ALGÈBRE 2: ANNEAUX, CORPS, THÉORIE DE GALOIS

PIERRE DEHORNOY

Ces notes correspondent au cours d'algèbre 2 enseigné à l'École normale supérieure de Lyon auprès des élèves de première année (niveau L3), au printemps 2023. Elles sont fortement inspirées des notes rédigées par Laurent Berger qui a précédemment enseigné ce cours, ainsi que des livres suivants, que nous recommandons:

- Grégory Berhuy, *Algèbre, le grand combat* (2018), Calvage et Mounet: un livre récent, très complet et détaillé;
- Michel Demazure, *Cours d'algèbre, primalité, divisibilité, codes* (1997), Cassini: un classique, très orienté cryptographie et qui détaille beaucoup d'aspects algorithmiques intéressants;
- Serge Lang, *Algèbre* (trad, rééd 2020) Dunod: très complet;
- Yvan Gozard, *Théorie de Galois* (2009), Ellipses: va (évidemment vu son titre) plus loin que les autres côté Galois;
- Daniel Perrin, *Cours d'algèbre* (1996), Ellipses: un classique assez condensé, plein d'exercices (voir aussi le corrigé des exercices par Pascal Ortiz, *Exercices d'algèbre* (2004), Ellipses).

Contents

Date: printemps 2023.

1. Anneaux commutatifs

On suppose connue la notion de groupe. La notion d'anneau ayant aussi déjà été évoquée en classe préparatoires ou à l'université, on va aller assez vite sur les définitions de base.

1.1. **Anneaux, sous-anneaux, morphismes.**

Définition 1.1. Un *anneau* est un ensemble A, contenant deux éléments notés 0_A et 1_A, muni de deux lois $+_A$ et $\cdot_A$, tels que

- $(A, +_A)$ est un groupe abélien de neutre 0_A;
- $(A, \cdot_A)$ est un monoïde associatif de neutre 1_A;
- $\cdot_A$ est ditributive à gauche et à droite par rapport à $+_A$.

La définition usuelle ne requiert pas que $\cdot_A$ soit commutative. Ainsi, $M_n(A)$ pour A un anneau quelconque, muni de l'addition et de la multiplication matricielles, est un anneau non commutatif. Cependant, dans ce cours, on ne considérera que des anneaux dits *commutatifs* au sens où la loi de multiplication est commutative.

Quand il n'y a pas d'ambiguïté, on note $0, 1, +$ et $\cdot$ à la place de $0_A, 1_A, +_A$ et $\cdot_A$, et même on supprime le symbole $\cdot$ quand c'est possible.

Comme pour les groupes abéliens, on note $-a$ l'opposé pour $+$ d'un élément a, et on abrège $a + (-b)$ en $a - b$.

Pour tout élément $x \in A$, on a $0 \cdot x = 0$. En effet, on a $0 \cdot x + x = (0 + 1) \cdot x = 1 \cdot x = x$.

Si jamais on a $0 = 1$, alors l'anneau tout entier est réduit à $\{0\}$.

Exemple 1.2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ et $\mathbb{Z}/n\mathbb{Z}$ (pour $n \in \mathbb{Z}$) munis des lois d'addition et de multiplication standards sont des anneaux.

Exemple 1.3. Si A_1, A_2 sont deux anneaux, le produit $A_1 \times A_2$ est naturellement muni d'une structure d'anneau où l'addition et la multiplication sont définies terme à terme.

Exemple 1.4. Si A est un anneau et I un ensemble, l'ensemble A^I des fonctions de I dans A, muni de l'addition et de la multiplication terme à terme, est aussi un anneau.

