Corps et théorie de Galois (HAX801X)-Prof

0. Introduction générale au cours

0.1. Organisation du cours

▶ **Prérequis :** le contenu des cours de L3 « Groupes et anneaux 1 » et « Groupes et anneaux 2 ».

▶ **Objectif :** maîtriser les outils de base de l'étude des corps ; introduire la correspondance de Galois, et le théorème de Galois sur la résolubilité des polynômes par radicaux.

▶ **Programme :**

1. Révisions sur les anneaux, les corps ; sous-corps premier, caractéristique d'un corps, morphisme de Frobenius, factorisation et critère d'Eisenstein.
2. Extensions de corps : formule des degrés, extensions algébriques, corps algébriquement clos, clôtures algébriques, corps de rupture, corps de décomposition, prolongements des morphismes de corps.
3. Le groupe de Galois ; sous-corps invariants, théorème d'Artin.
4. Les corps finis : groupe de Galois, sous-corps, correspondance de Galois.
5. Extensions normales, celles qui sont finies sont des corps de décomposition.
6. Polynômes et extensions séparables: définitions, composition des extensions séparables, corps parfaits (caractérisations), théorème de l'élément primitif.
7. Extensions galoisiennes : définition, éléments conjugués. Correspondance de Galois ; exemples et applications.
8. Résolution d'équations polynomiales : groupe de Galois d'un polynôme, action sur les racines, théorème de Galois de résolubilité par radicaux en caractéristique nulle.

▶ **Modalités de contrôle des connaissances**

- 2 contrôles continus (CC) de 2h, qui compteront chacun pour 25% de la note du module,
- 1 contrôle terminal (CT) de 3h qui comptera pour 50%.

▶ **Calendrier prévisionnel**

- cours
  - janvier : trois cours (jeudis 22/01, 22/01, 29/01)
  - février : cinq cours (jeudis 12/02, 19/02, 19/02, 26/02, 26/02)
  - mars : trois cours (jeudis 12/03, 19/03, 26/03)
  - avril : trois cours (jeudis 2/04, 9/04, 16/04)
- évaluations : CC1 le 26 février ; CC2 le 16 mars ; CT dans la semaine 4-7 mai

La référence principale pour le cours sera le livre :

[Bad25] Ioan Badulescu, *Anneaux, corps, polynômes et théorie de Galois*, Ellipses, 2025.

Certains passages du cours seront des copies fidèles du livre.

0.2. Qu'est-ce que la théorie de Galois ?

Au lycée, on apprend à exprimer les solutions de l'équation $ax^2 + bx + c = 0$ sous la forme

$$\frac{-b \pm \sqrt{\Delta}}{2a}, \qquad \Delta = b^2 - 4ac.$$

Au Moyen-Âge, les efforts des mathématiciens arabes et italiens Al-Khwârizmî, Tartaglia, Cardan, Ferrari ont permis d'étendre ces méthodes aux équations polynomiales de degré 3 et 4 pour exprimer leurs solutions à l'aide de radicaux. Ce faisant, ils ont inventé les nombres complexes (Cardan, 1545). Les équations de degré 5 leur résistaient...

Al-Khwârizmî (783-850) et Niccolò Fontana Tartaglia (1499-1557)


Gerolamo Cardano (1501-1576) et Ludovico Ferrari (1522-1565)

Plus de deux siècles plus tard, dans son *Mémoire sur les équations algébriques, où l'on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré* paru en 1824, Abel démontre l'impossibilité de résoudre l'équation de degré $\geqslant 5$ par radicaux, c'est-à-dire à l'aide des seules opérations

$$+ \quad - \quad \times \quad \div \quad \sqrt[n]{\ }$$

Galois donne une version nettement plus précise de ce théorème, qui en explique les ressorts profonds, dans l'article *Sur les conditions de résolubilité des équations par radicaux*, rédigé en 1831 et paru dans le Journal de mathématiques pures et appliquées en 1846. Il met au jour la notion de « groupe » et développe la théorie qui relie la complexité d'une équation polynomiale, non pas à la taille de son degré, mais à la structure algébrique du groupe de symétries de ses racines. Sa théorie lui permet d'exhiber des polynômes explicites dont les solutions ne peuvent être exprimées par radicaux. Galois a répondu par la négative à la question « peut-on exprimer les racines d'une équation polynômiale par radicaux » mais il a surtout introduit des concepts fondamentaux pour l'étude des propriétés des nombres, domaine extrêmement actif aujourd'hui encore.


Niels Henrik Abel (1802-1829) et Évariste Galois (1811-1832)

Niels Henrik Abel meurt de la tuberculose le 6 avril 1829, à l'âge de vingt-six ans. Évariste Galois, lui, est touché par balle à l'abdomen lors d'un duel et meurt d'une péritonite le lendemain, 31 mai 1832, à l'âge de vingt ans. Résoudre les équations polynomiales est-il une entreprise maudite ? Je n'irais pas jusque là, et j'encourage le lecteur, la lectrice à en goûter les plaisirs !

On pourra trouver un peu plus de détails sur la vie des mathématiciens cités ici dans le livre de Bertrand Hauchecorne et Daniel Suratteau : *Des mathématiciens de A à Z*, Ellipses, 3ème édition (2008) ou édition poche (2019). Il existe par ailleurs d'excellentes biographies de Galois et Abel.

Dans ce cours, nous allons exposer la théorie de Galois et nous conclurons en indiquant quelques grandes questions de recherche actuelles sur lesquelles cette théorie a débouché.

1A. Rappels sur les anneaux et les corps

Nous faisons des rappels sur le contenu des cours Groupes et anneaux 1 (HAX501X) et Groupes et anneaux 2 (HAX605X). Dans cette partie, les démonstrations seront parfois mélangées au texte, incomplètes voire absentes.

1A.1. Anneaux

▶ Anneaux

Un *anneau* est un triplet $(A, +, \times)$ composé d'un ensemble A et de deux lois internes $+$ et $\times$ telles que $(A, +)$ est un groupe commutatif de neutre 0_A et $\times$ est associative, distributive à gauche et à droite sur $+$, et possède un élément neutre 1_A.

Dans ce cours, nous considérerons presque exclusivement des anneaux commutatifs, et nous dirons simplement « anneau ». Les seuls anneaux non commutatifs qui apparaitront sont des anneaux de matrices, et si nous voulons souligner leur structure d'anneau nous dirons « anneau non commutatif ».

De plus :

- tous les anneaux ont un élément neutre pour la multiplication aussi appelé *unité* et noté 1 (ou 1_A si l'anneau s'appelle A),
- tous les morphismes d'anneaux $f : A \to B$ sont unitaires par définition, c'est-à-dire que $f(1_A) = 1_B$; si $A = B$ on dit que f est un endomorphisme et, s'il est bijectif, un automorphisme.

Il existe un unique anneau dans lequel $1 = 0$, c'est l'*anneau nul* $A = \{0\}$. En effet, si $1 = 0$ alors pour tout $a \in A$ on obtient $a = 1a = 0a = 0$.

▶ Sous-anneaux

Une partie $B \subset A$ est un *sous-anneau* si c'est un anneau pour les opérations de A et si $1_B = 1_A$. Ainsi $B := \mathbb{Z} \times \{0\}$ est un anneau pour les opérations induites par celles de $\mathbb{Z} \times \mathbb{Z}$ avec unité $(1, 0)$, mais ce n'est pas un sous-anneau de $A := \mathbb{Z} \times \mathbb{Z}$ car l'unité de A est $(1, 1)$.

L'exemple $\mathbb{Z} \times \mathbb{Z}$ ci-dessus est un cas particulier d'un *anneau produit* $A = A_1 \times A_2$, qui est le produit ensembliste muni des lois définies composante par composante, avec le neutre additif $(0, 0)$ et le neutre multiplicatif $(1, 1)$.

Voici quelques autres manières de fabriquer des sous-anneaux.

- Une intersection d'une famille quelconque de sous-anneaux $(A_j)_{j\in J}$ est un sous-anneau noté $\cap_{j\in J} A_j$.
- Si $S \subset A$ est une partie, l'ensemble des sommes finies de produits $s_{i_1} \cdots s_{i_n}$ avec $s_{i_j} \in S$ est égal à l'intersection de la famille des sous-anneaux de A contenant S. C'est aussi le plus petit sous-anneau contenant X au sens de l'inclusion. On le note $\mathbb{Z}[S]$ ou et on le nomme *sous-anneau engendré par* S.

1A.2. Corps

▶ Quelques propriétés des éléments

Un élément $x \in A$ est dit :

- *inversible* s'il possède un inverse multiplicatif,
- *nilpotent* s'il existe $n \geqslant 1$ tel que $x^n = 0$,
- *non diviseur de zéro* si $ax = 0$ implique $a = 0$.

Exercice. Soient A un anneau et a, x, y des éléments.

1. Supposons que $a = xy$. Alors a est inversible ssi x et y sont inversibles.
2. Si x et y sont nilpotents alors ax et $x + y$ sont nilpotents.
3. Si a est inversible et x est nilpotent alors $a + x$ est inversible.

Les points 1 et 2 de l'exercice ci-dessus montrent que

- l'ensemble $A^\times$ des éléments inversibles de A est un groupe multiplicatif,
- l'ensemble $\mathrm{Nil}(A) = \sqrt{0_A}$ des éléments nilpotents est un idéal appelé *nilradical*.

▶ Anneaux intègres, corps, sous-corps

On dit qu'un anneau A est :

- *intègre* si $A \neq 0$ et si tout élément non nul est non diviseur de zéro,
- un *corps* si $A \neq 0$ et si tout élément non nul est inversible.

Un *morphisme de corps* $f : K \to L$ est simplement un morphisme d'anneaux.

Un sous-anneau d'un anneau intègre est intègre. Tout anneau intègre A possède un corps de fractions $K = \mathrm{Frac}(A)$ construit comme l'ensemble des classes d'équivalence de fractions a/b avec $b \neq 0$, muni des opérations habituelles pour les fractions. On voit donc que « être un anneau intègre » est la même chose que « être un sous-anneau d'un corps ». Tout morphisme injectif $f : A \to B$ se prolonge en un morphisme de corps $f' : \mathrm{Frac}(A) \to \mathrm{Frac}(B)$.

L'intersection d'une famille quelconque de sous-corps est un sous-corps. Il existe une notion de *sous-corps engendré par une partie* $S \subset K$: c'est l'intersection des sous-corps de K contenant S, ou encore, le corps des fractions du sous-anneau de K engendré par S. En notant K_0 le sous-corps premier de K, le sous-corps engendré par S sera noté $K_0(S)$. Par exemple, dans le corps de fractions rationnelles $\mathbb{R}(X)$, le sous-anneau engendré par X est $\mathbb{Z}[X]$ et le sous-corps engendré par X est $\mathbb{Q}(X)$.

1A.3. Idéaux

▶ Idéaux et morphisme quotient

Un *idéal* est un sous-groupe additif $(I, +) \subset (A, +)$ qui est stable par multiplication par les éléments de A : si $a \in A$ et $i \in I$ alors $ai \in I$. C'est donc la même chose qu'un sous-A-module de A. Un idéal *strict* (on dit parfois aussi *propre*) est un idéal $I \neq A$.

Exemple. Il découle de la division euclidienne dans $\mathbb{Z}$ que ses idéaux sont les $n\mathbb{Z}$ avec $n \geqslant 0$.

Euclide (~300 av. JC)

Le noyau d'un morphisme d'anneaux est un idéal.

L'idéal $I = A$ est appelé l'idéal unité. Les conditions suivantes sont équivalentes :

$$I = A \quad ; \quad 1 \in I \quad ; \quad I \text{ contient un élément inversible.}$$

Si I est un idéal de A, c'est en particulier un sous-groupe de $(A, +)$ et le groupe quotient $(A/I, +)$ est bien défini. Il s'accompagne d'un morphisme de groupes surjectif $\pi : A \to A/I$ de noyau égal à I. Qui plus est, si $x, y \in A/I$ on peut choisir $a, b \in A$ tels que $x = \pi(a)$, $y = \pi(b)$ et l'élément

$$xy := \pi(ab)$$

ne dépend pas du choix de a et b à cause de la propriété d'idéal.

> Détail : d'autres choix d'antécédents de x, y sont de la forme $a' = a + i$ et $b' = b + j$, donc $a'b' = ab + (aj + bi + ij) \equiv ab \bmod I$ puis $\pi(a'b') = \pi(ab)$.

On munit ainsi A/I d'une structure d'anneau d'unité $1_{A/I} = \pi(1_A)$, tel que $\pi : A \to A/I$ est un morphisme d'anneaux.

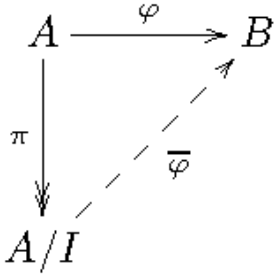
Théorème de quotient. Soit A un anneau et I un idéal. Alors :

1. L'ensemble $(A/I, +, \times)$ est un anneau. Le morphisme quotient $\pi : A \to A/I$ est surjectif et de noyau I.
2. Le quotient vérifie la propriété : pour tout anneau B et tout morphisme d'anneaux $\varphi : A \to B$ tel que $I \subset \ker(\varphi)$, il existe un unique morphisme d'anneaux $\bar{\varphi} : A/I \to B$ tel que $\varphi = \bar{\varphi} \circ \pi$.

3. Dans la situation de 2. on a $\mathrm{im}(\bar{\varphi}) = \mathrm{im}(\varphi)$ et $\ker(\bar{\varphi}) = \pi(\ker(\varphi))$.

Remarques.

- La propriété du point 2 s'appelle « propriété universelle du quotient ». Elle caractérise le quotient. On la représente par le diagramme :



  Cette propriété implique qu'il est naturel de définir un morphisme *depuis* un anneau quotient plutôt que *vers* un anneau quotient. On se souviendra de cette règle chaque fois que l'on souhaite relier deux anneaux par un morphisme, lorsque l'un des anneaux est un quotient.
- Dans le point 3 l'idéal $\pi(\ker(\varphi))$ est aussi $\ker(\varphi)/I$, le quotient au sens des groupes.
- On a dit plus haut que le noyau d'un morphisme d'anneaux est un idéal ; le théorème montre que réciproquement tout idéal I est le noyau d'un morphisme (à savoir, le morphisme $A \to A/I$).

Exemple. L'anneau $A = \mathbb{Z}/n\mathbb{Z}$ est le quotient de $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$.

- Il est intègre si et seulement si $n = 0$ ou n est un nombre premier, puisque si n n'est pas premier on a $n = ab$ avec $1 < a, b < n$ donc dans A on a $ab = 0$ alors que $a \neq 0$ et $b \neq 0$.
- C'est un corps si et seulement si n est un nombre premier.

Exercice. Soient A un anneau et $I \subset J$ une inclusion d'idéaux. Démontrez que le groupe quotient J/I est un idéal de l'anneau quotient A/I et qu'on a un isomorphisme d'anneaux

$$(A/I)/(J/I) \simeq A/J.$$

Exercice. Soit $A = R[X, Y]/(X^m, Y^n)$, où $m, n \geqslant 1$ sont deux entiers et R est un anneau. Calculez l'indice de nilpotence de $X + Y$ lorsque $R = \mathbb{C}$, $R = \mathbb{Z}$ puis $R = \mathbb{Z}/a\mathbb{Z}$.

Corollaire (théorème d'isomorphisme). Soit $f : A \to B$ un morphisme d'anneaux. Alors f induit un isomorphisme d'anneaux $\bar{f} : A/\ker(f) \xrightarrow{\sim} \mathrm{im}(f)$.

▶ Propriétés des idéaux

Un idéal $I \subset A$ est dit :

- *premier* si $I \neq A$ et pour tous $a, b \in A$ on a : $ab \in I \Longrightarrow a \in I$ ou $b \in I$. Il est équivalent de dire que l'anneau quotient A/I est intègre.
- *maximal* si $I \neq A$ et s'il est maximal pour l'inclusion des idéaux, c'est-à-dire que $I \subsetneq J \subset A$ implique $J = A$. Il est équivalent de dire que A/I est un corps.

▶ Opérations sur les idéaux ($\cap$, Σ, Π)

- Une intersection d'une famille quelconque d'idéaux $(I_j)_{j\in J}$ est un idéal noté $\cap_{j\in J} I_j$.
- Si $X \subset A$ est une partie, l'ensemble des sommes finies $\sum_{i=1}^{n} a_i x_i$ avec $a_i \in A$ et $x_i \in X$ est égal à l'intersection de la famille des idéaux de A contenant X. C'est aussi le plus petit idéal contenant X au sens de l'inclusion. On le note $\langle X \rangle$ ou (X) et on le nomme *idéal engendré par* X.
- L'idéal engendré par la réunion $X = \cup_{j\in J} I_j$ d'une famille d'idéaux est un idéal noté $\sum_{j\in J} I_j$ et appelé *somme* des I_j.

- L'idéal engendré par les produits $i_1 i_2$, avec $i \in I_1$ et $i_2 \in I_2$, est un idéal noté $I_1 I_2$ et appelé *produit* de I_1 et I_2. La définition s'étend de manière immédiate au cas du produit $I_1 \cdots I_n$ d'un nombre fini d'idéaux. Par exemple si $I_1 = I_2 = I$ on a l'idéal I^2 engendré par les produits ii' avec $i, i' \in I$.

Exercice. On a $IJ \subset I \cap J$. L'inclusion est stricte en général.

1A.4. Caractéristique ; Frobenius

▶ Caractéristique d'un anneau

- Tout anneau A possède un plus petit sous-anneau $A_0 \subset A$ appelé *sous-anneau premier* de A. C'est le sous-anneau engendré par 1, ou encore l'intersection de tous les sous-anneaux de A.
- Tout corps K possède un plus petit sous-corps $K_0 \subset K$ appelé *sous-corps premier* de K. C'est le sous-corps engendré par 1, ou encore l'intersection de tous les sous-corps de K.

On peut expliciter le sous-anneau premier (resp. le sous-corps premier) en considérant l'application $u : \mathbb{Z} \to A$ définie par $u(m) = m1_A$. C'est l'unique morphisme d'anneaux de $\mathbb{Z}$ dans A. Son noyau est un idéal de $\mathbb{Z}$ donc de la forme $n\mathbb{Z}$ pour un unique entier $n \geqslant 0$.

Définition. La *caractéristique* de A est le générateur $n \geqslant 0$ du noyau de u. Elle est notée $\mathrm{car}(A)$.

Comme $u(1) = 1$, on a $n \neq 1$ et c'est la seule contrainte sur n.

Proposition. Soient A un anneau et K un corps.

1. Le sous-anneau premier $A_0 \subset A$ est isomorphe à $\mathbb{Z}$ ou à $\mathbb{Z}/n\mathbb{Z}$ pour un entier $n \geqslant 2$.
2. Si A est intègre, A_0 est isomorphe à $\mathbb{Z}$ ou à $\mathbb{Z}/p\mathbb{Z}$ pour un entier p premier.
3. Le sous-corps premier K_0 est isomorphe à $\mathbb{Q}$ ou à $\mathbb{Z}/p\mathbb{Z}$ pour un entier p premier.

Démonstration : le théorème d'isomorphisme fournit un isomorphisme

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathrm{im}(u) \subset A.$$

Pour 2, si A est intègre l'entier n est soit nul soit un nombre premier puisque $\mathbb{Z}/n\mathbb{Z} \subset A$ est intègre. Enfin si K est un corps, son sous-anneau premier est $\mathbb{Z}$ ou $\mathbb{Z}/p\mathbb{Z}$ d'après le point précédent. Si c'est $\mathbb{Z}$, le morphisme u est injectif et s'étend aux corps de fractions (voir §1A.2) en $u' : \mathbb{Q} \hookrightarrow K$. ■

▶ Morphisme de Frobenius

Soit p un nombre premier. Pour tout entier $k \in \{2, \dots, p-1\}$ on a

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

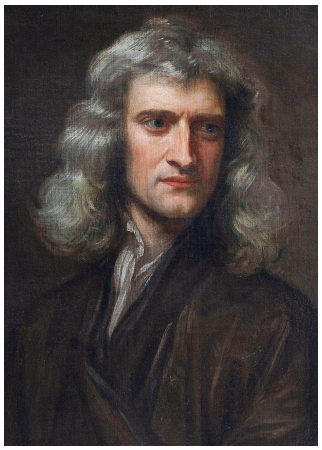
Ainsi p divise $k\binom{p}{k}$ et comme $\mathrm{pgcd}(k, p) = 1$, le lemme d'Euclide entraîne que p divise $\binom{p}{k}$.

Revenons à un anneau A. La relation $\binom{p}{k} = pm$ (pour un entier m) dans $\mathbb{Z}$ fournit la même relation dans A, en prenant l'image par u. Supposons que $p = 0$ dans A, c'est-à-dire que A est de caractéristique p. On a alors $\binom{p}{k} = 0$ lorsque $1 < k < p$. Dans la formule du binôme de Newton pour le développement de $(x + y)^p$, les termes intermédiaires s'annulent et on obtient

$$(x + y)^p = \sum_{k=1}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p$$

pour tous $x, y \in A$. Comme $(xy)^p = x^p y^p$ et $1^p = 1$, on obtient :

Théorème. Si A est un anneau de caractéristique p, l'application $F : A \to A$ définie par $F(x) = x^p$ est un endomorphisme d'anneaux appelé le *morphisme de Frobenius*.

Ferdinand Georg Frobenius (1849-1917) et Isaac Newton (1642-1727)

1A.5. Théorème des restes chinois

Dans un anneau A, on dit que deux idéaux I, J sont *étrangers* ou *comaximaux* lorsque $I + J = A$. Compte tenu des remarques faites au §1.3, il est équivalent de dire que $1 \in I + J$ c'est-à-dire qu'il existe $i \in I$ et $j \in J$ tels que $i + j = 1$.

Théorème des restes chinois. Soient I et J deux idéaux étrangers d'un anneau A. Alors :
(i) $IJ = I \cap J$,
(ii) le morphisme d'anneaux $\pi : A \to A/I \times A/J$ qui envoie $a \in A$ sur $(a + I, a + J)$ induit un isomorphisme

$$A/IJ \xrightarrow{\sim} A/I \times A/J.$$

Démonstration : fixons une écriture $i + j = 1$ avec $i \in I$, $j \in J$.
(i) Comme $IJ \subset I$ et $IJ \subset J$, on a $IJ \subset I \cap J$. Réciproquement si $a \in I \cap J$, on a $a = a(i + j) = ai + aj \in IJ$.

(ii) Le noyau de π est composé des $a \in A$ tels que $a \in I$ et $a \in J$, donc $\ker(\pi) = I \cap J$. D'après le point (i) c'est égal à IJ. Montrons par ailleurs que π est surjectif. Pour cela soit $(x + I, y + J)$ un élément de $A/I \times A/J$, représenté par des éléments $x, y \in A$. Posons $a = xj + yi$. Puisque $i + j = 1$, on a $i \equiv 1 \bmod J$ et $j \equiv 1 \bmod I$. On en déduit que

$$a \equiv xj \equiv x \bmod I \quad \text{et} \quad a \equiv yi \equiv y \bmod J.$$

Ceci démontre que $\pi(a) = (x + I, y + J)$. D'après le théorème d'isomorphisme π induit donc un isomorphisme $A/IJ \simeq A/I \times A/J$. ■

Remarque. Ce théorème se généralise par une récurrence immédiate au cas où l'on dispose de n idéaux étrangers deux à deux $I_1, \dots, I_n$. On obtient un isomorphisme :

$$A/I_1 \cdots I_n \xrightarrow{\sim} A/I_1 \times \cdots \times A/I_n.$$

1B. Rappels sur l'algèbre des polynômes

Nous faisons des rappels sur les notions du cours de L2 Arithmétique des polynômes (HAX303X). Comme dans la partie précédente, les démonstrations sont informelles et incomplètes.

