit A un anneau intègre. Alors $A[X]$ est aussi un anneau intègre.*

Démonstration. Soit P, $Q \in A[X]$ et $\deg P$, $\deg Q \geq 1$. On suppose $P(X) = \sum_{k=0}^{d} a_k X^k$ et $Q(X) = \sum_{k=0}^{D} b_k X^k$, où $a_d \neq 0$, $b_D \neq 0$. Alors

$$PQ = a_d b_D X^{d+D} + \sum_{k=0}^{d+D-1} \alpha_k X^k.$$

A est intègre implique $a_d b_D \neq 0$, donc $PQ \neq 0$.
En plus, on trouve que $\deg PQ = \deg P + \deg Q$. $\square$

Lemme 1.6. *Soit A un anneau intègre. Alors $A[X]^* = A^*$.*

Démonstration. Soit P, $Q \in A[X]$ et $PQ = 1$. Car $\deg PQ = \deg P + \deg Q$, on obtient que $\deg P = \deg Q = 0$. Alors $P(X) = a \in A$, donc $A[X]^* = A^*$. $\square$

Remarque 1.7. Dans un anneau quelconque (non nécessairement intègre) le résultat précédant est faux. Par exemple, posons $A = (\mathbb{Z}/4\mathbb{Z})$, on considère $P(X) = 2X + 1 \in A[X]$, alors $P^2(X) = 1 \Rightarrow P \in A[X]^*$.
Question : caractériser les unités de $A[X]$.

Sorite 1.8. *Soient a, $b \in A$ nilpotents, alors $a + b$ est nilpotent.*

Démonstration. On suppose $a^N = b^M = 0$, alors $(a+b)^{N+M-1} = \sum_{k=0}^{N+M-1} \binom{N+M-1}{k} a^k b^{N+M-1-k} = 0$. $\square$

Corollaire 1.9. *$N(X) = P(X) - a_0$ est nilpotent.*

Lemme 1.10. *Soit A un anneau. Soient $a \in A$ nilpotent et $b \in A$ inversible. Alors $a + b$ est inversible.*

Démonstration. On suppose $a^m = 0$, alors $a + b = b(1 + b^{-1}a) = b\Big(\sum_{k\in\mathbb{N}} (-1)^k b^{-k} a^k\Big)^{-1} = b\Big(\sum_{k=0}^{m-1} (-1)^k b^{-k} a^k\Big)^{-1}$ est inversible. $\square$

Proposition 1.11. *Soit A un anneau, alors $P(X) = \sum_{k=0}^{n} a_k X^k \in A[X]^*$ s.s.i. $a_0 \in A^*$ et a_i est nilpotent pour tout $i \in [\![1, n]\!]$.*

Démonstration. $\Leftarrow$: P est inversible par la sorite 1.8 et le lemme 1.10.
$\Rightarrow$: Il existe $Q = \sum_{k=0}^{m} b_k X^k \in A[X]$ tel que $PQ = 1$, on obtient directement $a_n b_m = 0$ et $a_0 b_0 = 1$.

On applique la méthode de récurrence pour montrer que $a_n^{k+1}b_{m-k} = 0$ pour tout $k \in [\![0, m]\!]$.

$$\begin{aligned} 0 &= \sum_{k=0}^{\min\{l+1,n\}} a_{n-k}b_{m-l-1+k} \\ \Rightarrow 0 &= a_n^{l+1} \sum_{k=0}^{\min\{l+1,n\}} a_{n-k}b_{m-l-1+k} \\ &= \sum_{k=0}^{\min\{l+1,n\}} a_{n-k}a_n^{l+1}b_{m-l-1+k} \\ \text{(l'hypothèse de récurrence)} &= a_n^{l+2}b_{m-l-1}. \end{aligned}$$

Alors $0 = a_n^{m+1}b_0 \Rightarrow 0 = a_n^{m+1} \Rightarrow a_n$ est nilpotent. Ensuite on sait que $P(X) - a_nX^n$ est encore inversible par le lemme 1.10. On applique la méthode de récurrence à $\deg P$ et on conclut que a_i est nilpotent pour tout $i \in [\![1, n]\!]$. $\square$

Définition 1.12. Soit A un anneau et soit I une partie de A. On appelle I **un idéal de** A si

— I est un sous-groupe de $(A, +)$;
— pour tout $(a, i) \in A \times I$, $ai \in I$.

Après on suppose A un anneau et I un idéal de A dans cette section.

Théorème 1.13. *A/I est bien défini et possède une structure naturelle d'anneau comme un quotient. La surjection canonique $\omega : A \to A/I$ est un morphisme d'anneaux.*

Sorite 1.14. *Soit B un anneaux et soit $f : A \to B$ un morphisme d'anneaux. Alors $\ker f$ est un idéal de A, $\operatorname{Im} f$ est un sous-anneau de B.*

Remarque 1.15. Mais $\operatorname{Im} f$ n'est pas en général un idéal de B. Posons $B = A \times A$ et $f = diag$: $\begin{array}{ccc} A & \longrightarrow & B \\ a & \longmapsto & (a,a) \end{array}$. Alors $\operatorname{Im} diag = \{(a, a),\ a \in A\}$ est l'ensemble de diagonal. $(1, 1) \in \operatorname{Im} diag$, mais $(1, 1)(a, b) = (a, b) \notin \operatorname{Im} diag$ si $a \neq b$, donc ce n'est pas un idéal.

Démonstration. Pour tous $x \in \ker f$ et $a \in A$, $f(ax) = f(a)f(x) = 0 \Rightarrow ax \in \ker f$.
Pour tous $x = f(a)$ et $y = f(b) \in \operatorname{Im} f$, $x + y = f(a) + f(b) = f(a + b) \in \operatorname{Im} f$, $xy = f(a)f(b) = f(ab) \in \operatorname{Im} f$. $\square$

Sorite 1.16. *Soit J un idéal de B, alors $f^{-1}(J)$ un idéal de A.*

Démonstration. Pour tous $a \in A$, $i \in f^{-1}(J)$, $f(ai) = f(a)f(i) \in J \Rightarrow ai \in f^{-1}(J)$. $\square$

Remarque 1.17. On suppose que I est contenu dans $\ker f$. On a le diagramme commutatif suivant.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\omega"'] \arrow[dr, phantom, "\circlearrowleft"] & B \\ A/I \arrow[ur, dashed, "\bar{f}"'] & \end{tikzcd}$$

On dit encore alors que f se factorise par A/I.

Sorite 1.18. *A est un corps s.s.i. ses seuls idéaux sont $\{0\}$ et A.*

Démonstration. $\Rightarrow$: Si $I \neq \{0\}$, alors il existe $i \in I$, $i \neq 0$, donc $1 = ii^{-1} \in I$. On obtient immédiatement que $I = A$.
$\Leftarrow$: Pour tout a non nul dans A, $aA = \{ab,\ b \in A\}$ est un idéal non nul de A, donc $aA = A$. On sait qu'il existe $b \in A$ tel que $ab = 1 \Rightarrow a \in A^*$. C'est à dire que A est un corps. □

Sorite 1.19. *Tout idéal de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$, où $n \in \mathbb{Z}$.*

Démonstration. On utilise la division euclidienne sur $\mathbb{Z}$. Soit I un idéal de $\mathbb{Z}$. Posons $n = \inf\big\{|i, \ , \ i \in I \backslash \{0\}\big\} \in \mathbb{N}$. Pour tout $i \in I$, $|i| = nq+r$, où $r \in [\![0, n-1]\!]$. Donc $r = |i|-nq \in I$, or $|r| \leq n$, alors $r = 0$. On conclut que $I = n\mathbb{Z}$. □

Sorite 1.20. *L'intersection d'une famille arbitaire d'idéaux est un idéal.*

Définition 1.21. Soit S une partie de A. On appelle le plus petit idéal contenant S **l'idéal engendré par** S, on le note (S).

Sorite 1.22. $(S) = SA := \{\sum\limits_{s \in S} a_s s,\ a_s = 0$ *sauf un nombre fini d'éléments de* $S\}$.

Démonstration. $SA \supset S$ est un idéal de A. Tout idéal contenant S contient SA. Alors $(S) = SA$. □

Définition 1.23. On appelle I **un idéal premier** si pour tous a, $b \in A$, $ab \in I$ implique $a \in I$ ou $b \in I$. On note $\mathcal{P}$ l'ensemble de tout idéal premier de A.
On appelle I un idéal maximal si tout idéal de A contenant strictement I est égal à A. On note $\mathbf{m}$ l'ensemble de tout idéal maximal de A.

Lemme 1.24. *I est premier s.s.i. A/I est intègre. I est maximal s.s.i. A/I est un corps. On a alors que tout idéal maximal est premier.*

Démonstration. A/I est intègre s.s.i. pour tous $\bar{a}$, $\bar{b} \in A/I$, $\bar{a}\bar{b} = 0$ implique $\bar{a} = 0$ ou $\bar{b} = 0$ s.s.i. pour tous a, $b \in A$, $ab \in I$ implique $a \in I$ ou $b \in I$ s.s.i. I est premier.
A/I est un corps s.s.i. pour tout $\bar{a}$ non nul, il existe $\bar{b} \in A/I$, $\bar{a}\bar{b} = 1$ s.s.i. pour tout $a \in A \setminus I$, il existe $b \in A$, $ab - 1 \in I$ s.s.i. pour tout $a \in A \setminus I$, $(I \cup \{a\}) = A$ s.s.i. I est maximal. □

Définition 1.25. Soit $\mathcal{E}$ un ensemble non vide ordonné tel que toute chaîne (sous-ensemble totalement ordonné) possède un majorant, alors on l'appelle **un enseble inductif**.

Proposition 1.26. *Si $I \subsetneq A$, alors il existe J un idéal maximal de A contenant I.*

Démonstration. On utilise le théorème de Zorn : tout ensemble inductif a un élément maximal.
Posons $\mathcal{E} = \{J,\ I \subset J \subset A$ et J est un idéal de $A\}$. On ordonne $\mathcal{E}$ par l'inclusion. Soit $(J_i)_{i\in\Lambda}$ une chaîne, alors $\bigcup\limits_{i\in\Lambda} J_i \in \mathcal{E}$ est un majorant. Donc $\mathcal{E}$ est un ensemble inductif et alors possède un élément maximal J_m par le théorème de Zorn.
J_m est maximal par définition, et alors on conclut. □

Sorite 1.27. *A est un corps s.s.i. $\{0\}$ est maximal.*

Exemple 1.28. Par localisation : déterminons les unités de l'anneau $A[X]$ par un anneau A arbitaire (non nécessairement intègre). On a déjà vu $A[X]^* = \{P(X) = \sum\limits_{k=0}^{n} a_k X^k,\ a_0 \in A^*,$ a_i nilpotent $\forall\ i \in [\![1, n]\!]\}$. On va donner une autre preuve.
Soit $P \in \mathcal{P}$ un idéal premier de A. Alors A/P est intègre. On obtient un diagramme commutatif canonique :

$$\begin{tikzcd} A \arrow[r] \arrow[d, hook] & A/P \arrow[d, hook] \\ A[X] \arrow[r] & (A/P)[X] \end{tikzcd}.$$

Soit $Q = \sum\limits_{k=0}^{n} a_k X^k \in A[X]^*$, alors $\bar{Q} \in (A/P)[X]^* = (A/P)^*$, c'est à dire que $a_k \in P$ pour tout $k \in [\![1, n]\!]$. C'est banal que a_0 est inversible.
Nous avons la caractérisation suivante du radical nilpotent d'un anneau.

Lemme 1.29. $\bigcap\limits_{P\in\mathcal{P}} P = \{a \in A,\ a$ *nilpotent*$\}$ *le radical nilpotent de A .*

Démonstration. Pour tout $a \in A$ nilpotent et tout $P \in \mathcal{P}$, il existe $n \in \mathbb{N}$, $a^n = 0 \in P$, donc $a \in P$ ou $a^{n-1} \in P$. On applique la méthode de récurrence et on obtient $a \in P$.
Réciproquement, pour tout $x \in \bigcap\limits_{P\in\mathcal{P}} P$, posons $\mathcal{E}$ l'ensemble d'idéaux de A qui est disjoint avec $\{x^n,\ n \in \mathbb{N}\}$ et on ordonne $\mathcal{E}$ par l'inclusion. Si x n'est pas nilpotent, alors $\mathcal{E}$ est non

vide. Pour tout chaîne $(I_j)_{j\in\Lambda}$, $J = \bigcup\limits_{j\in\Lambda} I_j$ est un majorant. Donc $\mathcal{E}$ est un ensemble inductif. On applique le théorème de Zorn et on trouve un élément maximal Q de E.
On va montrer que Q est un idéal premier par l'absurde. S'il existe $a,\ b \in A \setminus P$ tels que $ab \in Q$, alors $Q \subsetneqq Q+(a)$ et $Q \subsetneqq Q+(b)$. On sait qu'il existe $n,\ m \in \mathbb{N}$ tels que $x^n \in Q+(a)$ et $x^m \in Q+(b)$. On peut préciser que $x^n = q_a + sa$, $x^m = q_b + tb$, où $s,\ t \in A$. Donc $x^{n+m} = q_a q_b + q_a tb + q_b sa + stab \in P$. Contradiction ! Alors P est premier. Or $x \in \bigcap\limits_{P\in\mathcal{P}} P$ et $P \cap \{x^n,\ n \in \mathbb{N}\} = \varnothing$, ce n'est pas possible. On conclut que x est nilpotent. □

Lemme 1.30. $A \setminus A^* = \bigcup\limits_{m\in\mathbf{m}} m.$

Démonstration. Pour tout $a \in A \setminus A^*$, $(a) \neq A$. On peut trouver un idéal maximal m contenant (a) par la proposition 1.26. Donc $a \in \bigcup\limits_{m\in\mathbf{m}} m$.
Pour tout $x \in \bigcup\limits_{m\in\mathbf{m}} m$, x n'est pas inversible (sinon le seul idéal contenant x est A). □

Exemple 1.31. Posons $\mathcal{C} = \mathcal{C}([0,1],\mathbb{R})$, $\mathcal{A}_x = \{f \in \mathcal{C},\ f(x) = 0\}$, où $x \in [0,1]$.

Lemme 1.32. *$\mathcal{A}_x$ est un idéal maximal de $\mathcal{C}$ pour tout $x \in [0,1]$.*

Démonstration. C'est banal que $\mathcal{A}_x$ est un idéal. Pour tout $g \in \mathcal{C} \setminus \mathcal{A}_x$ et tout $c \in \mathcal{C}$, $c = \frac{c(x)}{g(x)}g + (c - \frac{c(x)}{g(x)}g) \in (g) + \mathcal{A}_x$. C'est à dire que $(g) + \mathcal{A}_x = \mathcal{C}$. Donc $\mathcal{A}_x$ est maximal. □

Lemme 1.33. *Tout idéal maximal de $\mathcal{C}$ est de la forme $\mathcal{A}_x$.*

Démonstration. $\mathcal{C}^* = \{f \in \mathcal{C},\ f \text{ ne s'annule nulle part}\}$.
Soit m un idéal maximal de $\mathcal{C}$ et $m \neq \mathcal{A}_x$ pour tout $x \in [0,1]$. Alors pour tout $y \in [0,1]$, il existe $f_y \in m$ telle que $f_y(y) \neq 0$. On peut trouver V_y un voisinage ouvert de y tel que $f_y^2 > 0$ sur V_y. $[0,1] \subset \bigcup\limits_{y\in[0,1]} V_y$, c'est un recouvrement ouvert du compact, donc on peut extraire un sous-recouvrement fini $(V_{y_n})_{1\leq n\leq N}$. Alors $\sum\limits_{n=1}^{N} f_{y_n}^2 \in m$ ne s'annule nulle part. C'est une contradiction et on finit la démonstration. □

Remarque 1.34. On observe que
$$\begin{aligned} \mathcal{C}/\mathcal{A}_x &\xrightarrow{\simeq} \mathbb{R} \\ f &\longmapsto f(x) \end{aligned}.$$

On va caractériser les idéaux premiers de $\mathcal{C}$.

Lemme 1.35. *Soit P un idéal premier de $\mathcal{C}$, alors il existe un unique idéal maximal contenant P. P est dense dans cet idéal maximal le contenant par la topologie de la convergence uniforme.*

Démonstration.

Cas 1 : si $P \subset \bigcap\limits_{u\in[x,y]\subset[0,1]}$. Pour tout $f \in P$, on définit

$$f_1(a) = \begin{cases} 1 & , \ 0 \le a \le x \\ \frac{2}{x-y}a + \frac{y+x}{y-x} & , \ x \le a \le \frac{x+y}{2} \\ 0 & , \ \frac{x+y}{2} \le a \le y \\ f(a) & , \ y \le a \le 1 \end{cases}, \quad f_2(a) = \begin{cases} f(a) & , \ 0 \le a \le x \\ 0 & , \ x \le a \le \frac{x+y}{2} \\ \frac{2}{y-x}a - \frac{y+x}{y-x} & , \ \frac{x+y}{2} \le a \le y \\ 1 & , \ y \le a \le 1 \end{cases}.$$

Alors $f_1,\ f_2 \in \mathcal{C} \setminus P$, mais $f_1 f_2 = f \in P$, contradiction !
Cas 2 : On suppose que $P \subset \mathcal{A}_x \cap \mathcal{A}_y$ et $x < y$. D'après le cas 1, il existe $z \in]x, y[$ tel que P n'est pas contenu dans $\mathcal{A}_z$, i.e. il existe $f_z \in P$ tel que $f_z(z) \neq 0$.
Il existe u, v tels que $x < u < z < v < y$ et f_z ne s'annule nulle part sur $[u, v]$. On définit

$$f_1(a) = \begin{cases} (f_z(a))^2 & , \ 0 \le a \le u \\ \frac{1-(f_z(u))^2}{v-u}a + \frac{v(f_z(u))^2-u}{v-u} & , \ u \le a \le v \\ 1 & , \ v \le a \le 1 \end{cases}, \quad f_2(a) = \begin{cases} 1 & , \ 0 \le a \le u \\ \frac{(f_z(a))^2}{f_1(a)} & , \ u \le a \le v \\ (f_z(a))^2 & , \ v \le a \le 1 \end{cases}.$$

Alors $f_1,\ f_2 \in \mathcal{C} \setminus P$, mais $f_1 f_2 = f_z^2 \in P$, contradiction !
Donc il existe un unique idéal maximal de $\mathcal{C}$ contenant P.

Après on suppose que $P \in \mathcal{A}_x$. Alors pour tout $y \neq x$, il existe $f_y \in P$ tel que $f_y(y) \neq 0$ et $\epsilon_y > 0$ tel que $f|^2_{]y-2\epsilon_y, y+2\epsilon_y[} > 0$. On note V_y l'ensemble $]y - \epsilon_y, y + \epsilon_y[$.
Pour tout $\epsilon > 0$, il existe $v > 0$ tel que $\left| f|_{]x-v,x+v[} \right| < \epsilon$.
$[0, x-v] \cup [x+v, 1] \subset \bigcup\limits_{y\neq x} V_y$, c'est un recouvrement ouvert du compact, donc on peut extraire un sous-recouvrement fini $(V_{y_i})_{1\le i\le N}$. Soit $(\chi_i)_{1\le i\le N}$ une partition de l'unité subordonnèe à ce recouvrement, i.e. $\chi_i \in \mathcal{C}$ pour tout i, $\chi_i|_{V^\complement_{y_i}} = 0$ et $\mathbb{1}_{\cup_i V_{y_i}} = \sum\limits_{1\le i\le N} \chi_i$.

Posons $g_i(x) = \begin{cases} \frac{\chi_i}{f_{y_i}} & , x \in V_{y_i} \\ 0 & , x \in V_{y_i} \end{cases} \in \mathcal{C}$. On observe que $\mathbb{1}_{\cup_i V_{y_i}} = \sum\limits_{1\le i\le N} \chi_i = \sum\limits_{1\le i\le N} g_i f_i \in P$. Pour tout $f \in \mathcal{A}_x$, posons $\tilde{f} = \mathbb{1}_{\cup_i V_{y_i}} f \in P$, donc

$$\sup_{[0,1]} |f - \tilde{f}| = \sup_{\cup_i V_{y_i}} |f - \tilde{f}| = \sup_{\cup_i V_{y_i}} |f| \le \sup_{[x-v,x+v]} |f| < \epsilon.$$

C'est à dire que P est dense dans $\mathcal{A}_x$ par la topologie de la convergence uniforme. $\square$

Proposition 1.36. *$\mathcal{C}$ possède des idéaux premiers non maximal.*

Corollaire 1.37. *Tout idéal premier fermé (par la topologie de la convergence uniforme) est maximal.*

Pour la montrer, on doit introduire le radical d'idéal.

Définition 1.38. $\sqrt{I} = \{a \in A,\ \exists\, m \in \mathbb{N}^*,\ a^m \in I\}$. On l'appelle **le radical de** I.

Sorite 1.39. *$\sqrt{I}$ est un idéal de A.*

Démonstration. Pour tous $a, b \in \sqrt{I}$ et $x \in A$, on suppose que a^n, $b^m \in I$, alors $(a+b)^{n+m-1} = \sum_{k=0}^{n+m-1} \binom{n+m-1}{k} a^k b^{n+m-1-k} \in I$ et $(ax)^n = a^n x^n \in I$, alors $\sqrt{I}$ est un idéal de A. □

Définition 1.40. On dit que I est **radical** si $\sqrt{I} = I$, i.e. $\sqrt{I} \subset I$.

Sorite 1.41. *Tout idéal premier est radical.*

Démonstration. Soit P un idéal premier de A. Pour tout $a \in \sqrt{P}$, il existe $n \in \mathbb{N}^*$ tel que $a^n \in P$. On a vu dans la démonstration de lemme 1.29 que ça implique que $a \in P$. Donc P est radical. □

Sorite 1.42. *I est radical s.s.i. le seul élément nilpotent de A/I est* 0.

Démonstration. Pour tout $a \in A$, $\bar{a} \in A/I$ est nilpotent s.s.i. il existe $n \in N^*$ tel que $\bar{a}^n = \bar{0}$ s.s.i. il existe $n \in N^*$ tel que $a^n \in I$ s.s.i. $a \in \sqrt{I}$. Donc I est radical s.s.i. $\sqrt{I} \subset I$ s.s.i. $\{\bar{a} \in A/I,\ \bar{a}$ est nilpotent$\} \subset \{\bar{0}\}$. □

Proposition 1.43.
- *$\sqrt{I}$ est le plus petit idéal radical contenant I.*
- *$\sqrt{I}$ est l'intersection des idéaux premiers contenant I.*

Remarque 1.44. On a caractériser les unités de $A[X]$. C'est le cas particulier de la deuxième affirmation si-dessus, ici $I = (0)$.

Démonstration.

- $\sqrt{\sqrt{I}} = \{a \in A,\ \exists\, m \in \mathbb{N}^*,\ a^m \in \sqrt{I}\} = \{a \in A,\ \exists\, m \in \mathbb{N}^*,\ \exists\, n \in \mathbb{N}^*,\ (a^m)^n \in I\} \subset \sqrt{I}$. Donc I est radical.

  Soit J un idéal radical de A contenant I, alors $J = \sqrt{J} \supset \sqrt{I}$. Donc $\sqrt{I}$ est le plus petit idéal radical contenant I.

— Pour tout P idéal premier contenant I, on a vu que $P = \sqrt{P} \supset \sqrt{I}$. Donc $\sqrt{I} \subset \bigcap_{\substack{P \in \mathcal{P} \\ I \subset P}} P$.

Réciproquement, pour tout $a \in A \setminus \sqrt{I}$, posons $\mathcal{E}$ l'ensemble d'idéaux contenant I qui est disjoint avec $\{x^n,\ n \in \mathbb{N}\}$ et on ordonne $\mathcal{E}$ par l'inclusion. Alors $\mathcal{E}$ est non vide ($I \in \mathcal{E}$). Pour tout chaîne $(I_j)_{j\in\Lambda}$, $J = \bigcup_{j\in\Lambda} I_j$ est un majorant. Donc $\mathcal{E}$ est un ensemble inductif. On invoque le théorème de Zorn et on trouve un élément maximal M de E. Pour tous x, $y \in A \setminus M$, $M + (x)$, $M + (y) \notin \mathcal{E}$, i.e. il existe n_x, $n_y \in \mathbb{N}^*$ tels que $a^{n_x} = m_x + bx$, $a^{n_m} = m_y + cy$, où m_x, $m_y \in M$ et b, $c \in A$. Alors $a^{n_x+n_y} = m_x m_y + m_x cy + m_y bx + bcxy \in M + (xy)$. Or $a^{n_x+n_y} \notin M \Rightarrow xy \notin M$. C'est à dire que M est premier. On conclut que $\sqrt{I} \supset \bigcap_{\substack{P \in \mathcal{P} \\ I \subset P}} P$ et finit la démonstration.

□

Démonstration. (de la proposition 1.36) On considère $I = \{f \in \mathcal{C},\ \forall\, n \in \mathbb{N},\ \lim_{x\to 0} \frac{f(x)}{x^n} = 0\}$.

— I est clairement un idéal.
— Pour tout $f \in \sqrt{I}$, il existe $n \in \mathbb{N}^*$ tel que $f^n \in I$ i.e. pour tout $m \in \mathbb{N}$, $\lim_{x\to 0} \frac{f^n(x)}{x^m} = 0$ s.s.i. pour tout $m \in \mathbb{N}$, $\lim_{x\to 0} \frac{f(x)}{x^{m/n}} = 0$. On choisit $m = nk$, $k \in \mathbb{N}$ et alors $f \in I$. Donc I est radical.

On invoque alors la deuxième affirmation de la proposition 1.43 : $I = \sqrt{I} = \bigcap_{\substack{P \in \mathcal{P} \\ I \subset P}} P$. On considère $x \to e^{-\frac{1}{x^2}} \in I$, alors le seul idéal maximal contenant I est $\mathcal{A}_0$, donc tout idéal premier P est contenu dans $\mathcal{A}_0$ par l'unicité. Or $\mathcal{A}_0$ contient des fonctions d'ordre d'annulation fini sur 0 : $x \to x^k$, où $k \in \mathbb{N}$, alors $I \subsetneqq \mathcal{A}_0$. On conclut qu'il existe un idéal premier non maximal de $\mathcal{C}$, sinon $I = \bigcap_{\substack{P \in \mathcal{P} \\ I \subset P}} P = \bigcup \mathcal{A}_0 = \mathcal{A}_0$. □

2 Réductibilité

Après on suppose que A est intègre dans cette section.

Définition 2.1. Pour tous a, $b \in A$, s'il existe $q \in A$ tel que $b = aq$ s.s.i. $(b) \subset (a)$, on la note $a|b$.

Remarque 2.2. 0 ne divise que lui-même (0 est absorbant). Pour tout $a \in A^*$, a divise tout $b \in A$.

Sorite 2.3. *Soient a, $b \in A$. Alors $a|b$ et $b|a$ s.s.i. il existe $u \in A^*$ tel que $a = ub$. On appelle que a et b sont associés.*

Démonstration. $\Rightarrow$: $a|b$ et $b|a$ s.s.i. il existe q et $r \in A$ tels que $b = aq$ et $a = br$. $a = br = aqr \Rightarrow a(1 - qr) = 0 \Rightarrow 1 = qr \Rightarrow q \in A^*$.
$\Leftarrow$: $a = ub$, $u \in A^*$, alors $b = u^{-1}a$ et donc $a|b$, $b|a$. $\square$

Définition 2.4. Soit $a \in A$. a est dit **irréductible** si a n'est pas un unité et pour tous x, $y \in A$, $a = xy$ implique $x \in A^*$ ou $y \in A^*$.

Sorite 2.5. *Si $a \in A$ est irréductible, alors pour tous $b \in A$*

- *soit a et b sont premiers entre eux i.e. $a \wedge b = 1$,*
- *soit $a|b$.*

Démonstration. Si $a \wedge b \neq 1$, alors il existe $c \in A \setminus A^*$ et r, $s \in A$ tels que $a = cr$ et $b = cs$. a est irréductible $\Rightarrow r \in A^*$, donc $b = cs = r^{-1}sa \Rightarrow a|b$. $\square$

Sorite 2.6. *Les irréductibles de $\mathbb{Z}$ sont $\pm p$, où $p \in \mathcal{P}$; les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 ou les polynômes quadratiques sans racines réelles.*

Lemme 2.7. *Soit $a \in A$ non nul, alors (a) est premier $\Rightarrow$ a est irréductible. La réciproque est fausse en général.*

Démonstration. Sinon, il existe b, $c \in A \setminus A^*$ tels que $a = bc$, alors b et $c \notin (a)$ par la sorite 2.3. Donc (a) n'est pas premier. Contradiction !
Pour la réciproque, on pose $A = \mathbb{Z}[\sqrt{-5}]$. Alors $3 \in A$ est irréductible mais (3) n'est pas premier. Si $3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$, alors $9 = |3|^2 = (a^2 + 5b^2)(c^2 + 5d^2) \Rightarrow (a, b, c, d) = (1, 0, 3, 0)$ ou $(3, 0, 1, 0)$ ou $(2, 1, 1, 0)$ ou $(1, 0, 2, 1)$, mais $3 \neq 2 + \sqrt{-5}$. Donc 3 est irréductible. Or $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 \in (3)$ et $(1 + \sqrt{-5}) \notin (3)$, $(1 - \sqrt{-5}) \notin (3)$. Donc (3) n'est pas premier. $\square$

Exemple 2.8. $\mathbb{Z}$: tous les concepts «d'indécomposabilité» coïncide. Les affirmations suivantes sont équivalentes.
i) $\mathbb{Z}/n\mathbb{Z}$ est un corps s.s.i. $n\mathbb{Z} = (n)$ est maximal.
ii) $\mathbb{Z}/n\mathbb{Z}$ est intègre s.s.i. $n\mathbb{Z} = (n)$ est premier.
iii) n est irréductible.
i) $\Rightarrow$ *ii*) est banal et on a vu que *ii*) $\Rightarrow$ *iii*) . Pour *iii*) $\Rightarrow$ *i*) (Bézout) : pour tout $m \notin (n)$ i.e. $n \nmid m$, n irréductible, alors $n \wedge m = 1$ i.e. n et m sont premiers entre eux. D'où il existe a, $b \in \mathbb{Z}$, $1 = an + bm$ i.e. $\mathbb{Z} + n\mathbb{Z} + m\mathbb{Z} = (n, m)$ i.e. (n) est maximal.

3 Anneaux principaux et euclidiens

Définition 3.1. Un anneau A est dit **pricipal** (PID) si A est intègre et tout idéal de A est principal (i.e. monogène).

Exercice 3.2. $(\mathbb{Z}, +, \cdot)$ est principal ; soit K un corps, alors K est principal.
Contre : $i)$ $\mathbb{Z}[X]$ n'est pas principal. On considère $(2, X)$. S'il existe $a \in \mathbb{Z}[X]$ tel que $(2, X) = (a)$, alors a est nécessairement 1, or $1 \notin (2, X)$. Contradiction !
$ii)$ Soit K un corps, alors $K[X, Y]$ n'est pas principal. On considère (X, Y). S'il existe $a \in K[X, Y]$ tel que $(X, Y) = (a)$, alors $\deg a < 1$, donc $a \in K^*$. Or $1 \notin (X, Y)$. Contradiction !
$iii)$ Posons $\mathcal{C} = \mathcal{C}([0, 1], \mathbb{R})$, alors les idéaux maximals $\mathcal{A}_x = \{f \in \mathcal{C},\ f(x) = 0\}$ ne sont pas principaux. S'il existe $f \in \mathcal{C}$ tel que $\mathcal{A}_x = (f)$, alors posons $g = (f^2)^{\frac{1}{4}}$ et $g(x) = 0 \Rightarrow g \in \mathcal{A}_x = (f)$. Donc il existe $h \in \mathcal{C}$ telle que $g = fh$. Pour tout x tel que $f(x) \neq 0$, $h(x) = \frac{g(x)}{f(x)} = \frac{\operatorname{sgn} f(x)}{\sqrt{|f(x)|}}$, alors lorsque $f(x) \to 0$, $h(x) \to \infty$. Mais on sait que h est borné, contradiction !

Remarque 3.3. $\tilde{\mathcal{C}} := \mathcal{C}^\infty([0, 1], \mathbb{R})$. On dispose du concept «d'ordre d'annulation en x». En particulier les $\mathcal{A}_x$ sont alors principaux. $\mathcal{A}_x = (f)$ pour toute f qui s'annulent en x à l'ordre 1 et nulle part ailleurs, e.g. $f(X) = X - x$, $\mathcal{A}_x = (X - x)$.