Exemple 1.5. Si A est un anneau commutatif, l'ensemble $A[X]$ des polynomes en une indéterminée X est un anneau. Ses éléments sont les séries presque nulles, c'est-à-dire de la forme $\sum_{i \in \mathbb{N}} a_i X^i$, avec $\forall i \in \mathbb{N}, a_i \in A$, et $\exists d \in \mathbb{N}, \forall i > d, a_i = 0$. La loi $+$ est donnée par l'addition terme à terme et la loi $\cdot$ par le produit de convolution :

$$(\sum_{i \in \mathbb{N}} a_i X^i) + (\sum_{i \in \mathbb{N}} b_i X^i) = \sum_{i \in \mathbb{N}} (a_i + b_i) X^i,$$

$$(\sum_{i \in \mathbb{N}} a_i X^i) \cdot (\sum_{i \in \mathbb{N}} b_i X^i) = \sum_{i \in \mathbb{N}} (\sum_{j=0}^{i} a_j b_{i-j}) X^i.$$

Noter que la multiplication n'est pas la multiplication terme à terme, de sorte que $A[X]$ est un anneau différent de $A^{\mathbb{N}} = A \times A \times \dots$ (en particulier on verra que $A[X]$ est intègre tandis que $A^{\mathbb{N}}$ ne l'est pas).

Exemple 1.6. Pour I un ensemble d'indices, on peut considérer des variables (formelles) $(X_i)_{i\in I}$, et l'anneau $A[(X_i)_{i\in I}]$ des polynomes en $(X_i)_{i\in I}$ comme l'ensemble des séries presque nulles, c'est-à-dire de la forme $\sum_{(k_i)_{i\in I}\in\mathbb{N}^I} a_{(k_i)_{i\in I}} \prod_{i\in I} X_i^{k_i}$, où seul un nombre fini de termes $a_{(k_i)_{i\in I}}$ sont non nuls, muni de l'addition terme à terme et de la mulitiplication par convolution.

On vérifie en particulier que pour $I = \{1, \dots, n\}$, on a $A[X_1, \dots, X_n] = A[X_1, \dots, X_{n-1}][X_n]$.

Exemple 1.7. Si A est un anneau commutatif, l'ensemble $A[[X]]$ des séries formelles en une indéterminée X muni de l'addition terme à terme et du produit par convolution est un aussi anneau.

Définition 1.8.
- Soit A un anneau commutatif et $x \in A$ un élément, on dit que x est *inversible* (ou une *unité* de A) s'il existe $y \in A$ tel que $x \cdot y = y \cdot x = 1$.
- On note $A^\times$ l'ensemble des éléments inversibles de A. On vérifie que c'est un groupe pour la loi $\cdot$.
- Si on a $A^\times = A \setminus \{0\}$, on dit que A est un *corps*.

Si A n'est pas commutatif, on peut définir les notions d'inverse à gauche et à droite, qui peuvent différer. Évidemment, cette subtilité disparait dans le cas commutatif.

Exemple 1.9.
- $\mathbb{Z}^\times = \{-1; 1\}$;
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps;
- $(A^I)^\times = (A^\times)^I$;
- si K est un corps, $K[[X]]^\times$ est formé des séries formelles dont le terme constant est non nul.

Définition 1.10. Soit A un anneau, un *sous-anneau* est un sous-ensemble B de A tel que
- B est un sous-groupe de A pour la loi $+$;
- B contient 1 et est stable par $\cdot$.

Exemple 1.11. $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, $\mathbb{Q}$ est un sous-anneau de $\mathbb{R}$, $\mathbb{R}$ est un sous-anneau de $\mathbb{C}$.

Exemple 1.12. Si A est un anneau de fonctions, l'ensemble des éléments A ayant une propriété supplémentaire est souvent un sous-anneau. Par exemple l'ensemble des fonctions continues (*resp.* C^k, *resp.* analytiques) est un sous-anneau de $\mathbb{R}^\mathbb{R}$. De même l'ensemble des fonctions holomorphes est un sous-anneau de $\mathbb{C}^\mathbb{C}$.