1B.1. Algèbres

▶ Algèbres

Soit K un corps.

- Une *K-algèbre* est un anneau A qui est muni d'une structure supplémentaire d'espace vectoriel telle que la multiplication $m : A \times A \to A$, $m(x, y) = xy$ est bilinéaire.
- Un *morphisme de K-algèbres* est une application $f : A \to B$ qui est à la fois un morphisme d'anneaux et un morphisme de K-espaces vectoriels.
- La *dimension* de A notée $\dim_K(A)$ est sa dimension en tant que K-espace vectoriel.

Exemples. L'algèbre des polynômes $K[X]$; l'algèbre des matrices $\mathrm{M}_n(K)$; tout anneau contenant K comme sous-anneau (voir ci-dessous).

Si A est une K-algèbre, l'application $u : K \to A$, $u(\lambda) = \lambda 1_A$ vérifie les propriétés :
(i) $u(\lambda + \mu) = (\lambda + \mu) \cdot 1 = \lambda 1 + \mu 1 = u(\lambda) + u(\mu)$,
(ii) $u(\lambda\mu) = (\lambda\mu)1 = \lambda(\mu 1) = \lambda(1(\mu 1)) = (\lambda 1)(\mu 1)) = u(\lambda)u(\mu)$,
(iii) $u(1_K) = 1_K 1_A = 1_A$.
(iv) $u(\lambda)a = (\lambda 1)a = \lambda(1a) = \lambda(a1) = a(\lambda 1) = au(\lambda)$.

Remarque. Comme nous l'avons déjà dit, nous considèrerons presque exclusivement des anneaux commutatifs et des algèbres commutatives. Dans ce cas la propriété (iv) est automatique.

Proposition. Soit A un anneau commutatif. La construction ci-dessus fournit une correspondance entre :

- les structures de K-algèbres sur A,
- les morphismes d'anneaux $u : K \to A$.

De plus, si A et B sont des K-algèbres décrites par des morphismes d'anneaux $u_A : K \to A$ et $u_B : K \to B$ alors un morphisme d'anneau $f : A \to B$ est un morphisme de K-algèbres si et seulement si $f \circ u_A = u_B$.

> **Démonstration :** nous avons associé à une structure d'algèbre un morphisme u. Réciproquement si u est donné, on peut munir A d'une loi externe par la formule $\lambda \cdot a := u(\lambda)a$. On vérifie que ceci fait de A un K-espace vectoriel et que sa multiplication est commutative. Les autres énoncés sont laissés en exercice. ■

De la proposition, on tire immédiatement deux manières de fabriquer des algèbres à partir d'une K-algèbre A :

1. Si $e : K_0 \to K$ est un morphisme de corps, le morphisme composé
$$K_0 \xrightarrow{e} K \xrightarrow{f} A$$
munit A d'une structure de K_0-algèbre (et f est alors un morphisme de K_0-algèbres).
2. Si $g : A \to B$ est un morphisme d'anneaux, le morphisme composé
$$K \xrightarrow{f} A \xrightarrow{g} B$$
munit B d'une structure de K-algèbre (et g est alors un morphisme de K-algèbres).
3. Comme car particulier de 2, si A est une K-algèbre et $I \subset A$ un idéal, alors A/I est une K-algèbre et $\pi : A \to A/I$ est un morphisme de K-algèbres.

▶ Sous-algèbres

Pour finir nous évoquons les *sous-K-algèbres* (on dit parfois simplement *sous-algèbre* lorsque K est clair d'après le contexte), c'est-à-dire les parties qui sont simultanément un sous-anneau et un sous-espace vectoriel.

- Une intersection d'une famille quelconque de sous-algèbres $(A_j)_{j\in J}$ est une sous-algèbre notée $\cap_{j\in J} A_j$.
- Si $S \subset A$ est une partie, l'ensemble des combinaisons K-linéaires de produits $s_{i_1} \cdots s_{i_n}$ avec $s_{i_j} \in S$ est égal à l'intersection de la famille des sous-algèbres de A contenant S. C'est aussi la plus petite sous-algèbre contenant X au sens de l'inclusion. On la note $k[S]$ ou et on la nomme *sous-algèbre engendrée par* S.

▶ Un mot sur le cas non commutatif (Ajout culturel)

- Si l'on accepte des anneaux éventuellement non commutatifs, comme par exemple les anneaux de matrices $\mathrm{M}_n(K)$, on peut étendre ces concepts en introduisant le *centre* $Z(A) = \{a \in A \mid \forall x \in A, ax = xa\}$, ensemble des éléments qui commutent avec tous les éléments de l'anneau. La propriété (iv) ci-dessus dit que u est un morphisme d'anneaux de K à valeurs dans $Z(A)$ et la proposition reste valable avec cette modification.
- En revanche, la construction n°2 qui permet d'utiliser une K-algèbre A et un morphisme d'anneaux $g : A \to B$ pour munir B d'une structure de K-algèbre ne fonctionne pas aussi bien que dans le cas commutatif, pour la raison que g n'envoie pas nécessairement le centre $Z(A)$ dans le centre $Z(B)$. C'est là une des subtilités de la notion de centre. Par exemple, prenons $A = K[X]$, $B = \mathrm{M}_n(K)$ et fixons une matrice $M \in B$. Alors l'image du centre $Z(A) = A$ par le morphisme $g : A \to B$, $g(P) = P(M)$ est la sous-K-algèbre $K[M] \subset B$ des polynômes en M. Cette image n'est incluse dans le centre $Z(B) = K \cdot \mathrm{I}_n$ que lorsque M est une matrice scalaire.

1B.2. L'algèbre des polynômes

L'ensemble des polynômes en une indéterminée X à coefficients dans K est une K-algèbre commutative. Il est muni d'une fonction degré $\deg : K[X] \to \mathbb{N} \cup \{-\infty\}$ telle que $\deg(P)$ est le degré habituel des polynômes, avec $\deg(0) = -\infty$. Ses propriétés les plus importantes sont :

- $\deg(P + Q) \leqslant \max(\deg(P), \deg(Q))$,
- $\deg(PQ) = \deg(P) + \deg(Q)$.

L'algèbre $K[X]$ possède une « propriété universelle » qui la caractérise parmi toutes les K-algèbres :

Théorème. Soit B une K-algèbre. Un morphisme de K-algèbres $f : K[X] \to B$ est entièrement déterminé par l'élément $b = f(X)$. Réciproquement pour tout choix de $b \in B$ il existe un unique morphisme $f : K[X] \to B$ tel que $f(X) = b$.

> **Démonstration :** en effet, si $b = f(X)$ alors pour tout polynôme $P = \sum_{i=0}^n a_i X^i$, puisque f est un morphisme d'anneaux K-linéaire on aura
>
> $$f(P) = f\Big(\sum_{i=0}^n a_i X^i\Big) = \sum_{i=0}^n a_i f(X^i) = \sum_{i=0}^n a_i f(X)^i = \sum_{i=0}^n a_i b^i.$$
>
> Ainsi f est déterminé par $f(X)$. Réciproquement, étant donné $b \in B$ on peut poser $f(P) = \sum_{i=0}^n a_i b^i$. On vérifie que cette expression définit un morphisme de K-algèbres $f : K[X] \to B$, avec bien sûr $f(X) = b$. ■

1B.3. Arithmétique dans l'algèbre des polynômes

▶ Division euclidienne et conséquences

On rappelle que $K[X]$ est un anneau intègre euclidien :

Théorème (division euclidienne). Pour tout couple de polynômes $(A, B) \in K[X]^2$ avec $B \neq 0$, il

existe un unique couple $(Q, R) \in K[X]^2$ tel que

$$\begin{aligned} &\text{(i)} \quad A = BQ + R, \\ &\text{(ii)} \quad \deg(R) < \deg(B). \end{aligned}$$

Remarque ★★★ Pour les polynômes à coefficients dans un anneau *quelconque*, la division euclidienne par un polynôme B à coefficient dominant inversible est toujours possible. ■

Il en découle que $K[X]$ est un anneau euclidien, donc principal. Ainsi tout idéal I est principal, c'est-à-dire engendré par un polynôme P. De plus P peut être choisi de manière unique en demandant que $P = 0$ si $I = (0)$, et P est unitaire sinon.

Comme on l'a vu au paragraphe 1B.1, tout quotient de $K[X]$ est encore une K-algèbre. La division euclidienne apporte des précisions précieuses sur ce quotient ; dans l'énoncé suivant on se limite aux quotients « non trivaux ».

Corollaire. Soit P un polynôme non constant et $n = \deg(P) \geqslant 1$. Alors la K-algèbre quotient $A = K[X]/(P)$ est de dimension finie égale à n avec pour base $(1, \bar{X}, \dots, \bar{X}^{n-1})$.

> **Démonstration :** Notons $K_{n-1}[X] = \mathrm{Vect}(1, X, \dots, X^{n-1})$ le sous-K-espace vectoriel des polynômes de degré $\leqslant n-1$. L'application $K[X] \to K_{n-1}[X]$ qui à un polynôme associe le reste de sa division euclidienne par P est K-linéaire, surjective, avec pour noyau l'idéal (P). En appliquant le théorème d'isomorphisme pour les applications linéaires, on déduit un isomorphisme $K[X]/(P) \simeq K_{n-1}[X]$ qui envoie la base (X^i) sur la base $(\bar{X}^i)$. ■

Théorème de Bézout. Soient A, B deux polynômes non tous deux nuls. Alors A et B sont premiers entre eux si et seulement s'il existe un couple $(U, V) \in K[X]$ tel que $UA + VB = 1$.

Exercice. Démontrez les compléments suivants au théorème de Bézout :

1. Lorsque A et B sont premiers entre eux, il existe un *unique* couple (U, V) tel que $\deg(U) < \deg(B)$ et $\deg(V) < \deg(A)$.
2. Soient A, B, D trois polynômes avec A, B non tous deux nuls. Alors $D = \mathrm{pgcd}(A, B)$ si et seulement s'il existe $(U, V) \in K[X]$ premiers entre eux tels que $UA + VB = D$.

▶ Primalité, pgcd, ppcm

La principalité entraine la factorialité, c'est-à-dire que l'on dispose des notions suivantes :

- la relation de divisibilité ; la relation d'association ;
- pour deux polynômes P, Q on a $P|Q \iff (Q) \subset (P)$;
- la notion d'irréductibilité ; l'ensemble $\mathcal{P}$ des polynômes irréductibles unitaires est un ensemble de représentants pour les irréductibles à association près ;
- la décomposition en facteurs irréductibles des $P \neq 0$;
- les notions de pgcd et ppcm (définis à un inversible près).

On dispose aussi des résultats classiques qui suivent.

Lemme. Soit $P \in K[X]$ un polynôme non nul. Les conditions suivantes sont équivalentes :

- le polynôme P est irréductible,
- l'idéal (P) est premier,
- l'idéal (P) est maximal.

ℹ Le cours du jeudi 22 janvier 2026 (deux séances) s'est arrêté ici.

Lemme d'Euclide. Soient P, A, B des polynômes avec P irréductible. Si $P|AB$, alors $P|A$ ou $P|B$.

Lemme de Gauss. Soient A, B, C des polynômes avec $\mathrm{pgcd}(A, B) = 1$. Si $A|BC$, alors $A|C$.

Algorithme d'Euclide. Soient $A, B \in K[X]$ tels que $B \neq 0$ et $\deg(A) \geqslant \deg(B)$.
On définit une suite (A_i, B_i) de la manière suivante :

- $A_0 = A$, $B_0 = B$,

puis tant que $B_{i-1} \neq 0$,

- $A_i = B$ et $B_i = R$ dans la division euclidienne $A_{i-1} = B_{i-1}Q + R$.

Alors le dernier reste non nul de l'algorithme est égal au pgcd de A et B.


Étienne Bézout (1730-1783) et Carl Friedrich Gauss (1777-1855)

1B.4. Fonctions polynomiales

Soit $P = \sum_{i=0}^{n} a_i X^i$ un élément de $K[X]$. Pour toute K-algèbre A et $a \in A$, la somme

$$P(a) := \sum_{i=0}^{n} a_i a^i$$

est un élement bien défini de A. Voici trois cas particuliers de cette construction.

1. La *substitution* : pour $A = K[X]$ et $a = Q \in K[X]$, l'élément $P(Q) = \sum_{i=0}^{n} a_i Q^i$ est appelé le polynôme obtenu en *substituant* Q *à* X dans P. Par exemple, si l'on prend $Q = X$ on trouve $P(X) = \sum_{i=0}^{n} a_i X^i = P$ ce qui explique que les deux notations P et $P(X)$ soient utilisées dans la pratique. Un autre exemple est le polynôme $P(X + 1)$.
2. Les *polynômes de matrices (ou d'endomorphismes)* : pour $A = \mathrm{M}_n(K)$ et $a = M$ une matrice, l'élément $P(M)$ est le polynôme de matrice utilisé classiquement dans la théorie de la réduction des endomorphismes (par exemple).
3. L'*évaluation en un point* : pour $A = K$ et $a = x$ égal à un élément de K, l'élément $P(x)$ est un élément de K appelé l'évaluation de P au point x. (Plus généralement on peut prendre $A = L$ un corps qui contient K.)

▶ Racines et leur multiplicité

Dans ce paragraphe nous nous concentrons sur le cas de l'évaluation.

- lorsqu'il est utile de distinguer le polynôme et la fonction, nous noterons

$$\tilde{P} : K \to K, \quad x \mapsto P(x)$$

la *fonction polynomiale associée à* P.
- on dit que $x_0 \in K$ est une *racine* de P si $P(x_0) = 0$,
- on appelle *multiplicité de* P *en* x_0 le plus grand entier $m \geqslant 0$ tel que $(X - x_0)^m$ divise P.

La multiplicité est notée $\mathrm{mult}_{x_0}(P)$. Une autre manière de la voir est comme l'exposant de $(X - x_0)$ dans la décomposition de P en facteurs irréductibles.

Lemme. Pour $P \in K[X]$ et $x_0 \in K$, les conditions suivantes sont équivalentes :

- x_0 est une racine de P,
- P est divisible par $X - x_0$,
- la multiplicité de P en x_0 est $m \geqslant 1$.

Pour étudier le cas où la multiplicité en x_0 est plus grande, on peut s'appuyer sur la dérivation. Si $P = \sum_{i=0}^{n} a_i X^i$, on définit

$$P' = \sum_{i=1}^{n} i a_i X^{i-1}.$$

La dérivée seconde est notée P'' et la dérivée m-ième est notée $P^{(m)}$.

Lemme. Pour $P \in K[X]$ et $x_0 \in K$, les conditions suivantes sont équivalentes :

- la multiplicité de P en x_0 est $m \geqslant 2$,
- $P(x_0) = P'(x_0) = 0$.

▶ Formule de Taylor

Brook Taylor (1685-1731)

Nous terminons ce paragraphe par un résultat important mais qui sera moins utile pour l'étude de la théorie de Galois.

En caractéristique $p > 0$, les choses sont compliquées par le fait que la dérivée de $P = X^p$ est $P' = pX^{p-1} = 0$. Par exemple, en caractéristique $p = 2$ l'annulation

$$P(x_0) = P'(x_0) = P''(x_0) = 0$$

n'implique pas que la multiplicité de P en x_0 est $m \geqslant 3$ comme le montre le cas de $P = X^2$. Pour caractériser les multiplicités quelconques, nous nous placerons en caractéristique nulle.

Formule de Taylor. Supposons que $\mathrm{car}(K) = 0$. Soit $P \in K[X]$. Alors on a :

$$P(X) = \sum_{i=1}^{n} \frac{P^{(i)}(x_0)}{i!}(X - x_0)^i.$$

Corollaire. Si $\mathrm{car}(K) = 0$, pour $P \in K[X]$, $x_0 \in K$ et $m \geqslant 0$, les conditions suivantes sont équivalentes :

- la multiplicité de P en x_0 est m,
- $P(x_0) = \cdots = P^{(m-1)}(x_0) = 0$ et $P^{(m)}(x_0) \neq 0$.

1B.5. Racines et factorisation

Un polynôme $P \in K[X]$ de degré $n \geqslant 0$ possède au plus n racines, comptées avec multiplicité. En effet, si $n = 0$ alors P est un polynôme constant non nul (on appelle que $\deg(0) = -\infty$) donc il possède 0 racine. Si $n \geqslant 1$ supposons que $x_1, \ldots, x_k$ sont des racines distinctes de multiplicités $m_1, \ldots, m_k$. Alors pour chaque i le polynôme $(X - x_i)^{m_i}$ divise P. Comme des polynômes sont premiers entre eux deux à deux, leur produit divise P :

$$(X - x_1)^{m_1} \cdots (X - x_k)^{m_k} | P.$$

En prenant les degrés on trouve $m_1 + \cdots + m_k \leqslant n$, comme annoncé.

On dit que P est *scindé* s'il est produit de polynômes de degré 1 :

$$P = \lambda \prod_{i=1}^{n} (X - x_i).$$

Par exemple tout polynôme de degré 0 est scindé ; on rappelle que par convention un produit indicé par l'ensemble vide est égal à 1.

▶ Relations coefficients-racines

Dans la suite supposons que P est unitaire, i.e. $\lambda = 1$. Dans ce cas, le développement du produit ci-dessus fournit les *relations coefficients-racines*. Par exemple pour $n = 3$, on a

$$(X - a)(X - b)(X - c) = X^3 - (a + b + c)X^2 + (ab + ac + bc)X - abc.$$

En général, en notant $\underline{x} = (x_1, \ldots, x_n)$ le n-uplet des racines, on introduit la *k-ième fonction symétrique des x_i* définie comme la somme des produits des racines prises k par k :

$$\sigma_k(\underline{x}) = \sum_{i_1 < \cdots < i_k} x_{i_1} \ldots x_{i_k}.$$

Voici alors la formule qui exprime les coefficients de P comme fonctions de ses racines.

Relations coefficients-racines, ou formules de Viète. On a :

$$\prod_{i=1}^{n} (X - x_i) = X^n - \sigma_1(\underline{x})X^{n-1} + \cdots + (-1)^{n-1}\sigma_{n-1}(\underline{x})X + (-1)^n\sigma_n(\underline{x}).$$

▶ Factorisation dans $\mathbb{C}$

Nous terminons cette partie 1 de rappels avec l'énoncé du *théorème fondamental de l'algèbre* ou *théorème de d'Alembert-Gauss*, qui figure au programme du cours Arithmétique des polynômes (HAX303X). Nous utiliserons ce théorème dès maintenant et en donnerons une démonstration au §2.7 du cours.

Théorème fondamental de l'algèbre (d'Alembert, Gauss).
Tout polynôme non constant à coefficients complexes possède une racine.

François Viète (1540-1603) et Jean Le Rond d'Alembert (1717-1783)

1B.6. Quelques critères d'irréductibilité des polynômes

Référence : Ivan Gozard, *Théorie de Galois*, Ellipses, 1997. Pages 10, 11, 12 accessibles ici.

Le calcul du polynôme minimal d'un élément algébrique nécessite de disposer de critères d'irréductibilité pour les polynômes. Voici trois énoncés classiques qui permettent de démontrer l'irréductibilité dans des cas favorables. Ces critères sont à connaître et peuvent être utilisés librement.

Proposition (racines rationnelles). Soit A un anneau factoriel et soit $K = \mathrm{Frac}(A)$. Soit $P(X) = a_n X^n + \cdots + a_0$ un polynôme à coefficients dans A, avec $a_n \neq 0$ et $a_0 \neq 0$. Si $\alpha \in K \setminus \{0\}$ est racine de $P(x)$, notant $\alpha = p/q$ une écriture irréductible (i.e. $p, q \in A$ non nuls avec $\mathrm{pgcd}(p, q) = 1$), alors p divise a_0 et q divise a_n.

Théorème (critère d'Eisenstein). Soit A un anneau factoriel et soit $K = \mathrm{Frac}(A)$. Soit $P(X) = a_n X^n + \cdots + a_0$ avec $a_i \in A$. Soit p un élément irréductible. On suppose :

1. $p \nmid a_n$,
2. $\forall i = 0, \ldots, n-1, p \mid a_i$,
3. $p^2 \nmid a_0$.

   Alors P est irréductible dans $K[X]$.

Théorème (réduction). Soit A un anneau factoriel et soit $K = \mathrm{Frac}(A)$. Soit I un idéal premier de A et $B = A/I$ qui est un anneau intègre de corps de fractions L. Soit $P(X) = a_n X^n + \cdots + a_0$ un polynôme de $A[X]$ et $\overline{P}$ sa réduction modulo I. On suppose $\overline{a}_n \neq 0$ dans B. Alors, si $\overline{P}$ est irréductible sur B ou L, le polynôme P est irréductible sur K.

Gotthold Eisenstein (1823-1852)

2. Extensions de corps

Voici le véritable commencement du cours.

À partir de maintenant nous considèrerons exclusivement des anneaux *non nuls*, c'est-à-dire dans lesquels $1 \neq 0$, et ceci ne sera pas répété. Il s'ensuit que le noyau d'un morphisme d'anneaux $f : A \to B$ est un idéal distinct de A, puisque $f(1) = 1 \neq 0$. En particulier,

Si K est un corps, tout morphisme d'anneaux $f : K \to B$ est injectif

puisque $\ker(f)$, étant un idéal strict d'un corps, est nul.

2.1. Extensions de corps ; degré

Définition. Soit K un corps.

- Une *extension de corps* E/K est un morphisme de corps $i : K \to E$.
- Étant données deux extensions $E/K'/K$, on dit que K'/K est une *sous-extension* de E/K.

Rappelons qu'un morphisme de corps est toujours injectif ; on le désigne aussi parfois par le terme de *plongement*. Souvent, au lieu de se donner un morphisme injectif i on se donne simplement un sous-corps K de E et on utilise alors la notation $K \subset E$ pour désigner l'extension. Dans ce contexte, une sous-extension est notée $K \subset K' \subset E$.

Par exemple, tout corps E est une extension de son sous-corps premier E_0, qui est soit $\mathbb{Q}$ (cas de caractéristique 0) soit $\mathbb{F}_p$ pour un nombre premier p (cas de caractéristique p.)

Si E/K est une extension, on a vu que E avait une structure naturelle de K-algèbre (cf §1B.1). La dimension de E sur K en tant qu'espace vectoriel est appelée *degré de l'extension* et notée

$$[E : K] := \dim_K(E) \ \in \mathbb{N} \cup \{\infty\}.$$

Définition. On dit que E/K est *finie* si $[E : K]$ est fini, et *infinie* sinon.

Théorème de la base télescopique. Soit E/K une extension avac une K-base $\mathscr{B}_1 = (e_i)_{i\in I}$.

1. Si V est un E-espace vectoriel et $\mathscr{B}_2 = (v_j)_{j\in J}$ une E-base de v, alors $\mathscr{B} = (e_i v_j)_{i\in I, j\in J}$ est une K-base de V.
2. Si E'/E est une extension, alors E'/K est finie si et seulement si E'/E et E/K sont finies, et dans ce cas on a l'égalité
$$[E' : K] = [E' : E][E : K].$$

   Démonstration : 1. On note que V étant un E-espace vectoriel, l'expression $e_i v_j$ est comprise comme l'action du scalaire e_i sur le vecteur v_j.