Pour établir qu'un anneau intègre est principal, on a suivant reconnu à l'algorithme d'Euclide i.e. au concept d'anneau euclidien.

Définition 3.4. A est dit **euclidien** (resp. **euclidien faiblement**) s'il est intègre et s'il existe une fonction d'Euclide $\varphi : A \setminus \{0\} \to \mathbb{N}\,(resp.\, \mathbb{Z})$ telle que pour tout $(a, b) \in A \times (A \setminus \{0\})$, il existe r, $q \in A$, $a = bq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$.

Exemple 3.5. $i)$ $\mathbb{Z}$: $\varphi : \begin{array}{rcl} \mathbb{Z} \setminus \{0\} & \longrightarrow & \mathbb{N} \\ n & \longmapsto & |n| \end{array}$ et la division euclidienne des entiers.

$ii)$ Soit K un corps, alors $K[X]$ est euclidien avec $\varphi : \begin{array}{rcl} K[X] \setminus \{0\} & \longrightarrow & \mathbb{N} \\ P & \longmapsto & \deg P \end{array}$.

Lemme 3.6. *Tout anneau euclidien est principal.*

Démonstration. Pour tout idéal I de A, il existe $x \in I$ tel que $\varphi(x) = \inf \varphi|_{I \setminus \{0\}}$. Alors pour tout $i \in I$, il existe r, $q \in A$ tels que $i = qx + r$ avec $r = 0$ ou $\varphi(r) < \varphi(x)$. Or $r = i - qx \in I$, donc $r = 0$ et $x|i$. Ceci donne que $I = (x)$. $\square$

Définition 3.7. $(A, +, \cdot)$ intègre est dit **euclidien fortement** si A est euclidien et la fonction d'Euclide véréfié que pour tous a, $b \in A \setminus \{0\}$, $\varphi(a) < \varphi(ba)$.

Proposition 3.8 (Rogers)**.** *Tout anneau intègre euclidien est un anneau euclidien fortement.*

Remarque 3.9. Il existe φ fonction d'Euclide qui ne satifait pas la monotonie $\varphi(a) \leq \varphi(ab)$.

Démonstration. Soit A un anneau intègre et soit φ une fonction d'Euclide (pas nécessairment forte). On définit $\psi : \begin{array}{rcl} A \setminus \{0\} & \longrightarrow & \mathbb{N} \\ a & \longmapsto & \min\limits_{d \in A\setminus\{0\}} \varphi(ad) \end{array}$.

— Pour tous $a,\, b \in A \setminus \{0\}$, $\psi(ab) = \min\limits_{d\in A\setminus\{0\}} \varphi(abd) \geq \min\limits_{d\in A\setminus\{0\}} \varphi(ad) = \psi(a)$.
— Pour tout $(a, b) \in A \times (A \setminus \{0\})$, il existe $c \in A \setminus \{0\}$ tel que $\psi(b) = \varphi(bc)$. En appliquant l'algorithme d'Euclide de φ à ac et bc, il existe $r,\, q \in A$, $ac = bcq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(bc)$ s.s.i. $a = bq$ ou $\psi(b) = \varphi(bc) > \varphi(r) = \varphi(c(a-bq)) \geq \psi(a-bq)$. ψ est ainsi une fonction d'Euclide de A.

□

Exemple 3.10. Soit K un corps. $K[[X]] = \{(a) = \sum\limits_{k\in\mathbb{N}} a_k X^k,\ a_k \in K \text{ pour tout } k \in \mathbb{N}\}$ est l'ensemble des séries formelles en X. Alors $K[[X]]$ est un anneau euclidien dont les idéaux sont (X^m), où $m \in \mathbb{N}$.
$(ab) = 1$ s.s.i. $a_0 b_0 = 1$ et $(ab)_k = \sum\limits_{l=0}^{k} a_l b_{k-l} = 0$. Lorsque $a_0 \neq 0$, on peut calculer (b) par récurrence. Donc $K[[X]]^* = \{(a) \in K[[X]],\ a_0 \neq 0\}$.
On définit $\varphi : \begin{array}{rcl} K[[X]] \setminus \{0\} & \longrightarrow & \mathbb{N} \\ (a) & \longmapsto & \inf\{k \in \mathbb{N},\, a_k \neq 0\} \end{array}$. Pour tout $a \in K[[X]] \setminus \{0\}$, a et $X^{\varphi(a)}$ sont alors associés. Donc pour tout $b = u_b X^{\varphi(b)} \in K[[X]] \setminus \{0\}$, $a = u_a X^{\varphi(a)} = \begin{cases} b u_b^{-1} u_a X^{\varphi(a)-\varphi(b)} & , \varphi(a) \geq \varphi(b) \\ b \cdot 0 + a & , \varphi(b) > \varphi(a) \end{cases}$, où $u_a,\, u_b \in K[[X]]^*$. φ est alors une fonction d'Euclide (au sens fort).
On conclut que $K[[X]]$ est unanneau euclidien au sens fort et donc il est principal. On a vu que pour tout idéal I de $K[[X]]$, $I = (a)$, où $\varphi(a) = \inf \varphi|_{I\setminus\{0\}}$. En même temps, a et $X^{\varphi(a)}$ sont alors associés, donc $I = (X^{\varphi(a)})$.

Théorème 3.11. *Un anneau intègre est pricipal s.s.i. tout son idéal premier est principal.*

Démonstration. Il suffit de montrer la réciproque par l'absurde. Posons $\mathcal{E}$ l'ensemble d'idéaux non principal de A et on ordonne $\mathcal{E}$ par l'inclusion. Alors $\mathcal{E}$ est non vide (d'après l'hypothèse). Pour tout chaîne $(I_j)_{j\in\Lambda}$, $J = \bigcup\limits_{j\in\Lambda} I_j$ est encore un idéal. S'il existe $a \in E$ tel que $J = (a)$, alors il existe $j \in \Lambda$, $a \in I_j$ et $J = (a) \subset I_j$. C'est impossible donc $\mathcal{E}$ est un ensemble inductif.

On invoque le théorème de Zorn et on trouve un élément maximal M de E.
Pour tout $x \in A \setminus M$, $M + (x) \notin \mathcal{E}$, alors il est pricipal, i.e. $M + (x) = (z)$, où $z \in A$. D'une part, il existe $m \in M$ et $p \in A$ tels que $z = n + px$; d'autre part, il existe $q \in A$ tel que $x = qz$. On considère $J = \{a \in A,\ ax \in M\}$, alors $J \supsetneqq M$ est principal car M n'est pas premier. On suppose que $J = (w)$, $w \in J \setminus M$. Alors $wz = wm + pwx \in M$ et pour tout $m = az \in M$, $ax = aqz = qm \in M$, donc $a \in J \Rightarrow a = bw$, $b \in A$. Alors $m = bwz \in (wz)$. On conclut que $M = (wz)$, contradiction ! Donc A est principal. □

Définition 3.12. Soit A un anneau principal. Pour tous a, $b \in A$, il existe c, $d \in A$ tel que $(a, b) = (c)$ et $(a) \cap (b) = (d)$. c et d sont déterminés à une unité près. On appelle $c = \mathrm{pgcd}(a, b) = a \wedge b$ et $d = \mathrm{ppcm}(a, b) = a \vee b$.

Théorème 3.13 (Bézout)**.** *Soit A un anneau principal et soient a, $b \in A$. Alors $a \wedge b = 1$ s.s.i. il existe x, $y \in A$ tels que $xa + yb = 1$.*

Démonstration. C'est tautologique ! En effet $a \wedge b = 1$ s.s.i. $(a, b) = (1) = A$ s.s.i. $\exists x$, $y \in A$, $xa + yb = 1$. Retour au point de vue classique : $d|a$ et $d|b$ s.s.i. $a \in (d)$ et $b \in (d)$ s.s.i. $(a, b) \subset (d)$ s.s.i. $(a \wedge b) \subset (d)$ s.s.i. d , $a \wedge b$. Alors tout diviseur commun de a et b divise $a \wedge b$, qui est un diviseur commun de a et b et donc $a \wedge b$ est un plus grand diviseur commun de a et b. Le théorème de Bézout est donc banal quel que soit le point de vue adapté. □

On pose la question de l'effectivité : à savoir a, $b \in A$, ils sont premiers entre eux, comment déterminer les x et $y \in A$ tels que $xa + by = 1$. En amont, ce pose la question de la détermisation du pgcd(a, b) *: la définition précédente n'étant absolument pas effective/constructive.*

Exemple 3.14. Construction du pgcd dans un anneau euclidien : soient a, $b \in A$ et $\varphi(b) \leq \varphi(a)$. Alors il existe q_0, $r_1 \in A$ tels que $a = bq_0 + r_1$, où soit $r_1 = 0$, soit $\varphi(r_1) < \varphi(b)$. Si $r_1 = 0$, alors $\mathrm{pgcd}(a, b) = b$; sinon, on continue.
Il existe q_1, $r_2 \in A$ tels que $b = r_1 q_1 + r_1$, où soit $r_2 = 0$, soit $\varphi(r_2) < \varphi(r_1)$. Si $r_2 = 0$, alors $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r_1) = r_1$; sinon, on continue.
Pour $k \in \mathbb{N}$, il existe q_{k-1}, $r_{k+1} \in A$ tels que $r_{k-2} = r_{k-1} q_{k-1} + r_k$, où soit $r_k = 0$, soit $\varphi(r_k) < \varphi(r_{k-1})$. Si $r_k = 0$, alors $\mathrm{pgcd}(r_{k-2}, r_{k-1}) = r_{k-1}$; et on itère tant que $r_k \neq 0$.
Or la fonction d'Euclide φ est minoré donc le processus s'arrête en au plus $\varphi(b)$ étape i.e. il existe $l \leq \varphi(b)$, $r_{l-2} = r_{l-1} q_{l-1} + r_l$, $\mathrm{pgcd}(r_{l-2}, r_{l-1}) = r_{l-1}$. On conclut en observant que pour tout $k < l$, $\mathrm{pgcd}(r_{k-2}, r_{k-1}) = \mathrm{pgcd}(r_{k-1}, r_k)$. Et donc par une récurrence finie et banale : $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r_1) = \mathrm{pgcd}(r_1, r_2) = \cdots = \mathrm{pgcd}(r_{l-2}, r_{l-1}) = r_{l-1}$. C'est un calcul effectif

du pgcd dans un anneau euclidien.
On en déduit une preuve constructive du théorème de Bézout-en particulier un moyen de déterminer-étant donné deux éléments a, b d'un anneau euclidiens premiers entre eux, les coefficients x, $y \in A$ tels que $ax + by = 1$. Plus généralement, l'argument va donner le calcul de x, $y \in A$ tels que $ax + by = a \wedge b$.
On procède par récurrence : $a - bq_0 = r_1$, et par hypothèse de récurrence il existe x_k, $y_k \in A$ tels que $ax_k + by_k = r_k$ pour tout $k < n$. À l'ordre n, $ax_{n-1}q_{n-1} + by_{n-1}q_{n-1} = r_{n-1}qn - 1 = r_{n-2} - r_n = ax_{n-2} + by_{n-2} - r_n$, c'est à dire que $r_n = a(x_{n-2} - x_{n-1}q_{n-1}) + b(y_{n-2} - y_{n-1}q_{n-1})$. En particulier $r_{l-1} = \text{pgcd}(a, b) = ax + by$, x, $y \in A$ où ils sont donnés par la récurrence double avec $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} 1 \\ -q_0 \end{pmatrix}$, $\begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} -q_1 \\ 1 + q_0q_1 \end{pmatrix}$ et $\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} x_{n-2} \\ y_{n-2} \end{pmatrix} - q_{n-1}\begin{pmatrix} x_{n-1} \\ y_{n-1} \end{pmatrix}$.

Lemme 3.15 (Gauß)**.** *Soit A un anneau principal et soient a, b, $c \in A$. On suppose $a|bc$ et $a \wedge b = 1$, alors $a|c$.*

Démonstration. C'est un corollaire du théorème de Bézout. $a|bc \Rightarrow$ il existe $d \in A$ tel que $ad = bc$; $a \wedge b = 1 \Rightarrow$ il existe x, $y \in A$ tel que $ax + by = 1$. Alors $c = acx + bcy = acx + ady \Rightarrow a|c$.
Il existe une autre preuve dans un anneau à pgcd i.e. pour tout $(a, b) \in A \times A$, il existe $c \in A$ un diviseur commun de a et b tel que tout diviseur commun de a et b divise c. On suppose sans reste de généralité que $c \neq 0$. $c|\text{pgcd}(ac, bc)$. On suppose que $\text{pgcd}(ac, bc) = cq$ et alors $ac = cqm$, $bc = cqn \Rightarrow q|a$, $q|b$. Donc $\text{pgcd}(ac, bc)|c\text{pgcd}(a, b) = c$. On a ainsi établi que $\text{pgcd}(ac, bc)$ et c sont associés. Ainsi $a|bc$ et $a|ac \Rightarrow a|\text{pgcd}(ac, bc) \Rightarrow a|c$. □

Lemme 3.16 (d'Euclide)**.** *Soit A un anneau principal et soit $p \in A$ irréductible. Pour tous a, $b \in A$, $p|ab \Rightarrow p|a$ ou $p|c$.*

Démonstration. C'est une conséquence de lemme de Gauß. Nous avons vu que pour p un élément irréductible, $p \wedge a = 1$ ou $p|a$ pour tout $a \in A$. Si $p \nmid a$ et $p \nmid b$. Alors $p \wedge a = 1$ et $p \wedge b = 1$ car p est irréductible. Le lemme de Gauß nous dit que $p \nmid bc$.
Il existe une autre preuve à la façon d'Euclide par l'absurde dans un anneau euclidien. On suppose que $p \in A$ irréductible, $p \nmid a$, $p \nmid b$ et $p|ab$. Posons $\mathcal{E} = \{c \in A,\ p|ac \text{ et } p \nmid c\} \ni b$. Considérons $d \in \mathcal{E}$ l'élément tel que $\varphi(d) = \inf \varphi|_{\mathcal{E}}$. Pour tout $k \in A$, $p|b(d + kp)$ et $p \nmid d + kp$, alors $d + kp \in \mathcal{E}$. On considère la division euclidienne de d par p : $d = pq + r$, où $\varphi(r) < \varphi(p)$ car $p \nmid d$. $r = d - pq \in \mathcal{E}$, donc $\varphi(d) \leq \varphi(r) < \varphi(p)$. On considère la division euclidienne de p par d : $d = ps + t$, où $\varphi(t) < \varphi(d)$ car $\varphi(d) < \varphi(p) \Rightarrow d \nmid p$. Alors $at = ad - aps \in (p)$ et $\varphi(t) < \varphi(d) < \varphi(p) \Rightarrow p \nmid t$, ça implique que $t \in \mathcal{E}$ mais $\varphi(t) < \varphi(d) = \inf \varphi|_{\mathcal{E}}$, contradiction ! □

Proposition 3.17. *Soit A un anneau principal et soit $a \in A \setminus \{0\}$. Alors les affirmations suivantes sont équivalentes :*
i) (a) est maximal i.e. $A/(a)$ est un corps.
ii) (a) est premier i.e. $A/(a)$ est intègre.
iii) a est irréductible.

Démonstration. $i) \Rightarrow ii) \Rightarrow iii)$ clairement.
Il suffit de montrer que $iii) \Rightarrow i)$. Soit I un idéal de A contenant (a). Il existe $b \in A$ tel que $I = (b)$ car A est principal. Donc il existe $c \in A$ tel que $a = bc$. Or a est irréductible donc soit $b \in A^*$, soit $c \in A^*$ i.e. $I = A$ ou $I = (a)$. De plus, a est irréductible $\Rightarrow a \notin A^*$, alors $(a) \neq A$. Donc (a) est maximal. □

Corollaire 3.18. *L'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est pas principal.*

Démonstration. On a vu que 3 est irréductible dans $\mathbb{Z}[i\sqrt{5}]$ mais (3) n'est pas premier, donc $\mathbb{Z}[i\sqrt{5}]$ n'est pas principal.
Ou plus directement(alternative à l'argument précédent), posons $I = \{a + ib,\ a + b \in 2\mathbb{Z}\}$. C'est banal que I est un idéal.
Soit J un idéal de A contenant I et soit $c + id\sqrt{5} \in I \setminus J$, alors $c + d \in 2\mathbb{Z} + 1$. On obtient que $1 = c + id\sqrt{5} - ((c-1) + id\sqrt{5}) \in J$, donc $J = \mathbb{Z}[i\sqrt{5}]$. $1 \notin I$ donc I est bien maximal.
Or I n'est pas principal. Supposons $a = x + iy\sqrt{5} \in I$ tel que $I = (a)$, alors $x + y \in 2\mathbb{Z}$. Pour tout $b \in \mathbb{Z}[i\sqrt{5}]$, $c = ab \in I$. On précise que $b = b_1 + ib_2\sqrt{5}$ et $c = c_1 + ic_2\sqrt{5}$. $c_1^2 + 5c_2^2 = |c|^2 = (x^2 + 5y^2)(b_1^2 + 5b_2^2)$. On considère $2 \in I$, donc $y = 0 \Rightarrow a = x \in 2\mathbb{Z}$. Posons $x = 2u$, alors $c_1^2 + 5c_2^2 = |c|^2 = 4u^2(b_1^2 + 5b_2^2) \in 4\mathbb{Z}$. Or $1 + i\sqrt{5} \in I$ mais $|1 + i\sqrt{5}|^2 = 6$, contradiction ! □

Exemple 3.19 (de l'anneau des nombres décimaux)**.** $\mathbb{D} = \{x \in \mathbb{Q},\ \exists\, n \in \mathbb{N},\ 10^n x \in \mathbb{Z}\}$. On note $ordre(x) := \min\{m \in \mathbb{N},\ 10^m x \in \mathbb{Z}\}$.

Sorite 3.20. *$\mathbb{D}$ est un sous-anneau de $\mathbb{Q}$.*

Lemme 3.21. *i) Soit $x = \frac{a}{b} \in \mathbb{Q}$, où a, $b \in \mathbb{Z}$ et $a \wedge b = 1$. Alors $x \in \mathbb{D}$ s.s.i. il existe m, $n \in \mathbb{N}$ tels que $b = 2^m 5^n$.*
ii) Tout décimal $x \in \mathbb{D}$ n'admet qu'une unique écriture $x = 2^m 5^n a$, où a, n, $m \in \mathbb{Z}$, $a \wedge 2 = 1$ et $a \wedge 5 = 1$.

Démonstration. $i)$ Si $b = 2^m 5^n$, alors $10^{n+m} x = a 2^n 5^m$ et donc $x \in \mathbb{D}$; réciproquement, $\mathbb{Z} \ni 10^l x = 10^l \frac{a}{b} \Rightarrow$ il existe $c \in \mathbb{Z}$ tel que $bc = 10^l a \Rightarrow b | 10^l a$. Or $b \wedge a = 1$, alors

$b|10^l = 2^l5^l \Rightarrow b = 2^m5^n$, où $m,\ n \in [\![0, l]\!]$.
$ii)$ On suppose sans reste de généralité que $x \notin \mathbb{Z}$. D'après $i)$, on sait que $x = \frac{a}{b} = 2^{-m}5^{-n}a$. On précise que $a = \tilde{a}2^k5^l$, où $\tilde{a} \wedge 2 = \tilde{a} \wedge 5 = 1$. Car $a \wedge b = 1$, on obtient $0 \in \{k, m\}$ et $0 \in \{l, n\}$. Alors $x = \tilde{a}2^{k-m}5^{l-n}$. Pour l'unicité, on suppose que $x = c2^a5^b = w2^u5^v$, où $a,\ b,\ c,\ u,\ v,\ w \in \mathbb{Z}$ et $c \wedge 2 = c \wedge 5 = w \wedge 2 = w \wedge 5 = 1$. On applique le lemme de Gauß, alors $c|w$ et $w|c$, donc $w = \pm c$, et $x = c2^a5^b = w2^u5^v$ nous dit que $w = c$. On obtient $2^{a-u} = 5^{v-b}$. Alors $a - u = v - b = 0$. □

4 Anneaux factoriels et Critère d'Irréductibilité des Polynômes

4.1 Anneaux factoriels

Les anneaux foctoriels sont de forme de propriété et ils sont beaucoup plus générals que les anneaux principaux.

Définition 4.1. On appelle **un système représentatif d'éléments irréductibles de** A un ensemble $\mathscr{P}$ d'élément irréductible de A tel que tout élément irréductible de A est associé à un seul élément de $\mathscr{P}$ i.e. $\mathscr{P} \overset{(bijection)}{\simeq} \mathscr{A}/\sim$, où $\mathscr{A} = \{a \in A,\ a \text{ est irréductible}\}$.

Exemple 4.2.
— $(\mathbb{Z}, +, \cdot)$, $\mathscr{P} = \mathcal{P}$.
— $K[X]$, $\mathscr{P}$ est l'ensemble des polynômes irréductibles unitaires. En factorisant, on emporte le coefficient du terme dominant : $P(X) = \sum_{k=0}^{n} a_kX^k$, $a_n \neq 0 \Rightarrow a_n \in K^* \Rightarrow P(X) = a_n\tilde{P}(X)$, où $\tilde{P}$ est unitaire.

Définition 4.3. Soit A un anneau intègre. On l'appelle **un anneau factoriel** s'il existe $\mathscr{P} \subset A$ tel que pour tout $x \in A \setminus \{0\}$, il existe une unique application $v : \mathscr{P} \to \mathbb{N}$ et un unique $u \in A^*$ telle que $x = u \prod_{\pi \in \mathscr{P}} \pi^{v(\pi)}$.

Sorite 4.4. *Les éléments de $\mathscr{P}$ sont alors nécessairement irréductibles et $\mathscr{P}$ forme un système représentatif d'éléments irréductibles de A.*

Démonstration. Dans un anneau factoriel, tout élément irréductible y a un unique élément associé dans $\mathscr{P}$. En effet, y possède une décomposition $y = u \prod_{\pi \in \mathscr{P}} \pi^{v_\pi}$. D'une part, $\sum_{\pi \in \mathscr{P}} v_\pi \geq 1$, sinon $y = u \in A^*$ mais y n'est pas inversible ; d'autre part, on a aussi $\sum_{\pi \in \mathscr{P}} v_\pi \leq 1$: il

existe $\rho \in \mathscr{P}$ tel que $v_{\rho \geq 1}$, on écrit alors $y = \rho(u\rho^{v_\rho - 1} \prod_{\pi \neq \rho} \pi^{v_\pi})$. y et ρ sont irréductibles $\Rightarrow \alpha = u\rho^{v_\rho - 1} \prod_{\pi \neq \rho} \pi^{v_\pi} \in A^*$. Or il y a une unique décomposition de $\alpha \Rightarrow \alpha = u$ et $v_\pi = 0$ pour tout $\pi \neq \rho$. Donc $y = u\rho$, alors y et ρ sont associés. On obtient l'unicité de ρ par l'unicité de décomposition.
On vient de voir que tout irréductible est associé à un unique élément de $\mathscr{P}$ i.e. $\mathscr{P}$ est un système représentatif d'irréductibles si on prouve plus que les éléments de $\mathscr{P}$ sont nécessairement irréductibles.
Supposons qu'il existe $\rho \in \mathscr{P}$ tel que $\rho = ab$, où a, $b \in A$. On en déduit une décomposition de $a = u \prod_{\pi \in \mathscr{P}} \pi^{v_\pi}$ et de $b = v \prod_{\pi \in \mathscr{P}} \pi^{w_\pi}$. Alors $\rho = ab = uv \prod_{\pi \in \mathscr{P}} \pi^{v_\pi + w_\pi}$. Or $\rho \in \mathscr{P} \Rightarrow$

$$\begin{aligned} 0 &= v_\pi + w_\pi, \quad \forall\, \pi \neq \rho \\ 1 &= v_\rho + w_\rho \\ 1 &= uv \end{aligned}$$

□

Alors $v_\pi = w_\pi = 0$ pour tout $\pi \neq \rho$ et soit $v_\rho = 0$ et $w_\rho = 1$, soit $v_\rho = 1$ et $w_\rho = 0$ i.e. $a \in A^*$ ou $b \in A^*$. C'est à dire que π est irréductible.

Sorite 4.5. *Soit A un anneau factoriel alors tout système représentatif d'élément irréductible $\mathscr{P}$ convient dans la définition d'anneau factoriel i.e. tout tel élément de A possède une décomposition unique sur $\mathscr{P}$ au sens de la définition d'anneau factoriel.*

Démonstration. Tout système représentatif d'éléments irréductibles est en bijection avec $\mathscr{B} = \mathscr{A}/\sim$, où $\mathscr{A} = \{a \in A,\ a \text{ est irréductible}\}$. Si $\mathscr{P}_1$ et $\mathscr{P}_2$ sont deux tels systèmes, ils sont alors en bijection. En effet, on précise $b_1 : \mathscr{P}_1 \to \mathscr{B}$, $b_2 : \mathscr{P}_2 \to \mathscr{B}$, alors $b = b_2^{-1} \circ b_1 : \mathscr{P}_1 \to \mathscr{P}_2$. Tout élément x de A possède une décomposition sur $\mathscr{P}_1$:

$$x = u \prod_{\pi \in \mathscr{P}_1} \pi^{v_\pi}.$$

Pour tout $\pi \in \mathscr{P}_1$, $b(\pi) \in \mathscr{P}_2$ avec π et $b(\pi)$ associés i.e. pour tout $\pi \in \mathscr{P}_1$, il existe $u_\pi \in A^*$ tel que $\pi = u_\pi b(\pi)$. Alors

$$x = u \prod_{\pi \in \mathscr{P}_1} (u_\pi b(\pi))^{v_\pi} = u \prod_{\pi \in \mathscr{P}_1} u_\pi^{v_\pi} \prod_{\pi \in \mathscr{P}_1} b(\pi)^{v_\pi}.$$

En reparamétrant le produit via b, on obtient alors

$$x = v \prod_{\rho \in \mathscr{P}_2} \rho^{v_{b^{-1}(\rho)}}.$$

Ceci établit l'existence d'une décoposition sur $\mathscr{P}_2$ à partir d'une décomposition sur $\mathscr{P}_1$. Reste à discuter l'unicité : toute décomposition sur $\mathscr{P}_2$ est unique s'il y a unicité de la décomposition sur $\mathscr{P}_1$: si $x \in A$ et

$$x = u \prod_{\rho \in \mathscr{P}_2} \rho^{v_\rho} = v \prod_{\rho \in \mathscr{P}_2} \rho^{w_\rho}.$$

Alors pour tout $\rho \in \mathscr{P}_2$, ρ est associé à $b^{-1}(\rho) \in \mathscr{P}_1$, il existe donc une unité $w_\rho \in A^*$ telle que $\rho = r_\rho b^{-1}(\rho)$. En substituant, il vient

$$\begin{aligned} x &= u \prod_{\rho \in \mathscr{P}_2} r_\rho^{v_\rho} \prod_{\rho \in \mathscr{P}_2} b^{-1}(\rho)^{v_\rho} \\ &= v \prod_{\rho \in \mathscr{P}_2} r_\rho^{w_\rho} \prod_{\rho \in \mathscr{P}_2} b^{-1}(\rho)^{w_\rho}. \end{aligned}$$

En reparamétranrt le produit via la bijection b, ceci se lit :

$$\begin{aligned} x &= u \prod_{\pi \in \mathscr{P}_1} r_{b(\pi)}^{v_{b(\pi)}} \prod_{\pi \in \mathscr{P}_1} b(\pi)^{v_{b(\pi)}} \\ &= v \prod_{\pi \in \mathscr{P}_1} r_{b(\pi)}^{w_{b(\pi)}} \prod_{\pi \in \mathscr{P}_1} b(\pi)^{w_{b(\pi)}}. \end{aligned}$$

Or il y a unicité de la décomposition sur $\mathscr{P}_1$, donc $u \prod\limits_{\pi \in \mathscr{P}_1} r_{b(\pi)}^{v_{b(\pi)}} = v \prod\limits_{\pi \in \mathscr{P}_1} r_{b(\pi)}^{w_{b(\pi)}}$ et $v_{b(\pi)} = w_{b(\pi)}$ pour tout $\pi \in \mathscr{P}_1$. En reportant alors $u \prod\limits_{\rho \in \mathscr{P}_2} r_\rho^{v_\rho} = v \prod\limits_{\rho \in \mathscr{P}_2} r_\rho^{w_\rho}$ et $v_\rho = w_\rho$ pour tout $\rho \in \mathscr{P}_2$. D'où l'unicité de la décomposition sur $\mathscr{P}_2$ à partir de l'unicité de la décomposition sur $\mathscr{P}_1$. □

Remarque 4.6. On considère $b : \mathscr{P}_1 \to \mathscr{P}_2$. $b^{-1} \circ b : \mathscr{P}_1 \to \mathscr{P}_1$ est l'identité de $\mathscr{P}_1$. Pour tout $\pi \in \mathscr{P}_1$, $b(\pi) = u_\pi \pi$; pour tout $\rho \in \mathscr{P}_2$, $b^{-1}(\rho) = v_\rho \rho$. Alors $\pi = b^{-1} \circ b(\pi) = v_{b(\pi)} b(\pi) = v_{b(\pi)} u_\pi \pi$. On en déduit l'identité : $v_{b(\pi)} = u_\pi^{-1}$.

Sorite 4.7. *Soit A un anneau factoriel et soit π un élément irréductible de A. On suppose $x \in A \setminus \{0\}$, alors $\{n \in \mathbb{N},\ \pi^n | x\}$ est majoré. On pose $v_\pi(x) = \max\{n \in \mathbb{N},\ \pi^n | x\}$. On l'appelle valuation $\pi -$ adique de x. On a alors $x = u \prod\limits_{\pi \in \mathscr{P}} \pi^{v_\pi(x)}$, où $u \in A^*$, pour tout $x \in A \setminus \{0\}$.*

Démonstration. Pour tout $\rho \in A$ irréductible, il existe un unique élément $\sigma \in \mathscr{P}$ associé à ρ. On suppose $\sigma = u\rho$, où $u \in A^*$. Pour tout $x \in A \setminus \{0\}$, on a une unique décomposition sur $\mathscr{P}$:

$$\begin{aligned} x &= v \prod_{\pi \in \mathscr{P}} \pi^{v_\pi} \\ &= v\sigma^{v_\sigma} \prod_{\pi \neq \sigma} \pi^{v_\pi} \\ &= vu^{v_\sigma} \rho^{v_\sigma} \prod_{\pi \neq \sigma} \pi^{v_\pi}. \end{aligned}$$

Donc $\rho^{v_\sigma} | x$ et alors $v_\sigma(x) \geq v_\sigma$. Par ailleurs, il existe $a \in A$ tel que $x = a\rho^{v_\sigma(x)}$. Alors on a une unique décomposition de a sur $\mathscr{P}$: $a = w \prod_{\pi \in \mathscr{P}} \pi^{w_\pi}$. Et donc

$$\begin{aligned} v \prod_{\pi \in \mathscr{P}} \pi^{v_\pi} = x &= a\rho^{v_\sigma(x)} \\ &= w\rho^{v_\sigma(x)} \prod_{\pi \in \mathscr{P}} \pi^{w_\pi} \\ &= wu^{-v_\sigma(x)} \sigma^{v_\sigma(x)} \prod_{\pi \in \mathscr{P}} \pi^{w_\pi} \\ &= wu^{-v_\sigma(x)} \sigma^{v_\sigma(x) + w_\sigma} \prod_{\pi \neq \sigma} \pi^{w_\pi} \end{aligned}$$

Or il y a unicité de la décomposition sur $\mathscr{P}$ donc en particulier $v_\sigma(x) \leq v_\sigma(x) + w_\sigma = v_\sigma \leq v_\sigma(x) \Rightarrow v_\sigma = v_\sigma(x)$. $\square$

Remarque 4.8. Avec les notations précédentes $x = v \prod_{\pi \in \mathscr{P}} \pi^{v_\pi}$, où $v_\pi = 0$ sauf un nombre fini. Alors tout corps est un anneau factoriel.