Définition 1.13. Soit A, B deux anneaux. Un *morphisme d'anneaux* est une application $f : A \to B$ telle que
- f est un morphisme de groupes pour les lois $+$;
- $f(1_A) = 1_B$ et $\forall x, y \in A, f(x \cdot_A y) = f(x) \cdot_B f(y)$.

Si en plus f est bijectif, on parle d'*isomorphisme d'anneaux*.

Noter que si $f : A \to B$ est un morphisme, l'image $f(A)$ est un sous-anneau de B.

Exemple 1.14. L'inclusion d'un sous-anneau dans un anneau induit un morphisme (injectif).

Exemple 1.15. Soit A un anneau et x un élément de A. Alors l'application $\mathrm{ev}_x : A[X] \to A$ définie par $\mathrm{ev}_x(\sum_{i\in\mathbb{N}} a_i X^i) = \sum_{i\in\mathbb{N}} a_i x^i$ est un morphisme d'anneaux, appelé *morphisme d'évaluation*.

Dans ce contexte, pour $B \subset A$ un sous-anneau, l'ensemble-image $\mathrm{Im}(\mathrm{ev}_x|_B) \subset A$ est noté $B[x]$. Par exemple on a $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2}; a, b \in \mathbb{Q}\} \subset \mathbb{R}$, et $\mathbb{Z}[\mathrm{i}] = \{a+b\mathrm{i}; a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

Exemple 1.16. Soit A un anneau et x un élément *nilpotent* de A (c'est-à-dire tel que $x^n = 0$ pour un certain entier n), alors l'application $\mathrm{ev}_x : A[[X]] \to A$ définie par $\mathrm{ev}_x(\sum_{i\in\mathbb{N}} a_i X^i) = \sum_{i\in\mathbb{N}} a_i x^i$ est bien définie, et c'est un morphisme d'anneaux, aussi appelé *morphisme d'évaluation*.

1.2. **Divisibilité, intégrité, irréductibilité et primalité.**

Définition 1.17. Soit A un anneau commutatif, soit a, b deux éléments de A. On dit que a *divise* b s'il existe c dans $A \setminus \{0\}$ tel que $b = ac$. Dans ce cas on note $a|b$.

Notons que si A est un corps, tout élément non nul divise 1 et donc divise tout élément non nul. La notion n'a donc d'intérêt que dans les anneaux qui ne sont pas des corps (par exemple dans $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, A[X], \dots$).

Définition 1.18. On dit qu'un anneau A est *intègre* s'il n'a pas de diviseur 0.

Ainsi les anneaux intègres sont ceux où l'on peut simplifier les produits, où sens où

$$ab = 0 \Rightarrow (a = 0) \vee (b = 0).$$

Exemple 1.19.
- $\mathbb{Z}$ et tous les corps sont des anneaux intègres.
- $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est un nombre premier.
- Si A_1, A_2 sont deux anneaux non triviaux, l'anneau-produit $A_1 \times A_2$ n'est jamais intègre.
- De même si I est un ensemble à au moins deux éléments et A un anneau non trivial, l'anneau des fonctions A^I n'est pas intègre.
- En revanche un sous-anneau d'un anneau non intègre peut être intègre. C'est le cas par exemple pour l'anneau des fonctions holomorphes sur un ouvert connexe de $\mathbb{C}$, vu comme sous-anneau de $\mathbb{C}^{\mathbb{C}}$.