   Montrons que la famille des $e_i v_j$ est génératrice. Soit $x \in V$ et $x = \sum_{j\in J'} \lambda_j v_j$ son écriture sur la base des v_j (avec J' fini). Notons $\lambda_j = \sum_{i\in I_j} \mu_{i,j} e_i$ l'écriture du scalaire $\lambda_j \in E$ sur la base des e_i (avec I_j fini). Alors

$$x = \sum_{j\in J'} \lambda_j v_j = \sum_{j\in J'} \Big(\sum_{i\in I_j} \mu_{i,j} e_i \Big) v_j = \sum_{j\in J', i\in I_j} \mu_{i,j} e_i v_j.$$

   Montrons que la famille des $e_i v_j$ est libre. Soit une combinaison K-linéaire nulle

$$\sum_{(i,j)\in T} \mu_{i,j} e_i v_j = 0,$$

indicée par une partie finie $T \subset I \times J$. Soit J' l'ensemble des j tels que l'ensemble $I_j := \{i \in I \mid (i,j) \in T\}$ est non vide ; c'est un ensemble fini car T l'est. L'égalité précédente se réécrit

$$\sum_{j\in J'} \sum_{i\in I_j} \mu_{i,j} e_i v_j = 0.$$

Comme la famille des v_j est libre, on déduit que $\sum_{i\in I_j} \mu_{i,j} e_i = 0$ pour tout j. Comme la famille des e_i est libre, on déduit que $\mu_{i,j} = 0$ pour tout (i,j).

2. La base $(e_i v_j)$ est indicée par l'ensemble produit $I \times J$. Or $I \times J$ est fini ssi I et J le sont, auquel cas on a $|I \times J| = |I| \times |J|$. Le résultat en découle. ■

Application. soit K'/K une extension de corps finis (nous étudierons les corps finis en détail dans la partie 3 du cours). Alors $\mathrm{car}(K) = \mathrm{car}(K') = p$ pour un certain nombre premier p, c'est-à-dire que le sous-corps premier est $\mathbb{F}_p$. De plus, les dimensions $m = [K : \mathbb{F}_p]$ et $n = [K' : \mathbb{F}_p]$ sont finies. La formule de la base téléscopique $[K' : \mathbb{F}_p] = [K' : K][K : \mathbb{F}_p]$ implique que m divise n. Ainsi *les sous-corps d'un corps fini à p^n éléments sont des corps à p^m éléments avec $m|n$*. Par exemple, un corps à 16 éléments n'a pas de sous-corps à 8 éléments, parce que $3 \nmid 4$.

2.2. Éléments algébriques

Notation. Soit E/K une extension de corps, et $x \in E$. On note :

- $K[x] \subset E$ la sous-algèbre de E engendrée par x,
- $K(x) \subset E$ la sous-extension de corps de E engendrée par x.

On dit qu'une extension E/K est *monogène* s'il existe $x \in E$ tel que $E = K(x)$.

D'après la propriété universelle de l'algèbre de polynômes $K[X]$ (voir §1B.2), il existe un unique morphisme de K-algèbres

$$\mathrm{ev}_x : K[X] \longrightarrow E$$

qui envoie X sur x ; explicitement on a $\mathrm{ev}_x(P) = P(x)$.

Définition. Soit E/K une extension et $x \in E$. On dit que x est

- *algébrique sur K* si $\ker(\mathrm{ev}_x) \neq (0)$,
- *transcendant sur K* sinon.

▶ Polynôme minimal

Dire que x est algébrique signifie donc qu'il existe $P \neq 0$ tel que $P(x) = 0$. Lorsque c'est le cas, comme $K[X]$ est principal, le noyau de ev_x est un idéal principal.

Définition. Soit x un élément algébrique d'une extension E/K.

- On appelle *polynôme minimal de x sur K* le polynôme unitaire générateur de $\ker(\mathrm{ev}_x)$.
- On le note $P_{x,K}$ (comme dans [Bad25]) ou parfois $\mu_{x,K}$.
- On appelle *degré de x* l'entier $\deg(x) = \deg_K(x) := \deg(P_{x,K})$.

ℹ Le cours du jeudi 29 janvier 2026 s'est arrêté ici.

Le polynôme minimal d'un élément algébrique x est aussi le polynôme unitaire de degré minimal qui annule x ; mais cette caractérisation est un peu plus faible car elle ne dit pas qu'il divise tous les polynômes annulateurs.

Supposons x algébrique. Par théorème de passage au quotient, le morphisme $\mathrm{ev}_x : k[X] \to E$ induit un isomorphisme

$$K[X]/(P_x) \xrightarrow{\sim} K[x].$$

Comme $K[x]$ est inclus dans E, c'est un anneau intègre, et il s'ensuit que (P_x) est un idéal premier donc P_x est irréductible dans $K[X]$. En résumé :

Fait. Le polynôme minimal d'un élément algébrique est irréductible.

⚠ **Le polynôme minimal $P_{x,K}$ ne dépend pas de E, mais il dépend de K.** En effet :

- soient des extensions $K \subset E \subset E'$. Alors on peut voir x comme un élément de E', et pour $P \in K[x]$ on aura ($P(x) = 0$ dans E ssi $P(x) = 0$ dans E'). Ceci montre que $P_{x,K}$ ne dépend pas du corps E dans lequel on voit x.
- soient des extensions $K \subset K' \subset E$. Alors le polynôme $P_{x,K}$ appartient à $K'[X]$ et annule x, ce qui signifie qu'il appartient au noyau du morphisme $\mathrm{ev}_{x,K'} : K'[X] \to E$. Comme ce noyau est engendré par $P_{x,K'}$ il s'ensuit que l'on a
$$P_{x,K'} \mid P_{x,K} \text{ dans } K'[X].$$
Cette relation de divisibilité est stricte en général : par exemple le polynôme minimal de i sur $\mathbb{Q}$ est $P_{x,K} = X^2 + 1$ alors que son polynôme minimal sur $\mathbb{Q}(i)$ est $P_{x,K'} = X - i$.

Remarque (sur le polynôme minimal en algèbre linéaire) : ce phénomène peut être mis en contraste avec le polynôme minimal des matrices, qui *ne dépend pas du corps* K au sens où si $M \in \mathrm{M}_n(K)$ et $K \subset K'$, on a $P_{M,K} = P_{M,K'}$. (Pour une démonstration de ce fait voir par exemple le corollaire 5.4.2 dans Cognet, *Algèbre linéaire*, Bréal (2000).) La raison de cette différence de comportement provient du fait que « changer de corps de base » n'a pas le même sens dans les deux cas : dans le cas des matrices, le changement de corps de base ne se fait pas par l'intermédiaire d'un sous-corps $K' \subset \mathrm{M}_n(K)$.

▶ **Exemple : racines de l'unité**

Définition. Pour tout corps K, on note $\mu_n(K)$ l'ensemble des racines n-ièmes de l'unité dans K. (Cet ensemble est noté $\mathbb{U}_n$ dans [Bad25].)

Lemme. Si G est un sous-groupe fini d'ordre n de $K^\times$, on a $G = \mu_n(K)$.

> **Démonstration :** D'après le théorème de Lagrange, tout élément $x \in G$ vérifie $x^n = 1$. Ainsi $G \subset \mu_n(K)$. Or les éléments de $\mu_n(K)$ sont racines du polynôme $X^n - 1$ donc sont en nombre $\leqslant n$. En conséquence, l'inclusion précédente est une égalité. ■

Ceci ne nous dit pas quand $K^\times$ possède un sous-groupe fini d'ordre n, et pas non plus que $|\mu_n(K)| = n$. En fait le nombre d'éléments de $\mu_n(K)$ dépend beaucoup du corps K. Par exemple, on a $\mu_2(\mathbb{R}) = \{\pm 1\}$ mais $\mu_n(\mathbb{R}) = \{1\}$ si n est impair (savez-vous dire pourquoi ?). Nous allons maintenant préciser la structure de ces sous-groupes finis.

Lemme. Tout sous-groupe fini du groupe multiplicatif $K^\times$ est cyclique.

> **Démonstration :** Soit G un sous-groupe fini d'ordre n de $K^\times$. On a une partition $G = \amalg_{d|n} G_d$ où G_d est l'ensemble des éléments d'ordre d dans G. Si G_d contient un élément x, on a l'inclusion $\{1, x, \dots, x^{d-1}\} \subset \mathrm{Rac}(X^d - 1)$. Comme $X^d - 1$ possède au plus d racines, l'inclusion est une égalité. En particulier tout $x \in G_d$ est dans $\{1, x, \dots, x^{d-1}\}$,

donc il y a $\varphi(d)$ tels éléments (φ est l'indicatrice d'Euler). Finalement $|G_d| = 0$ ou $\varphi(d)$. Or on sait d'après la théorie des groupes cycliques que $n = \sum_{d|n} \varphi(d)$. On en déduit que $n = |G| = \sum_{n|n} |G_d| \geqslant \sum_{n|n} \varphi(d) = n$. On doit donc avoir $|G_d| = \varphi(d)$ pour tout d. En particulier $|G_n| = \varphi(n) > 0$ donc il existe dans un G un élément d'ordre n et G est cyclique. ■

En résumé :

Corollaire. Soit K un corps.

1. Les sous-groupes finis de $K^\times$ sont les groupes $\mu_n(K)$. Ils sont cycliques.
2. Si K est fini, le groupe multiplicatif $K^\times$ est cyclique.

2.3. Extensions algébriques

Définition. On dit qu'une extension E/K est :

- *algébrique* si tous ses éléments sont algébriques sur K.
- *transcendante pure* si tout élément de $E \setminus K$ est transcendant.

Par exemple, une extension finie est algébrique, puisque $\dim K[X] = \infty$ alors que $[E : K] < \infty$.

Théorème. Soit E/K une extension. Soit $x \in E$.

1. Les conditions suivantes sont équivalentes :
   (i) x est algébrique sur K,
   (ii) $[K(x) : K]$ est fini,
   (iii) la dimension de $K[x]$ sur K est finie,
   (iv) x appartient à une sous-K-algèbre de E qui est de dimension finie sur K,
   (v) $K[x] = K(x)$ (autrement dit, $K[x]$ est un corps).
2. Si x est algébrique sur K et son polynôme minimal est de degré n, alors la dimension de $K[x] = K(x)$ sur K est n et $(1, x, x^2, \dots, x^{n-1})$ est une base de $K(x)$ sur K.

   Démonstration : 1. (i) ⇒ (ii). Si x est algébrique, l'algèbre $K[x] \simeq K[X]/(P_x)$ est intègre et de dimension finie $n = \deg(P_x)$, c'est donc un corps. Elle est donc égale à son corps de fractions : $K[x] = K(x)$, et on a $[K(x) : K] = n < \infty$.
   (ii) ⇒ (iii). On a $K[x] \subset K(x)$ donc $\dim_K K[x] \leqslant [K(x) : K]$ finie par hypothèse.
   (iii) ⇒ (iv). En effet, x appartient à $K[x]$.
   (iv) ⇒ (v). Soit A une sous-algèbre de E de dimension finie sur K. Alors $K[x] \subset A \subset E$ est intègre, de dimension finie, donc un corps.
   (v) ⇒ (i). Si x n'est pas algébrique, le morphisme ev_x induit un isomorphisme $K[X] \simeq K[x]$ or l'algèbre de polynômes $K[X]$ n'est pas un corps.

   2. Nous savons que $K[x] \simeq K[X]/(P_x)$ et nous avons vu au §1B.3, comme corollaire de la division euclidienne, que l'algèbre quotient $K[X]/(P_x)$ a pour base $(1, \bar{X}, \bar{X}^2, \dots, \bar{X}^{n-1})$. L'image de cette base dans $K[x]$ est $(1, x, x^2, \dots, x^{n-1})$. ■

Corollaire. Si E/K est finie, tout élément de E est algébrique sur K.

Démonstration : L'entier $[K(x) : K] \leqslant [E : K]$ est fini. ■

Corollaire. Soit E/K une extension de corps.

1. Si $x, y \in E$ sont algébriques sur K, alors $x + y$ et xy sont algébriques sur K.
2. Les éléments de E qui sont algébriques sur K forment un corps appelé *clôture algébrique de* K

dans E.

Démonstration : 1. Puisque y est algébrique sur K, il est aussi algébrique sur $K(x)$. Donc les degrés $[K(x) : K]$ et $[K(x)(y) : K(x)]$ sont finis par le théorème précédent. Par le théorème de la base téléscopique, $[K(x)(y) : K]$ est alors finie. Donc $x + y$ et xy sont contenus dans une extension finie de K, ils sont donc algébriques par le corollaire précédent.

2. Si $x \in E \setminus \{0\}$ est algébrique sur K, alors $K(x)/K$ est finie, et comme $x^{-1} \in K(x)$ on voit que x^{-1} est algébrique par le corollaire précédent. L'ensemble des éléments de E qui sont algébriques sur K est non vide parce qu'il contient K, c'est donc un sous-corps puisqu'il est stable par somme, produit et passage à l'inverse. ■

Corollaire. Soit E/K une extension. Supposons qu'un polynôme irréductible $P \in K[X]$ a une racine dans E. Alors $\deg(P)$ divise $[E : K]$.

Démonstration : Soit $x \in E$ une racine de P. Comme P est irréductible, il est égal au polynôme minimal de x, donc $K(x) \simeq K[X]/(P)$. D'après le théorème de la base téléscopique, on a $[E : K] = [E : K(x)][K(x) : K] = [E : K(x)] \deg(P)$. ■

Corollaire. Soit E/K une extension et soient $x, y \in E$ des éléments algébriques de degrés m, n premiers entre eux. Alors $[K(x, y) : K] = mn$.

Démonstration : Notons $d = [K(x, y) : K]$.

- Par la base téléscopique, les entiers $m = [K(x) : K]$ et $n = [K(y) : K]$ divisent d. Comme ils sont premiers entre eux, le produit mn divise d.
- D'un autre côté, comme $P_{x,K(y)}$ divise $P_{x,K}$ on a $[K(x, y) : K(y)] = \deg P_{x,K(y)} \leqslant \deg P_{x,K} = [K(x) : K]$. On en déduit que
$$d = [K(x, y) : K(y)][K(y) : K] \leqslant [K(x) : K][K(y) : K] = mn.$$
- De $mn|d$ et $d \leqslant mn$ découle que $d = mn$. ■

Théorème des extensions algébriques.

1. Toute extension finie est algébrique.
2. Une extension engendrée par un nombre fini d'éléments algébriques est finie.
3. Une extension engendrée par des éléments algébriques est algébrique.
4. Une extension algébrique d'une extension algébrique est algébrique : si E/K et E'/E sont algébriques, alors E'/K est algébrique.

Démonstration : 1. a déjà été vu.

2. On montre par récurrence qu'une extension engendrée par n éléments algébriques est finie. Pour $n = 0$ il n'y a rien à démontrer. Pour $n \geqslant 1$ notons $E = K(x_1, \dots, x_n)$ où les x_i sont algébriques sur K. Posons $K' = K(x_1, \dots, x_{n-1})$. Comme x_n est algébrique sur K, il l'est aussi sur K'. Par l'hypothèse de récurrence les extensions K'/K et E/K' sont finies, donc E/K est finie.

3. Soit E/K une extension engendrée par un ensemble $J \subset E$ d'éléments algébriques sur K. Soit U la clôture algébrique de K dans E. Alors U est un corps d'après l'un des corollaires situés juste au-dessus. Or U contient J, donc $U = E$ ce qui montre que tous les éléments de E sont algébriques sur K.

4. Soit $x \in E'$. Soit $P_x(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$ le polynôme minimal de x sur E. Les coefficients a_i sont dans E donc algébriques sur K par hypothèse. D'après le point 2, ils

engendrent donc une extension finie $U := K(a_0, a_1, \dots, a_{n-1})$ de K. Maintenant, x est algébrique sur U, parce que le polynôme P_x, qui s'annule en x, a ses coefficients dans U. Donc $U(x)/U$ est finie. Par le théorème de la base télescopique appliqué à $K \subset U \subset U(x)$, l'extension $U(x)/K$ est finie. Donc x est algébrique sur K parce qu'il est contenu dans une extension finie de K. ■

2.4. Corps de rupture, corps de décomposition

Dans ce paragraphe nous allons introduire deux corps priviligiés dans lesquels un polynôme acquiert une ou des racines.

▶ Corps de rupture

Définition. Soit $P \in K[X]$ un polynôme irréductible. On appelle *corps de rupture* de P sur K une extension K_P/K telle que P possède une racine x dans K_P, et cette racine engendre E, c'est-à-dire que $K_P = K(x)$.

ℹ Le cours du mardi 10 février 2026 s'est arrêté ici.

Théorème d'existence et unicité à isomorphisme près du corps de rupture. Soient $P \in K[X]$ un polynôme irréductible. Alors $K_P := K[X]/(P)$ est un corps de rupture de P sur K, et tout corps de rupture est K-isomorphe à K_P.

Démonstration : Considérons le corps $K_P = K[X]/(P)$ et le morphisme de quotient $\pi : K[X] \to K_P$. Notons $\alpha = \pi(X)$ l'image de X dans K_P. Par construction on a $P(X) \in \ker(\pi)$, donc $P(\alpha) = P(\pi(X)) = \pi(P(X)) = 0$. Maintenant soit E' un autre corps de rupture, avec une racine $x' \in E'$. Le morphisme de K-algèbres $f : K[X] \to E'$ qui envoie X sur x' envoie $P(X)$ sur $P(x') = 0$, donc il passe au quotient en un K-morphisme $K[X]/(P) \to E'$. Comme x' engendre E', ce morphisme est surjectif. Comme tout morphisme de corps, il est injectif. C'est donc un isomorphisme. ■

Notation. Pour tout polynôme irréductible $P \in K[X]$, on notera $\mathrm{Rup}_K(P)$ un corps de rupture de P sur K. Il est bien défini à isomorphisme près.

Lemme (propriétés de K_P). Soit K_P un corps de rupture et $x \in K_P$ une racine de P. Alors on a les propriétés suivantes :

1. Pour toute paire (K', x') composée d'une extension K'/K et une racine x' de P, il existe un unique morphisme $f : K_P \to K'$ tel que $f(x) = x'$.
2. Si une sous-extension $K' \subset K_P$ contient une racine de P, alors $K' = K_P$.

Démonstration : 1. Le morphisme de K-algèbres $u : K[X] \to K'$ qui envoie X sur x' envoie $P(X)$ sur $P(x') = 0$, donc il passe au quotient en un K-morphisme $f = \bar{u} : K[X]/(P) \to K'$ qui envoie x sur x'. Comme x engendre K_P, ce morphisme est unique.
2. Soit $K' \subset K_P$ une sous-extension qui contient une racine x' de P. D'après le point 1 il existe un morphisme $f : K_P \to K'$ tel que $f(x) = x'$. Comme tout morphisme de corps, le composé $K_P \to K' \hookrightarrow K_P$ est injectif. Comme K_P est de dimension finie sur K, ce morphisme est donc un isomorphisme. Il s'ensuit que $K' = K_P$. ■

Dans le livre [Bad25] c'est la propriété 2 du lemme ci-dessus qui est prise pour définition d'un corps de rupture : voir [Bad25, Déf. 5.4.1]. Bien sûr, il en résulte une définition équivalente.

Exemples.

1. Le sous-corps $\mathbb{Q}(i)$ de $\mathbb{C}$ est un corps de rupture de X^2+1 sur $\mathbb{Q}$. Il contient deux racines du polynôme et a donc deux $\mathbb{Q}$-automorphismes (corollaire 5.6).
2. Le polynôme $P(X) = X^3 - 2 \in \mathbb{Q}[X]$ a trois corps de rupture inclus dans $\mathbb{C}$: $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$, où $j := e^{2i\pi/3}$. Ils sont distincts (par exemple le premier est inclus dans $\mathbb{R}$, les deux autres non), isomorphes entre eux, et $\mathbb{Q}$-isomorphes à $\mathbb{Q}[X]/(X^3-2)$. Chacun de ces corps contient une seule racine de P.

Remarque. Si P n'est pas irréductible, il n'y a pas de notion utile de corps de rupture. Par exemple si $\deg(P) = 0$ (c'est-à-dire P constant non nul), il n'y a simplement aucune extension de K qui contient une racine de P. Si $\deg(P) \geqslant 1$ et P n'est pas irréductible, notons $P = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ sa décomposition en facteurs irréductibles. Alors l'un quelconque des corps $K_{P_i} = K[X]/(P_i)$ est une extension de K sur laquelle P acquiert une racine, mais les K_{P_i} ne sont pas isomorphes entre eux. On voit qu'on a encore la possibilité de trouver des corps sur lesquels P admet une racine x et qui sont engendrés par cette racine, mais on perd l'unicité à K-isomorphisme près.

▶ Corps de décomposition

Définition. Soit $P \in K[X]$ un polynôme non nul. On appelle *corps de décomposition* de P sur K une extension E_P/K telle que P est scindé dans E_P et ses racines engendrent E_P. On rencontre aussi parfois les terminologies *corps de scindement* et *corps des racines*.

Explicitement cela signifie que $P = \lambda \prod_{i=1}^{n}(X - x_i)$ avec $x_i \in E_P$, et que $E_P = K(x_1, \ldots, x_r)$.

Exemples.

1. Le sous-corps $\mathbb{Q}(i)$ de $\mathbb{C}$ est un corps de décomposition de X^2+1 sur $\mathbb{Q}$.
2. Le corps $\mathbb{Q}(\sqrt[3]{2}, j)$, avec $j := e^{2i\pi/3}$, est un corps de décomposition de X^3-2 sur $\mathbb{Q}$.

Lemme (extensions de scindement). Soit $P \in K[X]$ un polynôme de degré $n \geqslant 1$.

1. Si E est une extension de K sur laquelle P est scindé, alors E contient un et un seul corps de décomposition de P.
2. Il existe une extension E/K telle que P est scindé sur E. De plus, on peut choisir E de façon à ce que $[E : K] \leqslant n!$.

   Démonstration : 1. Comme P est scindé dans E, on a $P = \lambda \prod_{i=1}^{n}(X - x_i)$. Pour qu'un sous-corps $E' \subset E$ soit un corps de décomposition de P, il faut et il suffit qu'il contienne les x_i et que ceux-ci l'engendrent. Autrement dit $E' = K(x_1, \ldots, x_n)$ convient et c'est le seul possible.
   2. On fait une récurrence sur n. Si $n = 1$ on a $P = \lambda(X - x_1)$ avec $\lambda, x_1 \in K$ donc $E = K$ convient. Supposons $n \geqslant 2$ et le résultat démontré pour les polynômes de degré $\leqslant n-1$. Soit E_1 un corps de rupture pour P, donc $P = (X - x_1)Q$ dans $E_1[X]$. Par l'hypothèse de récurrence, il existe une extension E/E_1 telle que Q est scindé dans E et $[E : E_1] \leqslant (n-1)!$. Cette extension scinde P et $[E : K] = [E : E_1][E_1 : K] \leqslant n!$. ■

Théorème d'existence et unicité à isomorphisme près du corps de décomposition. Soient $P \in K[X]$ un polynôme. Alors, il existe un corps de décomposition E_P tel que $[E_P : K] \leqslant n!$. De plus, tout corps de décomposition de P est isomorphe à E_P.

Démonstration : D'après le lemme précédent, il existe une extension E/K telle que P est scindé sur E et les racines de P dans E engendrent une sous-extension qui est un corps de décomposition satisfaisant $[E_P : K] \leqslant [E : K] \leqslant n!$.

Pour démontrer la deuxième assertion, soient E, F deux corps de décomposition de P sur

K. Considérons l'ensemble des sous-extensions $L \subset E$ qui sont la source d'un K-morphisme $L \to F$. Cet ensemble est non vide car il contient K. De plus, les dimensions $[L : K]$ sont bornées par $[F : K]$ donc il existe un élément $L' \subset E$ de dimension maximale. On dispose d'un K-morphisme $f : L' \to F$; il fait de F une L'-algèbre. Nous allons montrer que $L' = E$.