Remarque 4.9. Une approche un peu plus formelle : soit A un anneau intègre. On pose $D(A) = \big(A \setminus \{0\}\big)/\sim$, où $\sim$ est une relation d'équivalence définie par : $a \sim b$ s.s.i. a et b sont associés. La multiplication de $(A, +, \cdot)$ induit sur $D(A)$ une structure de monoïde :

$$\begin{tikzcd} A \times A \arrow[r, "(\cdot)"] \arrow[d, "\omega\times\omega"'] & A \arrow[d, "\omega"] \\ D(A) \times D(A) \arrow[r, "(\cdot)"] & D(A) \end{tikzcd}.$$

Ça marche dès que le noyau de $\omega \times \omega$ est inclus dans le noyau $\omega \circ m$: $\ker(\omega \times \omega) = A^* \times A^*$, $(A^*, \cdot)$ forme un groupe et donc $\mathrm{Im}(\omega \circ m|_{A^* \times A^*}) \subset \omega(A^*) = \{1\}$. En fait, $\ker(\omega \times \omega) \subset \ker(\omega \circ m)$ car $\ker(\omega \circ m) = \{(a, b) \in A \times A,\ \omega(ab) = 1\} = \{(a, b) \in A \times A,\ ab \in A^*\} = A^* \times A^*$. La multiplication de $D(A)$ est associatif et commutatif car la multiplication de A l'est. Dans la catégorie des monoïdes associatifs et commutatifs, on a la notion de monoïdee libre F sur une partie P. Tout élément du monoïde F s'écrit de façon unique(à l'ordre près d'éléments) comme un produit fini d'éléments de la partie P. Donc A est factoriel s.s.i. $D(A)$ est libre sur les classes des éléments irréductibles de A.

Théorème 4.10. *Soit K un corps, alors $K[X]$ est un anneau factoriel.*

Démonstration. On choisit $\mathscr{P}$ l'ensemble des polynômes irréductibles unitaires. C'est une représentatif d'éléments irréductibles. Pour ce faire, on procède par récurrence sur le degré de P. Si $\deg P$=0, $P \in K \setminus \{0\} = K^*$, la conclusion est vraie. Si $\deg P > 0$, soit P est irréductible, soit $P = P_1P_2$, où P_1, $P_2 \in K[X]$ et $\deg P_1$, $\deg P_2 \geq 1$. Si P est irréductible, alors $P = a_n(a_n^{-1}P)$ et on le finit ; si $P = P_1P_2$, on applique l'hypothèse de récurrence aux P_1 et P_2, alors $P_1 = u_1 \prod\limits_{Q\in\mathscr{P}} Q^{v_{Q,1}}$, $P_2 = u_2 \prod\limits_{Q\in\mathscr{P}} Q^{v_{Q,2}}$. Donc $P = P_1P_2 = u_1u_2 \prod\limits_{Q\in\mathscr{P}} Q^{v_{Q,1}+v_{Q,2}}$, d'où l'existence de la décomposition est démontré.
Pour l'unicité on procède de même. D'après la partie précédente P possède une décomposition : $P = u \prod\limits_{Q\in\mathscr{P}} Q^{v_Q}$, où v_Q est nul sauf un nombre fini de Q. Supposons que P possède aussi la décomposition suivante $P = u' \prod\limits_{Q\in\mathscr{P}} Q^{v'_Q}$, où v'_Q est nul sauf un nombre fini de Q. Puisque $\deg P \geq \sum\limits_{Q\in\mathscr{P}} v_Q \geq 1$ si $P \notin K[X]^*$ et il existe Q_0 divise alors le produit $P = u' \prod\limits_{Q\in\mathscr{P}} Q^{v'_Q}$. Q est irréductible, d'après le lemme d'Euclide il divise Q'_0 l'une des éléments de $\mathscr{P}$. Alors $Q_0 = Q'_0$. L'identité des deux décompositions de P ci-dessus se lit $uQ_0^{v_{Q_0}} \prod\limits_{Q\neq Q_0} Q^{v_Q} = u'Q_0^{v'_{Q_0}} \prod\limits_{Q\neq Q_0} Q^{v'_Q}$ donc on en déduit que le P/Q possède les deux expressions

$$uQ_0^{v_{Q_0}-1} \prod_{Q\neq Q_0} Q^{v_Q} = u'Q_0^{v'_{Q_0}-1} \prod_{Q\neq Q_0} Q^{v'_Q}$$

Or le degré du polynôme $P/Q = \deg P - \deg Q < \deg P$. On applique donc l'hypothèse de récurrence au polynôme P/Q et l'unicité de sa décomposition sur les éléments irréductibles unitaires se lit alors : $u = u'$, $v_{Q_0} - 1 = v'_{Q_0} - 1$ et $v_Q = v'_Q$ pour tout $Q \neq Q_0$. On en déduit évidement $v_Q = v'_Q$ pour tout $Q \in \mathscr{P}$. On conclut donc à l'unicité de la décomposition de P, ce qui achève la démonstration du théorème. □

Définition 4.11. Soit A un anneau. On dit que A est **noethérien** si toutr suite croissante d'idéaux est stationnaire.

Proposition 4.12. *Tout anneau principal est noethérien.*

Démonstration. Soit $(I_i)_{i\in\mathbb{N}}$ une suite croissante d'idéaux de A. Alors $J = \bigcup\limits_{i\in\mathbb{N}} I_i$ est banalement un idéal. A est principal, donc il existe $x \in A$ tel que $J = (x)$. Alors il existe $i \in \mathbb{N}$ tel que

$x \in I_i$. On trouve que $J = (x) \subset I_i$, alors $J = I_i$. La suite $(I_i)_{i\in\mathbb{N}}$ est donc stationnaire. $\square$

Proposition 4.13. *Soit A un anneau intègre et noethérien. Alors tout élément non nul possède une décomposition $x = u \prod_{i=0}^{n} a_i$, où $u \in A^*$ et a_i est irréductible pour tout i.*

Démonstration. Soit $x \in A \setminus A^*$ non nul. On la montre par l'absurde. Si x n'admet pas de décomposition finie en éléments irréductibles. Alors par hypothèse x n'est pas irréductible. Donc $x = x_{-1}x_1$, où $x_{-1}, x_1 \in A \setminus A^*$. En particulier $(x) \subsetneqq (x_\epsilon)$, où $\epsilon \in \{\pm 1\}$. Par hypothèse, soit x_{-1}, soit x_1, n'admet pas de décomposition finie en éléments irréductibles. Alors on peut écrire $x_{\epsilon_1} = x_{\epsilon_1,-1}x_{\epsilon_1,1}$, où $\epsilon_1 \in \pm 1$ et $x_{\epsilon_1,-1}, x_{\epsilon_1,1} \in A \setminus A^*$. On obtient alors $(x_{\epsilon_1}) \subsetneqq (x_{\epsilon_1,\epsilon_2})$, où $\epsilon_2 \in \{\pm 1\}$.
Par récurrence sur $n \in \mathbb{N}$, on construit une suite d'éléments $x_{\epsilon_1,\cdots,\epsilon_n} \in A \setminus A^*$, o'u $\epsilon_i \in \{\pm 1\}$ pour tout $i \in \mathbb{N}$, telle que $(x_{\epsilon_1,\cdots,\epsilon_n}) \subsetneqq (x_{\epsilon_1,\cdots,\epsilon_{n+1}})$ pour tout $n \in \mathbb{N}$. Alors on trouve une suite d'idéaux croissante strictement, ceci contredit alors que A est un anneau noethérien. $\square$

Proposition 4.14. *Soit A un anneau intègre avec la propriété de décomposition donné par la proposition 4.13. Alors A est factoriel si pour tout élément irréductible p de A, (p) est premier.*

Démonstration. Il reste de vériefir que la décomposition en éléments irréductibles de l'hypothèse est unique.
Soit $\mathscr{P}$ un système représentatif d'éléments irréductibles. Toute décomposition $x = u \prod_{i=0}^{n} a_i^{v_i}$, se réécrit sur $\mathscr{P}$: pour tout $i \in [\![1, n]\!]$, il existe un unique élément irréductible π_1 de $\mathscr{P}$ tel que $a_i = u_i\pi_i$, où $u_i \in A^*$. En substituant, $x = u \prod_{i=0}^{n} a_i^{v_i} = u \prod_{i=0}^{n} u_i^{v_i} \prod_{i=0}^{n} \pi_i^{v_i}$. Dans cette écriture, il peut encore π_i avoir des répétitions. En regroupant, on écrit $x = u \prod_{\pi\in\mathscr{P}} \pi^{v_\pi}$, où $v_\pi = 0$ sauf un nombre fini d'éléments.
Si $x = v \prod_{\pi\in\mathscr{P}} \pi^{v_\pi} = w \prod_{\pi\in\mathscr{P}} \pi^{w_\pi}$, alors pour ρ un élément arbitaire de $\mathscr{P}$, sans perte de généralité, on suppose que $v_\rho > w\rho$, donc $v\rho^{v_\rho - w_\rho} \prod_{\pi\neq\rho} \pi^{v_\pi} = w \prod_{\pi\neq\rho} \pi^{w_\pi} \Rightarrow \rho | w \prod_{\pi\neq\rho} \pi^{w_\pi}$. Or par hypothèse (ρ) est premier car ρ est irréductible. Alors il existe $\pi \in \mathscr{P} \setminus \{\rho\}$, tel que $\rho|\pi$, i.e. ρ et π sont associés. Contradiction ! $\square$

Théorème 4.15. *Tout anneau principal est factoriel.*

Démonstration. Tout anneau principal est noethérien par proposition 4.12, alors tout élément non nul possède une décomposition d'éléments irréductibles par proposition 4.13, et la décomposition est unique par proposition 4.14. $\square$

Corollaire 4.16. *Soit K un corps, alors $K[X]$ est factoriel.*

Démonstration. On a vu que $K[X]$ est principal, ainsi il est factoriel. $\square$

Définition 4.17. Soit A un anneau factoriel et soit $\mathscr{P}$ un système représentatif d'éléments irréductibles. Pour $a,\, b \in A \setminus \{0\}$. On définit **le plus grand diviseur commun de a et b** par $\mathrm{pgcd}(a,b) = \prod_{\pi\in\mathscr{P}} \pi^{\min\{v_\pi(a), v_\pi(b)\}}$. La définition ne dépend pas du choix de $\mathscr{P}$ à unité près.

Proposition 4.18 (Gauß)**.** *Soit A un anneau factoriel et soient $a,\, b,\, c \in A$. On suppose $a|bc$ et $a \wedge b = 1$ i.e. $\mathrm{pgcd}(a,b) = 1$, alors $a|c$.*

Démonstration. Soit $\mathscr{P}$ un système représentatif d'éléments irréductibles. Alors on donne la décomposition des éléments : $a = u_a \prod_{\pi\in\mathscr{P}} \pi^{v_\pi(a)}$, $b = u_b \prod_{\pi\in\mathscr{P}} \pi^{v_\pi(b)}$, $c = u_c \prod_{\pi\in\mathscr{P}} \pi^{v_\pi(c)}$. Par $a \wedge b = 1$, pour tout $\pi \in \mathscr{P}$, soit $v_\pi(x) = 0$, soit $v_\pi(y) = 0$. Or $a|bc$ i.e.

$$\Big(u_a \prod_{\pi\in\mathscr{P}} \pi^{v_\pi(a)}\Big)\Big|\Big(u_b u_c \prod_{\pi\in\mathscr{P}} \pi^{v_\pi(b)+v_\pi(c)}\Big),$$

donc on obtient que $v_\pi(a) \leq v_\pi(b) + v_\pi(c)$. Si $v_\pi(a) > 0$, alors $v_\pi(b) = 0$ et $v_\pi(a) \leq v_\pi(c)$; si $v_\pi(a) = 0$, alors évidement $v_\pi(a) \leq v_\pi(c)$. On en déduit que $a|c$. $\square$

Corollaire 4.19. *Dans un anneau factoriel, l'idéal engendré par un élément irréductible est premier i.e. pour tout π irréductible et $x,\, y \in A$, $\pi|xy \Rightarrow \pi|x$ ou $\pi|y$.*

Démonstration. On a déjà établi cet énoncé dans tout anneau avec pgcd comme corollaire du lemme de Gauß dans les anneaux avec *pgcd*. On remarque que pour π irréductible et a quelconque dans A, soit $\pi \wedge a = 1$, soit $\pi|a$.
En effet, soit π un élément irréductible de A, alors le lemme de Gauß dans les anneaux factoriel implique que $\pi|xy \Rightarrow \pi|x$ ou $\pi|y$ pour tout $x,\, y$. Si $\pi \wedge x = 1$, alors $\pi|y$. $\square$

Exemple 4.20. $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel car 3 est irréductible et (3) n'est pas premier. Par ailleurs, $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel implique que $\mathbb{Z}[i\sqrt{5}]$ n'est pas principal.

4.2 Irréductibilité des Polynômes

Définition 4.21. Soit A un anneau avec pgcd et soit $P(X) = \sum_{k=0}^{d} a_k X^k$ un polynôme dans $A[X]$. On dit que P est **primitif** si ses coefficients $(a_k)_{k\in[\![1,d]\!]}$ sont premiers entre eux i.e. $\mathrm{pgcd}(a_1, \cdots, a_d) = 1$.

Sorite 4.22. *Pour tout $a \in A$, on introduit $\rho_a : A \to A/(a)$ la réduction modulo a, elle induit $\rho_a : A[X] \to A/(a)[X]$ un morphisme d'anneaux. Alors $P \in A[X]$ est primitif s.s.i. $\rho_a(P)$ pour tout a irreéductible de A.*

Démonstration. $\Leftarrow$: Si $P \in A[X]$ n'est pas primitif, i.e. $\operatorname{pgcd}(a_1, \cdots, a_d) = \delta = u \prod_{\pi \in \mathscr{P}} \pi^{v_\pi(\delta)} \notin A^*$. Alors il existe $\pi \in \mathscr{P}$ tel que $v_\pi(\delta) \geq 1$, donc $\pi|\delta$ et on obtient $\pi|a_k$ pour tout k. Alors $\rho_a(P) = 0$.
$\Rightarrow$: Soit $a \in A$ un élément irréductible tel que $\rho_a(P) = 0$ i.e. $\rho_a(a_k) = 0$ pour tout $k \in [\![1, d]\!]$ i.e. $a|a_k$ pour tout $k \in [\![1, d]\!]$ i.e. $a|\operatorname{pgcd}(a_1, \cdots, a_d) \Rightarrow P$ n'est pas primitif. $\square$

Lemme 4.23 (de Gauß)**.** *Soit A un anneau factoriel. On suppose que P et $Q \in A[X]$ sont primitifs, alors $PQ \in A[X]$ est primitif.*

Démonstration. On a vu que pour tout $a \in A$ irréductible, (a) est premier i.e. $A/(a)$ est intègre, donc $A/(a)[X]$ est intègre. On utilise la conclusion précédente : P et Q sont primitifs, alors $\rho_a(P) \neq 0$ et $\rho_a(Q) \neq 0$, et ainsi $\rho_a(PQ) = \rho_a(P)\rho_a(Q) \neq 0 \Rightarrow PQ$ est primitif. $\square$

Lemme 4.24. *Soit A un anneau factoriel et soit K_A son corps des fractions. On suppose que $P \in A[X]$ est primitif et $k \in K_A \setminus \{0\}$, alors $kP \in A[X] \Rightarrow k \in A \setminus \{0\}$.*

Démonstration. On suppose $k = \frac{a}{b}$, où $(a, b) \in A \times (A \setminus \{0\})$ et $a \wedge b = 1$. Par hypothèse $kP(X) = \frac{a}{b}P(X) = \sum_{k=0}^{d} \frac{a_k a}{b} X^k \in A[X]$ i.e. $b|a_k a$ pour tout $k \in [\![1, d]\!]$. Or le lemme de Gauß dans les anneaux factoriels nous dit que $b|a_k$ car $a \wedge b = 1$. Or P est primitif, donc $b \in A^*$ i.e. $k \in A \setminus \{0\}$. $\square$

Proposition 4.25. *Soit A un anneau factoriel, alors $A[X]$ est factoriel.*

Démonstration. On a vu que la conclusion est vraie si A est un coprs. Donc $K_A[X]$ est factoriel.
Dans un anneau avec pgcd, en particulier factoriel, tout $P \in A[X]$ s'écrit $P = \operatorname{pgcd}(a_1, \cdots, a_d)\tilde{P}$, où $\tilde{P}$ est primitif. Pour tout $P = \sum_{k=0}^{d} \frac{p_k}{q_k} X^k \in K_A[X]$ avec $p_k \wedge q_k = 1$ pour tout $k \in [\![1, d]\!]$, on pose $\tilde{P} = \frac{q}{\operatorname{pgcd}(q\frac{p_1}{q_1}, \cdots, q\frac{p_d}{q_d})} P$, où $q = \operatorname{ppcm}(q_1, \cdots, q_d)$. Alors $\tilde{P} \in A[X]$ est primitif. De plus, $\tilde{P}$ et P sont associés dans $K_A[X]$. Soit $\mathscr{P}$ un système représentatif d'éléments irréductibles de $K_A[X]$, $\mathscr{P}' = \{\tilde{P},\ P \in \mathscr{P}\}$ est alors un système représentatif d'éléments irréductibles de $K_A[X]$.
On donne la décomposition d'éléments irréductibles dans $K_A[X]$: $P = k \prod_{Q \in \mathscr{P}'} Q^{v_Q(P)}$. D'après

le lemme 4.23, $\prod_{Q\in\mathscr{P}'} Q^{v_Q(P)} \in A[X]$ est primitif. Si $P \in A[X]$, alors $k \in A\setminus\{0\}$ d'après le lemme 4.24. Car A est factoriel, on pose $\mathscr{P}_A$ un système représentatif d'éléments irréductibles de A, et on précise que $k = u\prod_{\pi\in\mathscr{P}_A}\pi^{v_\pi(k)}$, où $u \in A^* = A[X]^*$. Donc on construit une décomposition d'éléments irréductibles de $A[X]$:

$$P = u\prod_{\pi\in\mathscr{P}_A}\pi^{v_\pi(k)}\prod_{Q\in\mathscr{P}'}Q^{v_Q(P)}.$$

L'unicité de la décomposition est conséquence de l'uncité des décompositions dans $K[X]$ d'une part et dans A de l'autre. En effet, si $u\prod_{\pi\in\mathscr{P}_A}\pi^{v_\pi}\prod_{Q\in\mathscr{P}'}Q^{v_Q} = v\prod_{\pi\in\mathscr{P}_A}\pi^{w_\pi}\prod_{Q\in\mathscr{P}'}Q^{w_Q}$, par l'uncité des décompositions dans $K[X]$, on obtient que $u\prod_{\pi\in\mathscr{P}_A}\pi^{v_\pi} = v\prod_{\pi\in\mathscr{P}_A}\pi^{w_\pi}$ et $v_Q = w_Q$ pour tout $Q \in \mathscr{P}'$; par l'uncité des décompositions dans A, on obtient que $u = v$ et $v_\pi = w_\pi$ pour tout $\pi \in \mathscr{P}_A$.
Alors sur $\mathscr{P}_0 = \mathscr{P}'\cup\mathscr{P}_A$, il y a une unique décomposition de $A[X]$ et $\mathscr{P}_0$ est, en particulier, un système représentatif d'éléments irréductibles de $A[X]$. On conclut que $A[X]$ est factoriel. □

Théorème 4.26. *Soit A un anneau factoriel, alors $A[X_1,\cdots,X_n]$ est factoriel.*

Démonstration. C'est une corollaire de la proposition 4.25. Par récurrence sur n, l'isomorphisme $A[X_1,\cdots,X_n] = A[X_1,\cdots,X_{n-1}][X_n]$ donne la conclusion. □

Remarque 4.27. Donc la catégorie des anneaux factoriels est beaucoup plus grosse que celle des anneaux principaux.

Corollaire 4.28. *Soit A un anneau factoriel et soit K_A son corps des fractions. On suppose que $P \in A[X]\setminus A$, alors les affirmations suivantes sont équivalentes :*
i) P est irréductible dans $A[X]$;
ii) P est primitif et irréductible dans $K[X]$.

Démonstration. Au début, on construit $\mathscr{P}$ comme la proposition 4.24 un système représentatif d'éléments irréductibles de $K_A[X]$ où tout polynôme appartient à $A[X]$ et est primitif. On précise que $P(X) = \sum_{k=0}^{d} a_kX^k \in A[X]$ et on pose $\delta = \mathrm{pgcd}(a_1,\cdots,a_d)$.
$i) \Rightarrow ii)$: Si $\delta \in A\setminus A^*$, alors $P = \delta\frac{P}{\delta} \in A[X]$ n'est pas irréductible, donc $\delta \in A^*$. Donc P est primitif.
Si $P = QR$, où Q, $R \in K[X]$. D'après $K[X]$ est factoriel, on peut donner des décompositions uniques dans $K_A[X]$: $Q = q\prod_{T\in\mathscr{P}}T^{v_T(Q)}$ et $R = r\prod_{T\in\mathscr{P}}T^{v_T(R)}$. Alors $P = QR =$

$qr \prod_{T\in\mathscr{P}} T^{v_T(Q)+v_T(R)}$. Le lemme 4.23 entraîne que $S = \prod_{T\in\mathscr{P}} T^{v_T(Q)+v_T(R)}$ est primitif et le lemme 4.24 entraîne que $qr \in A\setminus\{0\}$. Or P est irréductible dans $A[X]$, alors $qr \in A^*$ et il existe un unique élément $T_0 \in \mathscr{P}$ tel que $v_T(Q)+v_T(R) = 0$ pour tout $T \neq T_0$ et $v_{T_0}(Q)+v_{T_0}(R) = 1$. Donc soit $Q = q$ et $R = rT_0$, soit $Q = qT_0$ et $R = r$. On conclut alors P est irréductible dans $K_A[X]$.

ii) $\Rightarrow$ *i)* : Par hypothèse, P est primitif et irréductible dans $K_A[X]$, alors la décomposition de P sur $\mathscr{P}$ s'écrit $P = kT$, où $k \in K[X]^* = K^*$ et $T \in \mathscr{P} \subset A[X]$. On applique le lemme 4.24 donc $k \in A\setminus\{0\}$ car T est primitif dans $A[X]$. P est primitif $k|\delta \Rightarrow k \in A^*$. Donc P est associé avec T dans $A[X]$ i.e. P est irréductible. □

Proposition 4.29. *Soit A un anneau factoriel et soit K_A son corps des fractions. On suppose que P et $Q \in A[X]$ sont unitaires et que Q divise P. Si $P \in A[X]$, alors $Q \in A[X]$.*

Démonstration. Au début, on construit $\mathscr{P}$ comme la proposition 4.24 un système représentatif d'éléments irréductibles de $K_A[X]$ où tout polynôme appartient à $A[X]$ et est primitif. On précise que $P = QR$, où $R \in K_A[X]$. On décompose P, Q et R sur $\mathscr{P}$: $P = p \prod_{T\in\mathscr{P}} T^{v_T(P)}$, $Q = q \prod_{T\in\mathscr{P}} T^{v_T(Q)}$ et $R = r \prod_{T\in\mathscr{P}} T^{v_T(R)}$, où p, q et $r \in K^*$.

Puisque $P = QR$ et de l'unité de la décomposition sur $\mathscr{P}$, on obtient $p = qr$ et $v_T(P) = v_T(Q) + v_T(R)$ pour tout $T \in \mathscr{P}$. D'après le lemme 4.23, $\prod_{T\in\mathscr{P}} T^{v_T(P)} \in A[X]$ est primitf et d'après le lemme 4.24, $qr = p \in A\setminus\{0\}$. Écrivons $q = \frac{q_1}{q_2}$ et $r = \frac{r_1}{r_2}$, où (q_1, q_2) et $(r_1, r_2) \in A \times (A\setminus\{0\})$. On peut supposer de plus que $q_1 \wedge q_2 = 1$, $r_1 \wedge r_2 = 1$. Donc $pq_2r_2 = q_1r_1$. Le lemme de Gauß implique que $q_2|r_1$ et $r_2|q_1$.

C'eat banal que R est unitaire car P et Q sont unitaires, il suffit de considerer le coefficient du terme de plus haut degré de P. Introduisons donc c le coefficient du terme de plus haut-degré du produit fini $\prod_{T\in\mathscr{P}} T^{v_T(R)}$. Alors $1 = \frac{r_1}{r_2}c$ i.e. $cr_1 = r_2$, donc $r_1|r_2$, mais $r_1 \wedge r_2 = 1$, on obtient ainsi $r_1 \in A^*$ et immédiatement $q_2 \in A^*$. Alors $q = \frac{q_1}{q_2} \in A$ et $Q = q \prod_{T\in\mathscr{P}} T^{v_T(Q)} \in A[X]$. □

On va en particulier établir le critère suivant, on le dit d'Eisenstein.

Théorème 4.30. *Soit A un anneau factoriel et soit $K = K_A$ son corps des fractions. On suppose $P(X) = \sum_{k=0}^{n} a_k X^k \in A[X]$, où $n = \deg P$. S'il existe un élément irréductible π de A tel que*

i) π ne divise pas a_n.

ii) π divise tous les a_k, $k \in [\![1, n-1]\!]$.

iii) π^2 ne divise pas a_0.

Alors $P(X)$ est irréductible dans $K_A[X]$.

Démonstration. Si P n'est pas irréductible dans $K_A[X]$, alors P n'est pas irréductible dans $A[X]$ par la sorite 4.22 et il possède une factorisation $P = QR$ dans $A[X]$ avec $q = \deg Q$, $r = \deg R \geq 1$. On considère la réduction modulo (π), i.e. la projection $\rho_\pi : A[X] \to A/(a)[X]$ qui est un morphisme d'anneaux, et ce qui justifie la notion d'idéal. Sous les hypothèses du théorème $\rho_\pi(Q)\rho_\pi(R) = \rho_\pi(P) = \rho_\pi(a_n)X^n$.
Les seuls diviseurs du polynôme $\rho_\pi(a_n)X^n$ sont de la forme $a_m X^m$ où $a_m \in A/(\pi)$. En effet, si $(a_{k_1}X^{k_1} + \cdots + a_{k_s}X^{k_s})(b_{l_1}X^{l_1} + \cdots + b_{l_t}X^{l_t}) = c_n X^n$ dans un anneau intègre, où $a_i \neq 0$ et $b_j \neq 0$ pour tout $i \in [\![1, s]\!]$ et $j \in [\![1, t]\!]$, alors $k_1 + l_1 = n$ et $a_k b_l = c_n$; si $s > 1$ et $t > 1$, $k_t + l_s < k_1 + l_1$ et $a_{k_s} b_{l_t} = 0$. Contradiction ! On en déduit que $\rho_\pi(Q) = bX^q$ et $\rho_\pi(R) = cX^r$, alors $\rho_\pi(b_0) = \rho_\pi(c_0) = 0$ i.e. $\pi | b_0$ et $\pi | c_0$. Donc $\pi^2 | b_0 c_0 = a_0$. Contradiction ! □

Corollaire 4.31. *Si P est de plus primitif, alors P est irréductible dans $A[X]$.*

Démonstration. C'est banal d'après la sorite 4.22 et le théorme 4.30. □

Corollaire 4.32. *Soit a un intègre non nul. On suppose qu'il existe $p \in \mathcal{P}$ tel que $v_p(a) = 1$, alors $X^n - a$ est irréductible dans $\mathbb{Q}[X]$.*

Remarque 4.33. On peut le généraliser dans tout anneau factoriel A.

Corollaire 4.34. *Soit p un intègre premier. On appelle $\Phi_p(X) = \sum\limits_{k=0}^{p-1} X^k = \frac{X^p - 1}{X - 1}$ le p-ième polynôme cyclotomique. Alors il est irréductible dans $\mathbb{Q}[X]$.*

Démonstration. Introduisons $\Psi_p(X) = \Phi_p(X+1) = \sum\limits_{k=0}^{p-1} \binom{p}{k+1} X^k$.
Pour tout $k \in [\![0, p-2]\!]$, $\binom{p}{k+1} = \frac{p!}{(p-k-1)!(k+1)!} \Rightarrow (p-k-1)!(k+1)! \big| p!$. Or $p \wedge (p-k-1)!(k+1)! = 1$, alors $(p-k-1)!(k+1)! \big| (p-1)!$ d'après le lemme de Gauß. On a alors $\binom{p}{k+1} = p\frac{(p-1)!}{(p-k-1)!(k+1)!}$ et donc $p | \binom{p}{k+1}$. (On peut aussi considerer $Q(X) = (X-1)^p = \sum\limits_{k=0}^{p} \binom{p}{k}(-1)^{p-k}X^k$ et $p | p(X-1)^{p-1} = Q'(X) = \sum\limits_{k=0}^{p-1}(k+1)\binom{p}{k+1}(-1)^{p-k}X^k$ et en déduit la conclusion.)
Maintenant on a vérifié les hypothèses du critère d'Eisenstein par $\Psi_p(X)$, donc $\Psi_p(X)$ est irréductible sur $\mathbb{Q}[X]$. Si $\Phi_p = QR$, où Q, $R \in \mathbb{Q}[X]$, alors $\Psi_p(X) = \Phi_p(X+1) = Q(X+1)R(X+1)$ et on obtient que $Q(X+1) \in \mathbb{Q}[X]^* = \mathbb{Q}^*$ ou $R(X+1) \in \mathbb{Q}^*$ i.e. $Q \in \mathbb{Q}^*$ ou $R \in \mathbb{Q}^*$. C'est à dire que $\Phi_p(X)$ est irréductible sur $\mathbb{Q}[X]$. □

Deuxième partie

Corps et Extensions de Corps

5 Corps

Un corps est un anneau non nul dont tous les éléments non ul sont inversibles i.e. $K^* = K \setminus \{0\}$.

Définition 5.1. Soient K et L deux corps. **Un isomorphisme de corps** $\varphi : K \to L$ est un morphisme d'anneaux unitaires.

Lemme 5.2. *Tout morphisme de corps non trivial est injectif.*

Démonstration. Pour tout $x \in K \setminus \{0\}$, il existe $x^{-1} \in K$ tel que $xx^{-1} = 1_K$. On prend l'image de l'équation par φ, alors $\varphi(x)\varphi(x^{-1}) = \varphi(1_K) = 1_L$. Donc $\varphi(x) = 0_L$ s.s.i. $x = 0_K$. En particulier, tout morphisme de corps non trivial $\varphi : K \to L$ est un isomorphisme sur son image, donc on identifie souvent K et $\varphi(K)$ sus-corps de L. □

Définition 5.3. Un morphisme de corps est appelé **une extension**. On dit que $\varphi : K \to L$ est un extension de K.

Remarque 5.4. Bien sûr, il existe des extensions qui ne sont pas des isomorphismes. Par exemple, $(\mathbb{R}, +, \cdot) \to (\mathbb{C}, +, \cdot)$. Mais tout endomorphisme d'un corps fini est donc un isomorphisme. L'extension d'une famille quelconque de sous-anneaux de L est encore un sous-anneau de L.

Définition 5.5. Soit A une partie de L, alors $\bigcap\limits_{\substack{B \text{ sous-anneau de } L \\ K \subset B, A \subset B}} B$ est encore un sous-anneau de L, on l'appelle **le sous-anneau engendré par** A sur K et on le note $K[A]$. Alors $K[A]$ est une $K-$algèbre intègre.
De même, l'intersection d'une famille arbitaire de sous-corps de L est encore un sous-corps de L. Il existe donc par tout partie A de L un plus petit sous-corps de L contenant K et A : $\bigcap\limits_{\substack{M \text{ sous-corps de } L \\ K \subset M, A \subset M}} M$. On l'appelle **le sous-corps engendré par** A sur K et on le note $K(A)$.

Définition 5.6. Soit $K \to L$ une extension de corps est de **type fini** s'il existe une partie finie $A \subset L$ telle que $L = K(A)$.