Définition 1.20. Soit A un anneau commutatif et x un élément de a.
- On dit que x est *irréductible* si x est non nul, non inversible et
$$\forall a, b \in A,\ x = ab \Rightarrow (a \in A^\times) \vee (b \in A^\times).$$
- On dit que x est *premier* si x est non nul, non inversible et
$$\forall a, b \in A,\ x|ab \Rightarrow (x|a) \vee (x|b).$$

Exemple 1.21.
- Dans $\mathbb{Z}$ on a $\{\text{irreductibles}\} = \{\text{premiers}\} = \{\pm\text{nombres premiers}\}$ (ouf).
- Dans $\mathbb{Z}/8\mathbb{Z}$, on a $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$. Les éléments non inversibles non nuls sont donc $2, 4, 6$. Parmi eux 2 et 6 sont irréductibles et premiers, tandis que 4 est réductible ($4 = 2 \cdot 2$) et non premier.
- Dans $\mathbb{Z}/12\mathbb{Z}$, on a $(\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}$. Les éléments non inversibles non nuls sont donc $2, 3, 4, 6, 8, 9, 10$. Parmi eux, 2 et 10 sont irréductibles et premiers, 3 et 9 sont premiers mais réductibles (puisque $3 \cdot 3 = 9$ et $3 \cdot 9 = 3$), tandis que $4, 6$ et 8 sont réductibles et non premiers.

Proposition 1.22. *Si un anneau commutatif A est intègre, alors tout élément de A premier est irréductible.*

Démonstration. Soit $p \in A$ un élément premier. Supposons qu'on a $p = ab$. Alors sans perte de généralité on peut supposer $p|a$, et donc il existe c dans A tel que $a = pc$, et donc $p = ab = pbc$, d'où $p(1 - bc) = 0$. Comme A est intègre et p non nul, on a $bc = 1$, donc b est une unité. □

Dans $\mathbb{Z}$, être irréductible est équivalent à être premier. Dans $K[X]$ aussi, mais c'est moins évident.

Dans $\mathbb{Z}[\sqrt{-5}]$, il n'y a pas équivalence. Ainsi $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ sont irréductibles (ce qui se voit en considérant la norme), mais pas premiers, puisqu'on a $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

1.3. **Idéaux et quotients.**

Définition 1.23. Soit A un anneau commutatif. Un *idéal* de A est une partie I telle que

- $(I, +)$ est un sous-groupe de $(A, +)$;
- I est stable par multiplication externe: $\forall i \in I, \forall a \in A, a \cdot i \in I$.

Exemple 1.24.
- Les idéaux de $\mathbb{Z}$ sont les ensembles $\{n\mathbb{Z}\,;\, n \in \mathbb{Z}\}$.
- Pour A un anneau quelconque, l'ensemble des polynomes sans terme constant est un idéal de $A[X]$.
- Pour A un anneau, E un ensemble, et $x_0 \in E$ quelconque, l'ensemble des fonctions s'annulant en x_0 est un idéal de A^E.
- Un peu plus généralement, pour A un anneau et a un élément de A, l'ensemble aA des multiples de A est un idéal de A. On le note (a).
- Plus généralement, pour A un anneau, $a_1, \ldots, a_n$ des éléments de A, l'ensemble $\{\sum_{i=1}^{n} \lambda_i a_i\,;\, \lambda_i \in A\}$ est un idéal de A. On le note $(a_1, \ldots, a_n)$.

Notons que pour $a, b \in A$, on a $a|b$ si et seulement si $b \in (a)$.

Les deux propriétés suivantes justifient que la notion d'idéal est fondamentale (par exemple plus que celle de sous-anneau), l'équivalent pour les anneaux des sous-groupes distingués.

Proposition 1.25. *Soit A un anneau et I un idéal de A. Alors l'ensemble-quotient A/I hérite d'une structure d'anneau canonique.*

Démonstration. Le point à vérifier est que les lois $+$ et $\cdot$ passent au quotient A/I.

En ce qui concerne $+$, comme la loi $+$ est commutative, $(I, +)$ est un sous-groupe distingué de $(A, +)$, donc le quotient A/I hérite d'une loi $+$ bien définie.