Supposons par l'absurde que $L' \neq E$. Puisque F est engendré par les racines de P, le polynôme P n'est pas scindé sur L'. Il existe donc une racine $x \in F$ de P qui n'appartient pas à (l'image par f de) L'. Soit $Q := P_{x,L'}$ le polynôme minimal de x sur U et $L'(x) := L'[X]/(Q)$ le corps de rupture de Q sur L. Alors Q divise $P_{x,K}$ qui divise P (parce que $P(x) = 0$), donc $Q \mid P$ dans $L'[X]$. Comme P est scindé sur F, alors Q l'est aussi donc il possède une racine y dans F. D'après le lemme ci-dessus (propriétés de K_P), il existe un morphisme de L'-extensions $f' : L'(x) \to F$ qui envoie x sur y. Ceci contredit le fait que L' est de dimension maximale.

Il s'ensuit qu'il existe un morphisme $E \to F$. En particulier $[E : K] \leqslant [F : K]$. Par le même raisonnement, il existe un morphisme $F \to E$ donc $[F : K] \leqslant [E : K]$. Finalement E et F sont K-isomorphes. ■

Notation. Pour tout polynôme $P \in K[X]$, on notera $\mathrm{Dec}_K(P)$ un corps de décomposition de P sur K. Il est bien défini à isomorphisme près.

▶Différences entre corps de rupture et corps de décomposition

1. Le corps de rupture de P est défini seulement si P est irréductible, tandis que le corps de décomposition est défini pour tout P non nul (nous avons discuté dans une remarque précédente des difficultés que pose le corps de rupture si P n'est pas irréductible).
2. On dispose d'une expression explicite $K_P = K[X]/(P)$ pour le corps de rupture, mais pas pour le corps de décomposition. En particulier, la dimension du corps de rupture de P est toujours $\deg(P)$ mais on n'a aucune formule générale pour la dimension du corps de décomposition.
3. Dans une extension E/K donnée, il y a au plus un corps de décomposition de P dans E alors qu'il peut y avoir plusieurs corps de rupture. Par exemple, le polynôme $X^3 - 2 \in \mathbb{Q}[X]$ a trois corps de rupture dans $\mathbb{C}$ mais un seul corps de décomposition, à savoir $\mathbb{Q}(\sqrt[3]{2}, j)$.

2.5. Corps algébriquement clos, clôture algébrique

L'énoncé suivant servira à caractériser la notion de corps algébriquement clos.

Théorème. Si K est un corps, les assertions suivantes sont équivalentes :

1. les polynômes irréductibles de $K[X]$ sont les polynômes de degré 1,
2. tout polynôme non constant à coefficients dans K est scindé sur K,
3. tout polynôme non constant à coefficients dans K admet une racine dans K,
4. si K' est un corps qui contient K et tel que K'/K est algébrique, alors $K' = K$.

Démonstration : 1 ⇒ 2. Soit $P \in K[X]$ non constant. Dans la décomposition de P en facteurs irréductibles, les facteurs sont tous de degré 1 donc P est scindé.
2 ⇒ 3. Tout polynôme non constant scindé possède une racine.
3 ⇒ 4. Soit $x \in K'$ et $P = P_{x,K}$ son polynôme minimal. Par hypothèse, il possède une racine $a \in K$, donc $X - a | P$. Comme P est irréductible, on déduit que $P = X - a$. De $P(x) = 0$ on déduit que $x = a \in K$. Ainsi $K' = K$.
4 ⇒ 1. Soit $P \in K[X]$ un polynôme irréductible et $n = \deg(P)$. Alors $K' = K[X]/(P)$ est une extension du corps K, finie de degré n donc algébrique. De l'hypothèse on déduit que

$K' = K$, donc $n = 1$. ■

Définition. Soit E/K une extension. On dit que :

- K est *algébriquement clos* s'il vérifie les conditions équivalentes du théorème précédent.
- E est une *clôture algébrique de* K si E est algébriquement clos et si E/K est algébrique.

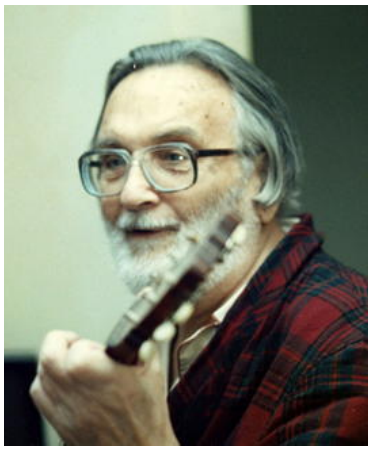
Nous allons démontrer (théorème ci-dessous) qu'une clôture algébrique existe et est unique à K-isomorphisme près. Nous nous appuierons sur le lemme de Zorn, résultat classique de théorie des ensembles, équivalent à l'axiome du choix, utilisé en algèbre notamment pour démontrer que tout idéal $I \neq A$ d'un anneau commutatif est inclus dans un idéal maximal. Rappelons la définition des termes de l'énoncé. Dans un ensemble ordonné $(E, \leqslant)$, on appelle :

- *chaîne* une partie $A \subset E$ telle que $(A, \leqslant)$ est totalement ordonné,
- *majorant* de A dans E un élément $m \in E$ tel que $a \leqslant m$ pour tout $a \in A$,
- *élément maximal* un élément $M \in E$ qui n'est majoré strictement par aucun élément de E, c'est-à-dire que $M \leqslant M' \Rightarrow M = M'$,
- *ensemble inductif* un ensemble ordonné $(E, \leqslant)$ dans lequel toute chaîne est majorée.

Lemme de Zorn. Tout ensemble inductif admet un élément maximal.

Références : pour des détails et une démonstration, nous renvoyons aux livres :

- Paul Halmos,: *Introduction à la théorie des ensembles*, Jacques Gabay, 2000. Voir le chap. 16, accessible ici.
- Jean-Pierre Ramis et André Warusfel : *Tout en un pour la Licence 1*, 4ème éd., Dunod, 2022. Voir les §5.3 et §6.1.3, accessibles ici (ne contient pas de démonstration).




Max Zorn (1906-1993) et Paul Halmos (1916-2006)

▶ Existence de la clôture algébrique

Nous utiliserons un petit lemme qui estime le cardinal d'une extension algébrique. Nous noterons indifféremment $\mathrm{card}(X)$ ou $|X|$ le cardinal d'un ensemble X.

Lemme. Soit E/K une extension algébrique. Notons $\aleph_0$ le cardinal de $\mathbb{N}$. Alors, on a :

$$\mathrm{card}(E) \leqslant \max(\aleph_0, \mathrm{card}(K)).$$

Démonstration : Si K est fini, alors E est au plus dénombrable, c'est-à-dire que $|E| \leqslant \aleph_0$ donc la conclusion est vérifiée. Supposons maintenant K infini. Nous avons besoin de quelques résultats standard sur les cardinaux des ensembles infinis. Notamment, en page 183 du livre de R. Cori et D. Lascar, *Logique mathématique*, tome 2, Dunod (accessible ici) on

trouve :

1. Si X et Y sont des ensembles non vides dont l'un au moins est infini, alors
$$\mathrm{card}(X \times Y) = \mathrm{card}(X \cup Y) = \sup(\mathrm{card}(X), \mathrm{card}(Y)).$$
2. Si $(X_i, i \in I)$ est une famille d'ensembles et si l'un des X_i est infini, alors
$$\mathrm{card}\Big(\bigcup_{i\in I} X_i \Big) \leqslant \sup\Big(\sup\{\mathrm{card}(X_i),\ i \in I\}, \mathrm{card}(I) \Big).$$

Le point 1 entraine que le cardinal de l'ensemble $K_n[X]$ des polynômes de degré n est égal au cardinal de K. Le point 2 entraine alors que le cardinal de $K[X]$ est égal au cardinal de K. Notons maintenant $E(P)$ l'ensemble des éléments de E de polynôme minimal égal à P. Comme $E = \amalg_{P\in K[X]} E(P)$ et chaque $E(P)$ est fini (de cardinal majoré par $\deg(P)$), le point 2 entraine que $|E| \leqslant |K[X]| = |K|$. Donc la conclusion est vérifiée. ■

ℹ Le cours du mardi 17 février 2026 s'est arrêté ici.

Théorème. Tout corps K possède une clôture algébrique.

Démonstration : L'idée de la construction est de produire des extensions K_P/K en ajoutant des racines de tous les polynômes $P \in K[X]$ et d'en prendre une sorte de « réunion ». Cette dernière opération pose des problèmes de théorie des ensembles : dispose-t-on d'un ensemble ambiant dans lequel prendre la réunion ? Quelle est la taille de l'ensemble d'indices de la réunion ? Pour contourner ces problèmes, nous allons plonger toutes les K_P dans un ensemble S assez grand, puis nous utiliserons le lemme de Zorn. Allons-y.

Soit S un ensemble tel que d'une part $K \subset S$, et d'autre part
$$\mathrm{card}(S) > C := \max(\aleph_0, \mathrm{card}(K)).$$
(Par exemple $S = K \amalg \mathscr{P}(\mathbb{N} \amalg K)$ convient, où $\mathscr{P}(-)$ désigne l'ensemble des parties.) Notons $\mathscr{E}$ l'ensemble des triplets $(L, +, \times)$ composés d'une partie L de S contenant K et d'une structure de corps sur L telle que $K \subset L$ est une extension algébrique de corps. On introduit un ordre sur $\mathscr{E}$ en posant $L_1 \leqslant L_2$ ssi $L_1 \subset L_2$ est un sous-corps. L'ensemble $\mathscr{E}$ est inductif, car toute chaîne $(L_i)_{i\in I}$ est majorée par la réunion $M := \cup_{i\in I} L_i$. Par le lemme de Zorn, il existe un élément maximal $L_0 \in \mathscr{E}$. Pour montrer que L_0 est une clôture algébrique de K, supposons qu'il existe un polynôme non constant $f \in L_0[X]$ qui n'a aucune racine dans L_0. Notons L'/L_0 le corps de rupture de f. Comme L'/K est algébrique, le lemme juste au-dessus montre que $\mathrm{card}(L') \leqslant C < \mathrm{card}(S)$. On en déduit qu'il existe une injection $i : L' \to S$ telle que $i(x) = x$ pour $x \in L_0$. Par transport de structure depuis L', on peut munir la partie $i(L')$ d'une structure de corps qui étend celle de L_0 et obtenir ainsi un élément de $\mathscr{E}$ qui est plus grand que L_0. C'est une contradiction. ■

2.6. Prolongements des morphismes de corps

La démonstration de l'unicité de la clôture algébrique à K-isomorphisme près s'appuiera sur l'énoncé suivant.

Théorème de prolongement. Soient E/K une extension algébrique et C un corps algébriquement clos. Alors tout morphisme $K \to C$ se prolonge en un morphisme $E \to C$.

Démonstration : Soit $\iota : K \to C$ un plongement. Soit $\mathscr{E}$ l'ensemble des couples (L, l) tels que L est une extension de K incluse dans E et $l : L \to C$ est un plongement de L dans C qui prolonge ι. L'ensemble $\mathscr{E}$ est non vide parce qu'il contient (K, ι). On définit une relation d'ordre sur $\mathscr{E}$ en posant $(L, l) \leqslant (L', l')$ ssi $L \subset L'$ et l' prolonge l. Montrons que $\mathscr{E}$ est inductivement ordonné. Soit $(L_i, l_i)_{i\in I}$ une famille totalement ordonnée d'éléments de $\mathscr{E}$.

Montrons qu'elle est majorée. Soit L_∞ la réunion de tous les corps L_i, $i \in I$. Il est facile de vérifier que L_∞ est un corps. Soit $x \in L_\infty$. Alors il existe $i_0 \in I$ tel que $x \in L_{i_0}$. On pose $l_\infty(x) := l_{i_0}(x) \in C$. Montrons que cette définition de $l_\infty(x)$ ne dépend pas du choix de i_0. Si $x \in L_j$ avec $j \neq i_0$, alors on a $i_0 < j$ ou $j < i_0$; alors soit l_j prolonge l_{i_0}, soit l_{i_0} prolonge l_j, ce qui montre que $l_j(x) = l_{i_0}(x)$. On obtient ainsi une application $l_\infty : L_\infty \to C$. Il est immédiat que l_∞ est un morphisme de corps, et que (L_∞, l_∞) est un élément majorant pour la suite des $(L_i, l_i)_{i\in I}$.

Puisque $\mathscr{E}$ est inductivement ordonné, le lemme de Zorn implique qu'il existe un élément maximal $(L_{\max}, l_{\max})$ dans $\mathscr{E}$. Il nous suffit de montrer que $L_{\max} = E$.

Supposons par l'absurde que $L_{\max} \neq E$. Soit K' l'image de $L_{\max}$ par $l_{\max}$. Alors K' est une extension de $\iota(K)$ dans C. Soit x un élément de $E \setminus L_{\max}$. Cet élément est algébrique sur K donc sur $L_{\max}$. Soit P_x le polynôme minimal de x sur $L_{\max}$. L'isomorphisme $l_{\max} : L_{\max} \to K'$ se prolonge de façon unique en un isomorphisme de K-algèbres de $L_{\max}[X]$ dans $K'[X]$ en posant $X \mapsto X$, isomorphisme qu'on note toujours $l_{\max}$. Alors $l_{\max}(P_x)$ est un polynôme irréductible de $K'[X]$. Puisque C est algébriquement clos, $l_{\max}(P_x)$ a une racine y dans C. De plus $l_{\max}(P_x)$ est le polynôme minimal de y sur K', parce qu'il est unitaire et irréductible. On a alors des K-isomorphismes

$$L_{\max}(x) \simeq L_{\max}[X]/(P_x) \simeq K'[X]/(l_{\max}(Px)) \simeq K'(y).$$

Alors $L_{\max}(x) \simeq K'(y)$ est un morphisme de $L_{\max}(x)$ dans C qui prolonge $l_{\max}$, ce qui contredit la maximalité de $(L_{\max}, l_{\max})$ dans $\mathscr{E}$. ■

▶ Unicité de la clôture algébrique

Corollaire. Deux clôtures algébriques de K sont K-isomorphes.

Démonstration : Soient $\overline{K}_1$ et $\overline{K}_2$ deux clôtures algébriques de K. Comme $\overline{K}_1/K$ est algébrique et $\overline{K}_2$ est algébriquement clos, d'après le théorème précédent le morphisme $K \to \overline{K}_2$ se prolonge en un K-morphisme $f : \overline{K}_1 \to \overline{K}_2$. Comme $\overline{K}_2/K$ est algébrique, alors $\overline{K}_2/\overline{K}_1$ l'est également. Comme $\overline{K}_1$ est algébriquement clos, il s'ensuit que f est un isomorphisme (voir les caractérisations données dans le théorème du début du §2.5). ■

▶ Autres conséquences du théorème de prolongement

Notons $\overline{K}$ la clôture algébrique de K, unique à K-isomorphisme près. Voici d'autres conséquences du théorème de prolongement, les deux premières étant des reformulations de la propriété de la clôture algébrique :

1. (Minimalité) En prenant $E = \overline{K}$, le théorème affirme que tout morphisme de K vers un corps algébriquement clos C se factorise par $\overline{K}$. Ceci signifie que $\overline{K}$ *est une extension algébriquement close de* K *qui est minimale*.
2. (Maximalité) En prenant $C = \overline{K}$, le théorème affirme que toute extension $K \hookrightarrow E$ qui est algébrique possède un plongement $E \hookrightarrow \overline{K}$. Ceci signifie que $\overline{K}/K$ *est une extension algébrique qui est maximale*.
3. (Extension des morphismes à la clôture algébrique) Toute extension de corps $K \hookrightarrow L$ s'étend en une extension de clôtures alébriques $\overline{K} \hookrightarrow \overline{L}$.

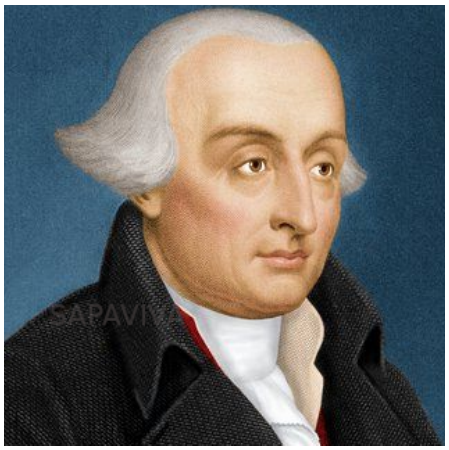
Exemple d'application. Voici un exemple de deux corps non isomorphes K et L tels qu'il existe des morphismes $K \hookrightarrow L$ et $L \hookrightarrow K$. On part du corps de fractions rationnelles en une infinité dénombrable de variables $k = \mathbb{Q}(X_1, X_2, X_3, \ldots)$, puis :

- $K := \overline{k}$, une clôture algébrique de k,
- $L := K(X_0)$, le corps des fractions rationnelles sur K en une variable.

On a une inclusion évidente $K \to L$. Pour construire un morphisme dans l'autre sens, on s'inspire de l'astuce de l'hôtel de Hilbert : on considère le morphisme $k \to k$ défini par $X_1 \mapsto X_2$, $X_2 \mapsto X_3$, etc. D'après le théorème de prolongement, ce morphisme s'étend aux clôtures algébriques en un morphisme $\varphi : K \to K$ qui envoie X_i sur X_{i+1} pour tout i. Comme X_1 est transcendant sur $\mathbb{Q}(X_2, X_3, \ldots)$, le morphisme $K[X_0] \to K$ qui étend φ en envoyant X_0 sur X_1 est injectif, et il s'étend au corps de fractions en un morphisme $K(X_0) \to K$. C'est le morphisme $L \to K$ espéré.

Annexe. Le corps des complexes est algébriquement clos

Nous allons démontrer que le corps $\mathbb{C}$ est algébriquement clos, par une méthode due à Lagrange.



Joseph-Louis Lagrange (1736-1813)

Nous établissons quelques lemmes préparatoires avant la démonstration.

Lemme 1. Tout polynôme $P \in \mathbb{R}[X]$ de degré impair possède une racine réelle.

> **Démonstration :** On peut supposer P unitaire. Alors $\lim_{x\to+\infty} P(x) = +\infty$ et $\lim_{x\to-\infty} P(x) = -\infty$. D'après le théorème des valeurs intermédiaires, P possède une racine réelle. ■

Lemme 2. Tout polynôme complexe $P = aX^2 + bX + c$ de degré 2 est scindé dans $\mathbb{C}$.

> **Démonstration :** Par la mise sous forme canonique du trinôme, on se ramène à montrer que le discriminant Δ possède une racine carré dans $\mathbb{C}$. Notons $\Delta = \alpha + i\beta$ et cherchons une racine carrée $\delta = x + iy$. L'équation $\delta^2 = \Delta$ fournit une égalité de parties réelles, une égalité de parties imaginaires et une égalité de modules :
>
> $$\begin{cases} x^2 - y^2 = \alpha \\ 2xy = \beta \\ x^2 + y^2 = \sqrt{\alpha^2 + \beta^2} \end{cases}$$
>
> On en déduit que $x^2 = \frac{1}{2}(\alpha + \sqrt{\alpha^2 + \beta^2})$ et $y^2 = \frac{1}{2}(-\alpha + \sqrt{\alpha^2 + \beta^2})$ avec la condition $2xy = \beta$ qui dit que x et y sont de même signe (si $\beta \geqslant 0$) ou de signe opposé (si $\beta < 0$). On trouve les deux solutions en extrayant les racines carrées réelles de $x^2 = \ldots$ et $y^2 = \ldots$ et en faisant attention aux signes. (La lectrice complètera les détails !) ■

Théorème fondamental de l'algèbre (d'Alembert, Gauss).
Tout polynôme non constant à coefficients complexes possède une racine.

Démonstration : Soit $P \in \mathbb{C}[X]$ on constant. Posons $F(X) = P(X)\bar{P}(X)$ où $\bar{P}$ est obtenu en prenant les complexes conjugués des coefficients de P. Alors $F \in \mathbb{R}[X]$ et si on sait trouver une racine pour F, on aura une racine a pour P ou pour $\bar{P}$, et alors $\bar{a}$ est une racine pour P. Donc il suffit de démontrer que F possède une racine complexe ; nous pouvons supposer F unitaire. Notons son degré

$$d = 2^n q$$

avec q impair. Nous faisons une récurrence sur n, la valuation 2-adique de d. Si $n = 0$, le degré d est impair et le lemme 1 affirme que F possède une racine réelle. Supposons maintenant que $n \geqslant 1$. Notons $K'/\mathbb{C}$ une extension de scindement de F. Dans K' on a une factorisation $F(X) = \prod_{i=1}^{d}(X - x_i)$ avec $x_i \in K'$. D'après les formules de Viète (relations coefficients-racines), les fonctions symétriques élémentaires en les x_i sont les coefficients de F, qui sont réels.

Pour un réel quelconque c, posons $y_{ij} = x_i + x_j + cx_ix_j$ pour $i \leqslant j$. Ces éléments sont en nombre $\frac{1}{2}d(d+1) = 2^{n-1}q(d+1)$ avec $q(d+1)$ est impair. Introduisons le polynôme

$$G(X) := \prod_{i \leqslant j}(X - y_{ij}).$$

Ses coefficients sont des fonctions des x_i qui sont des polynômes symétriques à coefficients réels en les x_i. D'après le Théorème fondamental des fonctions symétriques rappelé en annexe ci-dessous, ce sont donc des polynômes à coefficients réels en les $\sigma_i(x_1, \dots, x_d)$, qui sont réels (on l'a vu plus haut). En résumé on a $G \in \mathbb{R}[X]$ avec un degré de valuation 2-adique $n-1$. Par l'hypothèse de récurrence, ce polynôme admet une racine $z_c \in \mathbb{C}$. Puisqu'on connait les racines de G, il existe $i(c), j(c)$ tels que $y_{i(c),j(c)} = z_c$.

Comme $\mathbb{R}$ est infini, l'application $\mathbb{R} \to \{1, \dots, d\}^2$, $c \mapsto (i(c), j(c))$ n'est pas injective donc il existe $c \neq d$ tels que $i(c) = i(d) = r$ et $j(c) = j(d) = s$. On trouve un système en les inconnues $S = x_r + x_s$ et $P = x_r x_s$:

$$\begin{cases} x_r + x_s + cx_r x_s = z_c \\ x_r + x_s + dx_r x_s = z_d \end{cases}$$

Ce système de déterminant $d - c \neq 0$ est inversible et fournit S, P en fonction des complexes z_c, z_d. Le lemme 2 permet de trouver les solutions de l'équation $X^2 - SX + P = 0$ dans $\mathbb{C}$. Ces solutions sont x_r et x_s. ■

▶ Annexe : théorème fondamental des fonctions symétriques

On rappelle que pour un entier $n \geqslant 1$, le groupe symétrique S_n agit sur l'anneau $A[X_1, \dots, X_n]$ des polynômes en n variables à coefficients dans A en permutant les variables :

$$(\sigma \cdot P)(X_1, \dots, X_n) := P(X_{\sigma(1)}, \dots, X_{\sigma(n)}).$$

On dit que P est *symétrique* si $\sigma \cdot P = P$ pour tout $\sigma \in S_n$. On note

$$A[X_1, \dots, X_n]^{S_n} := \left\{ P \in A[X_1, \dots, X_n] \mid \sigma \cdot P = P \text{ pour tout } \sigma \in S_n \right\}$$

le sous-ensemble des polynômes symétriques, qui est un sous-anneau (et même une sous-A-algèbre). L'exemple fondamental de polynôme symétrique est la *fonction symétrique élémentaire en n variables et de degré k*, définie comme la somme des $\binom{n}{k}$ produits des X_i pris k par k :

$$\sigma_k^n := \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} X_{i_1} \cdots X_{i_k}.$$

Lorsque le nombre de variables n est clair d'après le contexte, on note σ_k au lieu de σ_k^n. Par exemple, $\sigma_1 = X_1 + \cdots + X_n$ et $\sigma_n = X_1 \cdots X_n$.