Lemme 5.7. *Soit $K \to L$ une extension de corps et soit $A \subset L$. Alors $K(A)$ coïncide avec le corps des fractions de $K[A]$ i.e. $K(A) = K_{K[A]}$.*

Démonstration.
$$K[A] = \bigcap_{\substack{B \text{ sous-anneau de } L \\ K \subset B, A \subset B}} B$$
$$K(A) = \bigcap_{\substack{M \text{ sous-corps de } L \\ K \subset M, A \subset M}} M.$$

En particulier, $K[A] \subset K(A) \subset L$ et donc $K[A]$ est intègre et on peut considérer $K_{K[A]}$ son corps des fractions qui contient canoniquement $K[A]$. On note $\iota : K[A] \to L$ l'inclusion et on introduit $\kappa : \begin{array}{ccc} K_{K[A]} & \longrightarrow & L \\ \frac{a}{b} & \longmapsto & \iota a \iota(b)^{-1} \end{array}$. Alors κ est un morphisme de corps i.e. d'anneaux unitaires. En effet,

$$\kappa(\frac{a}{b} + \frac{c}{d}) = \kappa(\frac{ad+bc}{bd}) = \iota(ad+bc)\iota(bd)^{-1} = \frac{\iota(a)\iota(d) + \iota(b)\iota(c)}{\iota(b)\iota(d)} = \frac{\iota(a)}{\iota(b)} + \frac{\iota(c)}{\iota(d)} = \kappa(\frac{a}{b}) + \kappa(\frac{c}{d}),$$
$$\kappa(\frac{a}{b} \cdot \frac{c}{d}) = \kappa(\frac{ac}{bd}) = \iota(ac)\iota(bd)^{-1} = \frac{\iota(a)\iota(c)}{\iota(b)\iota(d)} = \frac{\iota(a)}{\iota(b)} \cdot \frac{\iota(c)}{\iota(d)} = \kappa(\frac{a}{b}) \cdot \kappa(\frac{c}{d}).$$

Donc κ est bien un morphisme d'anneaux unitaires et donc de corps. En particulier κ est injectif et $K_{K[A]}$ s'injecte dans L. $K_{K[A]}$ s'envoie alors canoniquement dans L. Son image contient $\kappa(K[A]) = \iota(K[A]) = K[A]$ et est un sous-corps de L, comme image par un morphisme de corps d'un corps, elle contient donc $K(A)$. On a ainsi vérifié que $K(A) \subset \kappa(K_{K[A]})$. Réciproquement, $K(A)$ est un sous-corps de L contenant A et K, c'est en particulier un sous-anneau contenant A et K. Donc il contient $K[A] = \iota(K[A])$; comme $K(A)$ est un corps, il contient alors $\big(\iota(K[A]) \setminus \{0\}\big)^{-1}$ et $\iota(K[A])$, donc le produit $\iota(K[A])\big(\iota(K[A]) \setminus \{0\}\big)^{-1}$ qui est par construction l'image $\kappa(K_{K[A]})$ de κ. L'image du corps des fractions de $A[K]$ par le morphisme canonique κ est donc contenue dans $K(A)$ i.e. $\kappa(K_{K[A]}) \subset K(A)$. Alors on conclut que $K_{K[A]} \simeq K(A)$. □

Lemme 5.8. *Soit $K \to L$ une extension de corps et soient A B deux parties de L. Alors $(K(A))(B) = K(A \cup B)$.*

Démonstration. $(K(A))(B)$ est le plus petit corps contenant B et $K(A)$, donc il contient K, A et B et aloros $A \cup B$, ainsi $(K(A))(B) \supset K(A \cap B)$; de même, $K(A \cup B)$ est le plus petit corps contenant K et $A \cup B$, donc il contient $K(A)$ et B, ainsi $K(A \cap B) \supset (K(A))(B)$. On conclut que $(K(A))(B) = K(A \cup B)$. □

6 Sous-corps premiers

Définition 6.1. Toute corps contient en particulier un plus petit sous-corps : l'intersection de tous ses sous-corps non trivial. On l'appelle **le sous-corps premier** du corps.

Soit K un corps. Alors il existe un unique morphisme d'anneaux $\iota : \begin{array}{l} \mathbb{Z} \longrightarrow K \\ n \longmapsto n \cdot 1_k \end{array}$ *compatible à l'addition, où* $n \cdot 1_k := \underbrace{1_K + \cdots + 1_K}_{n}$*. C'est effectivement un morphisme d'anneaux :*

$$\iota(kl) = \underbrace{1_K + \cdots + 1_K}_{kl} = (\underbrace{1_K + \cdots + 1_K}_{k})(\underbrace{1_K + \cdots + 1_K}_{l}) = \iota(k)\iota(l).$$

Son noyau est un idéal de $\mathbb{Z}$*, qui est un anneau principal :* $\ker \iota = m\mathbb{Z}$, $m \in \mathbb{N}$.
a) Si $m = 0$*, alors* $ker(\iota) = \{0\}$ *et* ι *est injectif :* $\iota(n) \neq 0$ *pour tout* $n \in \mathbb{N}$. ι *se prolonge alors à* $\mathbb{Q}$ *:* $\iota(\frac{r}{s}) = \iota(r)\iota(s)^{-1}$ *canoniquement et uniquement en un monphisme de corps de* $\mathbb{Q}$ *et* $\iota(\mathbb{Q}) \subset K$*, où* ι *est injectif comme tout morphisme de corps.*

b) Si $m \in \mathbb{N}^*$*, on a le lemme suivant.*

Lemme 6.2. $m \in \mathcal{P}$.

Démonstration. Si $m = m_{-1}m_1$, où m_-1 et $m_1 \in \mathbb{N}^*$, alors $0 = \iota(m) = \iota(m_{-1})\iota(m_1)$. Or $Im(r)$ est un sous-anneau de K un corps qui est intègre, donc $\iota(m_{-1}) = 0$ ou $\iota(m_1) = 0$ i.e. $m|m_{-1}$ ou $m|m_1$. Alors la décomposition de m s'écrit $m = 1 \cdot m$, i.e. $m \in \mathcal{P}$. □

Définition 6.3. On appelle m dont $ker(\iota) = m\mathbb{Z}$ **la caractéristique** du corps K. On a vu que $m \in \mathcal{P}$ premier ou $m = 0$.

Remarque 6.4. $m = 1$ est exclus : car $1_K \neq 0_K$ dans un corps par définition.

On note $\mathbb{F}_p := \operatorname{Im} \iota = \mathbb{Z}/\ker(\iota) = \mathbb{Z}/p\mathbb{Z}$.

Alors les seuls sous-corps premier sont

- $\mathbb{Q}$ *en caractéristique 0 ;*
- $\mathbb{F}_p$ *avec* $p \in \mathcal{P}$ *en caractéristique* p.

Définition 6.5 (le Frobenius)**.** Soit K un corps de caractéristique positive $p \in \mathcal{P}$. On appelle l'application $Fr_K : \begin{array}{l} K \longrightarrow K \\ x \longmapsto x^p \end{array}$ **le Frobenius**. On not K^p l'image du Frobenius.

Proposition 6.6. *Le Frobenius est un morphisme de corps.*

Démonstration. a) $Fr_K(xy) = (xy)^p = x^p y^p = Fr_K(x)Fr_K(y)$;
a) $Fr_K(x+y) = (x+y)^p = x^p + y^p = Fr_K(x) + Fr_K(y)$. En effet, on a vu que $p|\binom{p}{k}$ pour tout $k \in [\![1, p-1]\!]$, et $(x+y)^p = \sum\limits_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p$.
Donc Fr_K est un morphisme de corps en particulier Fr_K est injectif. □

7 Racine de l'Unité dans un Corps

Soit K un corps et soit $n \in \mathbb{N}^*$.

Définition 7.1. On appelle le groupe des racines n-ièmes de l'unité dans K **le groupe multiplicatif**. On le note $\mu_n(K) = \{\xi \in K,\ \xi^n = 1\}$.
En effet, $\xi^n = 1 \Rightarrow \xi \neq 0 \Rightarrow \xi^{-1} \in K$, alors on observe que $\xi^{-1} = \xi^{n-1}$; $(\xi_1\xi_2)^n = \xi_1^n \xi_2^n = 1 \cdot 1 = 1$. Donc $\mu_n(K)$ est un groupe.

Lemme 7.2. $|\mu_n(K)| \leq n$.

Démonstration. Tout polynôme $P(X)$ de $K[X]$ de degré $d \in \mathbb{N}$ possède au plus d racines de K. En effet, car $K[X]$ est un anneau eucidien, si ξ est une racine de $P(X)$ dans K, il existe $Q \in K[X]$ et $R \in K$ tels que $P(X) = (X-\xi)Q(X) + R$. En spécialisant en $X = \xi$, on trouve que nécessairement $R = 0$: $X - \xi$ divise P et $P(X) = (X-\xi)Q(X)$, alors $\deg Q = \deg P - 1$. Or un polynôme non nul de degré 0 n'admet pas de racine ; en supportant qu'un polynôme de degré inférieur ou égal à $n-1$, $n \in \mathbb{N}^*$ possède au plus $n-1$ racines, l'argument précédent établit qu'un polynôme P de degré n, soit n'admet pas de racine sur K, soit s'écrit $P(X) = (X-\xi)Q(X)$. Un corpsétant intègre, toute racine de P distincte de ξ est racine de $Q(X)$ (pour unr telle racine ρ, $\rho - \xi \neq 0$) ; il y a par hypothèse de récurrence au plus $(n-1)$ telles racines de Q et P possède donc au plus n racines dans K.
On peut remplacer la division euclidienne par la remarque suivante : si $P(X) = \sum\limits_{k=0}^{d} a_k X^k$ possèdes une racin ξ alors $X - \xi$ divise P car $P(X) = P(X) - P(\xi) = \sum\limits_{k=0}^{d} a_k(X^k - \xi^k) = (X-\xi)\sum\limits_{k=0}^{d} a_k \sum\limits_{l=0}^{k-1} X^l \xi^{k-1-l}$.
En résumé : tout polynôme de $K[X]$ de degré au plus n possède au plus n racins dans K. □

Définition 7.3. $\xi \in \mu_n(K)$ est dite **une racine primitive** n-ième de l'unité si $\xi^d \neq 1$ pour tout $d \in [\![1, n-1]\!]$ i.e. si l'ordre de ξ dans le groupe $\mu_n(K)$ est exactement n.

Sorite 7.4. *S'il existe une racine primitive n-ième de l'unité dans K, alors elle engends $\mu_n(K)$: $\mu_n(K) = \langle \xi \rangle$.*

Démonstration. Les ξ^k, où $k \in [\![0, n-1]\!]$, sont alors 2 à 2 distincts : si $\xi^k = \xi^l$ et $l \geq k \Rightarrow \xi^{l-k} = 1 \Rightarrow l = k$ car ξ est primitif. En particulier, $|\langle \xi \rangle| = n \geq |\mu_n(K)|$, or $\langle \xi \rangle < \mu_n(K)$, donc $\langle \xi \rangle = \mu_n(K)$, et $\mu_n(K)$ est alors cyclique.
On considère $\varphi : \begin{array}{rcl} \mathbb{Z} & \longrightarrow & K \\ k & \longmapsto & \xi^k \end{array}$. Son noyau $n\mathbb{Z}$ car l'ordre de ξ est n. Le passage au quotient par $\ker(\varphi) = n\mathbb{Z}$ conduit à l'isomorphisme annoncé : $\mathbb{Z}/n\mathbb{Z} \to \langle \xi \rangle = \mu_n(K)$ dans ce cas où il existe une racine primitive n-ième de l'unité dans le corps K. □

Lemme 7.5. *S'il existe une racine primitive n-ième de l'unité dans K, alors le nombre des racines primitives n-ièmes de l'unité dans K est $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^*| = |\{d \in [\![1, n-1]\!],\ d \wedge n = 1\}|$.*

Démonstration. Par le théorème de Bachet-Bézout, c'est une corollaire facile que $d \wedge n = 1$ s.s.i. il existe a, $b \in \mathbb{Z}$ tels que $ad + bn = 1$ s.s.i. il existe $a \in \mathbb{Z}/n\mathbb{Z}$ tel que $ad = 1$ s.s.i. $d \in (\mathbb{Z}/n\mathbb{Z})^*$.
Soit ξ une racine primitive. Si $a \in (\mathbb{Z}/n\mathbb{Z})^*$ et alors $(\xi^a)^n = (\xi^n)^a = 1^a = 1$ et $(\xi^a)^k = 1 \Rightarrow 1 = (\xi^a)^{ka^{-1}} = \xi^{kaa^{-1}} = \xi^k \Rightarrow k \in \mathbb{Z}$. Donc ξ^a est une racine primitive n-ièmes de l'unité dans K.
Réciproquement, si $d|n \wedge a$ et $d > 1$, alors $1 \leq \frac{n}{d} \leq n-1$ et $(\varphi^a)^{\frac{n}{d}} = (\varphi^n)^{\frac{a}{d}} = 1^{\frac{a}{d}} = 1$. Donc ξ^a n'est pas primitif. □

Définition 7.6. Pour tout $m = \prod_{i=1}^{k} p_i^{a_i} \in \mathbb{N}^*$, où $p_i \in \mathcal{P}$ sont distincts. On note $m^* = \prod_{i=1}^{k} p_i$ et on l'appelle **le noyau de** m.

Définition 7.7. Pour $d \in \mathbb{N}^*$, on note $\omega(d)$ le nombre de facteurs premiers de d. On observe que en particulier $\omega(d) = \omega(d^*)$ pour tout $d \in \mathbb{N}^*$.
Après on définit la fonction de möbius

$$\mu(d) = \begin{cases} 0 & , \exists\, m \in \mathbb{N} \setminus \{1\},\ m^2 | d; \\ (-1)^{\omega(d)} & , sinon. \end{cases}$$

Lemme 7.8 (Legendre)**.** *Pour tout $m \in \mathbb{N}^*$ et tout $x \in \mathbb{R}^*$, on note $E_m(x) := \{n \in [\![1, \lfloor x \rfloor]\!],\ n \wedge m = 1\}$ et $N_m(x) = |E_m(x)|$. On a alors l'identité de Legendre*

$$N_m(x) = \sum_{d|m^*} (-1)^{\omega(d)} \lfloor \frac{x}{d} \rfloor = \sum_{d|m} \mu(d) \lfloor \frac{x}{d} \rfloor.$$

Démonstration. $\square$

Car m et m^* ont exactement les mêmes facteurs premiers, seulement les valuations p-adique sont différents, on a $n \wedge m = 1$ s.s.i. $n \wedge m^* = 1$. Alors $E_m(x) = E_{m^*}(x)$. On suppose $m = \prod_{i=1}^{k} p_i^{a_i} \in \mathbb{N}^*$ et donc $m^* = \prod_{i=1}^{k} p_i$. Pour établir l'identité de Legendre, on procède par récurrence sur k. In troduisons les entiers $m_j = \prod_{i=1}^{j} p_i$, on a alors :

— $N_{m_0}(x) = N_1(x) = \lfloor x \rfloor$;

—
$$\begin{aligned} E_{m_{j+1}}(x) &= \{n \in [\![1, \lfloor x \rfloor]\!],\ n \wedge m_{j+1} = 1\} \\ &= \{n \in [\![1, \lfloor x \rfloor]\!],\ n \wedge m_j = 1 \textit{ et } n \wedge p_{j+1} = 1\}. \end{aligned}$$

Alors
$$\begin{aligned} E_{m_j}(x) \setminus E_{m_{j+1}}(x) &= \{n \in [\![1, \lfloor x \rfloor]\!],\ n \wedge m_j = 1 \textit{ et } n \wedge p_{j+1} > 1\} \\ &= \{n \in [\![1, \lfloor x \rfloor]\!],\ n \wedge m_j = 1 \textit{ et } p_{j+1} | n\} \\ &= p_{j+1} \cdot \{n \in [\![1, \lfloor \frac{x}{p_{j+1}} \rfloor]\!],\ n' \wedge m_j = 1\} \\ &= p_{j+1} \cdot E_{m_j}(\frac{x}{p_{j+1}}). \end{aligned}$$

C'est à dire que $N_{m_j}(x) - N_{m_{j+1}}(x) = |E_{m_j}(x) \setminus E_{m_{j+1}}(x)| = |E_{m_j}(\frac{x}{p_{j+1}})| = N_{m_j}(\frac{x}{p_{j+1}})$.
En particulier
$$\begin{aligned} N_{m_1}(x) &= N_{m_0}(x) - N_{m_0}(\frac{x}{p_1}) \\ &= \lfloor x \rfloor - \lfloor \frac{x}{p_1} \rfloor \\ N_{m_2}(x) &= N_{m_1}(x) - N_{m_1}(\frac{x}{p_2}) \\ &= \lfloor x \rfloor - \lfloor \frac{x}{p_1} \rfloor - \lfloor \frac{x}{p_2} \rfloor + \lfloor \frac{x}{p_1 p_2} \rfloor. \end{aligned}$$

L'hypothèse de récurrence est naturellement

$$N_{m_j}(x) = \sum_{d | m_j} (-1)^{\omega(d)} \lfloor \frac{x}{d} \rfloor.$$

Pour $j+1$, on en déduit

$$\begin{aligned} N_{m_{j+1}}(x) &= N_{m_j}(x) - N_{m_j}(\frac{x}{p_{j+1}}) \\ &= \sum_{d|m_j}(-1)^{\omega(d)}\lfloor\frac{x}{d}\rfloor - \sum_{d|m_j}(-1)^{\omega(d)}\lfloor\frac{x}{p_{j+1}d}\rfloor \\ &= \sum_{d|m_j}(-1)^{\omega(d)}\lfloor\frac{x}{d}\rfloor - \sum_{\substack{p_{j+1}|d \\ d|m_jp_{j+1}}}(-1)^{\omega(d)-1}\lfloor\frac{x}{d}\rfloor \\ &= \sum_{d|m_j}(-1)^{\omega(d)}\lfloor\frac{x}{d}\rfloor + \sum_{\substack{p_{j+1}|d \\ d|m_jp_{j+1}}}(-1)^{\omega(d)}\lfloor\frac{x}{d}\rfloor \\ &= \sum_{d|m_{j+1}}(-1)^{\omega(d)}\lfloor\frac{x}{d}\rfloor. \end{aligned}$$

Alors on finit la démonstration de la première identité. Pour la deuxième, on observe que c'est trivial que $\sum_{d|m^*}(-1)^{\omega(d)}\lfloor\frac{x}{d}\rfloor = \sum_{d|m^*}\mu(d)\lfloor\frac{x}{d}\rfloor = \sum_{d|m}\mu(d)\lfloor\frac{x}{d}\rfloor$ *car* $\mu(d) = (-1)^{\omega(d)}$ *pour tout* $d|m^*$ *et* $\mu(d) = 0$ *pour tout facteur de* m d *qui ne divise pas* m^*.

Corollaire 7.9. $\varphi(n) = \sum_{d|n}\mu(d)\frac{n}{d} = n\prod_{\substack{p|n \\ p\in\mathcal{P}}}(1-\frac{1}{p})$.

Démonstration. Immédiatement, $\varphi(n) = N_n(n) = \sum_{d|n}\mu(d)\frac{n}{d}$.

D'autre part, l'identité de Legendre s'écrit $\varphi(n) = N_n(n) = \sum_{d|n^*}(-1)^{\omega(d)}\frac{n}{d}$. Or $n\prod_{\substack{p|n \\ p\in\mathcal{P}}}(1-\frac{1}{p}) = n\prod_{i=1}^{k}(1-\frac{1}{p_i})$. On obtient la conclusion en développant : pour rédiger proprement, on peut procèder par récurrence sur k. Posons $n_k = n_{k-1}p_k$, alors

$$\begin{aligned} n_k \prod_{i=1}^{k}(1-\frac{1}{p_i}) &= n_{k-1}p_k \prod_{i=1}^{k}(1-\frac{1}{p_i}) \\ &= p_k(1-\frac{1}{p_k}) \sum_{d|n_{k-1}} (-1)^{\omega(d)} \frac{n_{k-1}}{d} \\ &= \sum_{d|n_{k-1}} (-1)^{\omega(d)} \frac{p_k n_{k-1}}{d} - \sum_{d|n_{k-1}} (-1)^{\omega(d)} \frac{n_{k-1}}{d} \\ &= \sum_{d|n_{k-1}} (-1)^{\omega(d)} \frac{n_k}{d} - \sum_{d|n_{k-1}} (-1)^{\omega(d)} \frac{n_k}{dp_k} \\ &= \sum_{\substack{p_k \nmid d \\ d|n_k}} (-1)^{\omega(d)} \frac{n_k}{d} - \sum_{\substack{p_k | d \\ d|n_k}} (-1)^{\omega(d)} \frac{n_k}{d} \\ &= \sum_{d|n_k} (-1)^{\omega(d)} \frac{n_k}{d}. \end{aligned}$$

□

Remarque 7.10. On observe que φ est multiplicative par la deuxième identité.

Définition 7.11. Soient $f : \mathbb{N} \to \mathbb{C}$ et $g : \mathbb{N} \to \mathbb{C}$ deux fonctions arithmétiques. On note $(f*g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$. C'est bien une fonction arithmétique et on l'appelle **la convolution de f et g.**

Remarque 7.12. — commutativité :

$$\begin{aligned} (f*g)(n) &= \sum_{d|n} f(d)g(\frac{n}{d}) \\ &= \sum_{rs=n} f(r)g(s) \\ &= \sum_{d|n} g(d)f\frac{n}{d}) \\ &= (g*f)(n); \end{aligned}$$

— associativité :

$$\begin{aligned}(f*g)*h(n) &= \sum_{d|n} f*g(d)h(\frac{n}{d})\\ &= \sum_{rs=n} f*g(r)h(s)\\ &= \sum_{rs=n} h(s)\sum_{pq=r} f(p)g(q)\\ &= \sum_{pqs=n} f(p)g(q)h(s)\\ &= \sum_{rs=n} f(p)\sum_{qs=r} g(q)h(s)\\ &= \sum_{pr=n} f(p)g*h(r)\\ &= f*(g*h)(n).\end{aligned}$$

En effet,

$$\begin{array}{ccc}\{(d,\delta)\in[\![1,n]\!]^2,\ d|n,\ \delta|d\} & \longrightarrow & \{(d_1,d_2,d_3)\in[\![1,n]\!]^3,\ d_1d_2d_3=n\}\\ (d,\delta) & \longmapsto & (\delta,\frac{d}{\delta},\frac{n}{d})\end{array}$$

est une bijection, d'inverse on écrit

$$\begin{array}{ccc}\{(d_1,d_2,d_3)\in[\![1,n]\!]^3,\ d_1d_2d_3=n\} & \longrightarrow & \{(d,\delta)\in[\![1,n]\!]^2,\ d|n,\ \delta|d\};\\ (d_1,d_2,d_3) & \longmapsto & (d_1d_2,d_1)\end{array}$$

d'autre part,

$$\begin{array}{ccc}\{(d,\delta)\in[\![1,n]\!]^2,\ d|n,\ \delta|\frac{d}{n}\} & \longrightarrow & \{(d_1,d_2,d_3)\in[\![1,n]\!]^3,\ d_1d_2d_3=n\}\\ (d,\delta) & \longmapsto & (d,\delta,\frac{n}{d\delta})\end{array}$$

est une bijection, d'inverse on écrit

$$\begin{array}{ccc}\{(d_1,d_2,d_3)\in[\![1,n]\!]^3,\ d_1d_2d_3=n\} & \longrightarrow & \{(d,\delta)\in[\![1,n]\!]^2,\ d|n,\ \delta|\frac{d}{n}\}.\\ (d_1,d_2,d_3) & \longmapsto & (d_1,d_1)\end{array}$$

Donc on observe que les formules ci-dessus coïncident.

Définition 7.13. $\mathcal{E}(n)=\begin{cases}1 & ,n=1\\ 0 & ,sinon\end{cases}$ est une fonction arithmétique.

Remarque 7.14. $\mathcal{E}$ est l'élément neutre de $*$. En effet, $\mathcal{E} * f(n) = \sum_{d|n} \mathcal{E}(d) f(\frac{n}{d}) = f(n)$ i.e. $\mathcal{E} * f = f$.

Lemme 7.15. $1 * \mu = \mathcal{E}$*, outrement dit la fonction de möbius est l'inverse, pour la convolution, de la fonction constante et égale à* 1*.*

Démonstration. Si $n = 1$, $1 * \mu(1) = \mu(1) = 1 = \mathcal{E}(1)$;
Si $n > 1$, alors on suppose que $n = \prod_{i=1}^{k} p_i^{a_i}$ et on rappelle que $n^* = \prod_{i=1}^{k} p_i$, où (p_i) sont premiers et distincts. $1 * \mu(n) = \sum_{d|n} \mu(d) = \sum_{d|n^*} \mu(d) = \sum_{d|n^*} \mu(d) = \sum_{d|\frac{n^*}{p_1}} \mu(d) + \mu(p_1 d) = \sum_{d|\frac{n^*}{p_1}} (-1)^{\omega(d)} + (-1)^{\omega(p_1 d)} = \sum_{d|\frac{n^*}{p_1}} (-1)^{\omega(d)} - (-1)^{\omega(d)} = 0 = \mathcal{E}(n)$. □

Corollaire 7.16 (La formule d'inversion de Möbius)**.** *Soit* f *une fonction arithmétique et* $g = f * 1$*, alors* $f = \mu * g$*. Réciproquement, si* $f = \mu * g$*, alors* $g = f * 1$*.*

Démonstration. $\mu * g = \mu * (f * 1) = \mu * (1 * f) = (\mu * 1) * f = \mathcal{E} * f = f$. Réciproquement, $f * 1 = (\mu * g) * 1 = (g * \mu) * 1 = (g * \mu) * 1 = g * (\mu * 1) = g * \mathcal{E} = g$. □

Remarque 7.17. $1 * \mu = \mathcal{E}$ est équivalente à l'une quelconque des deux formules de Möbius. En effet, posons $f = \mathcal{E}$ dans la première ou $g = \mathcal{E}$ dans la seconde, alors elle donne $\mathcal{E} = \mu * 1$.

Corollaire 7.18. *Pour tout* $n \in \mathbb{N}^*$*,* $\sum_{d|n} \varphi(d) = n$

Démonstration. On rappelle qu'on a établi via la formule de Legendre l'identité suivante pour l'indicatrice d'Euler φ : $\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = \mu * Id_{\mathbb{N}^*}(n) =$. Alors $\sum_{d|n} \varphi(d) = \varphi * 1(n) = (\mu * Id_{\mathbb{N}^*}) * 1(n) = (Id_{\mathbb{N}^*} * \mu) * 1(n) = Id_{\mathbb{N}^*} * (\mu * 1)(n) = Id_{\mathbb{N}^*} * \mathcal{E}(n) = Id_{\mathbb{N}^*}(n) = n$.
Alternativement, on peut diriver l'identité $\sum_{d|n} \varphi(d) = n$ de l'expression suivant de l'indicatrice d'Euler : si $n = \prod_{i=1}^{k} p_i^{a_i}$, où $a_i \in \mathbb{N}^*$, (p_i) distincts et premiers, $\varphi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i}) = \prod_{i=1}^{k} (p_i - 1) p_i^{a_i - 1}$. Alors $\sum_{d|n} \varphi(d) = \sum_{\substack{(b_1, \cdots, b_k) \in \\ [\![0, a_1]\!] \times \cdots \times [\![0, a_n]\!]}} \varphi(\prod_{i=1}^{k} p_i^{b_i}) = \sum_{\substack{(b_1, \cdots, b_k) \in \\ [\![0, a_1]\!] \times \cdots \times [\![0, a_n]\!]}} \prod_{i=1}^{k} \varphi(p_i^{b_i}) = \prod_{i=1}^{k} \sum_{b_i \in [\![0, a_i]\!]} \varphi(p_i^{b_i}) = \prod_{i=1}^{k} (1 + \sum_{b_i \in [\![1, a_i]\!]} (p_i - 1) p_i^{b_i - 1}) = \prod_{i=1}^{k} \left(1 + (p_i - 1) \frac{p_i^{b_i} - 1}{p_i - 1}\right) = \prod_{i=1}^{k} p_i^{b_i} = n$. □

Proposition 7.19. $\mu_n(K)$ *est cyclique d'ordre un diviseur de* n*.*

Démonstration. Posons $m = |\mu_n(K)|$. Pour tout $\xi \in \mu_n(K)$, $\langle\xi\rangle$ est un sous groupe de $\mu_n(K)$ et par le théorème de Lagrange, on a $ord(\xi) = |\langle\xi\rangle|\big||\mu_n(K)| = m$. $\xi^{ord(\xi)} = \xi^n = 1$, on utilise la division euclidienne de n par d, et la définition de l'ordre de x implique que $ord(\xi)|n$. Alors $ord(\xi)|m \wedge n$, ce qui entraîne la partition suivante de $\mu_n(K)$:

$$\mu_n(K) = \bigsqcup_{d|m\wedge n} \Pi_d,$$

où $\Pi_d :=$ l'ensemble des racines primitives $ord(x)$-ième de l'unité dans K.
On a vu que si $\Pi_d \neq \varnothing$, alors $|\Pi_d| = \varphi(d)$. On en déduit $m = |\mu_n(K)| = \sum_{d|m\wedge n} |\Pi_d| \leq \sum_{d|m\wedge n} \varphi(d) = m \wedge n \leq m$. Donc avec égalité on en déduit $m = m \wedge n$ et $|\Pi_d| = \varphi(d)$ pour tout $d|m \wedge n$. En particulier, Π_m n'est pas vide. Pour tout $\xi \in \Pi_m$, $m = |\langle\xi\rangle| \leq \mu_n(K) = m$, alors $\mu_n(K) = \langle\xi\rangle$ est cyclique. □

Remarque 7.20. On rappelle que le théorème de Lagrange : l'ordre d'un sous-groupe H d'un groupe fini G divise l'ordre du groupe. Puls simplement, pour tout $x \in G$, g_x la multiplication par x à gauche est une bijection, d'inverse la multiplication par l'inverse de x à gauche, i.e. $(g_x)^{-1} = g_{x^{-1}}$, On introduit le produit $\prod_{g\in G} g = \prod_{g\in G}(xg) = x^{|G|} \prod_{g\in G} g$, alors $x^{|G|} = 1 \Rightarrow o(x) := \min\{k \in \mathbb{N}^*,\ x^k = 1\}\big||G|$.

Théorème 7.21. *Tout sous-groupe fini de* $(K^*, \cdot)$ *est cyclique.*

Démonstration. Soit G un sous-groupe fini de K^* et posons $m = |G|$. Par le théorème de Lagrange, tout élément de G est d'ordre un diviseur de $|G| = m$, G est donc in clus dans $\mu_m(K)$. Or $|\mu_m(K)| \leq m$, alors $G = \mu_m(K) \simeq \mathbb{Z}/m\mathbb{Z}$. En particulier G est cyclique. □

Corollaire 7.22. *Le groupe multiplisatif d'un corps fini est cyclique.*

Proposition 7.23. *Si K est infini, alors* $(K^*, \cdot)$ *n'est jamais cyclique.*

Démonstration. Si la caractéristique de K n'est pas 2, alors $-1 \neq 1$. S'il existe $a \in K^*$ tel que $K^* = \langle a\rangle$, alors il existe $k \in \mathbb{Z} \setminus \{0\}$ tel que $-1 = a^k \Rightarrow 1 = a^{2k} \Rightarrow ord(a)|2k$. Alors $\langle a\rangle$ est en particulier fini, contradiction !
Si la caractéristique de K est 2. Soit a un générateur de $(K^*, \cdot)$, alors $a \neq 1$. On en déduit $1+a \neq 0$ et $1+a \in K^*$. Il existe $k \in \mathbb{Z}\setminus\{0\}$ tel que $1+a = a^k$. Soit $k \in \mathbb{N}^*$, alors $a^k+a+1 = 0$; soit $-k \in \mathbb{N}^*$, alors $a^{-k} + a^{-k+1} + 1 = 0$. Dans tout les cas a est algébrique sur $\mathbb{F}_2$ et $\mathbb{F}_2[a]$ est donc un espace vectoriel de dimension finie sur $\mathbb{F}_2$. Pour tout $x \in \mathbb{F}_2[a] \setminus \{0\}$, m_x la multiplication par x est injective, puisque K est un corps et donc bijective. En particulier, 1 appartient à l'image de m_x et x est donc inversible. On a alors : $K = \mathbb{F}_2(a) = \mathbb{F}_2[a]$ □

est de dimension finie sur $\mathbb{F}_2$. On en déduit que K est fini, ce qui contredit $|K^*| = \infty$.

8 Extensions de Corps

Soit $\varphi : K \hookrightarrow L$ une extension de corps.

Définition 8.1. $\deg \varphi :=$ la dimension du K-espace vectoriel L, notée $[L : K] := \dim_K(L)$.

Définition 8.2. φ est dite **finie** si le degré $[L : K] \in \mathbb{N}$ et infinie sinon.

Exemple 8.3. *i*) $[\mathbb{C} : \mathbb{R}] = 2$, la base est $(1, i = \sqrt{-1})$;
ii) $[\mathbb{C} : \mathbb{Q}] = \infty$. Si il y a une base finie, alors on aurait $\mathbb{C} \simeq \mathbb{Q}^n$. Or un produit fini d'ensemble dénombrable est dénombrable, et $\mathbb{C}$ n'est pas dénombrable. *iii*) $[K(X) : K] = \infty$. On le voit par $(X^i)_{i \in \mathbb{N}}$ est une famille linéairement indépendante sur K.

Remarque 8.4. Ces deux «infini» sont «distincts>> :

— le premier a la puissance du continu : si $\mathbb{C}$ admettait une base dénombrable sur $\mathbb{Q}$, tout nombre $\mathbb{C}$ s'écrirait comme une combinaison linéaire finie sur cette base et on aurait $\mathbb{C} = \bigcup\limits_{n \in \mathbb{N}} vect_{\mathbb{Q}}(e_1, \cdots, e_n)$, où $vect_{\mathbb{Q}}(e_1, \cdots, e_n) \simeq \mathbb{Q}^n$ est dénombrable et donc $\mathbb{C}$ serait dénombrable comme une union dénombrable d'ensemble dénombrable.