En ce qui concerne $\cdot$, on ne peut dire que $(I, \cdot)$ est un groupe mutliplicatif (il ne contient en général pas le neutre, et les éléments ne sont pas inversibles). En revanche on vérifie que pour $a, b \in A$ et $i, j \in J$, on a $(a + i)(b + j) - ab = aj + ib + ij \in I$, donc la classe du produit ab modulo I ne dépend que de la classe de a et de celle de b. Donc la loi $\cdot$ passe bien au quotient. □

Pour $a \in A$, on note souvent $\bar{a}$ sa projection dans A/I. S'il y a plusieurs idéaux en jeu, on peut noter plus précisément $\bar{a}^I$, ou bien $a + I$ qui correspond à la description de la classe de a comme $\{a + i\,;\, i \in I\}$.

Proposition 1.26. *Soit A un anneau et I une partie de A. Alors I est un idéal de A si et seulement s'il existe un anneau B et un morphisme d'anneau $f : A \to B$ tel que $I = \ker(f)$.*

Démonstration. Commençons par le sens direct. Si I est un idéal de A, on peut considérer pour B l'anneau A/I et la projection canonique $\pi : A \to A/I$ qui est un morphisme d'anneaux. Alors on vérifie facilement qu'on a $I = \ker(f)$.

Réciproquement, supposons $I = \ker(f)$. Soit $a, b \in I$. Alors on a $f(a - b) = 0$, donc $a - b$ est dans $\ker(f)$, et donc $(\ker(f), +)$ est un sous-groupe de $(A, +)$. D'autre part, soit $a \in A, i \in I$. Alors on a $f(ai) = f(a)f(i) = 0$, donc I est stable par multiplication externe. □

Le dernier paragraphe montre même plus : si J est un idéal de B, alors $f^{-1}(J)$ est un idéal de A.

Exemple 1.27.
- Pour $n \in \mathbb{Z}$, $n\mathbb{Z}$ étant un idéal de $\mathbb{Z}$, on retrouve le fait que $\mathbb{Z}/n\mathbb{Z}$ est un anneau.
- Pour K un corps, et $P \in K[X]$ un polynome non nul, le quotient $K[X]/(P)$ est un anneau dont chaque classe est représentée par un unique polynome de degré strictement inférieur à celui de P.
- Le quotient $\mathbb{R}[X]/(X^2 + 1)$ est un anneau (isomorphe à $\mathbb{C}$).

Définition 1.28. Soit A un anneau et I un idéal de A. On dit que I est
- *principal* (ou *monogène*) s'il existe $a \in A$ tel que $I = (a)$;
- *de type fini* s'il existe $r \in \mathbb{N}$ et $a_1, \ldots, a_r \in A$ tels que $I = (a_1, \ldots, a_r)$;
- *propre* si on a $I \neq A$;
- *premier* si I est propre et $\forall x, y \in A, xy \in I \Rightarrow (x \in I) \wedge (y \in I)$);
- *maximal* si I est propre et $(I \subset J \subset A) \Rightarrow (I = J) \vee (J = A)$.

Remarquons qu'un élément $x \in A$ est premier si et seulement l'idéal (x) qu'il engendre est premier (ouf!). En effet on a

x premier ssi $\forall a, b \in A, x|ab \Rightarrow (x|a) \vee (x|b)$
ssi $\forall a, b \in A, ab \in (x) \Rightarrow a \in (x) \vee b \in (x)$
ssi (x) premier

Exemple 1.29.
- Les idéaux maximaux de $\mathbb{Z}$ sont de la forme $p\mathbb{Z}$ avec p premier, ce sont aussi les idéaux premiers.
- $6\mathbb{Z}$ n'est pas un idéal maximal de $\mathbb{Z}$ puisqu'on a par exemple $6\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}$.
- Si K est un corps, l'idéal $(X) \subset K[X, Y]$ est premier, mais pas maximal (car inclus dans l'idéal (X, Y)).

Proposition 1.30. *Soit A un anneau et I un idéal de A. Alors*
- *I est premier si et seulement si A/I est intègre;*
- *I est maximal si et seulement si A/I est un corps.*

On voit qu'en particulier I maximal implique I premier.