Théorème. Soit A un anneau et $n \geqslant 1$ un entier. Pour tout polynôme symétrique $P \in A[X_1, \dots, X_n]$, il existe un unique polynôme $Q \in A[T_1, \dots, T_n]$ tel que $P(X_1, \dots, X_n) = Q(\sigma_1, \dots, \sigma_n)$.

Autrement dit, le morphisme d'anneaux $f : A[T_1, \dots, T_n] \to A[X_1, \dots, X_n]$ tel que $f(T_k) = \sigma_k$ induit un isomorphisme $A[T_1, \dots, T_n] \simeq A[X_1, \dots, X_n]^{S_n}$.

> **Démonstration :** Pour l'application dans ce cours, nous n'avons besoin que de l'existence, donc nous laisserons la démonstration de l'unicité à la lectrice (elle s'obtient en scrutant la démonstration de l'existence). Nous utiliserons la formule $\sigma_k^n = \sigma_{k-1}^{n-1} \cdot X_n + \sigma_k^{n-1}$, qui s'obtient en séparant les monômes qui contiennent X_n et ceux qui ne le contiennent pas.
> Pour un polynôme $P \in A[X_1, \dots, X_n]$, notons d son degré total, égal au maximum des degrés totaux des monômes $\deg_{\text{tot}}(X_1^{d_1} \cdots X_n^{d_n}) = d_1 + \cdots + d_n$.
> Nous démontrons le théorème par récurrence sur l'entier $n + d$. Si $n + d = 1$, c'est-à-dire $n = 1$ et $d = 0$, le polynôme P est constant et il n'y a rien à démontrer. Supposons $n + d \geqslant 2$. Posons $Q(X_1, \dots, X_{n-1}) = P(X_1, \dots, X_{n-1}, 0)$ qui est de degré total $d' \leqslant d$. C'est un polynôme symétrique pour l'action de S_{n-1} par permutation des $n - 1$ premières variables, donc par l'hypothèse de récurrence il existe $R \in A[T_1, \dots, T_{n-1}]$ tel que $Q(X_1, \dots, X_{n-1}) = R(\sigma_1^{n-1}, \dots, \sigma_{n-1}^{n-1})$. Si on remplace chaque σ_k^{n-1} par σ_k^n (qui est de même degré k), le degré total ne change pas. On obtient un polynôme $R(\sigma_1^n, \dots, \sigma_{n-1}^n)$ en $X_1, \dots, X_n$ qui est symétrique et de degré d'.
> Considérons maintenant $P_1(X_1, \dots, X_n) = P(X_1, \dots, X_n) - R(\sigma_1^n, \dots, \sigma_{n-1}^n)$. Comme $\sigma_k^n = \sigma_{k-1}^{n-1} \cdot X_n + \sigma_k^{n-1}$, on a $P_1(X_1, \dots, X_{n-1}, 0) = 0$. Ainsi X_n divise P_1, et comme P_1 est symétrique, de même X_k divise P_1 pour tout k. Il en découle que $\sigma_n^n = X_1 \cdots X_n$ divise P_1 donc on a une écriture
>
> $$P(X_1, \dots, X_n) = R(\sigma_1^n, \dots, \sigma_{n-1}^n) + \sigma_n^n \cdot S(X_1, \dots, X_n)$$
>
> pour un certain polynôme $S(X_1, \dots, X_n)$ qui est symétrique de degré total $\leqslant d - n$. Par l'hypothèse de récurrence c'est un polynôme en $\sigma_1^n, \dots, \sigma_n^n$ et on a terminé. ■

3. Corps finis

3.1. Existence et unicité

Un fait fondamental pour l'étude d'un corps fini K est que son endomorphisme de Frobenius $F : K \to K$ est un *automorphisme*. Comme F est toujours injectif, il est équivalent de dire qu'il est surjectif, ou encore, que tout élément de K est une puissance p-ième. Nous saisissons cette occasion pour introduire la terminologie en vigueur.

Définition. Soit K un corps quelconque et $p = \text{car}(K) \geqslant 0$. On dit que K est :

- *parfait* si $p = 0$ ou si $p > 0$ et tout élément de K est une puissance p-ième.
- *imparfait* sinon.

Lemme. 1. Tout corps fini est parfait.
2. Tout corps algébriquement clos est parfait.
3. Le corps de fractions rationnelles $K = \mathbb{F}_p(X)$ est imparfait.

> **Démonstration :** 1. Frobenius est bijectif car sa source et son but ont même cardinal.
>
> 2. Si $p = 0$, K est parfait. Si $p > 0$, pour tout $a \in K$ le polynôme $X^p - a$ possède une racine donc a est une puissance p-ième ; donc F est surjectif.

3. Plus généralement soit $K = K_0(X)$ avec K_0 un corps de caractéristique $p > 0$. Le degré des polynômes s'étend aux fractions rationnelles par la formule $\deg(P/Q) = \deg(Q) - \deg(Q)$. De plus, pour toute fraction rationnelle $F \neq 0$ on a $\deg(F^p) = p \deg(F) \in p\mathbb{Z}$. Comme $\deg(X) = 1$ on voit que X n'est pas une puissance p-ième. ■

Passons au théorème principal de ce paragraphe. Si K est un corps fini de cardinal q, sa caractéristique est un nombre premier $p > 0$ et le morphisme injectif canonique $\mathbb{F}_p \to K$ munit K d'une structure de $\mathbb{F}_p$-espace vectoriel. En posant $n = \dim_{\mathbb{F}_p}(K)$, on a alors $q = p^n$.

Théorème d'existence et unicité des corps finis.
Existence : Soient p un nombre premier, n un entier naturel et $q = p^n$. Alors le corps de décomposition $\mathrm{Dec}_{\mathbb{F}_p}(X^q - X)$ est un corps fini de cardinal q.

Unicité : Réciproquement, soit K un corps fini et q son cardinal. Alors il existe un nombre premier p, un entier naturel n tel que $q = p^n$, et un isomorphisme $K \simeq \mathrm{Dec}_{\mathbb{F}_p}(X^q - X)$.

🛈 Le cours du jeudi 19 février 2026 s'est arrêté ici.

Démonstration. Nous utiliserons le fait élémentaire suivant (exercice) : si $\varphi : E \to E$ est un endomorphisme de corps, alors l'ensemble des points fixes $E^\varphi := \{x \in E\,;\, \varphi(x) = x\}$ est un sous-corps.

(Existence) Posons $P = X^q - X$ et $E = \mathrm{Dec}_{\mathbb{F}_p}(P)$. Notons E_0 le sous-corps des points fixes de l'endomorphisme $\varphi = F^n$. Ainsi, par définition

$$E_0 = \{x \in E\,;\, x^{p^n} = x\} = \{x \in E\,;\, x^q = x\} = \mathrm{Rac}_E(P).$$

Comme E est par définition engendré par les racines de P, on a $E_0 = E$. Par ailleurs P est scindé dans E, et sans racine double car $P' = qX^{q-1} - 1 = -1$ puisque $q = 0$ dans $\mathbb{F}_p$. Il s'ensuit que $|E| = |E_0| = q$.

(Unicité) Comme $|K| = q$, le groupe multiplicatif $K^\times$ est de cardinal $q - 1$. D'après le théorème de Lagrange, on a $x^{q-1} = 1$ pour tout $x \in K^\times$. En multipliant par x on déduit $x^q = x$ et ceci est donc vrai pour tout $x \in K$. Ceci démontre que le polynôme $P = X^q - X$ possède q racines dans K et que $K = \mathrm{Rac}_K(X^q - X)$. Il s'ensuit que K est un corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. ■

Remarque. La démonstration montre que K est exactement l'ensemble des racines du polynôme $X^q - X$. Le théorème d'existence de la clôture algébrique fournit d'ailleurs une manière très concrète de représenter les corps finis : pour tout $q = p^n$, l'ensemble des racines du polynôme $X^q - X$ dans une clôture algébrique de $\mathbb{F}_p$ est un corps à q éléments. On peut choisir n'importe quelle clôture algébrique ; chacune contient un unique sous-corps à q éléments.

Remarque. On note parfois $\mathbb{F}_q$ « le » corps à q éléments, et cette notation est justifiée par le fait qu'il existe un corps à q éléments qui est « unique ». Cette notation recèle cependant des dangers, car si K et K' sont deux corps à q éléments, il n'y a pas d'isomorphisme unique / canonique / naturel entre eux (sauf dans le cas où q est un nombre premier). Ceci a de nombreuses conséquences concrètes, comme par exemple le fait qu'il n'est pas possible de comparer directement des éléments $x \in K$ et $x' \in K'$. Pour cette raison, il est plus prudent de parler d'« un » corps à q éléments. Ces remarques sont développées dans le livre de Michel Demazure, *Cours d'algèbre*, Cassini, 2008, dans le chapitre consacré aux corps finis ; voir le §9.3.3 accessible ici.

Les mêmes remarques s'appliquent pour « le » corps de décomposition d'un polynôme et pour « la »

clôture algébrique d'un corps. Ces objets sont uniques à isomorphisme près, mais l'isomorphisme n'est pas unique et ce défaut est à l'origine d'éventuelles confusions ou erreurs. Pour cette raison il est plus sûr de parler d'*un* corps de décomposition et d'*une* clôture algébrique.

3.2. Propriétés

Dans tout ce paragraphe K est un corps fini à $q = p^n$ éléments. On note $K_0 = \mathbb{F}_p$.

Théorème (groupe multiplicatif). Le groupe $K^\times$ est cyclique.

> **Démonstration.** Nous avons vu au §2.2 que tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique. ■

Lemme (divisibilités). 1. Si $m \mid n$ alors $X^{p^m} - X \mid X^{p^n} - X$.
2. Si $P \mid P'$ dans $K[X]$, on a une extension de corps $\mathrm{Dec}_K(P) \hookrightarrow \mathrm{Dec}_K(P')$.

> **Démonstration :** 1. Notons $n = dm$. Pour tout entier s on a l'identité algébrique
>
> $$a - 1 \mid a^s - 1.$$
>
> Prenant $s = d$, on obtient $p^m - 1 \mid p^n - 1$ donc il existe un entier e tel que $p^n - 1 = e(p^m - 1)$. Prenant $s = e$, on trouve $X^{p^m-1} - 1 \mid X^{p^n-1} - 1$. Le résultat s'en déduit en multipliant par X.
>
> 2. En effet, P est décomposé dans $\mathrm{Dec}_K(P')$ donc ses racines engendrent une sous-extension isomorphe à $\mathrm{Dec}_K(P)$. ■

Théorème (extensions). 1. Il existe des extensions K'/K de tout degré d.
2. Toute extension de corps finis K'/K est monogène.

> **Démonstration :** 1. Posons $q' = q^d$, $P = X^q - X$, $P' = X^{q'} - X$. On sait que $K \simeq \mathrm{Dec}_{K_0}(P)$. Posons $K' = \mathrm{Dec}_{K_0}(P')$. Le lemme des divisibilités ci-dessus fournit une extension $K \hookrightarrow K'$. Comme $|K| = q$ et $|K'| = q^d$ on a $[K' : K] = d$.
>
> 2. Soit u un générateur du groupe cyclique $(K')^\times$. Il est clair que $K' = K(u)$. ■

3.3. Correspondance de Galois des corps finis

Nous commençons par quelques généralités.

Définition. Soit E/K une extension de corps.

- On appelle *groupe de Galois de* E/K l'ensemble des K-automorphismes du corps E, c'est-à-dire les automorphismes $f : E \to E$ tels que $f_{|K} = \mathrm{id}_K$. On le note $ ext{Gal}(E/K)$.
- Pour tout sous-groupe $H \subset \mathrm{Gal}(E/K)$, on note E^H l'ensemble des points fixes de H c'est-à-dire les $x \in E$ tels que $h(x) = x$ pour tout $h \in H$.

Lemme. La partie E^H est une sous-K-extension de E.

> **Démonstration :** Le fait que E^H est un corps résulte du fait que les éléments de H sont des automorphismes de corps. Le fait qu'il contient K provient de la définition de $\mathrm{Gal}(E/K)$. Le fait que E^H soit inclus dans E vient de sa définition même. ■

On peut noter que le fait que H soit un sous-groupe ne joue aucun rôle pour vérifier que E^H est une sous-K-extension de E. Cependant, si on note $\langle H \rangle$ le sous-groupe engendré par H, alors $E^H = E^{\langle H \rangle}$ et c'est pourquoi on se limite en pratique aux sous-groupes.

Le lemme suivant est l'idée centrale de toute la théorie de Galois : *les K-automorphismes de corps permutent les racines des polynômes à coefficients dans K.*

Lemme. Soient E/K une extension et $f \in \mathrm{Gal}(E/K)$. Soit $P \in K[X]$. Si $x \in E$ est une racine de P, alors $f(x)$ est une racine de P.

> **Démonstration :** Notons $P(X) = \sum_{i=0}^{N} a_i X^i$. Comme f est l'identité sur K, on a $f(a_i) = a_i$ pour tout i. En appliquant f à l'égalité $\sum_{i=0}^{N} a_i x^i = 0$, on trouve $\sum_{i=0}^{N} a_i f(x)^i = 0$, donc $f(x)$ est une racine de P. ■

La correspondance de Galois générale décrit les sous-extensions de E/K en termes des sous-groupes de $\mathrm{Gal}(E/K)$: c'est notre programme pour plus tard.

Nous revenons aux corps finis pour établir la correspondance de Galois pour ceux-ci. On note :

- K un corps fini à $q = p^n$ éléments,
- E/K une extension de degré d,
- $\Phi : E \to E$ la puissance n-ième de Frobenius, définie par $\Phi(x) = x^q$.

Théorème (automorphismes). Le groupe $\mathrm{Gal}(E/K)$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}$, engendré par Φ.

> **Démonstration :** D'abord on note que comme K est composé de racines du polynôme $X^q - X$ (dans une clôture algébrique, ou un corps de décomposition), l'endomorphisme Φ est l'identité sur K donc $\Phi \in \mathrm{Gal}(E/K)$.
>
> D'après le théorème du §3.2, l'extension E/K est monogène. Notons u un générateur, $P \in K[X]$ son polynôme minimal et R l'ensemble des racines de P dans E. D'après le lemme ci-dessus, pour tout automorphisme $f \in \mathrm{Gal}(E/K)$, on a $f(u) \in R$. Comme u engendre E, le morphisme f est entièrement déterminé par la valeur $f(u)$ et il en résulte une injection $\mathrm{Gal}(E/K) \hookrightarrow R$, $f \mapsto f(u)$. Comme $\deg(P) = [E : K] = d$, on en déduit que $|\mathrm{Gal}(E/K)| \leqslant |R| \leqslant d$.
>
> D'un autre côté, pour tout $i < d$ l'automorphisme Φ^i n'est pas égal à l'identité, car sinon on aurait $x^{q^i} = x$ pour tout $x \in E$ si bien que le polynôme $X^{q^i} - X$ aurait au moins p^{nd} racines, strictement plus que son degré p^{ni}. Ainsi l'ordre de Φ est au moins d, donc $|\mathrm{Gal}(E/K)| \geqslant d$.
>
> En conclusion $\mathrm{Gal}(E/K)$ est d'ordre d, engendré par Φ. ■

Le générateur de $\mathrm{Gal}(E/K)$ est parfois nommé *automorphisme de Frobenius de l'extension E/K*. Défini par $\Phi(x) = x^q$, il est en fait déterminé par le cardinal de K et est donc en un certain sens uniforme pour toutes les extensions E/K.

Théorème (sous-extensions). 1. Soit $m \mid d$ et $E_m = \{x \in E\,;\, x^{q^m} = x\}$ le sous-corps de points fixes de Φ^m. Alors E_m est une sous-K-extension de cardinal q^m.
2. Réciproquement, toute sous-extension de E est de la forme E_m pour un $m \mid d$.

> **Démonstration :** 1. Comme $X^{q^m} - X$ est un diviseur de $X^{q^d} - X$ (d'après le lemme « divisibilités » du §3.2), il est scindé dans E. On sait aussi que ses racines sont simples. Donc $|E_m| = |\mathrm{Rac}_K(X^{q^m} - X)| = q^m$.
>
> 2. Soit E' une sous-extension de E et $m = [E' : K]$. Le théorème de la base télescopique montre que $d = [E : K] = [E : E'] \cdot m$ donc $m \mid d$. Par ailleurs on sait que $E' \simeq \mathrm{Dec}_{K_0}(X^{q^m} - X)$ donc $X^{q^m} - X$ est scindé dans E'. Par raison de cardinal, $E' = \mathrm{Rac}_K(X^{q^m} - X) = E_m$. ■

Remarque. Comme nous l'avons fait remarquer au §3.1, la représentation concrète des corps finis et des inclusions entre eux se simplifie si on raisonne dans une clôture algébrique fixée E de $\mathbb{F}_p$. En effet, dans E il existe un unique sous-corps K_m de cardinal p^m, c'est l'ensemble des racines du polynôme $X^{p^m} - X$. De plus, on a les équivalences :

$$m \mid n \quad \Longleftrightarrow \quad X^{p^m} - X \mid X^{p^n} - X \quad \Longleftrightarrow \quad K_m \subset K_n.$$

Théorème de correspondance de Galois pour les corps finis.
Soit E/K une extension de corps finis. Les applications

$$\begin{array}{ccc} \left\{\text{sous-}K\text{-extensions de } E\right\} & \longleftrightarrow & \left\{\text{sous-groupes de } \mathrm{Gal}(E/K)\right\} \\ L & \overset{f}{\longmapsto} & \mathrm{Gal}(E/L) \\ E^H & \overset{g}{\longmapsto} & H \end{array}$$

sont des bijections réciproques l'une de l'autre, strictement décroissantes pour l'inclusion.

ℹ Le cours du jeudi 26 février 2026 s'est arrêté ici.

> **Démonstration :** Le théorème sur les automorphismes (ci-dessus) montre que
>
> $$\mathrm{Gal}(E/K) = \langle \Phi \rangle \simeq \mathbb{Z}/d\mathbb{Z}.$$
>
> Les sous-groupes d'un groupe cyclique sont connus : ils sont de la forme $H_m = \langle \Phi^m \rangle$ pour un $m \mid d$. Pour $H = H_m$, l'extension de points fixes est
> $g(H_m) = E^{H_m} = \{x \in E\,;\, x^{q^m} = x\} = E_m$.
>
> Dans l'autre sens, les sous-extensions de E sont les E_m. L'automorphisme de Frobenius de l'extension E/E_m est $\Psi : E \to E$ défini par $\Psi(x) = x^{q^m}$. Le théorème sur les automorphismes fournit donc $\mathrm{Gal}(E/E_m) = \langle \Psi \rangle = \langle \Phi^m \rangle = H_m$. Ainsi $f(E_m) = H_m$.
>
> Ainsi f et f sont inverses l'une de l'autre. ■

▶Feuille de route pour la suite

Nous venons d'établir une correspondance de Galois pour les extensions de corps finis. Notre objectif principal pour la suite du cours est d'établir une correspondance semblable pour des extensions de corps plus générales. Pour y parvenir, il nous sera très utile d'observer que dans cette partie, nous avons obtenu en cours de route l'égalité :

$$|\mathrm{Gal}(E/K)| = [E : K].$$

Celle-ci doit être vue comme une indication heuristique du fait que le nombre d'automorphismes et le nombre de sous-extensions sont comparables. Cette égalité n'a pas toujours lieu ; pour une extension finie arbitraire le cardinal du groupe de Galois sera plus petit. Notre tâche dans les sections suivantes est d'identifier les propriétés d'une extension qui garantissent que l'on ait bien $|\mathrm{Gal}(E/K)| = [E : K]$.

4. Extensions séparables

Pour un élément algébrique x, notons $N(x) = |\mathrm{Rac}_{\overline{K}}(P_{x,K})|$ le nombre de racines du polynôme minimal dans une clôture algébrique fixée. Certains x possèdent la propriété que $N(x)$ est strictement inférieur au degré de $P_{x,K}$, c'est-à-dire que celui-ci possède des racines multiples. Par exemple, si K est de caractéristique p et $t \in K$ n'est pas une puissance p-ième, le polynôme $P = X^p - t$ est irréductible et ne possède qu'une racine x dans $\overline{K}$. L'extension de rupture $E = K[X]/(P)$ est de degré p, mais $|\mathrm{Gal}(E/K)| = 1$.

C'est le comportement opposé qui est favorable : on dira que x est *séparable* si les racines de $P_{x,K}$ (dans une clôture algébrique fixée) sont simples. Cette bonne propriété a d'ailleurs déjà été rencontrée en algèbre linéaire, où les endomorphismes dont le polynôme minimal est scindé à racines simples sont les plus faciles à étudier. Cette section est consacrée à l'étude de la séparabilité.

Avant de commencer, juste une remarque sur un concept clé. Dans une extension de corps E/K, il se trouve que l'ensemble des éléments algébriques séparables forme une sous-K-extension de E, mais c'est bien plus difficile à établir que le fait analogue pour les éléments algébriques. La notion de *degré de séparabilité* fournit un outil très puissant pour démontrer ce fait et plus généralement pour développer la théorie de la séparabilité que nous exposons dans cette partie.

4.1. Séparabilité

Proposition. Soient K un corps, $P \in K[X]$ un polynôme non constant et E/K une extension telle que P est scindé sur E. Les assertions suivantes sont équivalentes :

1. Les racines de P dans E sont simples,
2. Les polynômes P et P' sont premiers entre eux dans $K[X]$,
3. Le discriminant de P est non nul.

La notion de discriminant est naturelle dans ce contexte mais n'est pas nécessaire pour la suite du cours ; elle est développée dans l'Annexe de cette partie, où on trouvera l'équivalence de la condition 3 avec les autres.

> **Démonstration :** nous nous contentons de démontrer que 1 $\Leftrightarrow$ 2.
>
> 1 $\Rightarrow$ 2. Si le polynôme $D := \mathrm{pgcd}(P, P')$ est différent de 1, il est de degré > 0. Comme il divise P, il possède une racine $x \in E$. Alors x est racine de P et P', donc c'est une racine double.
>
> 2 $\Rightarrow$ 1. Si $x \in E$ est une racine double, il annule P et P' donc ceux-ci sont tous les deux divisibles par $X - x$ et ne sont donc pas premiers entre eux. ■

Définition. On dit que $P \in K[X]$ est *séparable* si ses racines dans un corps de décompostion (ou dans une clôture algébrique) sont simples, ou encore, si $\mathrm{disc}(P) \neq 0$. On dit qu'il est *inséparable* sinon.

Il est clair que si P est séparable et Q divise P, alors Q est séparable.

Lemme. Soit K un corps de caractéristique $p > 0$ et $P \in K[X]$.

1. Supposons P irréductible. Alors P est inséparable si et seulement si $P' = 0$.
2. On a $P' = 0$ si et seulement si $P(X) = Q(X^p)$ pour un certain polynôme Q.