— Le second est dénombrable. En toute généralité, un degré est une dimension d'espace vectoriel et en tant que tel, c'est un cardinal.

En effet, $\mathbb{R}$ (et donc $\mathbb{C}$) n'est pas dénombrable. On peut utiliser l'argument de Cantor : $[0, 1] \subset \mathbb{R}$. À un nombre réel de $[0, 1]$, on aaocie son développement décimal $x = 0.a_1 \cdots a_n \cdots$. Si $[0, 1]$ était dénombrable, on aurait description exhaustive de $[0, 1]$ comme image de $\mathbb{N}$: $x_i = 0.a_{i,1} \cdots a_{i,n} \cdots$. Soit alors le réel X de développement décimal $X = 0.b_1 \cdots b_n \cdots$ avec $b_i = a_{i,i} + 5 \; mod \; 10$. Alors $X \neq x_i$ pour tout $i \in \mathbb{N}^*$, donc $X \notin [0, 1]$. Contradiction !

Théorème 8.5. *Soient K, L et M des corps. Soient $K \hookrightarrow L$ et $L \hookrightarrow M$ des extensions de corps. Alors $[M : K] = [M : L][L : K]$. En particulier l'extension $K \hookrightarrow M$ est finie s.s.i. $K \hookrightarrow L$ et $L \hookrightarrow M$ sont finies.*

Démonstration. Soient $(l_i)_{i \in I}$ une base de K-espace vectoriel L et $(m_j)_{j \in J}$ une base de L-espace vectoriel M. On considère $(l_i m_j)_{(i,j) \in I \times J}$ une famille dans le K-espace vectoriel M.
D'une part, pour toute $(k_{i,j})_{(i,j) \in I \times J}$ famille d'éléments de K nuls sauf un nombre fini d'éléments, si $0 = \sum\limits_{(i,j) \in I \times J} k_{i,j} l_i m_j$, alors $0 = \sum\limits_{j \in J} (\sum\limits_{i \in I} k_{i,j} l_i) m_j$. Or $(m_j)_{j \in J}$ est une base de L-espace vectoriel M, en particulier les m_j sont linéairement indépendents sur L, alors $0 = \sum\limits_{i \in I} k_{i,j} l_i$

pour tout $j \in J$. Or $(l_i)_{i\in I}$ est une base de K-espace vectoriel L, en particulier les l_i sont linéairement indépendents sur K, $0 = k_{i,j}$ pour tout $i \in I$ et tout $j \in J$. Donc cette famille $(k_{i,j})_{(i,j)\in I\times J}$ est libre sur K.
D'autre part, $(m_j)_{j\in J}$ engendre M comme L-espace vectoriel, alors pour tout $y \in M$, il existe $(x_j)_{j\in J}$ une famille d'éléments de L nuls sauf un nombre fini d'éléments telle que $y = \sum\limits_{j\in J} x_j m_j$. $(l_i)_{i\in I}$ engendre L comme K-espace vectoriel, alors pour tout $j \in J$, il existe $(w_{i,j})_{(i,j)\in I\times J}$ famille d'éléments de K nuls sauf un nombre fini d'éléments telles que $x_j = \sum\limits_{j\in J} w_{i,j} l_i$. On a ainsi $y = \sum\limits_{j\in J} x_j m_j = \sum\limits_{j\in J}(\sum\limits_{j\in J} w_{i,j} l_i) m_j = \sum\limits_{j\in J}\sum\limits_{j\in J} w_{i,j} l_i m_j$, où $(w_{i,j})$ nuls sauf un nombre fini d'éléments. Alors $(l_i m_j)_{(i,j)\in I\times J}$ engendre M sur K. $\square$

9 Algébricité et Transcendance

Définition 9.1. Soit $K \hookrightarrow L$ une extension de corps et soit $x \in L$. On dit que
i) x est **algébrique** sur K s'il existe un polynôme non nul $P \in K[X]$ tel que $P(x) = 0$ et **transcendant** sur K sinon ;
ii) l'extension est **algébrique** si tous les éléments de L sont algébriques sur K.

Exemple 9.2. *i*) $\mathbb{R} \hookrightarrow \mathbb{C}$ est une extension algébrique : pour tout $z \in \mathbb{C}$, $P(X) = (X - z)(X - \overline{z}) = X^2 - 2\,\mathrm{Re}(z)X + |z|^2 \in \mathbb{R}[X]$;
ii) $\sqrt{2}$ est algébrique sur $\mathbb{Q}$: il est une racine de polynôme $X^2 - 2 \in \mathbb{Q}[X]$.

Lemme 9.3. *L'enseble des réels algébriques sur $\mathbb{Q}$ est dénombrable, alors il existe des réels transcendants.*

Démonstration. On note $\overline{\mathbb{Q}}$ l'enseble des réels algébriques. Alors $\overline{\mathbb{Q}} = \bigcup\limits_{P\in\mathbb{Q}[X]} \{racines\ de\ P(X)\}$.
On note $\mathbb{Q}_d[X]$ l'ensemble des polynômes de degré au plus d, qui est isomorphisme à $\mathbb{Q}^{d+1}$ dénombrable. Donc $\mathbb{Q}[X]$ est une union d'un nombre dénombrable des ensembles dénombrables $(\mathbb{Q}_d[X])_{d\in\mathbb{N}}$, alors est dénombrable. $|\{racines\ de\ P(X)\}| \leq \deg P < \infty$, alors $\bigcup\limits_{P\in\mathbb{Q}[X]} \{racines\ de\ P(X)\}$ est une union d'un nombre dénombrable d'ensembles finis, donc $\overline{\mathbb{Q}}$ est dénombrable.
Or $\mathbb{R}$ n'est pas dénombrable, donc il existe des réels transcendants. $\square$

C'est un endroit où introduire naturellement π et e et établir qu'ils sont transcendants. Avant ça, Liouville avait déjà construit des nombres transcendants explicités.

Définition 9.4. On appelle **nombre de Liouville** tout élément de $\mathcal{L} = \left\{x \in \mathbb{R},\ \forall\ n \in \mathbb{N},\ il\ existe\ un\ nombre\ infini\ de\ (p,q) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})\ tel\ que\ 0 < |x - \frac{p}{q}| < \frac{1}{q^n}\right\}$

Lemme 9.5. *$x \in \mathbb{Q} \Rightarrow x \notin \mathcal{L}$.*

Démonstration. Soit $x = \frac{a}{b} \in \mathbb{Q}$, où $a \in \mathbb{Z}$ et $b \in \mathbb{N} \setminus \{0\}$. Alors $0 < |x - \frac{p}{q}| = |\frac{aq-pb}{bq}|$. $aq - pb \in \mathbb{Z} \setminus \{0\}$ i.e. $|aq - pb| \geq 1$, donc $|x - \frac{p}{q}| \geq \frac{1}{bq}$. Si $\frac{1}{q^n} > |x - \frac{p}{q}|$, alors $b > q^{n-1}$, donc $q \in [\![1, b^{\frac{1}{n-1}}]\!]$. Pour tout $q \in [\![1, b^{\frac{1}{n-1}}]\!]$, le choix de p est unique. Donc les couples (p, q) compatibles sont de nombre fini. Alors $\mathbb{Q} \cap \mathcal{L} = \varnothing$. □

Lemme 9.6. *Si $a \in \mathbb{R} \setminus \mathbb{Q}$ est algébrique, alors il existe $A \in \mathbb{R}^+$ tel que pour tout $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$, $|a - \frac{p}{q}| > \frac{A}{q^m}$.*

Démonstration. On suppose $P(X) = \sum\limits_{k=0}^{m} a_k X^k \in \mathbb{Q}[X]$ tel que $P(a) = 0$ et $\deg P = m$. On considère

$$A = \min\left(1, \frac{1}{\sup\limits_{[a-1,a+1]} |P'(x)|}, \min_{\substack{b \neq a \\ P(b)=0}} |a - b|\right).$$

A est bien défini car P possède un nombre fini de racines.
On suppose sans reste de généralité que $|a - \frac{p}{q}| \leq A$ et $a_k \in \mathbb{Z}$ pour tout $k \in [\![1, m]\!]$. En effet, $|a - \frac{p}{q}| > A$ implique $|a - \frac{p}{q}| > \frac{A}{q^m}$ pour tout $q \in \mathbb{N}^*$.
D'après $|a - \frac{p}{q}| \leq A \leq 1$, donc $\frac{p}{q} \in [a-1, a+1]$. D'une part, le théorème de la valeur moyenne donne l'existence d'un point x_0 dans l'interval entre a et $\frac{p}{q}$ tel que $P'(x_0) = \frac{P(a)-P(\frac{p}{q})}{a-\frac{p}{q}}$, on a alors

$$\left|a - \frac{p}{q}\right| = \frac{|P(a) - P(\frac{p}{q})|}{|P'(x_0)|} = \frac{|P(\frac{p}{q})|}{|P'(x_0)|}.$$

D'autre part, $|a - \frac{p}{q}| \leq A \Rightarrow \frac{1}{q^m} \sum\limits_{k=0}^{m} a_k p^k q^{m-k} = P(\frac{p}{q}) \neq 0$, alors $\sum\limits_{k=0}^{m} a_k p^k q^{m-k} \in \mathbb{Z} \setminus \{0\}$ et

$$\left|P\left(\frac{p}{q}\right)\right| = \frac{1}{q^m}\left|\sum_{k=0}^{m} a_k p^k q^{m-k}\right| \geq \frac{1}{q^m}.$$

Enfin, on obtient que

$$|a - \frac{p}{q}| = \frac{|P(\frac{p}{q})|}{|P'(x_0)|} \geq \frac{1}{q^m} \frac{1}{\sup\limits_{[a-1,a+1]} |P'(x)|} \geq \frac{A}{q^m}.$$

□

Proposition 9.7. *Les nombres de Liouville sont transcendants, i.e.* $\mathcal{L} \subset \mathbb{R} \setminus \overline{\mathbb{Q}}$.

Démonstration. Soit $x \in \mathcal{L}$. On a vu que $x \notin \mathbb{Q}$. Si x est algébique, i.e. $x \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$. On suppose $\deg x = m$, alors il existe $A_x \in \mathbb{R}_+^*$ tel que $|x - \frac{p}{q}| > \frac{A_x}{q^m}$ pour tout $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$. Il existe $k \in \mathbb{N}$ tel que $2^k A_x > 1$, si $q > 1$, alors $|x - \frac{p}{q}| > \frac{A_x}{q^m} > \frac{1}{2^k q^m} > \frac{1}{q^{m+k}}$.
Donc l'ensemble des (p, q) tels que $|x - \frac{p}{q}| < \frac{1}{q^n}$ est vide pour tout $n \geq m + k$, ce qui entraînne que $x \notin \mathcal{L}$. Contradiction ! □

Remarque 9.8. $\sum\limits_{n \in \mathbb{N}} 10^{-n!}$ est un nombre de Liouville :
Posons $x_n = \sum\limits_{k=0}^{n} 10^{-k!}$. Alors $|x - x_n| = \sum\limits_{k=n+1}^{\infty} 10^{-k!} < 10^{-(n+1)!} \sum\limits_{l=0}^{\infty} 10^{-l} < 2 \cdot 10^{-n!(n+1)} < 10^{-n!n}$. Pour tout $m \geq n$, $|x - x_m| < (10^{m!})^{-m} \leq (10^{m!})^{-n}$, donc il y a une infinité de tels entiers m pour tout $n \in \mathbb{N}$. Alors $x \in \mathcal{L}$.

Corollaire 9.9. $\sum\limits_{n \in \mathbb{N}} 10^{-n!}$ *est transcendant.*

Proposition 9.10. *Soit* $K \hookrightarrow L$ *une extension de corps et soit* $x \in L$. *Alors* $K[x]$ *coincide avec l'image du morphisme de* K*-algèbres l'évaluation en* x *suivant*

$$\begin{aligned} ev_x : K[X] &\longrightarrow L \\ P &\longmapsto P(x). \end{aligned}$$

Démonstration. $K[x] = \bigcap\limits_{\substack{B \text{ sous-anneau de } L \\ K \subset B, A \subset B}} B$, or $\mathrm{Im}(ev_x)$ est un sous-anneau de L contenant K et x, alors $K[x] \subset \mathrm{Im}(ev_x)$. Inversement, pour tout $P(X) = \sum\limits_{k=0}^{d} a_k X^k \in K[X]$, $ev_x(P) = P(x) = \sum\limits_{k=0}^{m} a_k x^k$ appartient à tout anneau contenant K et x et donc à leur intersection $K[x]$. Alors $\mathrm{Im}(ev_x) \subset K[x]$. □

Ceci donne un premier résultat de structure.

Théorème 9.11. *Soit* $K \hookrightarrow L$ *une extension de corps et soit* $x \in L$.
i) Si x *est transcendant sur* K, *on a alors*
- *le morphisme* ev_x *est alors injectif ;*
- *le* K*-espace vectoriel* $K[x]$ *est de dimension infinie ;*
- $K \hookrightarrow K(x)$ *est infinie.*

ii) Si x *est algébrique sur* K, *on a alors*
- *il existe un unique polynôme unitaire* P *de degré minimal annule par* x *i.e.* $P(x) = 0$ *;*

— *P est irréductible ;*
— *$K[x] = K(x)$;*
— *$K \hookrightarrow K[x]$ est finie et de degré* $\deg P$.

Définition 9.12. Si x est algébrique sur K, on appelle P **le polynôme minimal de x sur K**, on le note $P_{x,K}$.

Démonstration. *i)* x est transcendant sur K s.s.i. pout tout $P \in K[X] \setminus \{0\}$, $P(x) \neq 0$ s.s.i. ev_x est alors injectif. Alors le sous-anneau $K[x]$ engendré par x i.e. $\mathrm{Im}(ev_x)$ est isomorphe à $K[X]$. Donc le K-espace vectoriel $K[x] \simeq K[X]$ est de dimension infinie. De même, $K(x) \simeq K_{K[x]} \simeq K_{K[X]} \simeq K(x)$ a fortiori est un K-espace vectoriel de dimension infinie.
ii) Lorsque x est algébrique sur K, le noyau de ev_x est un idéal non nul. Or $K[X]$ est un anneaux pricipal, donc $\ker(ev_x)$ est donc engendré par un polynôme non nul P, de degré minimal parmi les polynômes s'annulant en x. Il est unique et complètement caractérisé si on exige de plus que P est unitaire. Alors $K[x] = \mathrm{Im}(ev_x)$ est isomorphe à l'anneau quotient $K[X]/(P)$.
Nous remarquons que nécessairement P est irréductible. Si $P = QR$ où Q, $R \in K[X]$, alors $0 = P(x) = Q(x)R(x) \Rightarrow 0 = Q(x)$ ou $0 = R(x)$ i.e. $Q \in \ker(ev_x)$ ou $R \in \ker(ev_x)$. Or P engendre $\ker(ev_x)$, donc $P|Q$ ou $P|R$, alors $R \in K[X]^*$ ou $Q \in K[X]^*$. Ça implique P est irréductible, alors (P) est premier et même maximal. Donc $K[x] = \mathrm{Im}(ev_x) \simeq K[X]/(P)$ est un corps. Donc $K[x] = K(x)$.
En particulier comme K-espace vectoriel, $K[x]$ est donc de dimension finie égale à $\deg P$. En effet, pout tout $Q \in K[X]$, par division euclidienne on obtient l'équation $Q = Pq + r$ avec q, $r \in K[X]$ et $\deg r < \deg P$, alors $Q(x) = r(x)$ et donc $K[x] \subset \mathrm{Im}(ev_x|_{K_{\deg P-1}[X]})$.
Par ailleurs, les polynômes $1, X, \cdots, X^{\deg P-1}$ qui engendrent $K[x]$ sont linéairement indépendants dans $K[X]/(P)$: si $\sum\limits_{k=0}^{\deg P-1} a_k X^k = 0$ dans $K[X]/(P) \simeq K[x]$, alors $P \left| \sum\limits_{k=0}^{\deg P-1} a_k X^k \right.$, où $\deg P > \deg \left(\sum\limits_{k=0}^{\deg P-1} a_k X^k \right)$. C'est impossible sauf si $\sum\limits_{k=0}^{\deg P-1} a_k X^k = 0$ i.e. $a_k = 0$ pour tout $k \in [\![0, n-1]\!]$. On conclut que $\dim_K K[x] = \deg P$. □

Corollaire 9.13. *Toute extension finie de corps est algébrique.*

Démonstration. Soit $K \hookrightarrow L$ une extension de corps et soit $x \in L$. Le K-espace vectoriel $K[x]$ est un sous-espace vectoriel du K-espace vectoriel L de dimension finie par hypothèse. $K[x]$ est donc un K-espace vectoriel de dimension dinie et d'après le théorème, x est algébrique sur K. □

Corollaire 9.14. *Toute extension $K \hookrightarrow L$ engendré par un nombre fini d'éléments algébriques sur K est finie et algébrique. En particulier, toute extension de corps algébrique et de type fini est finie.*

Démonstration. On procède par récurrence sur le cardinal de la partie $A \subset L$ qui engendre L i.e. $L = K(A)$. Si $A = \varnothing$, alors $L = K$ et le résultat est banal. C'est le cas d'extension de dgré 1.
Sinon, il existe $a \in A$ et on introduit $L' = K(A \setminus \{a\})$. L'hypothèse de récurrence entraîne que l'extension $K \hookrightarrow L'$ est finie. Par ailleurs a étant algébrique sur K, il l'est sur toute extension de K, en particulier sur L' : $L' \hookrightarrow L'(a) = K(A \setminus \{a\})(a) = K(A) = L$ est alors finie par le théorème 9.11.
Enfin, la composition de deux extensions de corps est finie s.s.i. les deux extensions le sont, comme il suit du théorème 8.5 : $[L : K] = [L : L'][L' : K]$ est finie et alors algébrique par le corollaire 9.13. □

Théorème 9.15. *Soit $K \hookrightarrow L$ une extension de corps. L'ensemble des éléments algébriques de L sur K est un sous-corps de L contenant K : en particulier cet ensemble forme une extension de corps de K algébrique.*

Démonstration. Soient x et y deux éléments non nuls de L algébriques sur K. Le corollaire 9.14 établit que l'extension de type fini $K(x, y)$ est finie, donc algébrique. x_y et $xy^{-1} \in K(x, y) \subset L$, donc ils sont algébriques. □

Définition 9.16. L'ensemble des éléments algébriques de L sur K est appelé **la clôture algébrique de K dans L**, notée $\overline{K}^L$

Définition 9.17. Soit $K \hookrightarrow L$ une extension de corps. On dit que K est **algébriquement clos** dans L s'il coïncide avec sa cloˆture algébriquement dans L i.e. $K = \overline{K}^L$.

Corollaire 9.18. *Toute extension $K \hookrightarrow L$ engendré par les éléments algébriques sur K est algébrique.*

Démonstration. Soit $A \subset L$ une partie algébrique sur K telle que $L = K(A)$. $\overline{K}^L$ la clôture algébrique de K dans L est un corps d'après le théorème 9.15, qui contient A. Alors $L = K(A) \subset \overline{K}^L \subset L$. On a alors $L = \overline{K}^L$ et tous les éléments de L sont ainsi algébrique sur K. □

Remarque 9.19. La réciproque du corollaire 9.13 est fausse cependant : $\overline{\mathbb{Q}}^{\mathbb{R}}$ l'ensemble des réels algébriques sur $\mathbb{Q}$ est une extension algébrique de $\mathbb{Q}$, mais $\mathbb{Q} \hookrightarrow \overline{\mathbb{Q}}^{\mathbb{R}}$ n'est pas finie.

En effet, $\overline{\mathbb{Q}}^{\mathbb{R}}$ contient des $\mathbb{Q}$-sous-espaces vectoriels de dimensions arbitairement grandes. Les polynômes $X^n - a$ de $\mathbb{Q}[X]$, $n \in \mathbb{N}^*$, où il existe $p \in \mathcal{P}$ tel que $val_p(a) = 1$, sont irréductibles dans $\mathbb{Q}[X]$ d'après la critère d'Eisenstein.
Par exemple, disons $a = 2 \in \mathcal{P}$. Par le théorème 9.10, $\mathbb{Q}(\sqrt[n]{2}) = \mathbb{Q}[\sqrt[n]{2}]$ est de degré $\deg(X^n - 2) = n$ et l'extension $\mathbb{Q} \hookrightarrow \overline{\mathbb{Q}}^{\mathbb{R}}$ n'est donc pas finie, mais elle est bien algébrique.

Théorème 9.20. *Soit $K \hookrightarrow L$ et $L \hookrightarrow M$ des extensions de corps. Alors $K \hookrightarrow M$ est une extension algébrique s.s.i. les extensions $K \hookrightarrow L$ et $L \hookrightarrow M$ le sont.*

Démonstration. $\Leftarrow$: C'est banal. Si $K \hookrightarrow M$ est algébrique sur K, tout élément m de M annule un polynôme $P \in K[X] \subset L[X]$ donc $L \hookrightarrow M$ est algébrique. De même $L \subset M$ et donc tout élément de L est algébrique sur K.
$\Rightarrow$: Pour tout $x \in M$, x est algébrique sur L, alors il existe un polynôme $P(X) = \sum\limits_{k=0}^{n} a_k X^k \in L[X]$ tel que $P(x) = 0$. Par hypothèse $K \hookrightarrow M$ est algébrique, donc aussi la sous-extension $K \hookrightarrow L' = K(p_1, \cdots, p_n)$ est finie d'après le corollaire 9.14, i.e. L' est un K-espace vectoriel de dimension finie.
Par ailleurs x est algébrique sur L', par le théorème 9.10, l'extension $L' \hookrightarrow L'(x)$ est alors finie ; par le théorème 8.5, $K \hookrightarrow L'$ est alors elle-même finie comme extension composé des extensions finies $K \hookrightarrow L$ et $L' \hookrightarrow L'(x)$. Donc $K \hookrightarrow L'$ est algébrique d'après le corollaire 9.13. Alors tous les éléments de $L'(x)$ sont algébriques sur K, et x en particulier est algébrique sur K. $\square$

10 Résultants

Retour sur le théorème 9.15, soit $K \hookrightarrow L$ une extension de corps et soient x et y deux éléments non nuls de L algébriques sur K. On a vu que $-x$, x^{-1}, $x + y$ et xy sont algébriques. Ceci n'était pas évident a priori en général.
Par exemple, on suppose que $P(X) = \sum\limits_{k=0}^{n} p_k X^k \in K[X]$ tel que $P(x) = 0$, alors posons $P_-(X) = \sum\limits_{k=0}^{n} p_k (-1)^k X^k$ et $P_{-1}(X) = \sum\limits_{k=0}^{n} p_k X^{n-k}$ et on obtient que $P_-(-x) = P(x) = 0$ et $P_{-1}(x^{-1}) = x^{-n} P(x) = 0$.
Mais il n'y a pas d'astuce éuivalente pour $x+y$ ou xy. Par le théorème 9.15 on sait que $x+y$ et xy sont alg'ebriques mais la démonstration du théorème ne formait pas les polynômes de $K[X]$ annulés par $x + y$ et xy. On suppose de plus que $Q(X) = \sum\limits_{k=0}^{m} q_k X^k \in K[X]$ tel que

$Q(y) = 0$. On obtient que $n = \deg P$ et $m = \deg Q$. Sans reste de généralité disons $n \geq m$. En outre, on définit l'isomorphsime d'anneaux entre $K[X]$ et $K^{\oplus \mathbb{N}}$:

$$\begin{aligned} \chi : \ K[X] &\longrightarrow \quad K^{\oplus \mathbb{N}} \\ \sum_{k=0}^{\infty} a_k X^k &\longmapsto (a_n)_{n \in \mathbb{N}} \end{aligned}$$

.

Définition 10.1. La matrice de Sylvester de P et Q, notée $Syl(P,Q)$, est la matrice $(n+m) \times (n+m)$ sur K suivante :

$$\begin{array}{cc}
 & \begin{array}{ccccccccc} 1 & 2 & \cdots & m & m+1 & m+2 & \cdots & \cdots & m+n \end{array} \\
\begin{array}{c} 1 \\ 2 \\ \vdots \\ \vdots \\ \vdots \\ n+1 \\ n+2 \\ \vdots \\ n+m \end{array} &
\begin{pmatrix}
p_n & 0 & \cdots & 0 & q_m & 0 & \cdots & \cdots & 0 \\
p_{n-1} & p_n & \ddots & \vdots & \vdots & q_m & \ddots & & \vdots \\
\vdots & p_{n-1} & \ddots & 0 & \vdots & & \ddots & \ddots & \vdots \\
\vdots & & \ddots & p_n & q_1 & & & \ddots & 0 \\
\vdots & & & p_{n-1} & q_0 & \ddots & & & q_m \\
p_0 & & & \vdots & 0 & \ddots & \ddots & & \vdots \\
0 & \ddots & & \vdots & \vdots & \ddots & \ddots & q_1 & \vdots \\
\vdots & \ddots & p_0 & \vdots & \vdots & & \ddots & q_0 & q_1 \\
0 & \cdots & 0 & p_0 & 0 & \cdots & \cdots & 0 & q_0
\end{pmatrix}
\end{array}$$

Définition 10.2. Le résultant de P et Q, notée $Res(P,Q)$, est définit par $Res(P,Q) := \det(Syl(P,Q))$.

Lemme 10.3. *Pour tout $a = (a_i)_{i \in [\![0,m-1]\!]} \in K^m$ et $b = (b_j)_{j \in [\![0,n-1]\!]} \in K^n$, on a*

$$Syl(P,Q) \begin{pmatrix} a_{m-1} \\ \vdots \\ a_0 \\ b_{n-1} \\ \vdots \\ b_0 \end{pmatrix} = \chi(\chi^{-1}(a)P + \chi^{-1}(b)Q).$$

Démonstration. Il suffit de développer le produit matriciel. Posons $A = \chi^{-1}(a) \in K[X]$ et

$B = \chi^{-1}(b) \in K[X]$, alors on obtient

$$
\begin{aligned}
Syl(P,Q)\begin{pmatrix} a_{m-1} \\ \vdots \\ a_0 \\ b_{n-1} \\ \vdots \\ b_0 \end{pmatrix} &= \begin{array}{c} 1 \\ \\ k \\ \\ m \\ \\ k \\ \\ n+1 \\ \\ k \\ \\ n+m \end{array} \begin{pmatrix} p_n a_{m-1} \\ \cdots \\ \sum_{l=0}^{k-1} p_{n+1-k+l} a_{m-1-l} \\ \cdots \\ \sum_{l=0}^{m-1} p_{n+1-m+l} a_{m-1-l} \\ \cdots \\ \sum_{l=0}^{m-1} p_{n+1-k+l} a_{m-1-l} \\ \cdots \\ \sum_{l=0}^{m-1} p_l a_{m-1-l} \\ \cdots \\ \sum_{l=0}^{n+m-k} p_l a_{n+m-l-k} \\ \cdots \\ p_0 a_0 \end{pmatrix} + \begin{array}{c} 1 \\ \\ k \\ \\ m+1 \\ \\ k \\ \\ n \\ \\ k \\ \\ n+m \end{array} \begin{pmatrix} q_m b_{n-1} \\ \cdots \\ \sum_{l=0}^{k-1} q_{m+1-k+l} b_{n-1-l} \\ \cdots \\ \sum_{l=0}^{m} q_l b_{n-1-l} \\ \cdots \\ \sum_{l=0}^{m} q_l b_{n+m-k-l} \\ \cdots \\ \sum_{l=0}^{m} q_l b_{m-l} \\ \cdots \\ \sum_{l=0}^{n+m-k} q_l b_{n+m-k-l} \\ \cdots \\ q_0 b_0 \end{pmatrix} \\
&= \begin{pmatrix} (AP)_{n+m-1} \\ \vdots \\ (AP)_0 \end{pmatrix} + \begin{pmatrix} (BQ)_{n+m-1} \\ \vdots \\ (BQ)_0 \end{pmatrix} \\
&= \chi(\chi^{-1}(a)P) + \chi(\chi^{-1}(b)Q) \\
&= \chi(\chi^{-1}(a)P + \chi^{-1}(b)Q).
\end{aligned}
$$

$\square$

Lemme 10.4. *Soit $R \in K[X]$ et on suppose que $R|P \wedge Q$ avec $\deg R \geq 1$, en effet P et Q ont une racine commune dans une extension de K (on va le voir plus tard), alors $\mathrm{Res}(P,Q) = 0$.*

Démonstration. C'est un corollaire immédiat du lemme 10.3 ci-dessus.
On suppose que $P = RS$ et $Q = RT$, où $S, T \in K[X]$. alors $TP - SQ = R(TS - ST) = 0$, où $0 \leq \deg T \leq \deg Q - 1$ et $0 \leq \deg S \leq \deg P - 1$ car $\deg R > 0$. Par le lemme 10.3,

$$TP - SQ = \chi^{-1}\left(Syl(P,Q) \begin{pmatrix} \chi(T) \\ -\chi(S) \end{pmatrix} \right).$$

Donc $TP = SQ$ entraîne que le vecteur $\begin{pmatrix} \chi(T) \\ -\chi(S) \end{pmatrix}$ appartient au noyau de la matrice de Syleveter $Syl(P,Q)$. Donc $Res(P,Q) = \det(Syl(P,Q)) = 0$. □

Corollaire 10.5. *Soit $K \hookrightarrow L$ une extension de corps et soient x et y deux éléments non nuls de L algébriques sur K. Alors $x+y$ et xysont algébriques sur K.*

Démonstration. On suppose que $P(X) = \sum_{k=0}^{n} p_k X^k$ et $Q(X) = \sum_{k=0}^{m} q_k X^k \in K[X]$ tel que $P(x) = Q(y) = 0$.
Pour $x+y$, on introduit $s = x+y$ et $P_S(X) = Q(S-X) \in K[S][X]$. Observons que $P_s(x) = Q(s-x) = Q(y) = 0 = P(x)$. Alors le résultant des polynômes $P(X)$ et $P_S(X)$ est un polynôme non nul en S à coefficients dans K, qui s'annule en $S = s$ d'après le lemme 10.4, puisque P_S et P ont en commun la racine x, $x \in L$. Pour $s = x+y$, s annule ainsi un polynôme non trivial de $K[X]$, ce qui fait de la somme $s = x+y$ un élément de l'extension L algébrique sur K sous l'hypothèse que x et y en sont.
Pour xy, on introduit $t = xy$ et $Q_T(X) = X^m Q(T/X) \in K[T][X]$. Observons que $Q_t(x) = x^m Q(\frac{t}{x}) = x^m Q(y) = 0 = P(x)$. Alors le résultant des polynômes $P(X)$ et $Q_T(X)$ est un polynôme non nul en T à coefficients dans K, qui s'annule en $T = t$ d'après le lemme 10.4, puisque Q_T et P ont en commun la racine x, $x \in L$. Pour $t = xy$, t annule ainsi un polynôme non trivial de $K[X]$, ce qui fait du produit $t = xy$ un élément de l'extension L algébrique sur K sous l'hypothèse que x et y en sont. □

11 Construction à la Règle et au Compas

11.1 La Constructibilité sur $\mathbb{R}^2$

Définition 11.1. Soit $\Sigma \subset \mathbb{R}^2$ une partie.

- On dit qu'une droite D est **définissable** sur Σ si $D = D(P,Q)$, où P, $Q \in \Sigma$ distincts ;
- On dit qu'un cercle C est **définissable** sur Σ si $C = C(P,Q) :=$ le cercle centré en P et passant par Q, où P, $Q \in \Sigma$ distincts.

Définition 11.2. Un point $P \in \mathbb{R}^2$ est dit **constructible sur** Σ s'il existe une suite finie croissante de parties de $\mathbb{R}^2$

$$\Sigma = \Sigma_0 \subsetneqq \Sigma_1 \subsetneqq \cdots \subsetneqq \Sigma_n \subset \mathbb{R}^2,$$

où $n \in \mathbb{N}^*$, avec $P \in \Sigma_n$. De plus, pour tout $i \in [\![1, n]\!]$, $\Sigma_i \setminus \Sigma_{i-1}$ est un singleton obtenu comme

- soit l'intersection de deux droites définissables sur Σ_{i-1} ;
- soit l'un des deux points de l'intersection d'une droite définissables sur Σ_{i-1} et d'un cercle définissables sur Σ_{i-1} ;
- l'un des deux points de l'intersection de deux cercles définissables sur Σ_{i-1}.