> **Démonstration :** 1. Si P est inséparable, dans un corps de décomposition il possède une racine double x. Comme P est irréductible, il est égal au polynôme minimal $P_{x,K}$ de x. Comme P' annule x, on a $P \mid P'$ donc $P' = 0$ par raison de degré. Réciproquement si $P' = 0$ alors toute racine de P est double.
>
> 2. Soit aX^i un monôme non nul de P, c'est-à-dire que $a \neq 0$. Le monôme dérivé iaX^{i-1} est nul si et seulement si $p \mid i$, c'est-à-dire $i = jp$ et $aX^i = a(X^p)^j$. Ainsi P est un polynôme en X^p. ■

Théorème clé. Soient K un corps et $P \in K[X]$ un polynôme irréductible de degré n.

1. Si $\mathrm{car}(K) = 0$ alors P est séparable.

2. Si $\mathrm{car}(K) = p > 0$, il existe un unique couple (Q, k) composé d'un polynôme irréductible séparable $Q \in K[X]$ et un entier $k \in \mathbb{N}$ tels que $P(X) = Q(X^{p^k})$. De plus, dans une extension où P est scindé, le nombre de racines distinctes de P est $m := \deg(Q) = n/p^k$ et les multiplicités des racines sont toutes égales à p^k.

   Démonstration : Comme P est irréductible, on a $\deg(P) = n > 0$.

   1. Soit aX^n, avec $a \neq 0$, le monôme dominant de P. Celui de P' est alors naX^{n-1}. Comme $\mathrm{car}(K) = 0$, on a $na \neq 0$ donc $P' \neq 0$. Par le lemme, P est séparable.

   2. Notons $P = \sum_{i \in I} a_i X^i$ où l'on n'a représenté que les monômes non nuls, i.e. $a_i \neq 0$. On voit que « il existe Q tel que $P(X) = Q(X^{p^k})$ » si et seulement si « $p^k \mid i$ pour tout $i \in I$ » auquel cas $Q = \sum_j a_{jp^k} X^j$. Soit k l'entier maximal avec cette propriété ; il existe car $p^k \leqslant n$. Comme P est irréductible, alors Q l'est aussi (une factorisation non triviale $Q = Q_1 Q_2$ donne immédiatement une factorisation non triviale pour P). Notons $m := \deg(Q)$, donc $n = mp^k$. L'égalité $P(X) = Q(X^{p^k})$ montre que a est racine de P si et seulement si $b = a^{p^k}$ est racine de Q. Ceci montre que si le corps de décomposition de P est $K(a_1, \dots, a_m)$ alors celui de Q est $K(a_1^{p^k}, \dots, a_m^{p^k})$, où les a_i sont les racines de P. On a alors :

$$(\star) \qquad P(X) = (X^{p^k} - a_1^{p^k}) \cdots (X^{p^k} - a_m^{p^k}) = (X - a_1)^{p^k} \cdots (X - a_m)^{p^k}.$$

   De plus Q est séparable car sinon, d'après le lemme ci-dessus on aurait $Q' = 0$ donc $Q(X) = R(X^p)$ puis $P(X) = R(X^{p^{k+1}})$ en contradiction avec la maximalité de k. Les $b_i = a_i^{p^k}$ sont donc distincts, donc les a_i le sont aussi par injectivité du morphisme de Frobenius. La forme $(\star)$ résume tout. ■

Remarques.

1. L'entier m n'est pas nécessairement premier avec p ; par exemple le polynôme $Q(X) = X^p + X$ est séparable (puisque $Q' = 1$) donc avec ce polynôme on aurait $m = 1$.
2. Avec les notations du théorème, notons E un corps de rupture de P sur K. L'écriture $n = mp^k$ s'interprète comme une factorisation du degré $[E : K]$ en produit de

- une « partie séparable » $[E : K]_s := m$,
- une « partie inséparable » $[E : K]_i := p^k$

que nous généraliserons à toute extension finie au §4.3.

Définition. Soient E/K une extension et x un élément de E algébrique sur K. On dit que :

- x est *séparable sur* K si son polynôme minimal est séparable, et *inséparable* sinon.
- E/K est *séparable* si tous ses éléments sont séparables sur K.
- x est *radiciel sur* K (ou *purement inséparable sur* K) s'il existe $n \geqslant 0$ tel que $x^{p^n} \in K$.
- E/K est *radicielle* (ou *purement inséparable*) si tous ses éléments sont radiciels sur K.

La vérification des faits suivants est élémentaire : si K'/K est une extension avec $K' \subset E$, alors x séparable sur K entraine x séparable sur K' puisque $P_{x,K'}$ divise $P_{x,K}$. Une sous-extension d'une extension séparable est séparable.

4.2. Corps parfaits

Définition. Soit K un corps quelconque et $p = \mathrm{car}(K) \geqslant 0$. On dit que K est :

- *parfait* si $p = 0$ ou si $p > 0$ et tout élément de K est une puissance p-ième.

- *imparfait* sinon.

Lemme. 1. Tout corps fini est parfait.
2. Tout corps algébriquement clos est parfait.
3. Le corps de fractions rationnelles $K = \mathbb{F}_p(X)$ est imparfait.

Démonstration : 1. Frobenius est bijectif car sa source et son but ont même cardinal.

2. Si $p = 0$, K est parfait. Si $p > 0$, pour tout $a \in K$ le polynôme $X^p - a$ possède une racine donc a est une puissance p-ième ; donc F est surjectif.

3. Plus généralement soit $K = K_0(X)$ avec K_0 un corps de caractéristique $p > 0$. Le degré des polynômes s'étend aux fractions rationnelles par la formule $\deg(P/Q) = \deg(Q) - \deg(Q)$. De plus, pour toute fraction rationnelle $F \neq 0$ on a $\deg(F^p) = p \deg(F) \in p\mathbb{Z}$. Comme $\deg(X) = 1$ on voit que X n'est pas une puissance p-ième. ■

Proposition. Un corps K est parfait si et seulement si tout polynôme irréductible sur K est séparable.

Démonstration : Supposons K parfait. Soit $P \in K[X]$. Si $P' = 0$, on a $P(X) = Q(X^p)$ pour un certain polynôme $Q = \sum_{i=0}^{n} a_i X^i$. Comme K est parfait, il existe b_i tel que $a_i = (b_i)^p$ donc

$$P(X) = \sum_{i=0}^{n} (b_i)^p X^{ip} = \Big(\sum_{i=0}^{n} b_i X^i \Big)^p.$$

En particulier P est réductible. Par contraposée, si P est irréductible on a $P' \neq 0$ et par le lemme du §4.1, P est séparable.

Réciproquement supposons que tout polynôme irréductible est séparable. Montrons que le morphisme de Frobenius de K est surjectif. Soit $t \in K$. Comme le polynôme $P := X^p - t \in K[X]$ a dérivée nulle, il n'est pas séparable, donc réductible. Notons $P = QR$ une factorisation avec $Q \in K[X]$ unitaire de degré $d \in \{1, \dots, p-1\}$. Soit a une racine de P dans une extension de scindement. Alors $P = (X - a)^p$ donc $Q = (X - a)^d$ et le coefficient de X^{d-1} est égal à $-da$. Comme $d \neq 0$ dans K, on en déduit que $a \in K$ ce qui montre que t est une puissance p-ème. ■

ℹ Le cours du jeudi 12 mars 2026 s'est arrêté ici.

Théorème. Si K est parfait, toute extension algébrique E/K est séparable.

Démonstration : En effet, le polynôme minimal d'un élément $x \in E$ sur K est irréductible. Comme K est parfait, par la proposition ci-dessus ce polynôme est séparable. ■

4.3. Degré de séparabilité

Nous allons maintenant relier la séparabilité à un phénomène déjà observé au §2.4 : alors même que le corps de rupture vérifie une propriété universelle qui le rend unique, un corps de décomposition ou une clôture algébrique peut en contenir plusieurs incarnations différentes. Nous l'avons constaté par exemple pour le corps de rupture $K_P = \mathbb{Q}[X]/(P)$ du polynôme $P = X^3 - 2$ sur $\mathbb{Q}$, qui possède trois plongements différents $a, b, c : K_P \to \overline{\mathbb{Q}}$:

$$X \overset{a}{\longmapsto} \sqrt[3]{2}, \quad X \overset{b}{\longmapsto} j\sqrt[3]{2}, \quad X \overset{c}{\longmapsto} j^2\sqrt[3]{2}.$$

Définition. soit E/K une extension finie. On appelle *degré de séparabilité de* E/K et on note

$$[E : K]_s := \operatorname{card} \operatorname{Hom}_K(E, \overline{K})$$

le cardinal de l'ensemble des K-morphismes de E dans une clôture algébrique de K.

Dans l'exemple $E = K_P$ qui prècède la définition, on a $[E : K]_s = 3$. Pour une extension monogène $E = K(x)$, c'est-à-dire que E est le corps de rupture d'un polynôme irréductible $P(X) = Q(X^{p^k})$ comme dans le Théorème clé, on a $[E : K]_s = m$.

Remarque. L'entier $[E : K]_s$ ne dépend pas du choix d'une clôture algébrique car si $\overline{K}_1$ et $\overline{K}_2$ sont deux clôtures algébriques, il existe un K-isomorphisme $i : \overline{K}_1 \to \overline{K}_2$ et l'application $f \mapsto i \circ f$ est une bijection entre $\operatorname{Hom}_K(E, \overline{K}_1)$ et $\operatorname{Hom}_K(E, \overline{K}_2)$.

Nous introduisons maintenant une terminologie pour désigner un entier très utile pour les démonstrations par récurrence des résultats ci-dessous concernant le degré de séparabilité. Cette définition n'est pas standard.

Définition. Soit E/K une extension finie. On appelle *rang de* E/K et on note $r(E/K)$ le cardinal minimal d'une famille génératrice de l'extension E/K.

Théorème de la base télescopique séparable. Le degré de séparabilité $[E : K]_s$ d'une extension finie est fini. De plus, si $E'/E/K$ sont des extensions finies, on a :

$$[E' : K]_s = [E' : E]_s \, [E : K]_s.$$

Démonstration : On démontre l'énoncé par récurrence sur $r = r(E'/E)$.

Initialisation. Si $r = 0$, on a $E' = E$ donc $[E' : E]_s = 1$ et l'égalité est vérifiée.

Intermède. Si $r = 1$, on a $E' = E(x)$. Notons P le polynôme minimal de x sur E et n son degré, de sorte que E' est un corps de rupture de P. Avec les notations du « Théorème clé » (§4.1) on a $P(X) = (X - a_1)^{p^k} \cdots (X - a_m)^{p^k}$ où les $a_i \in \overline{K}$ sont distincts, et disons $a_1 = x$. Pour chaque K-morphisme $f : E \to \overline{K}$, il est équivalent de se donner un K-morphisme $f' : E' \to \overline{K}$ qui prolonge f ou l'image $f(x)$ qui est l'un des a_i. Pour chaque f, il y a donc m choix possibles pour f'. Ceci démontre que

$$(\star) \quad \text{si } r(E'/E) = 1, \text{ on a } [E' : K]_s = m \, [E : K]_s.$$

Hérédité. Supposons que $r \geqslant 1$. On peut écrire $E' = E_0(x)$ où E_0/E est engendrée par $r - 1$ éléments et $r(E'/E_0) = 1$. D'après $(\star)$, on a $[E' : K]_s = m \, [E_0 : K]_s$ et $[E' : E]_s = m \, [E_0 : E]_s$. Par ailleurs, d'après l'hypothèse de récurrence on a $[E_0 : K]_s = [E_0 : E]_s [E : K]_s$. En multipliant par m, on obtient le résultat. ■

Théorème. Soit K un corps d'exposant caractéristique $p = \max(1, \operatorname{car}(K))$. Si E/K est une extension finie, il existe un entier $[E : K]_i$ égal à une puissance de p tel que

$$[E : K] = [E : K]_s \, [E : K]_i.$$

Démonstration : On démontre l'énoncé par récurrence sur $r = r(E/K)$.

Si $r = 0$, on a $E = K$ donc $[E : K] = [E : K]_s = 1$. On pose $[E : K]_i = 1$ et l'énoncé est vérifié.

Supposons maintenant que $r \geqslant 1$. On peut écrire $E = E_0(x)$ où E_0/K est engendrée par $r - 1$ éléments et $r(E/E_0) = 1$. Notons P le polynôme minimal de x sur E_0 et n son degré. Avec les notations du « Théorème clé », on a :

$$[E : E_0] = n = mp^k = [E : E_0]_s \, p^k.$$

De plus, par l'hypothèse de récurrence il existe un entier $[E_0 : K]_i = p^l$ tel que
$$[E_0 : K] = [E_0 : K]_s \, p^l.$$
En utilisant le théorème de la base télescopique séparable, on déduit :
$$[E : K] = [E : E_0]\,[E_0 : K] = [E : E_0]_s \, [E_0 : K]_s \, p^{k+l} = [E : K]_s \, p^{k+l}.$$
En posant $[E : K]_i = p^{k+l}$, on obtient le résultat annoncé. ■

Définition. soit E/K une extension finie. On appelle *degré d'inséparabilité de* E/K l'entier $[E : K]_i$ défini par le théorème.

Théorème de la base télescopique inséparable. Si $E'/E/K$ sont des extensions finies, on a
$$[E' : K]_i = [E' : E]_i \, [E : K]_i.$$

Démonstration : Ceci découle du théorème de la base télescopique couplé avec le théorème de la base télescopique séparable. ■

4.4. Extensions séparables

Théorème. Si E/K est une extension finie, on a $[E : K]_s = [E : K]$ si et seulement si E/K est séparable.

Démonstration : Supposons que $[E : K]_s = [E : K]$. Soit $x \in E$. En utilisant les théorèmes de base télescopique ordinaire et séparable, l'hypothèse fournit :
$$[E : K(x)]_s \, [K(x) : K]_s = [E : K(x)]\,[K(x) : K].$$
Comme le degré séparable est inférieur ou égal au degré, ceci force
$$[E : K(x)]_s = [E : K(x)] \quad \text{et} \quad [K(x) : K]_s = [K(x) : K].$$
Avec les notations du « Théorème clé » (§4.1), l'égalité $[K(x) : K]_s = [K(x) : K]$ s'écrit $m = n$, c'est-à-dire $k = 0$ et le polynôme minimal $P = Q$ est séparable. Ainsi x est séparable donc l'extension E/K l'est.

Réciproquement supposons E/K séparable. Dans le cas monogène on peut écrire $E = K(x)$ et avec les notations du Théorème clé encore, le fait que x soit séparable montre que $m = n$ donc $[K(x) : K]_s = [K(x) : K]$. Dans le cas général l'extension E est une composé $E_0 = K \subset E_1 \subset \cdots \subset E_s = E$ d'extensions monogènes $E_i \subset E_{i+1}$. D'après ce qui précède $[E_{i+1} : E_i]_s = [E_{i+1} : E_i]$ donc les théorèmes de base télescopique ordinaire et séparable entrainent que $[E : K]_s = [E : K]$. ■

Considérons par exemple le cas d'une extension monogène $E = K(x)$, c'est-à-dire que E est le corps de rupture d'un polynôme irréductible $P(X) = Q(X^{p^k})$ comme dans le Théorème clé. Le théorème affirme que E/K est séparable si et seulement si $m = n$, c'est-à-dire $k = 0$, c'est-à-dire P séparable. En particulier l'extension $K(x)$ engendrée par un élément séparable est séparable.

Corollaire (clôture séparable). Soit E/K une extension de corps. Les éléments de E qui sont séparables sur K forment une sous-K-extension de E.

Démonstration : Soient $x, y \in E$ deux éléments algébriques séparables sur K. Alors y est séparable sur $K(x)$ car le polynôme minimal $P_{y,K(x)}$ divise $P_{y,K}$ qui est séparable. En utilisant les théorèmes de base télescopique et le théorème précédent, on déduit :
$$\begin{aligned}[K(x, y) : K] &= [K(x, y) : K(x)]\,[K(x) : K] \\ &= [K(x, y) : K(x)]_s \, [K(x) : K]_s \\ &= [K(x, y) : K]_s.\end{aligned}$$
Ceci démontre que $K(x, y)/K$ est séparable. En particulier $x + y$, xy et l'inverse x^{-1} d'un

$x \neq 0$ sont séparables sur K. Comme les éléments de K le sont aussi, le résultat en découle. ■

Définition. Soit K un corps.

- Pour toute extension E/K, la sous-extension composée des éléments de E qui sont séparables sur K est appelée la *clôture séparable de K dans E*.
- Dans une clôture algébrique $\overline{K}$, la sous-extension composée des éléments séparables sur K est appelée *clôture séparable de K*.

De la même manière que deux clôtures algébriques sont K-isomorphes, deux clôtures séparables sont K-isomorphes.

Théorème des extensions séparables. 1. Une extension séparable d'une extension séparable est séparable : si E'/E et E/K sont séparables alors E'/K est séparable.
2. Une extension engendrée par des éléments séparables est séparable.

Démonstration : 1. Supposons d'abord $E'/E/K$ finies. Dans ce cas, en utilisant la caractérisation de la séparabilité par le degré de séparabilité établie dans le théorème ci-dessus, on trouve :

$$[E' : K]_s = [E' : E]_s\,[E : K]_s = [E' : E]\,[E : K] = [E' : K].$$

Il en découle que E'/K est séparable. Sans supposer $E'/E/K$ finies, soit $x' \in E'$ et $P = P_{x,E}$ son polynôme minimal sur E. Soit $F = K(a_0, \dots, a_{n-1})$ la sous-extension de E engendrée par les coefficients de P. Soit $F' = F(x)$. Alors $F'/F/K$ sont finies, F'/F est séparable et F/K est séparable. D'après le cas précédent il s'ensuit que F'/K est séparable, donc x est séparable sur K.

2. Soit E/K une extension engendrée par une famille $\{x_i\}_{i\in I}$ d'éléments séparables sur K. Soit $x \in E$. Comme $E = K(x_i)$, il existe une partie finie $\{x_1, \dots, x_n\} \subset E$ telle que $x \in K(x_1, \dots, x_n)$. Soit $E_i = K(x_1, \dots, x_i)$. Alors chaque extension E_{i+1}/E_i est séparable, donc E_n/K est séparable d'après le point 1. Comme $x \in E_n$, on voit que x est séparable, donc E/K est séparable. ■

Théorème de l'élément primitif. Toute extension finie séparable est monogène.

Démonstration : Notons E/K l'extension.

Si K est fini, alors E est fini et on sait que le groupe $E^\times$ est cyclique. Si u en est un générateur, on a $E = K(u)$.

Si K est infini, posons $n := [E : K]$. Soit $\overline{K}$ une clôture algébrique de K. Comme E/K est séparable, on a $[E : K]_s = [E : K] = n$ donc les K-plongements de E dans $\overline{K}$ sont au nombre n ; notons-les $\sigma_1, \dots, \sigma_n$. Si $1 \leqslant i < j \leqslant n$ on pose $V_{i,j} := \{x \in E, \sigma_i(x) = \sigma_j(x)\}$. C'est un sous-$K$-espace vectoriel de E, distinct de E puisque $\sigma_i \neq \sigma_j$. Comme K est infini, la réunion $U := \cup_{i,j} V_{i,j}$ est distincte de E (voir [Bad25], lemme 7.17). Soit alors x un élément de $E \setminus U$. Alors $\sigma_i(x) \neq \sigma_j(x)$ pour tout $i \neq j$, donc $\sigma_1(x), \sigma_2(x), \dots, \sigma_n(x)$ sont des éléments distincts de $\overline{K}$. Mais alors les restrictions des σ_i à $K(x)$ sont distinctes, donc $[K(x) : K]_s \geqslant n$. En particulier $n \leqslant [K(x) : K] \leqslant [E : K] = n$ donc $K(x) = E$ et x est ainsi un élément primitif. ■

On trouvera dans [Bad25, Théorème 7.20] une démonstration plus effective du théorème de l'élément primitif, au sens où elle décrit un moyen de trouver un générateur x pour l'extension.

Contre-exemple. Voici un exemple d'extension finie non monogène, non séparable. Notons $E = \mathbb{F}_p(x, y)$ le corps des fractions rationnelles en deux indéterminées x et y (corps des fractions de l'anneau de polynômes $\mathbb{F}_p[x, y]$). Notons $F : E \to E$ le morphisme de Frobenius et K son image. C'est le sous-corps des puissances p-ièmes, qui sont les fractions rationnelles en les indéterminées $t = x^p$ et $u = y^p$. En d'autres termes, on a $K = \mathbb{F}_p(t, u)$ et E est engendrée sur K par les deux éléments x et y, de polynômes minimaux respectifs $P(X) = X^p - T$ et $Q(Y) = Y^p - U$. On a un isomorphisme de K-algèbres $E \simeq K[X, Y]/(X^p - T, Y^p - U)$. La partie $(x^i y^j, 0 \leqslant i, j \leqslant p-1)$ est une base pour E donc $[E : K] = p^2$. Si E était monogène engendré par un élément z, on aurait $a := z^p = F(z) \in K$ et le polynôme minimal de z sur K serait $P(Z) = Z^p - a$. De l'isomorphisme $E \simeq K[Z]/(Z^p - a)$ on déduirait que $[E : K] = p$, contradiction. ■

ℹ Le cours du jeudi 19 mars 2026 s'est arrêté ici.

Annexe. Discriminant d'un polynôme

Référence : J.-P. Ramis et A. Warusfel, *Mathématiques, Tout-en-un pour la Licence 2*, 4ème édition, Dunod, 2023. Paragraphe §I.7.2 accessible ici.

Ce paragraphe n'est pas nécessaire pour le développement de la théorie de Galois et sa lecture peut être omise. Son but est d'introduire le *discriminant*, un scalaire $\operatorname{disc}(P)$ de K qui permet de détecter la présence de racines doubles de P dans une clôture algébrique $\overline{K}$.

Soient K un corps $K_n[X]$ l'espace vectoriel des polynômes de degré $< n$, avec sa base composée des monômes $(X^{n-1}, \dots, X, 1)$.

Définition. Soient $n, m \in \mathbb{N}$ et $P = \sum_{i=0}^{n} a_i X^i$ et $Q = \sum_{j=0}^{m} b_j X^j$ polynômes de $K[X]$.

- On appelle *application de Bézout* l'application linéaire
$$K_m[X] \times K_n[X] \longrightarrow K_{p+q}[X], \quad (U, V) \longmapsto UP + VQ.$$
- On appelle *matrice de Sylvester* notée $\operatorname{Syl}(P, Q)$ (ou $S_{P,Q}$) la matrice de l'application de Bézout dans les bases monomiales à la source et au but.
- On appelle *résultant de P et Q* noté $\operatorname{Res}(P, Q)$ le déterminant de la matrice de Sylvester.

Précisons : ce que nous appelons « base monomiale » à la source est la réunion de la famille $((X^{m-1}, 0), \dots, (X, 0), (1, 0))$, de cardinal m, et de la famille $((0, X^{n-1}), \dots, (0, X), (0, 1))$, de cardinal n. Au but, c'est plus simple, c'est la base $(X^{n+m-1}, \dots, X, 1)$.

$$S_{P,Q} := \begin{pmatrix} a_n & 0 & \cdots & 0 & b_m & 0 & \cdots & 0 \\ a_{n-1} & a_n & \cdots & 0 & b_{m-1} & b_m & \cdots & 0 \\ a_{n-2} & a_{n-1} & \ddots & 0 & b_{m-2} & b_{m-1} & \ddots & 0 \\ \vdots & \vdots & \ddots & a_n & \vdots & \vdots & \ddots & b_m \\ a_0 & a_1 & \cdots & \vdots & b_0 & b_1 & \cdots & \vdots \\ 0 & a_0 & \ddots & \vdots & 0 & b_0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & a_1 & \vdots & \vdots & \ddots & b_1 \\ 0 & 0 & \cdots & a_0 & 0 & 0 & \cdots & b_0 \end{pmatrix}$$

Exemple. Si $P = aX^2 + bX + c$ et $Q = dX + e$, la matrice de Sylvester est

$$\mathrm{Syl}(P,Q) = \begin{pmatrix} a & d & 0 \\ b & e & d \\ c & 0 & e \end{pmatrix}$$

de sorte que $\mathrm{Res}(P,Q) = ae^2 - bde + cd^2$. En particulier, $\mathrm{Res}(P,P') = -a(b^2-4ac)$.

Proposition. Si $\deg(P) = n$ et $\deg(Q) = m$, les conditions suivantes sont équivalentes :

1. Le résultant de P et Q est nul.
2. Le pgcd de P et Q est $\neq 1$.
3. Les polynômes P et Q ont une racine commune dans une clôture algébrique $\overline{K}/K$.

Démonstration : Notons $D := \mathrm{pgcd}(P,Q)$.

$1 \Rightarrow 2$. Si $\mathrm{Res}(P,Q) = 0$, l'application de Bézout a un déterminant nul donc elle n'est pas injective. Ainsi il existe $U \in K_m[X]$ et $V \in K_n[X]$ tels que $UP + VQ = 0$. Alors P divise VQ, mais P ne divise pas V puisque $\deg(V) < \deg(P)$. D'après le lemme de Gauss, ceci implique $D \neq 1$.

$2 \Rightarrow 3$. Une racine de D dans $\overline{K}$ est une racine commune de P et Q.

$3 \Rightarrow 1$. Pour calculer le résultant, on peut se placer dans $\overline{K}$. Soit $\lambda \in \overline{K}$ une racine commune de P et Q. Écrivons $P = (X-\lambda)A$ et $Q = (X-\lambda)B$ avec $\deg(A) < n$ et $\deg(B) < m$. Alors $BP = (X-\lambda)AB = AQ$ donc l'application de Bézout a l'élément non nul $(B,-A)$ dans son noyau et son déterminant $\mathrm{Res}(P,Q)$ est nul. ■

Dans l'exemple ci-dessus où $\deg(P) = 2$, on a vu que le résultant $\mathrm{Res}(P,P')$ est divisible par le coefficient dominant a. C'est un fait général, conséquence du fait que la première ligne de la matrice $\mathrm{Syl}(P,P')$ est multiple de a_n : ses deux seuls termes non nuls sont les coefficients dominants de P et P', c'est-à-dire a_n et na_n. Ceci légitime la définition suivante.

Définition. On appelle *discriminant* d'un polynôme $P = \sum_{i=0}^{n} a_i X^i$ de degré n le scalaire

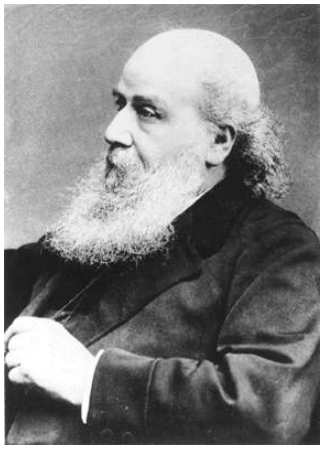
$$\mathrm{disc}(P) = \frac{(-1)^{n(n-1)/2}}{a_n}\mathrm{Res}(P,P') \quad \in K.$$

Par exemple, $\mathrm{disc}(aX^2+bX+c) = b^2-4ac$ et $\mathrm{disc}(X^3+pX+q) = 4p^3+27q^2$.

Corollaire. Les conditions suivantes sont équivalentes :

1. Dans une clôture algébrique, toutes les racines de P sont simples ;
2. Le discriminant de P est non nul.

Démonstration : comme les racines doubles sont les racines communes à P et P' (voir §1B.4), c'est un cas particulier de la proposition précédente. ■



James Joseph Sylvester (1814-1897)

5. Extensions normales et galoisiennes

Il y a un autre phénomène qui peut empêcher l'égalité $|\mathrm{Gal}(E/K)| = [E : K]$, c'est le fait que pour un polynôme $P \in K[X]$ donné, lorsqu'une extension de corps provoque la rupture elle ne provoque pas forcément la décomposition. Un exemple typique est fourni par l'extension de rupture $E = \mathbb{Q}(\alpha)$ du polynôme à coefficients rationnels $P = X^3 - 2$, avec $\alpha = \sqrt[3]{2}$. En effet P ne possède qu'une racine dans E et il en découle que $|\mathrm{Gal}(E/K)| = 1$. Comme nous allons voir, l'extension de décomposition (ou de scindement) ne présente pas cette pathologie ; on dira qu'elle est *normale*. La conjonction des deux propriétés « séparable et normale » fournira la notion d'*extension galoisienne*, pour laquelle nous pourrons établir la correspondance de Galois.

5.1. Extensions normales

Définition. Soit E/K une extension algébrique. On dit que E/K est *normale* si tout polynôme irréductible $P \in K[X]$ qui a une racine dans E est scindé sur E.

Proposition. Soit E/K une extension normale et soit L une extension de K dans E. Alors E/L est normale.

> **Démonstration :** Soit $P \in L[X]$ un polynôme irréductible qui a une racine x dans E. Comme P est irréductible, il est égal (à un scalaire près) au polynôme minimal de x sur L, donc divise le polynôme minimal de x sur K. Or, ce dernier est scindé sur E parce qu'il a une racine dans E et E/K est normale. Donc P est scindé sur E. Donc E/L est normale. ■

Exemples.

1. Toute extension de degré 2 est normale, car si $P \in K[X]$ est irréductible et a une racine x dans E, alors $\deg(P) = [K_P : K] \leqslant 2$ donc P est scindé sur E.
2. L'extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ n'est pas normale, parce que le polynôme irréductible $X^4 - 2$ possède une racine dans $\mathbb{Q}(\sqrt[4]{2})$ mais aussi deux racines non réelles.
3. Attention : une extension normale d'une extension normale n'est pas forcément normale. Ceci découle des exemples précédents, car les extensions $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ sont toutes deux normales car de degré 2.

Théorème des extensions normales. Soit E/K une extension finie. Alors les conditions suivantes sont équivalentes :

1. L'extension E/K est normale,
2. Pour toute extension E'/E et tout K-plongement $f : E \to E'$, on a $f(E) = E$,

3. Il existe un polynôme $P \in K[X]$ non constant tel que E est un corps de décomposition de P.

On note que dans la condition 2, on identifie E avec son image dans E'. C'est en ce sens qu'il faut comprendre la propriété $f(E) = E$.

> **Démonstration :** 1 ⇒ 3. Soit $e_1, \dots, e_n$ une K-base de E. Pour chaque i, soit P_i le polynôme minimal de e_i sur K, et soit $P = P_1 \cdots P_n$. D'après l'hypothèse, P_i est scindé dans E, donc P également. De plus E est engendré par les racines de P, puisqu'il est déjà engendré par les e_i. Il s'ensuit que E est un corps de décomposition de P sur K.
>
> 3 ⇒ 2. Soit E'/E une extension et $f : E \to E'$ un K-morphisme. Comme E est un corps de décomposition de P, alors $f(E)$ également. Or il existe un unique sous-corps de E' qui est un corps de décomposition : c'est le sous-corps engendré par E et les racines de P. Il s'ensuit que $f(E) = E$.
>
> 2 ⇒ 1. Soit $P \in K[X]$ un polynôme irréductible qui possède une racine x dans E. Nous voulons démontrer que P est scindé sur E. Soient E' une clôture algébrique de E et $x = x_1, x_2, \dots, x_n$ les racines de P dans E', avec $n = \deg(P)$. Pour chaque $i = 1, \dots, n$, par propriété du corps de rupture il existe un unique K-morphisme $f_i : K(x) \to E'$ tel que $f_i(x) = x_i$. D'après le théorème de prolongement (§2.6) ce morphisme se prolonge en un K-morphisme $f_i' : E \to E'$. D'après l'hypothèse on a $f_i'(E) = E$, donc $x_i = f_i'(x) \in E$, d'où le résultat. ■

Corollaire. Soit E/K une extension engendrée par une famille finie $\{x_i\}_{i \in I}$ d'éléments algébriques sur K. Alors E/K est normale et seulement si les polynômes minimaux des x_i sur K sont tous scindés sur E.

> **Démonstration :** Si E/K est normale, alors pour tout $i \in I$ le polynôme minimal P_i de x_i sur K a une racine dans E (à savoir, x_i) et est donc scindé sur E.
>
> Réciproquement supposons que les polynômes minimaux des x_i sur K sont scindés sur E. Alors leur produit, noté P, est scindé sur E. Comme de plus E est engendrée par les x_i, c'est le corps de décomposition de P sur K. D'après l'implication 1 ⇒ 3 du théorème, E/K est normale. ■

Exemples.

1. L'extension $\mathbb{Q}(j, \sqrt[3]{2})/\mathbb{Q}$ est normale. En effet, c'est le corps de décomposition du polynôme $X^3 - 2$.
2. Si p est un nombre premier, l'extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ est normale. En effet c'est le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$ (noter que le polynôme n'a pas à être irréductible).
3. Si p est un nombre premier, $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ est normale. En effet, c'est le corps de décomposition de $P = X^p - t^p = (X - t)^p \in \mathbb{F}_p(t^p)$.

▶Clôture normale

Proposition. Soit E/K une extension finie. Il existe une extension finie N/E avec les propriétés suivantes :

1. L'extension N/K est normale,
2. Si $E \subset N' \subset N$ avec N'/K normale, alors $N' = N$.
   De plus, cette extension est unique à K-isomorphisme près.

> **Démonstration :** nous nous contentons d'indications de construction et la lectrice pourra compléter la démonstration. On peut choisir un système de générateurs $x_1, \dots, x_r$ de E/K

et construire N comme corps de décomposition du polynôme $P = P_1 \cdots P_r$, où P_i est le polynôme minimal de x_i sur K. Alternativement, on peut noter $\sigma_1, \dots, \sigma_d$ les $d = [E : K]_s$ plongements de E dans une clôture algébrique $\overline{K}$, et construire N comme sous-corps de $\overline{K}$ engendré par $\sigma_1(E), \dots, \sigma_d(E)$. ■

Définition. Soit E/K une extension finie. L'extension N/K de la proposition précédente est appelée la *clôture normale* de E/K.

5.2. Extensions galoisiennes

Définition. Soit E/K une extension. On dit que E/K est *galoisienne* si elle est algébrique, séparable et normale.

Remarque. Nous nous intéresserons surtout aux extensions galoisiennes *finies* (et nous énoncerons la correspondance de Galois dans ce cadre), d'une part par simplicité et d'autre part car l'étude des extensions galoisiennes infinies se ramène au cas des extensions finies. Certains des énoncés ci-dessous ne sont donc pas énoncés avec le niveau de généralité maximum. Voici un exemple d'extension galoisienne infinie, peut-être le plus intéressant de toute la théorie : l'extension $\overline{\mathbb{Q}}/\mathbb{Q}$ fournie par une clôture algébrique de $\mathbb{Q}$. En effet elle est algébrique par définition, séparable puisque de caractéristique 0, et normale car tout polynôme y est scindé.

Proposition. Soit E/K une extension. Il y a équivalence entre :

1. L'extension E/K est galoisienne et finie,
2. Il existe $P \in K[X]$ irréductible séparable tel que E est un corps de décomposition de P sur K.
3. Il existe $P \in K[X]$ non constant séparable tel que E est un corps de décomposition de P sur K.

Démonstration : 1 ⇒ 2. Si l'extension finie E/K est galoisienne, elle est séparable, donc monogène par le théorème de l'élément primitif. Soit alors $x \in E$ tel que $E = K(x)$ et P le polynôme minimal de x sur K. Alors E est un corps de rupture de P, mais comme E/K est normale, c'est un corps de décomposition. Enfin, puisque E/K est séparable, x est séparable et donc P est séparable.

2 ⇒ 3 car un polynôme irréductible est non constant.

3 ⇒ 1. Si E est un corps de décomposition d'un polynôme $P \in K[X]$ non constant séparable, l'extension E/K finie. De plus, elle est normale par le théorème des extensions normales. De plus, E est engendré par les racines de P. Mais, si x est une racine de P, alors le polynôme minimal $P_{x,K}$ divise P. Comme P est séparable, on déduit que $P_{x,K}$ est séparable donc x est séparable. Ainsi, E/K est engendrée par des éléments séparables, elle est donc séparable (théorème des extensions séparables). Nous avons montré que E/K est finie, séparable et normale. ■

Corollaire. Soit E/K une extension finie galoisienne. Si L est une extension de K dans E, alors E/L est galoisienne.

Démonstration : En effet, E est un corps de décomposition d'un polynôme $P \in K[X]$ séparable sur K, donc c'est aussi un corps de décomposition de P sur L. ■

Exemples et contre-exemples.

1. Une extension de degré 2 en caractéristique différente de 2 est toujours galoisienne.
2. Une extension galoisienne d'une extension galoisienne n'est pas forcément galoisienne (voir paragraphe précédent).

3. Une sous-extension d'une extension galoisienne n'est pas forcément galoisienne : par exemple $\mathbb{Q}(j, \sqrt[3]{2})/\mathbb{Q}$ est galoisienne mais sa sous-extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n'est pas normale.
4. L'extension $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ est normale mais elle n'est pas séparable, donc pas galoisienne.
5. Une extension de corps finis est toujours galoisienne.

▶Clôture galoisienne

Si E/K est une extension finie et séparable, la construction de sa clôture normale N/K comme corps de décomposition du polynôme $P = P_1 \cdots P_r$, où $x_1, \dots, x_r$ sont des générateurs de E/K de polynômes minimaux P_i, montre que N/L est séparable. Dans ce cas on parle de *clôture galoisienne* de E/K.

5.3. Groupe de Galois

Définition. Si E/K est une extension de corps, on note $\mathrm{Gal}(E/K)$ le groupe des K-automorphismes de E, et on l'appelle le groupe de Galois de l'extension E/K. Si $P \in K[X]$ est un polynôme, on appelle *groupe de Galois de* P le groupe de Galois de son corps de décomposition.

Théorème d'inégalité. Soit E/K une extension finie. On a alors l'inégalité

$$|\mathrm{Gal}(E/K)| \leqslant [E : K].$$

De plus $|\mathrm{Gal}(E/K)| = [E : K]$ si et seulement si E/K est galoisienne.

> **Démonstration :** Notons $n = [E : K]$.
>
> Supposons d'abord E/K galoisienne. Par le théorème de l'élément primitif, elle est monogène : choisissons un générateur x et notons P son polynôme minimal. Comme $E = K(x)$, on a $\deg(P) = [E : K] = n$ et par ailleurs E/K étant normale et séparable, P est scindé sur E avec n racines distinctes $x = x_1, \dots, x_n$. La donnée d'un K-automorphisme $f : K(x) \to K(x)$ est équivalente à la donnée de l'image de x, qui peut être n'importe laquelle des racines x_i, comme nous l'avons énoncé il y a longtemps dans le §2.4 sur les propriétés du corps de rupture. Ceci fait n possibilités pour f donc $|\mathrm{Gal}(E/K)| = n$.
>
> Supposons ensuite E/K non galoisienne. Si elle n'est pas séparable, on a $[E : K]_s < [E : K]$. En appliquant les définitions on voit que :
>
> $$|\mathrm{Gal}(E/K)| = |\mathrm{Hom}_K(E, E))| \leqslant |\mathrm{Hom}_K(E, \overline{K})| = [E : K]_s < [E : K].$$
>
> Si elle est séparable mais pas normale, d'après le théorème de l'élément primitif on peut écrire $E = K(x)$ où x est un générateur, et P son polynôme minimal qui est de degré n. Comme précédemment le cardinal de $\mathrm{Gal}(E/K)$ est égal au nombre de racines distinctes de P dans E. Ce nombre est $< n$ car sinon E serait un corps de décomposition de P sur K et serait donc une extension normale. ■

🛈 Le cours du jeudi 26 mars 2026 s'est arrêté ici.

Corollaire. Soit E/K une extension finie galoisienne et posons $G := \mathrm{Gal}(E/K)$. On a alors $E^G = K$.

> **Démonstration :** notons $K' = E^G$ la sous-extension de points fixes. Alors $\mathrm{Gal}(E/K) \subset \mathrm{Gal}(E/K')$ par définition de K' et $\mathrm{Gal}(E/K') \subset \mathrm{Gal}(E/K)$ puisque $K' \supset K$. Ces deux groupes sont donc égaux. Par ailleurs E/K et E/K' sont galoisiennes, donc par le théorème précédent $|\mathrm{Gal}(E/K)| = [E : K]$ et $|\mathrm{Gal}(E/K')| = [E : K']$. On en déduit que $[E : K'] = [E : K]$ donc $[K' : K] = 1$ puis $K' = K$. ■

Théorème d'Artin. Soit E un corps et soit $\mathrm{Aut}(E)$ le groupe des automorphismes de E. Soit G un sous-

groupe fini de $\mathrm{Aut}(E)$. On pose $K = E^G$. Alors E/K est une extension finie galoisienne, et son groupe de Galois est G. En particulier $[E : K] = |G|$.

Démonstration : Notons $n = |G|$ et $G = \{\sigma_1, \dots, \sigma_n\}$.

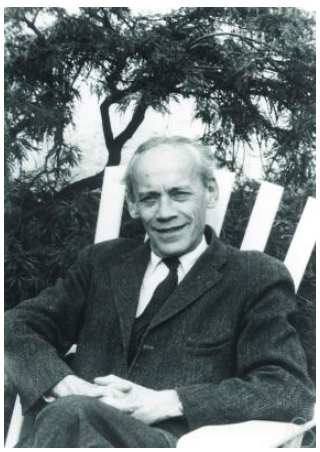
On démontre d'abord que E/K est galoisienne. Soit $x \in E$. Le groupe G agit sur E et l'orbite de x est de cardinal $k \leqslant n$. On la note $O_G(x) = \{\sigma_1(x), \dots, \sigma_k(x)\}$ quitte à renuméroter les σ_i. L'action de G sur E s'étend en une action sur $E[X]$ en agissant simplement sur les coefficients des polynômes, c'est-à-dire $\sigma \cdot \sum a_i X^i := \sum \sigma(a_i) X^i$. Considérons le polynôme :

$$P(X) = \prod_{i=1}^{k} (X - \sigma_i(x)).$$

Comme chaque $\sigma \in G$ agit comme une permutation des éléments de l'orbite $O_G(x)$, qui sont les racines de P, on a $\sigma \cdot P = P$. D'après le corollaire précédent ceci implique que $P \in K[X]$. On a ainsi démontré que chaque $x \in E$ est annulé par un polynôme à coefficients dans K, scindé à racines simples dans E. Ceci démontre que E est séparable et normale, donc galoisienne.

On démontre ensuite que E/K est finie de degré $\leqslant n$. On a vu à l'instant que les éléments de E sont tous de degré $\leqslant n$. Notons $N := \max(\deg(x),\ x \in E)$ et soit $x \in E$ qui réalise ce max i.e. $\deg(x) = N$. Si $K(x) \neq E$, il existe $y \in E \setminus K(x)$. L'extension $K(x, y)/K$ est finie car x, y sont algébriques, séparable car c'est une sous-extension de l'extension séparable E. Par le théorème de l'élément primitif $K(x, y)/K$ est monogène. Comme $[K(x, y) : K] > [K(x) : K]$, ceci contredit la maximalité de N. Ainsi E/K est finie de degré $\leqslant n$.

Comme $K = E^G$, on a $G \subset \mathrm{Gal}(E/K)$. En utilisant le théorème précédent, on trouve $n = |G| \leqslant \mathrm{Gal}(E/K) \leqslant [E : K] \leqslant n$. Toutes les inégalités sont donc des égalités, en particulier E/K est finie galoisienne de degré n. ■



Emil Artin (1898-1962)

Remarque. L'étude des racines d'un polynôme à coefficients dans un corps K amène naturellement à privilégier un point de vue sur les extensions : on fixe un corps de base K et on en construit, étude, décrit les extensions E. Le théorème d'Artin offre un point de vue différent : dans cet énoncé, on part d'un corps E et on en construit des sous-corps. Le point de vue est renversé car c'est alors E qui est considéré comme le corps de départ, supposé bien compris, et c'est le corps K qui reste à élucider. Il est d'ailleurs utile de préciser que le calcul de sous-corps d'invariants E^G est en général délicat.

5.4. Correspondance de Galois

Après deux petits lemmes, nous serons prêts pour démontrer le théorème de correspondance de Galois.

▶ **Rappels sur les sous-groupes distingués**
Dans un groupe G, un sous-groupe H est dit *distingué* s'il est stable par conjugaison par des éléments de G, c'est-à-dire que pour tout $g \in G$ on a $gHg^{-1} \subset H$. Par exemple, le noyau d'un morphisme de groupes $f : G \to G'$ est toujours distingué.

Lemme de suite exacte. Soient E/K une extension finie galoisienne et L une sous-extension de E. Soit H_L le sous-groupe de $\mathrm{Gal}(E/K)$ formé des éléments σ qui vérifient $\sigma(L) = L$. Alors tout $\sigma \in H_L$ induit un K-automorphisme σ_L de L. L'application $f : H_L \to \mathrm{Gal}(L/K)$ définie par $f(\sigma) = \sigma_L$ est un morphisme surjectif de groupes et son noyau est $\mathrm{Gal}(E/L)$, ce que l'on représente par la suite exacte

$$0 \longrightarrow \mathrm{Gal}(E/L) \longrightarrow H_L \longrightarrow \mathrm{Gal}(L/K) \longrightarrow 0.$$

En particulier $\mathrm{Gal}(E/L)$ est un sous-groupe distingué de H_L et f induit un isomorphisme $\bar{f} : H_L/\mathrm{Gal}(E/L) \simeq \mathrm{Gal}(L/K)$.

> **Démonstration :** Lorsque σ et τ stabilisent H, on a $(\sigma \circ \tau)_H = \sigma_H \circ \tau_H$ donc f est un morphisme de groupes. Montrons que f est surjective. D'après le théorème de prolongement du §2.6, tout K-morphisme $\varphi : L \to L$ se prolonge en un morphisme $\varphi' : E \to \overline{K}$. Comme E/K est normale, on a $\varphi'(E) \subset E$ donc φ' induit un K-morphisme $\sigma : E \to E$ qui prolonge φ, comme souhaité. Calculons le noyau de f. Si $\sigma : E \to E$ est dans le noyau de f, c'est l'identité sur L, c'est-à-dire que $\sigma \in \mathrm{Gal}(E/L)$. Les dernières affirmations sont des conséquences directes. ■

Lemme. Soient E/K une extension finie galoisienne et L une sous-extension de E. Les conditions suivantes sont équivalentes :

1. L'extension L/K est galoisienne.
2. Le sous-groupe $\mathrm{Gal}(E/L) \subset \mathrm{Gal}(E/K)$ est distingué.

> **Démonstration :** 1 ⇒ 2. D'après le théorème des extensions normales (§5.1), pour tout K-morphisme $\sigma : E \to E$ on a $\sigma(L) \subset L$. Le morphisme $L \to L$ induit par σ est un endomorphisme injectif d'un K-espace vectoriel de dimension finie, donc un isomorphisme et $\sigma(L) = L$. Ainsi le groupe H_L du lemme précédent est égal à $\mathrm{Gal}(E/K)$. La conclusion du lemme fournit le fait que $\mathrm{Gal}(E/L)$ est distingué dans $\mathrm{Gal}(E/K)$.
>
> 2 ⇒ 1. Démontrons que pour tout $\sigma : E \to E$ on a $\sigma(L) = L$. Par le corollaire du §5.2, on sait que E/L est galoisienne. Par le corollaire du §5.3, on a donc $L = E^H$ où $H = \mathrm{Gal}(E/L)$. On fait alors le calcul suivant : si $h \in H$ et $x \in L$, on a
>
> $$h(\sigma(x)) = (h\sigma)(x) = (\sigma\sigma^{-1}h\sigma)(x) = \sigma((\sigma^{-1}h\sigma)(x)) = \sigma(x),$$
>
> puisque $\sigma^{-1}h\sigma \in H$ et x est fixe sous H. Ceci montre que $\sigma(x) \in E^H = L$, donc $\sigma(L) \subset L$ puis comme ci-dessus $\sigma(L) = L$. Avec les mêmes notations que précédemment, ceci signifie que $H_L = \mathrm{Gal}(E/K)$. En utilisant ① le lemme précédent ② le théorème d'inégalité du §5.3 et ③ le théorème de la base téléscopique, on trouve :
>
> $$|\mathrm{Gal}(L/K)| \overset{①}{=} \frac{|Gal(E/K)|}{|Gal(E/L)|} \overset{②}{=} \frac{[E:K]}{[E:L]} \overset{③}{=} [L:K].$$
>
> Le théorème d'inégalité entraine alors que L/K est galoisienne. ■

Théorème de correspondance de Galois. Soit E/K une extension finie galoisienne. Les applications

$$\begin{array}{ccc} \{\text{sous-}K\text{-extensions de } E\} & \longleftrightarrow & \{\text{sous-groupes de } \mathrm{Gal}(E/K)\} \\ L & \overset{f}{\longmapsto} & \mathrm{Gal}(E/L) \\ E^H & \overset{g}{\longmapsto} & H \end{array}$$

sont des bijections réciproques l'une de l'autre, strictement décroissantes pour l'inclusion. De plus L/K est galoisienne si et seulement si $\mathrm{Gal}(E/L)$ est un sous-groupe distingué de $\mathrm{Gal}(E/K)$.