Définition 11.3. Un sous-ensemble fini $E \subset \mathbb{R}^2$ est dit **constructible sur** Σ s'il existe une suite finie croissante de parties de $\mathbb{R}^2$

$$\Sigma = \Sigma_0 \subsetneqq \Sigma_1 \subsetneqq \cdots \subsetneqq \Sigma_n \subset \mathbb{R}^2,$$

où $n \in \mathbb{N}^*$, avec $E \in \Sigma_n$. De plus, pour tout $i \in [\![1, n]\!]$, $\Sigma_i \setminus \Sigma_{i-1}$ est un singleton obtenu comme ci-dessus.

Remarque 11.4. Les points d'un enmble constructible sont nécessairement constructibles. La réciproque n'est pas toujours vraie. Voir ci-dessous : tout point dans $\mathbb{Q}$ est constructible sur $\{0, 1\}$, mais $|\mathbb{Q}| = \infty$.

On a cependant le résultat suivant.

Sorite 11.5. *tout sous ensemble E fini de $\mathbb{R}^2$, dont tous les points sont constructibles sur Σ est lui-même constructible sur Σ.*

Démonstration. On suppose que $E = \{p_1, \cdots p_k\}$, $k \in \mathbb{N}$ et

$$\Sigma \subsetneqq \Sigma_{i,1} \subsetneqq \cdots \subsetneqq \Sigma_{i,n_i} \ni p_i$$

pour tout $i \in [\![1, k]\!]$, avec $\Sigma_{i,j} \setminus \Sigma_{i,j-1}$ est un singleton obtenu comme ci-dessus.
On considère la suite

$$\begin{aligned}
\Sigma &\subsetneqq \Sigma_{1,1} \subsetneqq \cdots \subsetneqq \Sigma_{1,n_1} \\
&\subsetneqq \left(\Sigma_{2,1} \cup \Sigma_{1,n_1}\right) \subsetneqq \cdots \subsetneqq \left(\Sigma_{2,n_2} \cup \Sigma_{1,n_1}\right) \\
&\subsetneqq \cdots \\
&\subsetneqq \Big(\Sigma_{i,1} \cup \bigcup_{j=1}^{i-1} \Sigma_{j,n_j}\Big) \subsetneqq \cdots \subsetneqq \Big(\Sigma_{i,n_i} \cup \bigcup_{j=1}^{i-1} \Sigma_{j,n_j}\Big) \\
&\subsetneqq \cdots \\
&\subsetneqq \Big(\Sigma_{k,1} \cup \bigcup_{j=1}^{k-1} \Sigma_{j,n_j}\Big) \subsetneqq \cdots \subsetneqq \Big(\Sigma_{k,n_k} \cup \bigcup_{j=1}^{k-1} \Sigma_{j,n_j}\Big).
\end{aligned}$$

Alors on obtient immédiatement que E est alors constructible sur Σ. □

Définition 11.6. Soit $\Sigma \subset \mathbb{R}^2$ une partie.

- On dit qu'une droite D est **f-définissable** sur Σ si elle est définissable sur une paire de points eux-même constructibles sur Σ i.e. $D = D(P, Q)$, où P, Q distincts et définissable sur Σ ;
- On dit qu'un cercle C est **f-définissable** sur Σ s'il est définissable sur une paire de points eux-même constructibles sur Σ i.e. $C = C(P, Q)$, où P, Q distincts et définissable sur Σ.

Sorite 11.7. *La perpendiculaire et la parallèle à une droite D f-constructible sur Σ et passant par un point R constructible sur Σ sont f-constructibles sur Σ.*

Démonstration. Soient A un point arbitaire dans la droite distinct de R.
i) On la fait selon les étapes suivants :
1)$C(R, A)$;
2)$\{A, A'\} = C(R, A) \cap D$;
3)$C(A, A') \cap C(A', A) = \{R_1, R_2\}$;
4)$D(R_1, R_2)$.
ii) D'après i) on peut construit D_1 la perpendiculaire à D passant par R. On note H

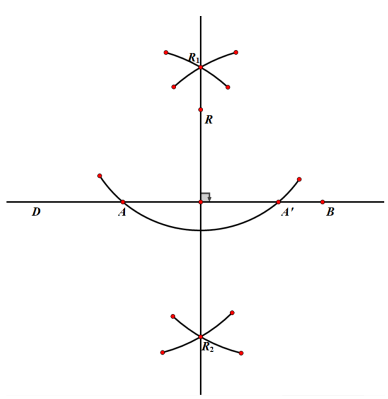

FIGURE 11.1 – la perpendiculaire

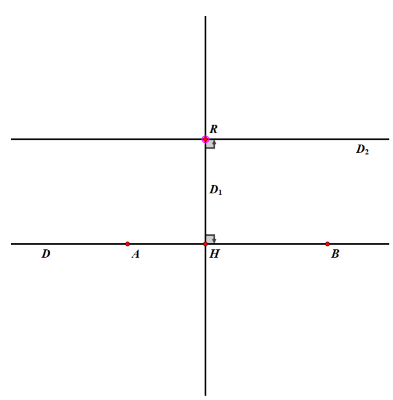

FIGURE 11.2 – la parallèle

l'intersection de D_1 et D. Alors on construit D_2 la perpendiculaire à D_1 passant R est la parallèle à D passant par R. □

Sorite 11.8. *Le cercle de centre un point O constructible et de rayon la distance entre deux points A et B constructibles est f-constructible.*

Démonstration. Le cas générique où les trois points ne sont pas alignés : observons que $D(O,B)$ et $D(A,B)$ sont f-constructibles, alors d'après la sorite 11.7 on construit D_1 la parallèle à $D(A,B)$ passant par O et D_2 la parallèle à $D(O,B)$ passant par A. Notons I le point d'intersection de D_1 et D_2, alors $|OI| = |AB|$ et on obtient que le cercle de centre O et est de rayon $|AB|$ construictible ;

Le cas dégénéré où les trois points sont alignés : pour un point $C \notin D(A,B)$ arbitaire, on

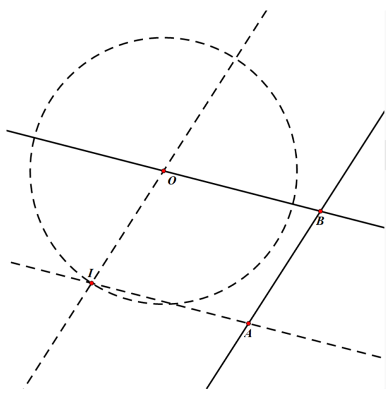

FIGURE 11.3 – le cas générique

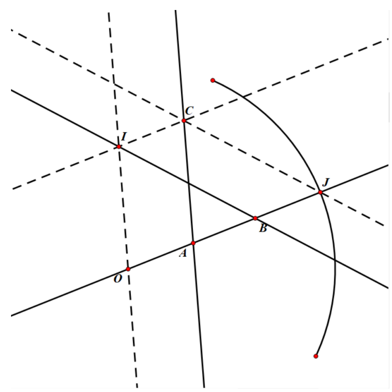

FIGURE 11.4 – le cas dégénéré

applique le cas générique à C, O, A et on construit I, on applique le cas générique à B, C, I et on construit J. On observons que $|OJ| = |AB|$ et le cercle cherché est alors $C(O,J)$. □

À titre d'exemple de géométrie exotique en caractéristique positive : soit K un corps de caractéristique et soient (A_1, A_2, A_3) un triangle arbitaire de K^2.

Proposition 11.9. *Les trois médianes i.e. les droites joignant un sommet au milieu du coté opposé sont parallèles.*

Démonstration. Pour tout $i \in \{\bar{0}, \bar{1}, \bar{2}\} = \mathbb{Z}/3\mathbb{Z}$,

$$\begin{aligned}
\overrightarrow{M_iA_i} &= \overrightarrow{OA_i} - \frac{1}{2}(\overrightarrow{OA_{i+1}} + \overrightarrow{OA_{i+2}}) \\
&= \overrightarrow{OA_i} - 2(\overrightarrow{OA_{i+1}} + \overrightarrow{OA_{i+2}}) \\
&= \overrightarrow{OA_i} + (\overrightarrow{OA_{i+1}} + \overrightarrow{OA_{i+2}}) \\
&= \overrightarrow{OA_1} + \overrightarrow{OA_2} + \overrightarrow{OA_3}.
\end{aligned}$$

□

11.2 Sous-ensembles constructibles de $\mathbb{R}$

Définition 11.10. Soit $\Sigma \supset \{0,1\}$ un sous-ensemble de $\mathbb{R}$. On dit qu'un nombre réel x est **constructible sur** Σ si c'est l'abscisse d'un point P constructible de $\mathbb{R}^2$ sur $\Sigma \times \{0\}$ au sens précédent.

Sorite 11.11. *$x \in \mathbb{R}$ est constructible sur Σ s.s.i. $(x,0)$ l'est sur $\Sigma \times \{0\}$*

Démonstration. Si $x \in \mathbb{R}$ est constructible sur Σ, alors il existe $(x,y) \in \mathbb{R}^2$ constructible sur $\Sigma \times \{0\}$. Par la sorite 11.7, on peut construire la perpendiculaire à Ox passant par (x,y), et on obtient que l'intersection $(x,0)$ est alors constructible sur $\Sigma \times \{0\}$. La réciproque est clair par définition. □

Théorème 11.12. *Soit $\Sigma \supset \{0,1\}$ un sous-ensemble de $\mathbb{R}$. Alors l'ensemble $\mathcal{C}_\Sigma$ l'ensemble constructibles sur Σ est un sous-corps de $\mathbb{R}$. De plus, pour tout $x \in \mathcal{C}_\Sigma$, $\sqrt{|x|} \in \mathcal{C}_\Sigma$.*

Démonstration. Soient x, y constructibles non nul sur Σ. On abuse la notation et on note $r = (r,0)$ pour tout $r \in \mathbb{R}$. On note O le point $(0,0)$ et note Ox la droite $D(O,x)$.
Au début, on construit D_O la perpendiculaire à Ox en O et $\{P,-P\} = C(O,1) \cap D_O$.
$i)$ L'opposé : $C(0,x) \cap Ox = \{-x,x\}$, donc $-x$ est constructible sur Σ.
Après on suppose que x, $y \in \mathbb{R}_+$ sans reste de généralité.
$ii)$ La somme : on a vu la construction d'un cercle C de centre 0 et de rayon la distance entre $(-x,0)$ et $(y,0)$ dans la sorite 11.8, donc $x+y$ est constructible sur Σ. Alternativement, on la fait selon les étapes suivants :
1)D_y la perpendiculaire à Ox en y ;
2)D la perpendiculaire à D_O en P ;
3)$P' = D_y \cap D$;
4)D' une parallèle à $D(P,x)$ en P' ;
5)$(x+y,0) = D' \cap Ox$.
$iii)$ L'inverse : 1)$\{P_x,-P_x\} = C(O,x) \cap D_O,$;
2)D la parallèle à $D(P_x,1)$ en P ;
3)$(\frac{1}{x},0)$ ou $(-\frac{1}{x},0) = D \cap Ox$.
$iv)$ Le produit : 1)$\{P_y,-P_y\} = C(O,y) \cap D_O,$;
2)D la parallèle à $D(P,x)$ en P_y ;
3)$(xy,0)$ ou $(-xy,0) = D \cap Ox$.
$v)$ La racine carrée : 1)$\{C_1,C_2\} = C(-1,x) \cap C(x,-1)$;
2)$Q = D(C_1,C_2) = (\frac{x+1}{2},0) \cap Ox$;

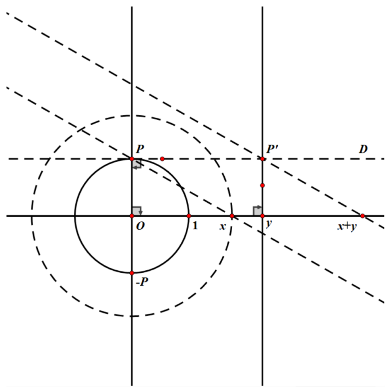

FIGURE 11.5 – la somme

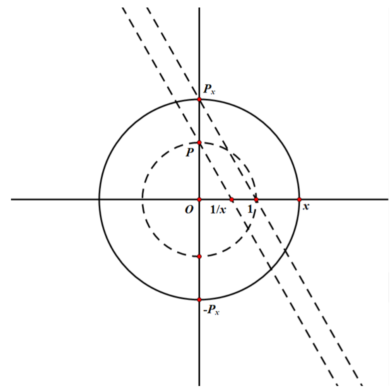

FIGURE 11.6 – l'inverse

3)$\{P_1, P_2\} = C(Q, x) \cap D_O = \{(0, \pm\sqrt{x})\}$ car les triangles (O, x, P_1) et $(O, -1, P_1)$ sont semblables puisque $(-1, x, P_1)$ est droit en P_1, et alors le théorème de Thalès entraîne l'identité $\frac{h}{x} = \frac{1}{h}$ i.e. $h = \sqrt{x}$.

□

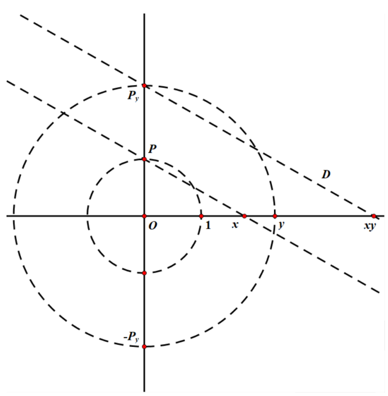

FIGURE 11.7 – le produit

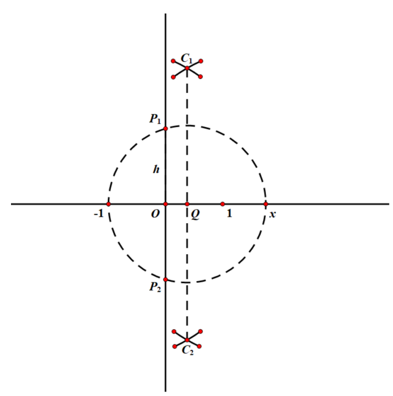

FIGURE 11.8 – la racine carrée

Corollaire 11.13. *$x \in \mathbb{R}$ est constructible sur $\{0, 1\}$ s.s.i. x est constructible sur $\mathbb{Q}$.*

Démonstration. $\mathcal{C}_{\{0,1\}}$ est un corps d'après le théorème 11.12. Or $\mathbb{Q}$ est l'intersection des sous-corps de $\mathbb{R}$ contenant 0 et 1. Donc $\mathbb{Q} \subset \mathcal{C}_{\{0,1\}}$. C'est à dire que x est constructible sur $\mathbb{Q}$. Il y a rien à démontrer pour la réciproque. □

11.3 Extensions quadratiques

Définition 11.14. Soit $K \hookrightarrow L$ une extension de corps. On dit l'extension est **quadratique** si $[L : K] = 2$.

Lemme 11.15. *Soit K un corps de caractéristique différente de 2 et soit $K \hookrightarrow L$ une extension quadratique de corps. Alors il existe $x \in L \setminus K$ tel que $x^2 \in K$ et $L = K[x] = K(x)$.*

Démonstration. Pour y un élément arbitaire de $L \setminus K$, $(1, y)$ est libre linéairement sur K, c'est donc une base du K-espace vectoriel L et il existe a, $b \in K$ tels que $y^2 = ay + b$. On suppose que $x = cy + d$ pour c, $d \in K$ tels que $x^2 \in K$, alors $K \ni x^2 = c^2y^2 + 2cdy + d^2 = (ac + 2d)cy + c^b + d^2 \Rightarrow (ac + 2d)c = 0$. Soit $c = 0 \Rightarrow x \in K$, soit $d = -\frac{ac}{2}$ et $x \in L \setminus K$.
Par exemple, on pose $c = 2$ et $d = -a$, alors $x^2 \in K$ et de plus $K[x] = K[y] = L$. □

Remarque 11.16. Le résultat est faux en caractéristique 2 : $\mathbb{F}_2 \hookrightarrow \mathbb{F}_2[X]/(X^2+X+1) \simeq \mathbb{F}_2(x)$, où x est une racine de $X^2 + X + 1$. On suppose que $y = ax + b$ avec a, $b \in \mathbb{F}_2$, dès lors $y^2 = a^2x^2 + b^2 = a^2x + a^2 + b^2 \in \mathbb{F}_2 \Rightarrow a^2 = 0 \Rightarrow a = 0 \Rightarrow y \in \mathbb{F}_2$.

Théorème 11.17 (Wantzel)**.** *Soit K un sous-corps de R et soit x un réel. Alors x est constructible sur K s.s.i. il existe une suite d'extensions*

$$K = K_0 \underset{\neq}{\subsetneq} K_1 \underset{\neq}{\subsetneq} \cdots \underset{\neq}{\subsetneq} K_n \subset \mathbb{R}$$

telle que

- $[K_i : K_{i-1}] = 2$ *pour tout* $i \in [\![1, n]\!]$ *;*
- $x \in K_n$.

Démonstration. Soit L un sous-corps de $\mathbb{R}$.
$i)$ Le point d'intersection de 2 droites non-parallèles définissable sur L i.e. définies pas deux points dont les coordonnées sont dans L, a ses coordonnées dans L : on précise les équations de droites

$$L_1 = D(P_1, Q_1) : |X - P_1, Q_1 - P_1| = a_1x + b_1y + c_1 = 0,\ a_1,\ b_1,\ c_1 \in L,$$
$$L_2 = D(P_2, Q_2) : |X - P_2, Q_2 - P_2| = a_2x + b_2y + c_2 = 0,\ a_2,\ b_2,\ c_2 \in L.$$

L'intersection de L_1 et L_2 est alors donnée par le système

$$\begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}.$$

$D_1 \nparallel D_2$ s.s.i. $A = \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}$ est inversible, donc on obtient

$$\begin{pmatrix} x \\ y \end{pmatrix} = A^{-1} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \in L^2.$$

ii) L'intersection non vide d'une droite définissable sur L et d'un cercle définissable sur L a ses coordonnées dans L : on précise les équations de droite et de cercle

$$\begin{aligned} L &: ax + by + c = 0, & a,\, b,\, c \in L \\ C &: (x - x_0)^2 + (y - y_0) = R^2, & x_0,\, y_0,\, R \in L. \end{aligned}$$

D est une droite implique que $a \neq 0$ ou $b \neq 0$, sans reste de généralité on suppose que $b \neq 0$. En substituant : $(x - c_1)^2 + (\frac{-c-ax}{b} - c_2) - R^2 = 0$, alors x est une solution de l'équation quadratique ci-dessus.

iii) L'intersection non vide de 2 cercles distincts définissable sur L a ses coordonnées dans L : on précise les équations de cercles

$$\begin{aligned} C_1 &: (x - x_1)^2 + (y - y_1) = R_1^2, & x_1,\, y_1,\, R_1 \in L, \\ C_2 &: (x - x_2)^2 + (y - y_2) = R_2^2, & x_2,\, y_2,\, R_2 \in L. \end{aligned}$$

En soustrayant

$$(x_2 - x_1)(2x - x_1 - x_2) + (y_2 - y_1)(2y - y_1 - y_2) = R_1^2 - R_2^2.$$

L'intersection est non vide implique que $x_1 \neq x_2$ ou $y_1 \neq y_2$, sans reste de généralité on suppose que $y_1 \neq y_2$. On résout en y et on substitut dans l'équation de C_1 pour coordonnée x de l'intersection comme solution d'une équation quadratique. On résout ensuite en y avec l'équation linéaire.

$\Rightarrow$: Soit x un réel constructible sur K, alors $(x, 0) \in \mathbb{R}^2$ est constructible sur $K \times \{0\}$ i.e. il existe

$$K \times \{0\} = \Sigma_0 \subsetneqq \Sigma_1 \subsetneqq \cdots \subsetneqq \Sigma_n \subset \mathbb{R}^2,$$

avec $(x, 0) \in \Sigma_n$ et pour tout $i \in [\![1, n]\!]$, $\Sigma_i \setminus \Sigma_{i-1}$ est un singleton (x_i, y_i) obtenu comme

- soit l'intersection de deux droites définissables sur Σ_{i-1} ;
- soit l'un des deux points de l'intersection d'une droite définissables sur Σ_{i-1} et d'un cercle définissables sur Σ_{i-1} ;
- l'un des deux points de l'intersection de deux cercles définissables sur Σ_{i-1}.

On note $K_0 = K$ et $K_i = K_{i-1}(x_i)$ pour tout $i \in [\![1, n]\!]$. On a vu que soit $x_i \in K_{i-1}$ i.e. $[K_i : K_{i-1}] = 1$, soit x_i est de degré 2 sur K_{i-1} i.e. $[K_i : K_{i-1}] = 2$. Donc on trouve une suite de corps qu'on veut.
$\Leftarrow$: Réciproquement, pour tout $x \in K_n$, on raisonne par récurrence sur n la longueur de la suite.
Soit $x \in K_{n-1}$, alors il n'y a rien à démontrer ; soit $x \in K_n \setminus K_{n-1}$, alors $K_n = K_{n-1}(x)$, par le lemme 11.15 il existe $y \in K_n$ tel que $y - x \in K_{n-1}$ et $y^2 \in K_{n-1}$, par l'hypothèse de récurrence y^2 est constructible sur K et alors par le théorème 11.12 y l'est. On obtient que $x = y - (y - x)$ est bien constructible sur K.
Ceci clôt du sens direct du théorème de Wantzel. □

Corollaire 11.18. *Soit K un sous-corps de R et soit x un réel. Alors x est constructible sur K implique que x est algébrique sur K de degré une puissance de 2.*

Démonstration. Par le théorème de Wantzel, il existe une suite d'extensions

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

telle que
- $[K_i : K_{i-1}] = 2$ pour tout $i \in [\![1, n]\!]$;
- $x \in K_n$.

$[K_n : K] = \prod_{i=1}^{n} [K_i : K_{i-1}] = 2^n$. On introduisons $K \hookrightarrow K(x) \hookrightarrow K_n$. De même, $2^n = [K_n : K] = [K_n : K(x)][K(x) : K] \Rightarrow [K(x) : K] | 2^n$, donc il existe $k \in [\![1, n]\!]$ tel que $[K(x) : K] = 2^k$. □

Corollaire 11.19 (Duplication du cube)**.** *C'est impossible de construire un cube dont le volume est deux fois plus grand qu'un cube donné.*

Démonstration. Le problème est équivalant que $\sqrt[3]{2} \in \mathcal{C}_{\{0,1\}} = \mathcal{C}_{\mathbb{Q}}$. Or le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbb{Q}$ est $X^3 - 2$, donc $\sqrt[3]{2}$ est de degré 3, ce n'est pas une puissance de 2. □

Corollaire 11.20 (Trisection de l'angle)**.** $\frac{\theta}{3}$ *est constructible à partir de θ s.s.i. $X^3 - 3X - 2\cos\theta$ a une racine dans $\mathbb{Q}(\theta)$.*

Démonstration. $\cos 3\phi = 4\cos^3\phi - 3\cos\phi$, donc $P(X) = 4X^3 - 3X - \cos\theta = \frac{1}{2}((2X)^3 - 3(2X) - 2\cos\theta)$ a une racine $\cos\frac{\theta}{3}$. Si P est irréductible sur $\mathbb{Q}(\cos\theta)$, alors $\cos\frac{\theta}{3}$ est de degré 3 et donc n'est pas constructible sur $\mathbb{Q}(\cos\theta)$.
Si P est réductible sur $\mathbb{Q}(\cos\theta)$, alors soit $\cos\frac{\theta}{3}$ est une racine d'un facteur linéaire et donc

dans $\mathbb{Q}(\cos\theta)$, soit $\cos\frac{\theta}{3}$ est une racine d'un facteur quadratique et alors constructible sur $\mathbb{Q}(\cos\theta)$. □

Remarque 11.21. $\frac{\pi}{9}$ n'est pas constructible à la règle et au compas parce que $X^3 - 3X - 1$ est irréductible sur $\mathbb{Q}$.

Corollaire 11.22 (Quadrature du cercle)**.** *C'est impossible de construire un carré de même aire qu'un disque donné.*

Démonstration. Le problème est équivalant que $\sqrt{\pi} \in \mathcal{C}_{\{0,1\}} = \mathcal{C}_{\mathbb{Q}}$. Or π est transcendant (Lindemann), donc $\sqrt{\pi}$ n'est pas algébrique ou constructible. □

12 Corps de Rupture et Corps de Décomposition

12.1 Corps de Rupture

Définition 12.1. $P(X) \in K[X]$ est **scindé sur** L, où L est une extension de K si P s'écrit comme un produit de facteurs de degré 1 dans $L[X]$.

Proposition 12.2. *Soit K un corps et soit $P \in K[X]$ irréductible. Il existe alors une extension K_P de K dans laquelle P admet (au moins) une racine x_p. De plus K_P coincide alors avec $K(x_P)$.*

Démonstration. $K[X]$ ètant principal on note $K[X]/(P) := K_P$ un corps et note $\omega : K[X] \to K[X]/(P) = K_P$ le passage au quotient. Si $Q(X) = \sum_{k=0}^{\deg Q} b_k X^k$, alors $\omega(Q) = \sum_{k=0}^{\deg Q} \omega(b_k)\omega(x)^k$. En effet $\omega(P) = 0$ et ω est un morphisme d'anneaux, clairement injectif sur K. En identifiant K et son image $\omega(K)$ dans $K[X]/(P)$,
Introduisons $x_P = \omega(X)$, on a alors $0 = \omega(P) = P(x_P)$.On dispose de l'application

$$\begin{aligned} ev_{x_P} : K[X] &\longrightarrow K[x_P] \subset K_P \\ Q &\longmapsto Q(x_P) \quad . \end{aligned}$$

ev_{x_P} descend à $K[X]/(P)$ car $\ker ev_{x_P} = (P)$:

$$\begin{aligned} \tilde{ev}_{x_P} : K[X]/(P) = K_P &\longrightarrow K[x_P] \\ \bar{Q} &\longmapsto Q(x_P) \end{aligned}$$

$\tilde{ev_{x_P}}$ est automatiquement injective piusque $K[X]/(P)$ est un corps et ev_{x_P} un morphisme d'anneaux. $\tilde{ev_{x_P}}$ est surjective car ev_{x_P} est surjective d'après la description de $K[X]$ comme $\{Q(x_P),\ Q \in K[X]\}$. Donc $\tilde{ev_{x_P}}$ est un isomorphisme sur $K[x_P]$.
En aprticulier, x_P est algébrique sur K et donc $K[x_P]$ est un corps et coïncide avec $K(x_P)$. □

Définition 12.3. Le corps K_P est appelé **corps de rupture de** P.

Exemple 12.4. *i)* $\mathbb{C}$ est le corps de rupture de tout polynôme P quadratique sur $\mathbb{R}$ sans racine réelle. En effet P est alors irréductible dans $\mathbb{R}$ et $\mathbb{R}[X]/(P) = \mathbb{R}_P = \mathbb{R}[x]$, où $P(x) = 0$ et $x \in \mathbb{C} \setminus \mathbb{R}$. Or $\dim_{\mathbb{R}} \mathbb{R}[x] \leq 2$, donc $\dim_{\mathbb{R}} \mathbb{R}[x] = 2$ et $\mathbb{R}[x] = \mathbb{C}$.
ii) $\mathbb{Q}(\sqrt[3]{2})$ est un corps due rupture de $P(X) = X^3 - 2$. P est irréductible sur $\mathbb{Q}$ par la critère d'Eisenstein est satisfait. Donc $\mathbb{Q}_P = \mathbb{Q}[X]/(P) \simeq \mathbb{Q}(\sqrt[3]{2})$. De même pour $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$, où $j = e^{\frac{2\pi}{3}}$. Remarquez que $X^3 - 2$ n'est pas scindé sur $\mathbb{Q}(\sqrt[3]{2})$, ni sur $\mathbb{Q}(j\sqrt[3]{2})$ ou $\mathbb{Q}(j^2\sqrt[3]{2})$.

Définition 12.5. Soit $i : K \hookrightarrow L_1$ et $j : K \hookrightarrow L_2$ deux extensions de K. On appelle **K-morphisme de L_1 et L_2** un morphisme de corps $\sigma : L_1 \to L_2$ qui coïncide avec l'identité sur K i.e. $\sigma \circ i = j$.

Proposition 12.6. *Soit K un corps et soit $P \in K[X]$ irréductible. Pour toute extension $K \hookrightarrow L$ et toute racine x de P dans L, il existe un unique K-morphisme $K_P \hookrightarrow L$ qui envoie x_P sur x.*

Démonstration. On introduit le morphisme d'anneaux $ev_x : K[X] \to L$ qui s'annule en $P \in K[X]$ et descend donc au quotient $KX/(P) = K_P$ pour fournir $\tilde{ev_{x_P}}$ un K-morphisme de K_P vers L, qui envoie $x_P = \omega(X)$ sur x. Alors on obtient le diagramme commutatif

$$\begin{tikzcd} K[X] \arrow[r, "ev_x"] \arrow[d, "\omega"'] & L \cdot \\ K_P \arrow[ur, "\tilde{ev_{x_P}}"'] & \end{tikzcd}$$

$\tilde{ev_{x_P}}$ envoie x_P sur x ; tout morphisme ϕ d'anneau sur $K_P \simeq K(x_P) = K[x_P]$ est complètement déterminé par $\phi|_K$ et $\phi(x_P)$, d'où on voit l'unicité. □

Corollaire 12.7. *Soit K un corps et soit $P \in K[X]$ irréductible. On suppose que x_1 et x_2 sont deux racines de P dans deux extensions L_1 et L_2 de K, alors $K(x_1)$ et $K(x_2)$ sont K-isomorphisme.*

Démonstration. On a vu que par la proposition 12.6 on peut construit

$$\begin{tikzcd} & K_P \arrow[dl, hook', "\phi_1"'] \arrow[dr, hook, "\phi_2"] & \\ K[x_1] = K(x_1) & & K(x_2) = K[x_2] \end{tikzcd} .$$

ϕ_1 et ϕ_2 sont des morphismes de corps injectifs à ce titre. Or ils sont aussi clairement surjectifs. Donc ϕ_1 et ϕ_2 sont isomorphismes et l'isomorphisme de $K(x_1)$ avec $K(x_2)$ est donné par la composition : $\psi = \phi_2 \circ \phi_1^{-1}$. ϕ_1 et ϕ_2 sont des K-morphismes et donc ψ un K-isomorphisme. □

Remarque 12.8. Il n'y a, en général, pas unicité de l'isomorphisme : si $K(x_2) = K(x_3)$, où $x_2 \neq x_3$ sont racines de P, on peut alors envoyer x_1 sur x_3 par un autre isomorphisme. Par contre, il existe sous les hypothèse du corollaire 12.7, un unique isomorphisme de $K(x_1)$ sur $K(x_2)$ envoyant x_1 sur x_2 à cause du résultat d'unicité de la proposition 12.7.

12.2 Corps de Décomposition de scindement

Théorème 12.9. *Soit K un corps et soit $P \in K[X]$. Alors*

— *il existe une extension finie $K \hookrightarrow L$ dans laquelle $P(X)$ est scindé, de racine $x_1, \cdots,$ x_d telle que $L = K(x_1, \cdots, x_d)$;*

— *toutes deux telles extensions sont isomorphismes.*

Démonstration. Pour l'existence, on procède par récurrence sur le degré d de P.
Si $d = 1$, alors $L = K$, $P(X) = X - k \in K[X]$ où $k \in K$.
Si $d > 1$, on suppose Q est un facteur irréductible de P dans $K[X]$ un anneau factoriel, alors on note K_Q le corps de rupture de Q. Dans K_Q, P admet une racine x_Q et par la division euclidienne, $P(X) = (X - x_Q)R(X)$, où $R \in K_Q[X]$ et $\deg R = d - 1$. On applique l'hypothèse de récurrence à R pour obtenir un corps de décomposition $K_Q \hookrightarrow L$ de R sur K_Q. R est ainsi scindé dans $L[X]$, de racine $(x_1, \cdots, x_{d-1})$. Alors P est aussi scindé dans $L[X]$, de racines $(x_1, \cdots, x_{d-1}), x_Q$. Enfin, $L = K_Q(x_1, \cdots, x_{d-1}) = K(x_Q)(x_1, \cdots, x_{d-1})$, donc L est bien le corps de décomposition de P car $K(x_Q)(x_1, \cdots, x_{d-1}) = K(x_1, \cdots, x_{d-1}, x_Q)$.
Pour l'unicité, on procède encore par récurrence sur le degré d de P.
Soient $K \hookrightarrow L_1$, $K \hookrightarrow L_2$ deux corps de décomposition de P. On suppose $x_1 \in L_1$ et $x_2 \in L_2$ tels que $Q(x_1) = 0$ et $Q(x_2) = 0$. Alors $K(x_1) \in L_1$, $K(x_2) \in L_2$ sont deux corps de rupture de P, alors il existe un K-isomorphisme de $K(x_1)$ avec $K(x_2)$ envoyant x_1 sur x_2 par le corollaire 12.7. Il permet de considérer L_2 comme une extension de $K(x_1)$: $K(x_1) \simeq K(x_2) \hookrightarrow L$.
Or $P(X) = (X - x_1)R_1(X)$, où $R_1 \in K(x_1)[X]$, alors L_1 et L_2 deux extensions de $K(x_1)$ sont des corps de décomposition de R_1 sur $K(x_1)$. L'hypothèse de récurrence que l'on applique au polynôme $R_1 \in K(x_1)[X]$ entraîne que L_1 et L_2 sont $K(x_1)$-isomorphisme, ceci implique que L_1 et L_2 sont alors K-isomorphisme. □

12.3 Corps de Décomposition de scindement

Définition 12.10. Un corps Ω est dit **algébriquement clos** si tout polynôme non constant de $\Omega[X]$ a une racine dans Ω.

Sorite 12.11. *Sur un corps algébriquement clos tout polynôme est scindé.*

Démonstration. On procède par récurrence sur le degré du polynôme P. Si x est une racine de P sur Ω, alors $(X-x)|P$, il existe un polynôme $Q \in \Omega[X]$ tel que $P(X) = (X-x)Q(X)$, où $\deg Q = \deg P - 1$. On applique l'hypothèse de récurrence à Q pour conclut. □

Définition 12.12. On appelle **clôture algébrique** d'un corps K une extension algébrique de corps $K \hookrightarrow \Omega$ où Ω est un corps algébriquement clos.

Exemple 12.13. $\mathbb{C}$ est algébriquement clos ; $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$; mais $\mathbb{C}$ n'est pas une clôture algébrique de $\mathbb{Q}$ parce que $\mathbb{Q} \hookrightarrow \mathbb{C}$ n'est pas algébrique. Les nombres algébriques sur $\mathbb{Q}$ forment un sous-ensemble $\bar{\mathbb{Q}}$ dénombrable de $\mathbb{C}$.

Proposition 12.14. *Soit $K \hookrightarrow L$ une extension algébrique de corps. On fait l'hypothèse que tout polynôme de $K[X]$ est scindé sur L, en effet, on peut remplacer l'hypothèse plus faible : tout polynôme de $K[X]$ admet au moins une racine dans L. Alors L est une clôture algébrique de K.*

Démonstration. Soit $Q \in L[X]$ irréductible et soit x une racine de Q dans une extension de L. x est alors algébrique sur L et par hypothèse $K \hookrightarrow L$ est algébrique, x est algébrique sur K. Soit $P_{x,K} \in K[X] \subset L[X]$ le polynôme minimal de x sur K. Puisque $Q(x) = 0$ et que Q est irréductible sur L, $Q|P$. Mais par hypothèse, $P \in K[X]$ est scindé sur L et il en ou alors de même du polynôme Q qui divise P. En particulier Q a une unique racine x dans L. Pour conclure, remarquons que tout élément de $L[X]$ est un produit de polynômes irréductibles et est donc scindé, en particulier admet une racine, sur L, ce qui fait du corps L une clôture algébrique de K. □

Proposition 12.15. *Soit Ω un corps algébriquement clos et soit $K \subset \Omega$ un sous-corps. L'ensemble des éléments de Ω qui sont algébriques sur K forment une clôture algébrique de K, i.e. la clôture algébrique d'un corps dans une extension algébriquement close est une clôture algébrique.*

Démonstration. On a vu que pour une extension $K \hookrightarrow \Omega$, l'ensemble

$$\bar{K} = \{x \in \Omega,\ x \text{ est algébrique sur } K\}$$

forment une sous-corsp de Ω. Soit $P \in \bar{K}[X]$ non constant et soit x une racine de P dans Ω. x est aussi par définition algébrique sur $\bar{K}$ et est par le théorème 9.20 algébrique sur K. Donc $x \in \bar{K}$, $\bar{K}$ est ainsi une clôture algébrique de K, puisque $K \hookrightarrow \bar{K}$ est algébriquement et que tout polynôme de $\bar{K}[X]$ admet au moins une racine dans $\bar{K}$. En fait, il est alors scindé sur $\bar{K}$ comme on l'a vu. □

Théorème 12.16 (Steinitz)**.** *Tout corps admet une clôture algébrique.*

Démonstration. — Le cas où K est dénombrable : $K[X]$ est alors dénombrable comme $\mathbb{Q}[X]$ qu'on a vu. Donc $K[X] = \{P_n,\ n \in \mathbb{N}\}$, on pose alors $K_0 = K$, et $K_n =$ le corps de décomposition de P_n sur K_{n-1}, ainsi K_n est une extension algébrique finie de K_{n-1}. On a une tour d'extensions finies et algébriques : $K = K_0 \subset K_1 \subset \cdots \subset K_n \subset \cdots$. On pose $L = \bigcup_{n\in\mathbb{N}} K_n$. Comme la suite des K_n est monotone croissante pour l'inclusion, l'hérite d'une structure de corps, canoniquement, et pour laquelle les K_n sont des sous-corps de L.
Par ailleurs, car $K \hookrightarrow K_n$ est fini et alors algébrique, donc pour tout $l \in L$, il existe $n \in \mathbb{N}$ tel que $l \in K_n$ et donc l est algébrique sur K. On obtient que l'extension $K \hookrightarrow L$ est algébrique.
Pour conclure : tout polynôme de $K[X]$ est l'un des $(P_n)_{n\in\mathbb{N}}$, par construction il est scindé dans K_k, a fortiori dans $L = \bigcup_{n\in\mathbb{N}} K_n$. Par la proposition 12.14, l'extension L est alors une clôture algébrique de K.

— Le cas général : On introduit l'anneau de polynôme

$$A = K\left[(X_{P,i})_{\substack{P\in\mathscr{P}\\ i\in[\![0,\deg P]\!]}}\right],$$

où $\mathscr{P}$ est l'ensemble des polynômes unitaire non constant de $K[X]$.
On introduit aussi les notations suivantes. Pour tout $P \in \mathscr{P}$ et $k \in [\![0, \deg P - 1]\!]$,

$$\sum_{k=0}^{\deg P-1} a_{P,k}X^k = \tilde{P}(X) = P(X) - \prod_{k=0}^{\deg P-1} (X - X_{P,k}) \in A[X].$$

On note $\mathcal{A}$ l'idéal de A engendré par les $a_{P,k}$, i.e. $\mathcal{A} = \langle (a_{P,k})_{\substack{P\in\mathscr{P}\\ i\in[\![0,\deg P]\!]}} \rangle$.
i) Si $1 \in \mathcal{A}$, alors il existe $r \in \mathbb{N}$, $(b_k)_{i\in[\![0,r]\!]} \in A^r$ et $(P_i)_{i\in[\![0,r]\!]} \in \mathscr{P}^r$ tels que

$$1 = \sum_{i=1}^{r} a_{P_i,k_i} b_i.$$

Soit $K \hookrightarrow K'$ une extension de corps dans laquelle tous les $(P_i)_{i\in[\![1,r]\!]}$ sont scindé et de racines $(x_{i,k})_{\substack{i\in[\![1,r]\!]\\ k\in[\![0,\deg P_i-1]\!]}}$. On obtient l'existence de K' par une récurrence finie banale à partir du théorème donnant l'existence du corps de décomposition d'un polynôme : soit $P_k \in K[X] \subset K_{k-1}[X]$, où K_{k-1} le corps de décomposition du $(P_1, \cdots, P_{k-1})$; le théorème assure l'existence d'une extension K_k de K_{k-1} telle que K_k le corps de décomposition de P_k sur K_{k-1} i.e. $K_k = K_{k-1}(x_{k,0}, \cdots, x_{k,\deg P_k-1})$, alors c'est l'extension recherchée,

$$K_k = K_{k-1}(x_{k,0}, \cdots, x_{k,\deg P_k-1}) = K(x_{1,0}, \cdots, x_{1,\deg P_1-1}, \cdots, x_{k,0}, \cdots, x_{k,\deg P_k-1}),$$

et tous les $(P_i)_{i\in[\![1,k]\!]}$ sont scindés sur K_k. On introduit alors le morphisme de K-algèbre suivant :

$$\begin{aligned} m : A &\longrightarrow \quad K' \\ X_{Q,l} &\longmapsto \begin{cases} x_{i,l} & , Q = P_i,\ \text{où } l \in [\![0, \deg P_i - 1]\!] \\ 0 & , \text{sinon} \end{cases} \end{aligned}.$$

On étends m un morphisme d'anneaux en

$$\begin{aligned} m : A[X] &\longrightarrow \quad K'[X] \\ \sum_{l=0}^{d} s_l X^l &\longmapsto \sum_{l=0}^{d} m(s_l) X^l. \end{aligned}$$

On a alors dans $K'(X)$

$$\begin{aligned} M(\tilde{P}_i)(X) &= M(P_i)(X) - M(\prod_{k=0}^{\deg P_i-1} (X - X_{P_i,k})) \\ &= P_i(X) - \prod_{k=0}^{\deg P_i-1} (X - m(X_{P_i,k})) \\ &= P_i(X) - \prod_{k=0}^{\deg P_i-1} (X - x_{i,k})) \\ &= P_i(X) - P_i(X) = 0. \end{aligned}$$

Or

$$0 = M(\tilde{P}_i)(X) = M(\sum_{k=0}^{\deg P-1} a_{P,k} X^k) = \sum_{k=0}^{\deg P-1} m(a_{P,k}) X^k,$$

c'est à dire que $m(a_{P,k}) = 0$ pour tout $k \in [\![0, \deg P_i - 1]\!]$. Il reste à prendre l'image par

$m : A \to K'$ de l'identité ci-dessus pour obtenir : $1_{K'} = m(1_A) = \sum_{i=1}^{r} m(a_{P_i,k_i})m(b_i) = 0_{K'}$, contradiction ! Donc $\mathcal{A} \neq A$. Soit alors $\mathbf{m}$ un idéal maximal contenant $\mathcal{A}$, alors $L = A/\mathbf{m}$ est en particulier un corps.

ii) On va vérifier que $K \hookrightarrow L$ est une extension algébrique.

Pour $P \in \mathscr{P}$ arbitaire, on suppose que $\deg P = n$. On note $\omega : A \to L = A/\mathbf{m}$ le passage au quotient. C'est un K-morphisme puisque $\mathbf{m} \neq A$ et alors $K \cap \mathbf{m} = \{0\}$. Pour tout $k \in [\![0, n-1]\!]$, $\overline{X}_{P,k} := \omega(X_{P,k})$. On étends ω l'application quotient $\tilde{\omega} : A[X] \to L[X]$. $\tilde{P}$ a ses coefficients dans $\mathcal{A}$, donc dans $\mathbf{m}$, alors $\tilde{\omega}$ envoie $\tilde{P}$ sur 0, ce qui se lit encore :

$$\begin{aligned}
\tilde{\omega}(P(X)) &= \tilde{\omega}\Big(\prod_{k=0}^{\deg P-1} (X - X_{P,k})\Big) \\
\Rightarrow P(X) &= \prod_{k=0}^{\deg P-1} (X - \omega(X_{P,k})) \\
\Rightarrow P(X) &= \prod_{k=0}^{\deg P-1} (X - \overline{X}_{P,k}).
\end{aligned}$$

Donc tous les $\overline{X}_{P,k}$ sont algébriques sur K puisque ils sont racines de $P \in K[X]$. De plus, tout polynôme unitaire non constant appartenant à $\mathscr{P}$, est scindé dans L. Par la proposition 12.14, L est alors une clôture algébrique de K.

$\square$

Lemme 12.17. *Soit K un corps et soit Ω une clôture algébrique de K. On suppose $x \in \Omega \backslash K$ et note $L = K(x)$, $P = P_{x,K}$ le polynôme minimal de x sur K. Alors toute extension $K \xrightarrow{\sigma} \Omega$ se prolonge à L en $L \xrightarrow{\tilde{\sigma}} \Omega$ i.e.*

$$\begin{tikzcd} K \arrow[r, hook, "\iota"] \arrow[d, "\sigma"'] & L \arrow[dl, "\tilde{\sigma}"] \\ \Omega & \end{tikzcd}$$

, où $\tilde{\sigma} \circ \iota = \sigma$.

On parle de prolongement de σ à L en $\tilde{\sigma}$ et on dit encore que σ se prolonge à L en $\tilde{\sigma}$. De plus, le nombre de ces prolongements est égal au nombre de racines distincts de P dans son corps de décomposition.

Démonstration. $L = K(x) = K[X]/(P)$ est le corps de rupture de $P(X)$ sur K. Un K-isomorphisme $\tilde{\sigma} : L \to \Omega$, c'est la donnée de $\tilde{\sigma}(x)$ dans Ω. Par ailleurs, il existe une contrainte sur $\tilde{\sigma}(x)$: l'extension se factorise par $K[X]/(P)$: on a donc la condition nécessaire $P(x) =$

$0 \Rightarrow \sigma(P(x)) = 0$, et $\tilde{\sigma}$ étant un K-isomorphisme implique que l'identité se lit

$$0 = \tilde{\sigma}(P(x)) = \sum_{k=0}^{\deg P} \tilde{\sigma}(a_k)\tilde{\sigma}(x)^k = \sum_{k=0}^{\deg P} a_k \tilde{\sigma}(x)^k = P(\tilde{\sigma}(x)),$$

c'est à dire que $\tilde{\sigma}(x)$ est une racine de P dans Ω. Cette condition est clairement suffisante. On a ainsi autant de telles extensions $\tilde{\sigma}$ que de racines de P dans Ω, ou encore dans le sous-corps de Ω engendré par ces racines, qui est un corps de décomposition de P. $\square$

Lemme 12.18. *Soit $K \hookrightarrow L$ une extension de corps et soit Ω une clôture algébrique de K. Alors toute extension $\sigma : K \hookrightarrow \Omega$ se prolonge à L.*

Démonstration. Si $K \hookrightarrow L$ est finie i.e. de type fini, c'est un corollaire de lemme 12.17. On peut raisonner par récurrence sur le nombre de générateurs. Pour $n = 1$, c'est le lemme précédent. On suppose que la conclusion est satisfaite pour $L' = K(x_1, \cdots, x_{k-1})$, où $k \in \mathbb{N} \setminus \{0, 1\}$. On écrit : $L = K(x_1, \cdots, x_k) = K(x_1, \cdots, x_{k-1})(x_k) = L'(x_k)$. Par l'hypothèse de récurrence on obtient

$$\begin{tikzcd}
K \arrow[r, hook, "\sigma"] \arrow[d, hook] & \Omega . \\
L' \arrow[ur, hook, "\tilde{\sigma}"] \arrow[d, hook] & \\
L \arrow[uur, hook, "\tilde{\tilde{\sigma}}"'] &
\end{tikzcd}$$

et $\tilde{\tilde{\sigma}}$ répond à la question.

Pour le cas général, on introduit

$$\mathcal{F} := \big\{(M, \sigma_M),\ K \hookrightarrow M \hookrightarrow L,\ \sigma_M|_K = \sigma\big\},$$

on ordonne $\mathcal{F}$ comme : $(M, \sigma_M) \leq (M', \sigma_{M'})$ s.s.i. $M \subset M'$ et $\sigma_{M'}|_M = \sigma_M$. $\mathcal{E}$ est clairement non vide d'après le cas finie qu'on a vu. Pour tout chaîne $(M_j, \sigma_j)_{j \in \Lambda}$ de $\mathcal{F}$, $M = \bigcup\limits_{j \in \Lambda} M_j$ est un sous-corps de L, et $\tilde{\sigma} : M \to \Omega$ est canoniquement induit par $\tilde{\sigma}|_{M_j} = \sigma_j$, alors $(M, \tilde{\sigma})$ est un majorant de la famille. Donc $\mathcal{F}$ est un ensemble inductif. On applique le théorème de Zorn et on trouve un élément maximal $(M_\infty, \sigma_\infty) \in \mathcal{F}$.

L étant une extension algébrique de K, tout $x \in L$ est algébrique sur K, a fortiori sur M_∞. Par le cas précédant on peut étendre σ_∞ à $M_\infty(x)$ en $\tilde{\sigma_\infty} : M_\infty \to \Omega$. Par maximalité de $(M_\infty, \sigma_\infty)$, on a nécessairement $M_\infty(x) = M_\infty$ et donc $x \in M_\infty$, c'est à dire : $L \subset M_\infty \subset L$, alors $L = M_\infty$. $\square$

Théorème 12.19. *Toute clôture algébrique d'un corps est unique à isomorphisme près.*

Démonstration. Soient Ω et Ω' deux clôtures algébriques de K. On suppose $\sigma : K \hookrightarrow \Omega$ et $\sigma' : K \hookrightarrow \Omega'$ deux extensions de K. Par le lemme 12.18, σ' se prolonge en $\tilde{\sigma'} : \Omega \hookrightarrow \Omega'$. Or Ω est algébriquement clos, donc aussi $\tilde{\sigma'}(\Omega)$ car le morphisme est injectif. On a alors la double extension

$$\Omega \hookrightarrow \tilde{\sigma'}(\Omega) \hookrightarrow \Omega'.$$

Ω' est ainsi une extension algébrique de $\tilde{\sigma'}(\Omega)$ car Ω' est algébrique sur K, où $\tilde{\sigma'}(\Omega)$ est lui-même algébriquement clos. Ceci force Ω' à coïncide avec $\tilde{\sigma'}(\Omega)$: pour tout $x' \in \Omega'$, x' algébrique sur $\tilde{\sigma'}(\Omega)$, alors il existe $Q \in \tilde{\sigma'}(\Omega)[X]$ tel que $Q(x') = 0$, mais $\tilde{\sigma'}(\Omega)$ étant algébriquement clos, les racines de Q, en particulier x', appartiennent à $\tilde{\sigma'}(\Omega)$. On a ainsi établi que pour tout $x' \in \Omega'$, $x' \in \tilde{\sigma'}(\Omega)$, c'est à dire l'inclusion $\Omega' \subset \tilde{\sigma'}(\Omega) \subset \Omega'$.
Le petit argument qui précède établit que toute extension algébriquement d'un corps algébriquement clos est triviale, en particulier l'extension $\tilde{\sigma'}(\Omega) \hookrightarrow \Omega'$ à être triviale et $\tilde{\sigma'}$ à être un K-isomorphisme de Ω et Ω'. $\square$

Il y a deux pathologies possible pour $K \hookrightarrow L$ une extension de corps :
$i)$ Il existe P un polynôme irréductible de $K[X]$ qui admet une racine dans L sans être scindé sur L. C'est à dire que un corps de rupture n'est pas généralement un corps de décomposition.
$ii)$ Il existe P un polynôme irréductible de $K[X]$ qui peut avoir des racines multiples dans son corps de décomposition.
Si $i)$ n'arrive pas, l'extension est dite normale ; si $ii)$ n'arrive pas, l'extension est dite séparable ; si tous les deux n'arrivent pas, l'extension est dite galoisienne.

13 Extension normales

Définition 13.1. Une extension algébrique $K \hookrightarrow L$ est dite **normale** si tout polynôme irréductible de $K[X]$ admettant au moins une racine dans L est scindé sur L.

Proposition 13.2. *Toute extension d'un corps dans une clôture algébrique est normale.*

Démonstration. Toute polynôme de $K[X]$ est scindé dans une clôture algébrique $\overline{K}$ de K. □

Avertisement : tous les résultats de ce chapitre, énoncés ici pour des extensions finies, se généralisent avec les mêmes arguments à des extensions arbitaires.

Théorème 13.3. *Soit $K \hookrightarrow L$ une extension de corps. On a que les affirmations suivantes sont équivalentes :*
$i)$ $K \hookrightarrow L$ est finie et normale ;
$ii)$ L est le corps de décomposition d'un polynôme de $K[X]$.

Démonstration. $i) \Rightarrow ii)$: Soit $(x_1, \cdots, x_n)$ une base de L vu comme K-espace vectoriel et où $n = [L : K]$. On introduit les polynômes $P_i \in K[X]$, $i \in [\![1, n]\!]$ et P_i est le polynôme minimal de x_i. Par hypothèses $K \hookrightarrow L$ étant normale, donc P_i est scindé dans $L[X]$, $P = \prod_{i=1}^{n} P_i$ de même.
Or $L = K[x_1, \cdots, x_n] = K(x_1, \cdots, x_n)$. $K(x_1, \cdots, x_n) \subset K(\{x \in L,\ \exists\ i \in [\![1, n]\!],\ P_i(x) = 0\}) \subset L = K(x_1, \cdots, x_n)$. Alors $L = K(\{x \in L,\ \exists\ i \in [\![1, n]\!], P_i(x) = 0\})$ et L est bien un corps de décomposition de $P \in K[X]$. $ii) \Rightarrow i)$: On suppose que L est un corps de décomposition d'un polynôme $Q \in K[X]$, alors c'est une extension finie de K. Soit $P \in K[X]$ irréductible admettant une raine x dans Let soit M le corps de décomposition de $P \in L[X] \supset K[X]$. Il reste à établi que pour toute racine y de P dans M, alors y appartient

à L.
On introduit les extensions $L(x)$ et $L(y)$. On suppose que $(x_1, \cdots, x_n)$ sont les racines de Q et alors $L = K(x_1, \cdots, x_n)$. Donc $L(x)$ et $L(y)$ sont respectivement le corps de décomposition de Q sur $K(x)$ et $K(y)$. En effet, Q est décomposé sur L, et l'est sur toute extension, en particulier sur $L(x)$ et $L(y)$.
Observons que $K(x)$ et $K(y)$ sont isomorphismes à un corps de rupture de P sur K, donc $L(x) = K(x_1, \cdots, x_n)(x) = K(x)(x_1, \cdots, x_n) \overset{\sigma}{\simeq} K(y)(x_1, \cdots, x_n) = K(x_1, \cdots, x_n)(y) = L(y)$. Considérons alors les deux extensions suivantes de $K(x)$:

$$K(x) \hookrightarrow L(x)$$
$$K(x) \xrightarrow{\sigma} K(y) \hookrightarrow L(y).$$

$L(x)$ et $L(y)$ sont deux corps de décomposition de Q sur $K(x)$. Par isomorphie des corps de décomposition, ces deux extensions sont isomorphes, elles ont en particulier même degré : $[L : K(x)] = [L(x) : K(x)] = [L(y) : K(x)] = [L(y) : L][L : K(x)]$. Donc $[L(y) : L] = 1$ i.e. $L(y) = L$ et $y \in L$. $\square$

Corollaire 13.4. *Soit $K \hookrightarrow M$ une extension finie et normale de corps et soit $K \hookrightarrow L \hookrightarrow M$ une extension intermédière. L'extension $L \hookrightarrow M$ est alors normale.*

Démonstration. D'après le théorème 13.3, on suppose que M est un corps de décomposition de $P \in K[X]$ i.e. $M = K(\{x \in M,\ P(x) = 0\}) \subset L(\{x \in M,\ P(x) = 0\}) \subset M$ alors M est aussi un corps de décomposition de $P \in L[X]$. $\square$

Remarque 13.5.
- En général $K \hookrightarrow L$ n'a pas de raison d'être normale : $X^n - p$ est irréductible sur $\mathbb{Q}$ par la critère d'Eisenstein si $p \in \mathcal{P}$. Si $n \geq 3$, $\mathbb{Q}(\sqrt[n]{p}) \subsetneqq \mathbb{Q}(\sqrt[n]{p}, e^{\frac{2\pi i}{n}})$.
- La composé de deux extensions normales n'est pas normal en général : considérons la composition d'extensions quadratiques $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$. Le polynôme minimal de $\sqrt[4]{2}$ est $X^2 - \sqrt{2}$ sur $\mathbb{Q}(\sqrt{2})$ mais est $X^4 - 2$ qui n'est pas scindé sur $\mathbb{Q}$.

Proposition 13.6. *Soit $K \hookrightarrow L$ une extension finie de corps et soit Ω une clôture algébrique de K. Alors $K \hookrightarrow L$ est normale s.s.i. tous les K-isomorphismes de L dans Ω ont même image.*

Démonstration. $\Rightarrow$: $K \subset L$ une extension normale de corps implique que L est le corps de décomposition d'un polynôme $Q \in K[X]$ d'après le théorème 13.3. Posons $E = \{x \in \Omega,\ Q(x) = 0\}$, alors $K(E)$ est aussi un corps de décomposition de Q sur K et on obtient que

$L \simeq K(E)$.
Pour tout K-isomorphisme $\sigma : L \hookrightarrow \Omega$, en effet, $Q(X) = \prod_{x\in E}(X-x)^{r_x} \in \Omega[X]$. σ induit $\Sigma : L[X] \to \Omega[X]$ et on prend l'image par Σ,

$$\prod_{x\in E}(X-x)^{r_x} = Q(X) = \Sigma(Q)(X) = \prod_{x\in E}(X-\sigma(x))^{r_x} = \prod_{x\in\sigma(E)}(X-x)^{r_{\sigma^{-1}(x)}}.$$

$\Omega[X]$ est factoriel, alors on obtient l'unicité de la décomposition en irréductible, en particulier $\sigma(E) = E$. Pour toute racine t de Q dans L, $Q(\sigma(t)) = \sigma(Q(t)) = \sigma(0) = 0$, ainsi $\sigma(t) \in E$ et alors $\operatorname{Im}\sigma = \sigma(L) \subset K(E)$. Or $\sigma(L) \simeq L \simeq K(E)$, donc $\sigma(L) = K(E)$. En particulier $\operatorname{Im}\sigma$ ne dépend pas de σ.
$\Leftarrow$: On suppose que tous les K-isomorphismes de L dans Ω ont même image $M \subset \Omega$. Soit $P \in K[X]$ irréductible admettant une racine $x \in L$ et une racine $y \in \Omega$. On introduit les corps de rupture de P $K(x) \subset L$ et $K(y) \subset \Omega$ qui sont isomorphes par σ. Par le lemme 12.18, σ s'étend en un K-isomorphsime $\tilde\sigma : L \to \Omega$, par hypothèse d'image $\operatorname{Im}\tilde\sigma = M$:

$$\begin{tikzcd} K(x) \arrow[r, "\sigma"] \arrow[d, phantom, "\cap"] & K(y) \arrow[r, phantom, "\subset"] & \Omega . \\ L \arrow[urr, "\tilde\sigma"'] & & \end{tikzcd}$$

Alors $K(y) = \operatorname{Im}\sigma \subset \operatorname{Im}\tilde\sigma = M$. En particulier $y \in \operatorname{Im}\tilde\sigma = M$ et P est alors scindé sur M. Or M et L sont K-isomorphe. Donc P est aussi scindé sur L. □

Corollaire 13.7. *Soit $K \subset L$ une extension finie de corps et soit Ω une clôture algébrique de L. Alors $K \hookrightarrow L$ est normale s.s.i. tous les K-isomorphismes de L dans Ω induisent naturellement des K-automorphismes de L.*

Proposition 13.8. *Soit $K \hookrightarrow M$ une extension finie et normale de corps et soit $K \hookrightarrow L \hookrightarrow M$ une extension intermédière. Alors l'extension $K \hookrightarrow L$ est normale s.s.i. pour tout K-isomorphisme f de M, $f(L) = L$.*

Démonstration. Soit Ω un corps algébriquement clos contenant M.
$\Leftarrow$: Par le lemme 12.18, tout K-isomorphisme $\sigma : L \to \Omega$ se prolonge à M en $\tilde\sigma$. Puisque l'extension $K \hookrightarrow M$ est normale, l'image de ce prolongement est M. Il induit aussi un K-automorphisme de M et par l'hypothèsee $\tilde\sigma(L) = L$. Puisque $\tilde\sigma|_L = \sigma$, on en déduit $\sigma(L) = L$ et grâce à la proposition 13.6, on conclut enfin que l'extension $K \hookrightarrow L$ est normale.
$\Rightarrow$: Tout K-automorphisme f de M induit par restriction un K-morphisme de $L \subset M$ dans $M \subset \Omega$. Par la proposition 13.6, l'extension $K \subset L$ étant normale et $f(L) = L$. □

Proposition 13.9. *Soit $K \hookrightarrow L$ une extension finie et normale de corps. Tout automorphisme de K se prolonge en un automorphisme du corps L.*

Démonstration. Soit $\sigma : K \xrightarrow{\sim} K$ un automorphisme de K. Par le théorème de Steinitz, il existe un corps algébriquement clos Ω contenant L. Par le lemme 12.18, la tour d'extensions

$$\begin{tikzcd} K \arrow[r, "\sigma"] \arrow[d, hook] & K \arrow[r, hook] & L \arrow[r, phantom, "\subset"] & \Omega . \\ L \arrow[urrr, "\tilde{\sigma}"'] & & & \end{tikzcd}$$

De plus, par la proposition 13.6, $\operatorname{Im} \tilde{\sigma} = L$ et donc $\tilde{\sigma} \in Aut(L)$. □

Théorème 13.10. *Soit $K \hookrightarrow L$ une finie extension de corps et soit Ω une clôture algébrique de L. Il existe une plus petite extension M de L dans Ω telle que l'extension $K \hookrightarrow M$ soit normale. Cette extension $K \hookrightarrow M$ est elle-même une extension finie de K.*

Démonstration. Soit $(x_1, \cdots, x_n)$ une base de L considéré comme K-espace vectoriel. Soit P_i le polynôme minimal de x_i pour tout $i \in [\![1, n]\!]$. Soit $M \subset \Omega$ le sous-corps de Ω engendré par les racines de $P = \prod_{i=1}^{n} P_i(X)$ sur lequel donc P se décompose, et qui, s'écrivant $K(\{x \in \Omega,\ \exists\ i \in [\![1, n]\!],\ P_i(x) = 0\})$, est même un corps de décomposition de $P \in K[X]$. Par le théorème 13.3, l'extension $K \hookrightarrow M$ est finie et normale. Pour conclure, il faut vérifier que cette extension est minimale parmi les extensions normales de K.

Pour toute extension N, $L \subset N \subset \Omega$ telle que $K \hookrightarrow N$ est normale, les polynômes $(P_i)_{i \in [\![1,n]\!]}$ ont chacun au moins une racine dans N car $x_i \in L \subset N$ est une racine de P_i. $K \hookrightarrow N$ étant normale, P_i est alors scindé dans N car P_i est irréductible. Il en va de même du produit $P = \prod_{i=1}^{n} P_i$ et les racines de P sont alors dans N. Or M est, par construction, engendré par les racines de P, et donc contenu dans N qui contient toutes ces racines. La minimalité de M est établie. □

Définition 13.11. Cette extension est appelée **clôture normale de L dans Ω**. On la note $\overline{L}^{\Omega}$.

14 Extension séparable

14.1 Polynôme séparable

Soit $K \hookrightarrow L$ une extension de corps.

Définition 14.1. $P \in K[X]$ est dit **séparable** s'il n'a pas de racines multiples dans son corps de décomposition ; P est dit **inséparable** s'il n'est pas séparable.

Lemme 14.2. *P est séparable s.s.i. $P \wedge P' = 1$.*

Démonstration. i) pgcd(P, Q) est indépendent de l'extension d'anneaux, où P, $Q \in K[X] \subset L[X]$. En effet le pgcd peut se calculer par l'algorithme d'Euclide dans $K[X]$, indépendemment de l'extension $K \hookrightarrow L$ considérée.
ii) Si M un corps de décomposition de P, si

$$P(X) = \prod_{i=1}^{k}(X - x_i)^{v_i},$$

où $v_i \in \mathbb{N}^*$ et $x_i \in M$. Alors

$$P' = \sum_{i=1}^{k}(X - x_i)^{v_i - 1}\prod_{j \neq i}(X - x_j)^{v_j}.$$

Alors $(X - x_i)|P \wedge P'$ s.s.i. $(X - x_i)|P'$ s.s.i. $v_i \geq 2$. Donc pgcd$(P, P') = 1$ s.s.i. les racines de P dans L sont simples. □

Lemme 14.3. *Soit $P \in K[X]$ un polynôme irréductible.*
i) P est séparable s.s.i. $P' \neq 0$.
ii) P est inséparable s.s.i. $car(K) = p > 0$ et $P \in K[X^p]$.