Démonstration : On sait que pour toute sous-extension L, l'extension E/L est galoisienne (cor. du §5.2). Ceci implique que $|\mathrm{Gal}(E/L)| = [E : L]$. En particulier f est strictement décroissante, car si $L \subsetneq L'$ alors $[E : L] > [E : L']$ donc $|\mathrm{Gal}(E/L)| > |\mathrm{Gal}(E/L')|$ et $\mathrm{Gal}(E/L') \subsetneq \mathrm{Gal}(E/L)$.

Le théorème d'Artin (§5.3) nous dit que pour tout sous-groupe $H \subset \mathrm{Gal}(E/K)$, on a $f(g(H)) = \mathrm{Gal}(E/E^H) = H$. Soit alors L une sous-extension. Par définition du groupe de Galois, les éléments de L sont fixes sous $\mathrm{Gal}(E/L)$ donc $L \subset E^{\mathrm{Gal}(E/L)} = g(f(L))$. L'égalité $f(g(H)) = H$ démontrée ci-dessus, appliquée pour $H = f(L)$, fournit $f(g(f(L))) = f(L)$. Comme f est *strictement* décroissante, ceci implique que l'inclusion $L \subset g(f(L))$ est une égalité. Ainsi f et g sont des bijections réciproques l'une de l'autre. Dans cette circonstance, si f est strictement décroissante alors g l'est automatiquement aussi.

Pour finir, le fait que sous-extensions L/K galoisiennes et sous-groupes $\mathrm{Gal}(E/L)$ distingués se correspondent à été vu dans le lemme précédent. ■

Exemple. Alors que les sous-extensions de E/K peuvent sembler mystérieuses a priori, les sous-groupes d'un groupe fini peuvent être énumérés au moins dans des exemples de taille raisonnable. Considérons par exemple l'extension $E = \mathbb{Q}(\alpha, j)$ avec $\alpha = \sqrt[3]{2}$, corps de décomposition de $P = X^3 - 2$. Son groupe de Galois est isomorphe au groupe symétrique $G = S_3$ engendré par le 3-cycle σ tel que $\sigma(\alpha) = j\alpha$ et $\sigma(j) = j$, et la transposition τ telle que $\tau(\alpha) = \alpha$ et $\tau(j) = j^2$. Avec le théorème de correspondance de Galois, on peut énumérer les 6 sous-groupes de G et en déduire que Epossède 6 sous-extensions :

Sous-groupes H	G	$\langle\sigma\rangle$	$\langle\tau\rangle$	$\langle\sigma\tau\rangle$	$\langle\sigma^2\tau\rangle$	$\{1\}$
Sous-extensions L	$\mathbb{Q}$	$\mathbb{Q}(j)$	$\mathbb{Q}(\alpha)$	$\mathbb{Q}(j^2\alpha)$	$\mathbb{Q}(j\alpha)$	$\mathbb{Q}(\alpha, j)$
$[G : H] = [L : K]$	1	2	3	3	3	6

Commentaires. Grâce à la notion de clôture galoisienne, on peut dire que le théorème de correspondance de Galois s'applique au cas d'extensions finies séparables non normales : on plonge tout simplement une telle extension dans sa clôture galoisienne, pour laquelle la correspondance de Galois s'applique.
En revanche, le théorème de correspondance n'apporte aucune information sur les extensions non séparables.

6. Résolubilité par radicaux des équations polynomiales

Au début du cours, nous nous sommes demandés : est-il possible de résoudre toute équation polynomiale par radicaux ? Plus précisément, peut-on exprimer par des formules utilisant les cinq opérations élémentaires

$$+ \quad - \quad \times \quad \div \quad \sqrt[n]{\ }$$

les racines de n'importe quelle équation polynomiale $P(x) = 0$? La théorie de Galois permet de répondre à cette question. En effet, ces opérations s'interprètent facilement dans la théorie des corps : les quatre premières sont des opérations internes à un corps K, et la dernière, l'extraction d'une racine n-ième d'un élément $a \in K$, revient à construire une extension monogène $K(x)$ avec $x^n = a$. Utiliser un nombre fini de ces opérations revient donc à se placer dans une extension du type suivant.

Définition. Une *extension par radicaux* est une extension finie E/K qui est une composée $K = K_0 \subset K_1 \subset \cdots \subset K_n = E$ telle que pour tout i on a $K_{i+1} = K_i(x_i)$ avec $(x_i)^{m_i} \in K_i$, pour un certain entier m_i premier avec l'exposant caractéristique de K.

Remarque. En caractéristique 0, la condition sur les m_i est toujours vérifiée ; elle a pour conséquence qu'une extension radicale est toujours séparable. En caractéristique p, nous reviendrons plus loin sur le bien-fondé de cette condition.

Ce qu'a compris Évariste Galois, c'est qu'une extension par radicaux possède un groupe de Galois d'un type très particulier, que nous introduisons maintenant.

6.1. Groupes résolubles

Définition. Soit G un groupe.

- On appelle *sous-groupe dérivé* de G le sous-groupe engendré par les commutateurs $[x, y] := xyx^{-1}y^{-1}$, avec $x, y \in G$. On le note $D(G)$.
- On appelle *suite dérivée* de G la suite décroissante de sous-groupes définie par $D^0(G) = G$ et $D^{i+1}(G) = D(D^i(G))$ pour tout $i \geq 0$.
- On dit que G est *résoluble* si la suite dérivée $D^i(G)$ stationne à $\{1\}$ pour un certain i.

Notons que l'inverse d'un commutateur est un commutateur, mais le produit de deux commutateurs n'est pas un commutateur en général, si bien que l'on doit bien définir $D(G)$ comme sous-groupe *engendré par* les commutateurs.

**Exemples et contre-exemples$$, cités par ordre croissant de complexité algébrique :

1. *Résolubles.* Les groupes abéliens, les p-groupes (groupes finis dont l'ordre est une puissance d'un nombre premier p), les groupes diédraux, les groupes S_3, S_4, A_3, A_4, le groupe des matrice triangulaires supérieures, sont tous résolubles.
2. *Non résolubles.* Pour $n \geqslant 5$, les groupes alternés A_n et symétriques S_n ne sont pas résolubles, car $D(S_n) = D(A_n) = A_n$. Mis à part les cas $(n = 2, K = \mathbb{F}_2)$ et $(n = 2, K = \mathbb{F}_3)$ les groupes $\mathrm{GL}_n(K)$ et $\mathrm{SL}_n(K)$ ne sont pas résolubles car $D(\mathrm{GL}_n(K)) = D(\mathrm{SL}_n(K)) = \mathrm{SL}_n(K)$.

Lemme (propriétés du groupe dérivé). Soient G un groupe et H un sous-groupe distingué.

1. Le groupe G est abélien si et seulement si $D(G) = 1$.
2. Le sous-groupe $D(G)$ est distingué et le quotient $G/D(G)$ est abélien.
3. Le quotient G/H est abélien si et seulement si $D(G) \subset H$.
4. Tout morphisme de groupes $f : G \to G'$ envoie $D(G)$ dans $D(G')$.

Démonstration : 1. Ceci découle du fait que $[x, y] = 1$ si et seulement si $xy = yx$.

2. Le conjugué d'un commutateur est un commutateur :

$$g[x, y]g^{-1} = g(xyx^{-1}y^{-1})g^{-1} = gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1} = [gxg^{-1}, gyg^{-1}].$$

Comme tout élément $h \in D(G)$ est un produit de commutateurs, on voit ainsi que $ghg^{-1} \in D(G)$. Ainsi $D(G)$ est distingué. Ensuite notons $\pi : G \to G/D(G)$ le

morphisme de quotient. Soient $\bar{x}, \bar{y}$ deux éléments de $G/D(G)$ représentés par $x, y \in G$ et calculons leur commutateur :

$$[\bar{x}, \bar{y}] = \bar{x}\bar{y}\bar{x}^{-1}\bar{y}^{-1} = \overline{xyx^{-1}y^{-1}} = 1$$

puisque le commutateur $xyx^{-1}y^{-1}$ appartient au noyau de π. On a montré que tous les commutateurs de $G/D(G)$ sont triviaux, donc $G/D(G)$ est abélien.

3. Notons $f : G \to G/H$ le morphisme de quotient. Alors G/H est abélien ssi tous les commutateurs $[\bar{x}, \bar{y}]$ dans G/H sont triviaux, ssi tous les commutateurs $[x, y]$ dans G appartiennent à $\ker(f) = H$, ssi le sous-groupe engendré par les commutateurs est inclus dans H.

4. Ceci découle du fait que $f([x, y]) = [f(x), f(y)]$. ■

Lemme (reformulation de la résolubilité). Soit G un groupe. Les conditions suivantes sont équivalentes :

1. Il existe une suite de sous-groupes $G_0 = G \supset G_1 \supset \cdots G_{n-1} \supset G_n = \{1\}$ telle que G_{i+1} est distingué dans G_i et G_i/G_{i+1} est abélien, pour tout $i = 0, \dots, n-1$.
2. La suite dérivée $D^i(G)$ stationne à $\{1\}$ pour un certain i, c'est-à-dire G est résoluble.

Démonstration : 1 ⇒ 2. On montre par récurrence que $D^i(G) \subset G_i$ pour tout $i \leq n$. Initialisation : pour $i = 0$, on a $D^0(G) = G = G_0$ et la propriété est vérifiée. Hérédité : on suppose que $D^i(G) \subset G_i$. Comme G_i/G_{i+1} est abélien, on a $D(G_i) \subset G_{i+1}$. On en déduit que $D^{i+1}(G) = D(D^i(G)) \subset D(G_i) \subset G_{i+1}$.

2 ⇒ 1. La propriété est vérifiée en prenant $G_i = D^i(G)$. ■

Lemme (transfert de la résolubilité). Soient G un groupe et H un sous-groupe distingué. Alors les conditions suivantes sont équivalentes :

1. Le groupe G est résoluble,
2. Les groupes H et G/H sont résolubles.

Démonstration : On suppose G résoluble et on note $\pi : G \to G/H$ le quotient.
1 ⇒ 2. Par deux récurrences immédiates, on a $D^i(G) \subset D^i(G)$ et $D^i(G/H) = \pi(D^i(G))$. Il s'ensuit que si pour un certain i on a $D^i(G) = 1$, alors $D^i(H) = D^i(G/H) = 1$, donc H et G/H sont résolubles.
2 ⇒ 1. Comme G/H et H sont résolubles, par le lemme précédent il existe deux suites de sous-groupes distingués à quotients successifs abéliens :
$K_0 = G/H \supset K_1 \supset \cdots \supset K_s = \{1\}$ et $H_s = H \supset H_{s+1} \supset \cdots H_t = \{1\}$. Pour chaque $i = 0, \dots, s-1$ notons H_i la préimage de K_i par le morphisme $\pi : G \to G/H$ et notons que le groupe H_i/H_{i+1} est isomorphe à K_i/K_{i+1}, donc abélien. En mettant bout à bout les deux suites on obtient une suite

$$H_0 = G \supset H_1 \supset \cdots \supset H_s = H \supset H_{s+1} \supset \cdots H_t = \{1\}$$

de sous-groupes distingués à quotients successifs abéliens. Ceci démontre que G est résoluble. ■

6.2. Groupes de Galois d'extensions résolubles

Lemme. Soit E/K une extension galoisienne finie et $\zeta \in \overline{K}$ une racine de l'unité d'ordre m premier avec la caractéristique. Alors $E(\zeta)/K(\zeta)$ est galoisienne. De plus, si $\mathrm{Gal}(E(\zeta)/K(\zeta))$ est résoluble alors $\mathrm{Gal}(E/K)$ est résoluble.

Démonstration : Par hypothèse sur E/K il existe un polynôme non constant séparable $P \in K[X]$ tel que E est un corps de décomposition de P. Alors $Q = (X^m - 1)P$ est non constant séparable, et $E(\zeta)$ est un corps de décomposition de Q. Donc $E(\zeta)/K(\zeta)$ est galoisienne.
Supposons maintenant $\mathrm{Gal}(E(\zeta)/K(\zeta))$ résoluble. On sait que $K(\zeta)/K$ est galoisienne car c'est le corps de décomposition de $X^m - 1$, et son groupe de Galois est isomorphe à $(\mathbb{Z}/m\mathbb{Z})^\times$ car un K-automorphisme $f : K(\zeta) \to K(\zeta)$ doit envoyer ζ sur une racine primitive m-ième de l'unité ζ^i pour un $i(\mathbb{Z}/m\mathbb{Z})^\times$. Ce groupe est abélien donc résoluble.
Selon le lemme de suite exacte (§5.4) on a une suite exacte

$$0 \longrightarrow \mathrm{Gal}(E(\zeta)/K(\zeta)) \longrightarrow \mathrm{Gal}(E(\zeta)/K) \longrightarrow \mathrm{Gal}(K(\zeta)/K) \longrightarrow 0,$$

et le lemme de transfert de la résolubilité (§6.1) implique que $\mathrm{Gal}(E(\zeta)/K)$ est résoluble. Utilisant encore le lemme de suite exacte, on voit que $\mathrm{Gal}(E/K)$ est un quotient de $\mathrm{Gal}(E(\zeta)/K)$, donc il est résoluble. ■

Théorème. Si E/K est une extension radicale galoisienne, le groupe $\mathrm{Gal}(E/K)$ est résoluble.

Démonstration : Écrivons $K = K_0 \subset K_1 \subset \cdots \subset K_n = E$ avec $K_{i+1} = K_i(x_i)$ avec $(x_i)^{m_i} \in K_i$ et m_i premier avec l'exposant caractéristique de K. Notons m le produit des m_i et soit $\zeta \in \overline{K}$ une racine de l'unité d'ordre m. Il est clair que $E(\zeta)/K$ et $E(\zeta)/K(\zeta)$ sont radicales. D'après le lemme, si $\mathrm{Gal}(E(\zeta)/K(\zeta))$ est résoluble alors $\mathrm{Gal}(E/K)$ le sera. On peut donc supposer que $\zeta \in E$, ce que nous faisons désormais.
Comme E/K est galoisienne, les extensions E/K_i le sont. D'autre part K_{i+1}/K_i est galoisienne de groupe de Galois $\mathbb{Z}/m_i\mathbb{Z}$ car les automorphismes de cette extension sont exactement les K_i-morphismes $f : K_{i+1} \to K_{i+1}$ tels que $f(x_i) = \zeta^d x_i$ pour un $d \in \mathbb{Z}/m_i\mathbb{Z}$.
Posons $G_i = \mathrm{Gal}(E/K_i)$. On a une suite d'inclusions
$G_0 = \mathrm{Gal}(E/K) \supset G_1 \supset \cdots G_{n-1} \supset G_n = \{1\}$ avec G_{i+1} distingué dans G_i et $G_i/G_{i+1} \simeq \mathrm{Gal}(K_{i+1}/K_i) \simeq \mathbb{Z}/m_i\mathbb{Z}$ pour tout $i = 0, \dots, n-1$. Comme on l'a vu au §6.1, ceci implique que $\mathrm{Gal}(E/K)$ est résoluble. ■

6.3. Exemples d'équations non résolubles par radicaux

Dans ce paragraphe nous allons donner un exemple de polynôme non constant dont les racines ne peuvent pas s'exprimer par radicaux.

Définition. Soit P un polynôme non constant à coefficients dans un corps K. On dit que *les racines de P peuvent s'exprimer par radicaux* si tout corps de décomposition de P est inclus dans une extension par radicaux, ou de manière équivalente, s'il existe une extension par radicaux dans laquelle P est scindé.

Lemme. 1. Soient E_1/K et E_2/K deux extensions par radicaux. Alors la sous-extension de $\overline{K}$ engendrée par E_1 et E_2 est par radicaux.
2. Soit E/K une extension par radicaux. Alors sa clôture galoisienne N/K est une extension par radicaux.

Démonstration : 1. Notons $E_1 = K(x_0, \dots, x_{n-1})$ où les x_i vérifient les conditions de la définition d'une extension par radicaux. Notons de même $E_2 = K(y_0, \dots, y_{m-1})$. Alors l'extension engendrée par E_1 et E_2 s'écrit $K(x_0, \dots, x_{n-1}, y_0, \dots, y_{m-1})$ qui est une extension par radicaux.

2. Notons $\sigma_1, \dots, \sigma_d$ les $d = [E : K]_s$ plongements de E dans une clôture algébrique $\overline{K}$. La clôture galoisienne N est le sous-corps de $\overline{K}$ engendré par $\sigma_1(E), \dots, \sigma_d(E)$. D'après le

point précédent, c'est une extension par radicaux. ■

Soit $P \in K[X]$ un polynôme non constant dont les racines peuvent s'exprimer par radicaux. Soit D un corps de décomposition pour P. D'après le point 2 du lemme, il existe une extension par radicaux galoisienne E/K qui contient D. D'après le théorème du paragraphe précédent, le groupe $\mathrm{Gal}(E/K)$ est résoluble. Comme le groupe $\mathrm{Gal}(D/K)$ est un quotient de $\mathrm{Gal}(E/K)$ (voir lemme de suite exacte, §5.4), il est également résoluble. Dans la fin de ce paragraphe, nous allons montrer comment construire des polynômes dont le corps de décomposition a un groupe de Galois non résoluble, répondant ainsi par la négative à la question de donner des formules par radicaux pour exprimer les racines.

Voici d'abord deux exemples de groupes non résolubles.

Lemme. Soit $n \geqslant 5$ un entier. Alors $D(S_n) = D(A_n) = A_n$. En conséquence, les groupes S_n et A_n ne sont pas résolubles.

Démonstration : Nous utilisont le fait classique que le groupe A_n est engendré par les 3-cycles. Démontrons que dans A_n, tout 3-cycle est un commutateur. Soit (a, b, c) un 3-cycle, comme $n \geqslant 5$ il existe dans $\{1, 2, \dots, n\}$ deux lettres d, e distinctes et distinctes de a, b, c. Posons $u = (b, c)(d, e)$. On vérifie par un petit calcul que $(a, b, c) = u(a, b, c)u^{-1}(a, c, b) = [u, (a, b, c)]$ qui est un commutateur. Il en découle que $D(A_n) = A_n$.
Comme $A_n \subset S_n$, on a $A_n = D(A_n) \subset D(S_n)$ donc pour démontrer que $D(S_n) = A_n$ il suffit de démontrer que $D(S_n) \subset A_n$. Or ceci est une conséquence du fait que tout commutateur est une permutation paire, puisque

$$\epsilon([x, y]) = \epsilon(x)\epsilon(y)\epsilon(x)^{-1}\epsilon(y)^{-1} = 1.$$

Il s'ensuit que $D^i(S_n) = D^i(A_n) = A_n$ pour tout $i \geqslant 1$, donc les suites dérivées de S_n et de A_n ne sont pas stationnaires à 1. Ces groupes ne sont pas résolubles. ■

Voici maintenant des parties génératrices de S_p lorsque p est premier.

Lemme. Soit p un nombre premier. Alors toute partie $\{\sigma, \tau\}$ composée d'un p-cyle σ et d'une transposition τ engendre S_p.

Démonstration : Il est standard que $(1, 2)$ et $(1, 2, \dots, p)$ engendrent S_p, nous l'admettons. Quitte à renuméroter les symboles, on peut supposer que $\tau = (1, 2)$. Écrivons $\sigma = (1, i_2, \dots, i_p)$. L'une des lettres i_k vaut 2, c'est-à-dire que $\sigma^k(1) = 2$. Comme p est premier, l'entier k est premier avec lui de sorte que σ^k est d'ordre p. Or $\sigma^k(1, 2, j_3, \dots, j_p)$ et quitte à renuméroter les $p - 2$ derniers symboles, on peut supposer que $\sigma^k = (1, 2, \dots, p)$. Alors τ et σ^k engendrent S_p. ■

Théorème. Soit $P \in \mathbb{Q}[X]$ un polynôme irréductible de degré p premier. On suppose que P possède exactement deux racines non réelles. Soit D un corps de décomposition de P. Alors $\mathrm{Gal}(D/\mathbb{Q}) \simeq S_p$.

Démonstration : Si $p = 2$ l'énoncé est facile à vérifier et nous supposons donc que $p \geqslant 3$. Le groupe $\mathrm{Gal}(D/\mathbb{Q})$ se plonge dans le groupe des permutations des racines de P dans D, isomorphe à S_p. Soit $x \in D$ une racine de P, alors $p = [\mathbb{Q}(x) : \mathbb{Q}]$ divise $[D : \mathbb{Q}] = \mathrm{Gal}(D/\mathbb{Q})$. D'après le lemme de Cauchy, le groupe $\mathrm{Gal}(D/\mathbb{Q})$ possède une élément σ d'ordre p ; dans S_p tous les éléments d'ordre p sont des p-cycles. Par ailleurs la conjugaison complexe $\tau(z) = \bar{z}$ définit un automorphisme de $\mathbb{C}$ qui stabilise D puisque D est normale. Comme P possède exactement deux racines non réeelles, la permutation τ les échange et elle fixe toutes les autres racines, autrement dit vue dans S_p c'est une

transposition. D'après le lemme précédent σ et τ engendrent S_p, donc $\mathrm{Gal}(D/\mathbb{Q}) \simeq S_p$. ■

Il ne nous reste qu'à trouver un polynôme qui satisfait les hypothèses du théorème.

Exemple. Posons $P(X) = X^5 - 4X^2 + 2$. On a $P(-1) < 0$, $P(0) > 0$, $P(1) < 0$ et $P(2) > 0$, donc par le théorème des valeurs intermédiaires P a au moins 3 racines réelles distinctes. Par le théorème de Rolle, entre deux racines réelles de P se trouve une racine réelle de sa dérivée. Si P avait 4 racines réelles, P' en aurait au moins 3 et $P'' = 20X^3 - 8$ au moins 2. Comme P'' a une seule racine réelle, on déduit que P a exactement trois racines réelles.