Démonstration. i) Par le lemme 14.2 P est inséparable s.s.i. $P \wedge P'$ n'est pas une unité s.s.i. $\deg(P \wedge P') \geq 1$. Si $\deg P \geq 1$ et $P' = 0$, $\deg(P \wedge P') = \deg P \geq 1$, alors P est inséparable ; réciproquement si P est inséparable, $P \wedge P' = \text{pgcd}(P, P')|P$, or P irréductible implique que $P \wedge P' = P$. Mais aussi $P \wedge P'|P' \Rightarrow P|P' \Rightarrow P' = 0$ (sinon on aurait $\deg P' \geq \deg P$, contradiction !).
C'est à dire que P est séparable s.s.i. $P' \neq 0$.
ii) On suppose que $P(X) = \sum\limits_{k=0}^{n} a_k X^k$, avec $n \geq 1$ et $a_n \neq 0$. Alors $P'(X) = \sum\limits_{k=1}^{n} k a_k X^{k-1}$.
Alors P est inséparable s.s.i. $P' = 0$ s.s.i. $k a_k = 0$ pour tout $k \in [\![1, n]\!]$.
En caractéristique 0, $k \neq 0$, alors $a_k = 0$ pour tout $k \in [\![1, n]\!]$, ce qui contredit l'hypothèse $\deg P \geq 1$ i.e. en caractéristique 0, tout polynôme irréductible est donc séparable.
En caractéristique positive, $p > 0$, on obtient que le système est équivalent aux $a_k = 0$ pour tout $k \notin p\mathbb{N}$. Donc si $car(K) = p > 0$, P est inséparable s.s.i. $P \in K[X^p]$. □

14.2 Extensions séparables

Définition 14.4. Soit $K \hookrightarrow L$ une extension de corps. Un élément l de L est **séparable sur** K s'il est algébrique sur K et si son polynôme minimal $P_{l,K}$ est séparable.
L'extension $K \hookrightarrow L$ est **séparable** si tout élément de L est séparable sur K.

Proposition 14.5. *Soit $K \hookrightarrow L$ une extension algébrique de corps. Pour tout morphisme de corps σ de K dans un corps algébriquement clos, le cardinal de l'ensemble*

$$P_\sigma := \{\tilde{\sigma} : L \to \Omega,\ \tilde{\sigma}|_K = \sigma\}$$

est indépendant du corps algébriquement clos Ω et de l'extension $\sigma : K \hookrightarrow \Omega$.

Démonstration. Le lemme 12.18 établit l'existence d'un prolongement $\tilde{\sigma} : L \hookrightarrow \Omega$ au morphisme $\sigma : K \hookrightarrow \Omega$ dès que Ω est algébriquement clos. L'extension $\iota : K \hookrightarrow L$ étant algébrique, il en va de même de l'extension isomorphe $\tilde{\sigma} \circ \iota : K \hookrightarrow \sigma(L)$.
$\tilde{\sigma}$ étant un K-isomorphisme et une extension de $\sigma : K \hookrightarrow \Omega$, $l \in L$ est une racine de $Q(X) = \sum_k a_k X^k \in K[X]$ s.s.i. $\tilde{\sigma}(l)$ est une racine de $\sum_k \sigma(a_k) X^k \in \sigma(K)[X] \subset \Omega[X]$ l'image de Q.
$\sigma(L)$ est donc incluse dans $\overline{K}^{\Omega}$, la clôture algébrique de K dans Ω, qui constitue une clôture algébrique $\overline{K}$ de K puisque Ω est algébriquement clos d'après la proposition 12.15.
Soient $\iota_1 : K \to \Omega_1$ et $\iota_2 : K \to \Omega_2$ deux extensions de corps, où Ω_1 et Ω_2 sont algébriquement clos. On note $K_1 = \overline{K}^{\Omega_1}$ et $K_2 = \overline{K}^{\Omega_2}$. Deux clôture algébrique d'un corps K étant K-isomorphes, il existe un K-isomorphisme χ faisant commuter le diagramme suivant pour toute extension $(\sigma_1 : K \to \Omega_1) \in P_{\iota_1}$:

$$\begin{tikzcd}
 & \tilde{\sigma_1}(L) & \subset & K_1 \arrow[dd, "\simeq"', "\chi"] & \subset & \Omega_1 , \\
L \arrow[ur, "\tilde{\sigma_1}"] & K \arrow[l, hook', "\iota"'] \arrow[u, hook, "\sigma_1"'] \arrow[drr, hook, "\sigma_2"'] & \circlearrowleft & & & \\
 & & & K_2 & \subset & \Omega_2
\end{tikzcd}$$

où $\sigma_2 = \chi \circ \sigma_1 = \chi \circ \tilde{\sigma}_1 \circ \iota$, donc $\chi \circ \tilde{\sigma}_1$ est bien un prolongement de σ_2 à L. La composition par χ établit ainsi une correspondance bijective entre P_{σ_1} et P_{σ_2}, d'inverse donné par la composition par χ^{-1}. Donc $|P_{\iota_1}| = |P_{\iota_2}|$. □

Définition 14.6. Le cardinal de cet ensemble P_σ est appelé **degré séparable** de l'extension $K \hookrightarrow L$ et on le note $[L : K]_s$.

Lemme 14.7. *Pour toute tour d'extensions algébriques $K \hookrightarrow L \hookrightarrow M$, on a alors $[M : K]_s = [M : L]_s[L : K]_s$*

Démonstration. Soit Ω une extension algébriquement close de M et $\mathcal{E}$ l'ensemble des K-isomorphismes de L dans Ω, alors $|\mathcal{E}| = [L : K]_s$. Pour tout $\sigma \in \mathcal{E}$, on note $\mathcal{E}_\sigma$ l'ensemble des K-isomorphismes de M dans Ω dont la restriction sur L est σ, alors la proposition 14.5 établit que le cardinal de $\mathcal{E}_\sigma$ est indépendent de $\sigma \in \mathcal{E}$ et $|\mathcal{E}_\sigma| = [M : L]_s$. On a donc $[M : L]_s[L : K]_s$ K-isomorphismes distincts de M dans Ω.
Inversement, tout K-isomorphisme $M \hookrightarrow \Omega$ se restreint à L en l'un des $\sigma \in \mathcal{E}$ et correspond donc à l'un des $\tau \in \mathcal{E}_\sigma$. En particulier, on obtient $[M : K]_s = [M : L]_s[L : K]_s$. □

Théorème 14.8. *Pour toute extension finie de corps $K \hookrightarrow L$*

$$1 \leq [L : K]_s \leq [L : K],$$

et on prend l'égalité s.s.i. $K \hookrightarrow L$ est finie et séparable s.s.i. $K \hookrightarrow L$ est engendré par un nombre fini d'éléments séparables de L.

Démonstration. La démonstration utilise la multiplicativité des degrés séparables, à l' de la multiplicativité des dgrés d'extensions établie précédemment.

— Le cas monogène : si $L = K(x)$, où $x \in L$, alors l'extension est algébrique puisque finie par l'hypothèse. Le lemme 12.17 établit que $[L : K]_s$ coïncide avec le nombre de racines distinctes du $P_{x,K}$ polynôme minimal de x dans un corps de décomposition. Le nombre de racines deux à deux distincts d'un polynôme étant majoré par le degré, on conclut $1 \leq [L : K]_s \leq [L : K]$ avec l'égalité s.s.i. x est séparable.
— Le cas général : si $L = K(x_1, \cdots, x_n)$, $n \in \mathbb{N}^*$, on introduit la tour d'extensions monogènes (on dit encore simples)

$$K \hookrightarrow K(x_1) \hookrightarrow \cdots \hookrightarrow K(x_1, \cdots, x_n).$$

Posons $x_0 = 1$ et le lemme 14.7 entraîne par une récurrence finie et banale

$$[K(x_0, \cdots, x_n) : K]_s = \prod_{k=1}^{n} [K(x_0, \cdots, x_k) : K(x_0, \cdots, x_{k-1})]_s.$$

La même récurrence entraînant pour les degrés d'extensions l'identité

$$[K(x_0,\cdots,x_n):K]=\prod_{k=1}^{n}[K(x_0,\cdots,x_k):K(x_0,\cdots,x_{k-1})]$$

à partir de la multiplicativité des degrés d'extensions. Degré et degré séparable étant des cardinaux, les inégalités

$$[K(x_0,\cdots,x_k):K(x_0,\cdots,x_{k-1})]_s\leq[K(x_0,\cdots,x_k):K(x_0,\cdots,x_{k-1})]$$

déduite du cas monogène entraîne la majoration annoncée du degré séparable par le degré ordinaire :

$$\begin{aligned}1\leq[L:K]_s&=\prod_{k=1}^{n}[K(x_0,\cdots,x_k):K(x_0,\cdots,x_{k-1})]_s\\&\leq\prod_{k=1}^{n}[K(x_0,\cdots,x_k):K(x_0,\cdots,x_{k-1})]\\&=[L:K].\end{aligned}$$

Si $(x_i)_{i\in[\![1,n]\!]}$ sont a fortiori séparables sur toute extension de K et particulier sur $K(x_1,\cdots,x_n)$ car le polynôme minimal d'un élément d'une extnsion L sur une extension intermédiaire M divise le polynôme minimal de x sur K i.e. $P_{x,M}|P_{x,K}$ pour $K\hookrightarrow M\hookrightarrow L\ni x$. Le cas d'égalité pour une extension monogène entraîne alors les identités

$$[K(x_0,\cdots,x_k):K(x_0,\cdots,x_{k-1})]_s=[K(x_0,\cdots,x_k):K(x_0,\cdots,x_{k-1})]$$

pour tout $i\in[\![1,n]\!]$ et donc en utilisant la multiplicativité des degrés et degrés séparables d'extensions l'identité annoncée

$$\begin{aligned}[L:K]_s&=\prod_{k=1}^{n}[K(x_0,\cdots,x_k):K(x_0,\cdots,x_{k-1})]_s\\&=\prod_{k=1}^{n}[K(x_0,\cdots,x_k):K(x_0,\cdots,x_{k-1})]\\&=[L:K].\end{aligned}$$

Réciproquement, si $[L:K]_s=[L:K]$, la première partie appliquée à la double extension $K \hookrightarrow K(x) \hookrightarrow L$, où x est un élément arbitaire de L, entraîne les majorations $[L : K(x)]_s \leq [L : K(x)]$ et $[K(x) : K]_s \leq [K(x) : K]$, et donc $[L : K]_s = [L : K(x)]_s[K(x) : K]_s \leq [L : K(x)][K(x) : K] = [L : K] = [L : K]_s$. On obtient que les inégalités ci-dessus sont des égalités, en particulier $[K(x) : K]_s = [K(x) : K]$ puisque $[L : K(x)]$ le degré d'une extension de corps est strictement positif. Le cas d'égalité pour une extension monogène établit alors que x est séparable sur K. Puisque x est un élément arbitaire de L, on a établi que sous l'hypothèse $[L : K]_s = [L : K]$.

En résumé, on vient de démontrer les implications $L = K(x_1, \cdots, x_n)$ et $(x_i)_{i\in[\![1,n]\!]}$ sont séparables $\Rightarrow [L : K]_s = [L : K] \Rightarrow K \hookrightarrow L$ est séparable et finie. Puisque l'implication $K \hookrightarrow L$ est séparable et finie $\Rightarrow L = K(x_1, \cdots, x_n)$, où $(x_i)_{i\in[\![1,n]\!]}$ sont séparables sur K est vraie, on en déduit les équivalances annoncés : $[L : K]_s = [L : K]$ s.s.i. $K \hookrightarrow L$ est finie et séparable s.s.i. $K \hookrightarrow L$ est engendré par un nombre fini d'éléments séparables de L.

□

On aura encore besoin d'un autre outil. Il existe des extensions finies qui ne sont pas simples i.e. monogènes, par exemple : $\mathbb{F}_p(X^p, Y^p) = (\mathbb{F}_p(X, Y))^p \to \mathbb{F}_p(X, Y)$, *de degré* p^2, *tandis que pour tout* $z \in \mathbb{F}_p(X, Y)$, $z^p \in \mathbb{F}_p(X^p, Y^p)$ *et donc* $[\mathbb{F}_p(X^p, Y^p)(z) : \mathbb{F}_p(X^p, Y^p)] \in \{1, p\}$. *Alors* $\mathbb{F}_p(X^p, Y^p)(z) \subsetneqq \mathbb{F}_p(X, Y)$ *pour tout* $z \in \mathbb{F}_p(X, Y)$. *Mais toute extension séparable de type fini est monogène.*

Théorème 14.9 (de l'élément primitif)**.** *Soit* $K \hookrightarrow L$ *une extension finie de corps telle que* $L = K(x, y_1, \cdots, y_n)$, *où* x *et* $(y_i)_{i\in[\![1,n]\!]}$ *sont dans* L. *On suppose que les* $(y_i)_{i\in[\![1,n]\!]}$ *sont séparables sur* K, *alors il existe un élément* z *de* L *tel que* $L = K(z)$.

Démonstration. — Si K est fini, l'extension est encore un corps fini, et isomorphe à $K^{[L:K]}$ comme K-espace vectoriel. Le théorème 7.21 entraîne donc qu'il existe un élément z de L^* tel que $(L^*, \cdot) = \langle z \rangle$. Et donc a fortiori $K(z)$ le sous-corps de L engendré sur K par z coïncide avec L i.e. $K[z] = K(z) = L$.

— Si K est infini, on suppose au début que $L = K(x, y)$ où $y = y_0$ est séparable sur K. On note $P = P_{x,K}$ et $Q = P_{y,K}$ qui se scindent alors sur ses corps de décomposition respectifs :

$$P(X) = (X - x) \prod_{i=1}^{r} (X - x_i)$$

$$P(X) = (X - y) \prod_{i=1}^{s} (X - y_i)$$

où $(y_i)_{i\in[\![0,s]\!]}$ sont deux à deux distincts puisque y et donc son polynôme minimal Q sont séparables par hypothèse. Introduisons $z = x + ty \in L = K(x, y)$ pour tout $t \in K$ de telle sorte que $P(z - ty) = P(x) = 0$ et $P(z - ty_i) = P(x - t(y_i - y)) \neq 0$ pour tout $i \in [\![1, s]\!]$. C'est à dire que $x - t(y_i - y) \notin \{x_i,\ i \in [\![1, r]\!]\} \cup \{x\}$ i.e. $t \notin \{-\frac{x-x_i}{y-y_j},\ i \in [\![1, r]\!],\ j \in [\![1, s]\!]\} \cup \{0\}$. Un tel t existe toujours dans K si $|K| = +\infty$. Sous cette condition $Q \in K[X]$ et $R_t(X) = P(z - tX)$ ont exactement une racine commune y dans l'extension $K(x, y, x_1, \cdots, x_r, y_1, \cdots, y_s)$. Leur pgcd, qui appartient à $K(z)[X]$ puisque Q et $R \in K(z)[X]$ et que le pgcd se calcule dans cet anneau par l'algorithme d'Euclide, est donc égal à $(X - y)$. En particulier, $y \in K(z)$, et donc $x = z - ty \in K(z)$, ce qui implique $L = K(x, y) = K(z)$.
Pour conclure avec le cas général où $L = K(x, y_1, \cdots, y_n)$, on procède par récurrence sur l'entière n. En écrivant $K(x, y_1, \cdots, y_n) = K(x, y_1, \cdots, y_{n-1})(y_n)$, par hypothèse de récurrence à l'ordre $n-1$, il existe $w \in K(x, y_1, \cdots, y_{n-1})$ tel que $K(x, y_1, \cdots, y_{n-1}) = K(w)$ et le cas $n = 1$ établi ci-dessus entraîne alors l'existence d'un élément z de $K(x, y_1, \cdots, y_n)$ tel que $K(x, y_1, \cdots, y_n) = K(x, y_1, \cdots, y_{n-1})(y_n) = K(w)(y_n) = K(w, y_n) = K(z)$ dès que y_n est séparable sur K, ce qui clôt la démonstration du théorème de l'élément primitif.

□

15 Théorie de Galois

15.1 Groupe de Galois d'une Extension

Définition 15.1. Le groupe de Galois d'un extension de corps $K \hookrightarrow L$ est le groupe des K-automorphismes de L. On rappelle qu'un K-morphisme de L est un morphisme de corps défini sur L et donc la restriction à K est l'identité. On note $Gal(L/K)$ ce groupe.

On a alors le critère suivant.

Théorème 15.2. *Soit $K \hookrightarrow L$ une extension finie de corps. Alors $|Gal(L/K)| \leq [L : K]_s \leq [L : K]$.*

Démonstration. Soit Ω une extension algébriquement close de K dont l'existence est annoncée par le théorème de Steinitz. On introduit l'espace

$$\mathcal{M} = M_{K,L,\Omega} := \{\sigma : L \hookrightarrow \Omega,\ \sigma|_K = \iota : K \hookrightarrow \Omega\}$$

sur lequel $G := Gal(L/K)$ agit à droite par composition à la source, i.e. $\sigma \cdot g := \sigma \circ g$ pour tout $g \in G$ et tout $\sigma \in \mathcal{M}$.
Pour tout $\sigma \in \mathcal{M}$, $\sigma \circ g = \sigma$ s.s.i. $g = Id_L$ car σ est injectif comme morphisme de corps. Alors cette action était libre. On a pour tout $\sigma \in \mathcal{M}$,

$$|Gal(L/K)| = |G| = |\sigma \cdot G| \leq |\mathcal{M}| \leq [L : K]_s.$$

□

Lemme 15.3. *L'action de $G = Gal(L/K)$ sur $\mathcal{M}$ introduite ci-dessus est transitive s.s.i. tous les morphisme de $\mathcal{M}$ ont même image.*

Démonstration. Pour ce faire on démontre que deux K-isomorphsime σ_1 et $\sigma_2 \in \mathcal{M}$ appartiennent à la même orbite sous G s.s.i. ils ont même image dans Ω i.e. $\operatorname{Im}\sigma_1 = \sigma(L_1) = \sigma(L_2) = \operatorname{Im}\sigma_2$.
$\Leftarrow$: S'il existe $g \in G$ tel que $\sigma_2 = \sigma_1 \circ g$, g étant surjectif puisque un automorphisme de L. Alors on a nécessairement $\operatorname{Im}\sigma_2 = \operatorname{Im}(\sigma_1 \circ g) = \operatorname{Im}\sigma_1$.
$\Rightarrow$: Réciproquement, si $\sigma_1(L) = \sigma_2(L)$, σ_1 étant de plus injectif comme morphisme de corps, c'est un isomorphisme sur son image $\operatorname{Im}\sigma_1 = \operatorname{Im}\sigma_2$ et la décomposition $\sigma_1^{-1} \circ \sigma_2$ définit alors un K-automorphisme de L car σ_1 et σ_2 fixent K en tant que K-morphsime. C'est à dire un élément $g = \sigma_1^{-1} \circ \sigma_2$ de $Gal(L/K)$ tel que $\sigma_1 \cdot g = \sigma \circ g = \sigma \circ (\sigma_1^{-1} \circ \sigma_2) = \sigma_2$. σ_1 et σ_2 appartiennent donc à la même $G = Gal(L/K)$ orbite dès que leurs image donc Ω coïncident. □

Théorème 15.4. *Soit $K \hookrightarrow L$ une extension finie de corps. Alors $|Gal(L/K)| = [L : K]_s$ s.s.i. $K \hookrightarrow L$ est normale.*

Démonstration. L'égalité l'orbite de σ $\sigma \cdot G = \mathcal{M}$ s.s.i. l'action de G sur $\mathcal{M}$ est transitive. Pour relier la normalité de l'extension $K \hookrightarrow L$ à la transitivité de l'action du groupe de Galois sur $\mathcal{M}$ on a l'énoncé précédent.
Par le corollaire 13.7 une extension de corps $K \hookrightarrow L$ est normale s.s.i. tous les K-morphsimes de L dans Ω ont même image. On peut donc conclure que $|Gal(L/K)| = [L : K]_s$ s.s.i. G agit transitivement sur $\mathcal{M}$ s.s.i. $\operatorname{Im}\sigma_1 = \operatorname{Im}\sigma_2$ pour tout σ_1, $\sigma_2 \in \mathcal{M}$ s.s.i. $K \hookrightarrow L$ est normale. □

15.2 Extensions galoisiennes

Définition 15.5. L'extension $K \hookrightarrow L$ est dite **galoisienne** si elle est séparable et normale.

Proposition 15.6. *Pour une extension finie de corps on a l'équivalence : $K \hookrightarrow L$ est galoisienne s.s.i. $|Gal(L/K)| = [L : K]$.*

Démonstration. C'est un corollaire banal du théorème 15.3 et 15.4. □

L'énoncé suivant nous sera utile.

Proposition 15.7. *Pour toute extension finie et normale $K \hookrightarrow L$, et pour tout polynôme P de $K[X]$ séparable et scindé sur L, le groupe de Galois $Gal(L/K)$ agit par permutation sur les racines de P. Cette action est transitive s.s.i. P est irréductible dans $K[X]$.*

Démonstration. Tout $\sigma \in Gal(L/K) = G$ étant un automorphisme de L fixant K point par point, l'extension Σ de σ à $L[X]$ fixe $P \in K[X]$, et pour tout racine x_i de P,

$$0 = \sigma(0) = \sigma(P(x_i)) = \Sigma(P)(\sigma(x_i)) = P(\sigma(x_i)).$$

Alors σ envoie donc les racines de P sur des racines de P et étant injectif. Il induit donc une permutation de celle-lui.

$\Rightarrow$: On établit la contraposée, si $P = QR$, avec $Q,\ R \in K[X]$ et $\deg Q,\ \deg R \geq 1$, Q et R n'ont aucune racine commune puisque P est séparable par hypothèse. Le petit argument ci-dessus établissant que tout élément de G envoie les racines de Q sur des racines de Q et celles de R sur des racines de R. L'action de G n'est pas transitive.

$\Leftarrow$: L'extension $K \hookrightarrow L$ étant normale par hypothèse . Par le théorème 13.3, il existe un polynôme $Q \in K[X]$ dont L est un corps de décomposition. Soient x et y deux racines de P, où $P \in K[X]$ irréductible sur K et scindé sur L. Les extensions monogènes $K(x)$ et $K(y)$ sont alors K-isomorphes, puisque K-isomorphes au corps de rupture du polynôme irréductible P de $K[X]$. Plus précisément, il existe un K-isomorphe $\sigma : K(x) \to K(y)$ envoyant x sur y. Les extensions $\iota_x : K(x) \hookrightarrow L$ et $\iota = \iota_y \circ \sigma$ sont deux extensions de décomposition de Q, $Q \in K(x)[X]$. D'après l'unicité du corps de décomposition établie par le théorème 12.9, les extensions ι_x et ι sont K-isomorphes i.e. il existe $g \in Aut_K(L) = Gal(L/K)$ tel que $g \circ \iota_x = \iota$. Puisque ι_x, ι_y et σ sont des K-isomorphismes, il en va de même de $\iota = \iota_x \circ \sigma$ et de g à cause de $g \circ \iota_x = \iota$. Alors on obtient

$$g(x) = g \circ \iota_x(x) = \iota(x) = \iota_y \circ \sigma(x) = \sigma(x) = y.$$

Étant données deux racines quelconques x et y de $P \in K[X]$ qui est irréductible sur K et scindé sur L, il existe aussi un élément g du groupe de Galois de l'extension $K \hookrightarrow L$ tel que $g(x) = y$. Donc $Gal(L/K)$ agit donc transitivement sur l'enseble des racines de P. □

15.3 Correspondance de Galois

Slogan : Les extensions intermédiaires d'une extension finie galoisienne correspondent bijectivement aux sous-groupes du groupe de Galois. Plus précisément, introduisons les ensembles $\mathcal{G} := \{H,\ H < Gal(L/K) = G\}$ *et* $\mathcal{E} := \{M,\ K \hookrightarrow M \hookrightarrow L\}$ *et les applications* $\Phi : \begin{array}{ccc} \mathcal{G} & \longrightarrow & \mathcal{E} \\ H & \longmapsto & L^H \end{array}$ *et* $\Psi : \begin{array}{ccc} \mathcal{E} & \longrightarrow & \mathcal{G} \\ M & \longmapsto & Gal(L/M) \end{array}$ *, où* $L^H := \{l \in L,\ h(l) = l, \forall\, h \in H\}$.
On a alors

Lemme 15.8. *Pour toute extension de corps galoisienne et finie* $K \hookrightarrow L$*,* $K = L^{Gal(L/K)}$.

Démonstration. On peut observer l'inclusion banale $K \subset L^{Gal(L/K)}$. Tout élément de $(Gal(L/K))$ fixant K point par point comme K-automorphisme.
Pour l'inclusion réciproque, remarquons que pour tout élément x de $L^{Gal(L/K)}$, son polynôme minimal $P := P_{x,K}$ est scindé sur L puisque $K \hookrightarrow L$ est galoisienne. Soit y une racine arbitaire de P dans L. L'extension $K \hookrightarrow L$ étant normale puisque galoisienne, alors P est séparable et scindé sur L et irréductible sur K. Donc le groupe $Gal(L/K)$ agit transitivement sur les racines de P et il existe donc un élément $g \in Gal(L/K)$ tel que $y = g(x)$. Mais x appartient à L et fixé par g et on peut alors conclure $y = g(x) = x$. Le polynôme P n'a qu'une racine x et étant séparable, son degré est alors 1. On a ainsi $P(X) = X - x$, et puisque $P \in K[X]$, son coefficient constant x appartient alors à K, ce qui établit l'inclusion recherchée : $L^{Gal(L/K)} \subset K$. □

Théorème 15.9 (Lemme d'Artin)**.** *Pour tout corps* L *et tout sous-groupe fini de son groupe d'automorphismes* $H \in Aut(L)$*,* L^H *est une extension de corps galoisienne finie de groupe de Galois* H*.*

Démonstration. Pour tout élément x de L, on introduit le polynôme de $L[X]$, $P(X) := \prod_{y \in Hx}(X - y)$, où Hx est l'orbite de x sous l'action de H. Par sa définition même Pest fixé par H :

$$(h \cdot P)(X) = \prod_{y \in Hx}(X - hy) = \prod_{y \in Hx}(X - y) = P(X).$$

puisque toute orbite d'un groupe est globalement stable sous l'action de ce groupe par définition même de ce qu'est une orbite.
Les coefficients de $P \in L[X]$ sont donc en fait dans L^H et $P \in L^H[X]$. P étant par ailleurs séparable par définition. Considérons le polynôme minimal de x, P_{x,L^H}, le divisant P_{x,L^H} est lui-même séparable, tout comme x. De plus le degré de x, c'est à dire de P_{x,L^H}, est majoré

par le degré de P, lui-même majoré par le cardinal de H, par définition de P.
L'étape suivante consiste à établir que tout élément x de L de degré maximal engendre L i.e. pour tout $x \in L$, $deg(P_{x,L^H}) = \max \deg(P_{l,L^H})$ implique que $L = L^H(x)$.
x étant séparable le théorème de l'élément primitif établit que pour tout $y \in L$, l'extension $L^H(x,y)$ est simple. C'est à dire qu'il existe $z \in L^H \subset L$ tel que $L^H(x,y) = L^H(z)$. On a alors

$$L^H \hookrightarrow L^H(x) \hookrightarrow L^H(z) = L^H(x,y),$$

et considérons l'identité

$$[L^H(z) : L^H] = [L^H(z) : L^H(x)][L^H(x) : L^H].$$

La maximalité du degré de x par hypothèse entraîne alors $[L^H(z) : L^H(x)] = 1$, c'est à dire $L^H(x) = L^H(z) = L^H(x,y)$. En par ticulier $y \in L^H(x)$ et comme y est un élément arbitaire de L, on a établi l'identité annoncé : $L = L^H(x)$.
Un premier corollaire de ce résultat est que $L = L^H(x)$ est une extension finie de degré majoré par le cardinal de H, comme établi ci-dessus, et on a

$$|H| \leq |Gal(L/L^H)| \leq [L : L^H] = [L^H(x) : L^H] \leq |H|.$$

On a donc égalité partout dans la ligne ci-dessus. Mais le cas d'égalité de la proposition 15.6 entraîne alors que l'extension $L^H \hookrightarrow L$ est normale et séparable puisque $|Gal(L/L^H)| = [L : L^H]$, c'est à dire qu'elle est galoisienne.
Pour conclure, H étant par l'inclusion banale un sous-goupe de $Gal(L/L^H)$, et l'identité $|H| = |Gal(L/L^H)|$ entraîne l'égalité $H = Gal(L/L^H)$, ce qui achève la démonstration du lemme d'Artin. □

Théorème 15.10 (Correspondance de Galois)**.** *Pour toute extension de corps galoisienne finie $K \hookrightarrow L$,*
i) les applications Φ et Ψ introduites ci-dessus sont des bijections inverses l'une de l'autre, i.e. $\Phi \circ \Psi = Id_{\mathcal{E}}$ et $\Psi \circ \Phi = Id_{\mathcal{G}}$;
ii) pour tout $H \in \mathcal{G}$, l'extension $K \hookrightarrow L^H$ est galoisienne s.s.i. le sous-groupe H est distingué dans $Gal(L/K)$. Dans ce cas le groupe de Galois de l'extension $K \hookrightarrow L^H$ est isomorphe au quotient G/H.

Démonstration. Observons que les indusions $M \subset \Phi \circ \Psi(M)$ et $H \subset \Psi \circ \Phi(H)$ découlent des définitions de Φ et Ψ d'après lesquelles $\Phi \circ \Psi(M) = L^{Gal(L/M)}$ et $\Psi \circ \Phi(H) = Gal(L/L^H)$.
Pour démontrer l'identité $M = \Phi \circ \Psi(M)$, commençons par rappeler que l'extension $M \hookrightarrow L$

est normale et séparable. L'identité recherchée est alors corollaire immédiat du lemme 15.8 précédent. On obtient alors l'identité $M = L^{Gal(L/M)}$ pour toute extension intermédiaire $K \hookrightarrow M \hookrightarrow L$ d'une extension galoisienne finie $K \hookrightarrow L$.

L'identité $H = \Psi \circ \Phi(H)$ i.e. $H = Gal(L/L^H)$ pour tout sous-groupe fini H de $Gal(L/K)$ est précisément la conclusion du lemme d'Artin appliqué à L et H.

Pour la seconde partie de l'énoncé, soit H un sous-groupe du groupe de Galois $Gal(L/K)$. Pour tout $g \in Gal(L/K)$, $g(L^H) = L^{gHg^{-1}}$. En effet, $h(l) = l$ s.s.i. $ghg^{-1}(g(l)) = gh(l) = l$ pour tout $g \in Gal(L/H)$ et tout $l \in L$. Donc $l \in L^H$ s.s.i. $gl \in L^{gHg^{-1}}$.

L'extension $K \hookrightarrow L$ étant normale puisque galoisienne par hypothèse, l'extension $K \hookrightarrow L^H$ est alors normale s.s.i. l'image par tout K-automorphisme de L, i.e. par tout élément g du groupe de Galois $Gal(L/K)$, de L^H est exactement égale à L^H, c'est à dire, en utilisant l'identité $g(L^H) = L^{gHg^{-1}}$, si $L^{gHg^{-1}} = L^H$, pour tout $g \in Gal(L/K)$, mais $L^{gHg^{-1}} = \Phi(gHg^{-1})$ et $L^H = \Phi(H)$ par la définition même de l'application Φ. Φ étant injective par la première partie de l'énoncé déjà établie, l'identité $L^{gHg^{-1}} = L^H$ est équivalente à $gHg^{-1} = H$ pour tout $g \in Gal(L/K)$, c'est à dire à ce que le sous-groupe H soit distingué de $Gal(L/K)$.

Dans ce cas i.e. H est un sous-groupe distingué de $Gal(L/K)$ ou de façon équivalente, si l'extension $K \hookrightarrow L^H$ est normale, l'identité $g(L^H) = L^{gHg^{-1}}$ montre que le sous-corps L^H est globalement stable sous l'action de $Gal(L/K)$, cee qui permet d'introduire l'application restriction à L^H :

$$\begin{aligned} \rho :\ Gal(L/K) &\longrightarrow Gal(L^H/K)\ , \\ g &\longmapsto g|_{L^H} \end{aligned}$$

qui est un morphisme de groupe et surjectif par la proposition 13.9 appliqué à l'extension $j : L^H \hookrightarrow L$. On observera que l'extension $\tilde{h}$ à L d'un K-automorphisme h de L^H est évidemment un K-automorphisme. En notant $\iota : K \hookrightarrow L^H$, on a en effet par définition même de prolongement : $\tilde{h} \circ j = j \circ h$, et donc $\tilde{h} \circ j \circ \iota = j \circ h \circ \iota = j \circ \iota$, i.e. $\tilde{h}|_K = Id|_K$ comme annoncé. Le noyau du morphisme ρ, coïncide avec

$$\{g \in Gal(L/K),\ g|_{L^H} = Id|_{L^H}\} = Aut_{L^H} L = Gal(L/L^H).$$

C'est à dire avec $\Psi \circ \Phi(H)$, qui coïncide avec le sous-groupe H par la première partie de l'énoncé, établie précédemment $\Psi \circ \Phi = Id_{\mathcal{G}}$. On a ainsi établi :

$$Gal(L/K)/H = Gal(L/K)/\ker \rho \simeq \operatorname{Im} \rho = Gal(L^H/K),$$

ce qui clôt la démonstration du théorème. $\square$