Démonstration. Pour la première équivalence, on a

$$\begin{aligned} I \text{ premier} \quad &\text{ssi} \quad \forall a, b \in A, ab \in I \Rightarrow a \in I \vee b \in I \\ &\text{ssi} \quad \forall a, b \in A, \bar{a}\bar{b} = \bar{0} \Rightarrow \bar{a} = \bar{0} \vee \bar{b} = \bar{0} \\ &\text{ssi} \quad \forall \bar{a}, \bar{b} \in A/I, \bar{a}\bar{b} = \bar{0} \Rightarrow \bar{a} = \bar{0} \vee \bar{b} = \bar{0} \\ &\text{ssi} \quad A/I \text{ intègre.} \end{aligned}$$

Supposons maintenant I maximal. Soit $a \in A \setminus I$. On considère l'idéal (a, I) qui contient strictement I. Par maximalité on a $(a, I) = A$, donc il existe $b \in A, i \in I$ tel que $ab + i = 1$. On a alors $\bar{a}\bar{b} = \bar{1}$, donc $\bar{a}$ est inversible dans A/I.

Réciproquement, supposons que A/I est un corps. Soit J un idéal de A tel que $I \subset J$ et l'inclusion est stricte. Alors il existe un élément $j \in J \setminus I$. Comme A/I est un corps, $\bar{j}$ admet un inverse, c'est-à-dire qu'il existe $k \in A$ tel que $\bar{j}\bar{k} = \bar{1}$, donc $jk \in 1 + I \subset 1 + J$, et donc $1 \in J$, donc $J = A$. □

Exemple 1.31.
- Dans $A[X]$, l'idéal (X) est premier si et seulement $A[X]/(X) \simeq A$ est intègre. En effet, s'il existe $a, b \in A$ tels que $ab = 0$, alors a, b ne sont pas dans (X) mais leur produit $ab = 0$ l'est.

Définition 1.32. Pour A un anneau, I et J deux idéaux de A, on construit les trois idéaux

- $I + J = \{i + j\,;\, i \in I, j \in J\}$;
- $I \cap J$;
- $IJ = (ij)_{i\in I, j\in J} = \{\sum_{i\in I, j\in J} a_{ij} i j \,|\, a_{i,j} \in A\}$.

L'idéal $I + J$ est le plus petit idéal de A contenant à la fois I et J, on peut aussi le noter (I, J). Faire attention qu'on ne peut simplement définir IJ comme l'ensemble des produits ij puisque cet ensemble n'est pas stable par addition; c'est pourquoi on considère l'idéal engendré par les termes de cette forme.

On a toujours les inclusions $IJ \subset I \cap J \subset I \subset I + J$. Certaines inclusions peuvent bien sûr être des égalités, mais ce n'est pas le cas en général.

Exemple 1.33. Dans $\mathbb{Z}$, pour $I = 4\mathbb{Z}$ et $J = 6\mathbb{Z}$, on a $IJ = 24\mathbb{Z}, I \cap J = 12\mathbb{Z}$, et $I + J = 2\mathbb{Z}$.

1.4. **Coprimalité et théorème des restes chinois.** Dans le calendrier chinois, chaque année correspond à un animal (rat, bœuf, tigre, lapin, dragon, serpent, cheval, chèvre, singe, coq, chien, cochon) selon un cycle de période 12 et à un élément (métal, bois, eau, feu, terre) selon un cycle de période 5. Il se trouve que ces deux éléments déterminent l'année modulo 60. En termes de groupes additifs, cela correspond à un isomorphisme $\mathbb{Z}/60\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Cet isomorphisme peut être renforcé en un isomorphisme d'anneaux. Voici la version élémentaire du théorème:

Théorème 1.34. *Soit $n_1, \ldots, n_k$ des entiers deux à deux premiers entre eux. Alors l'anneau $\mathbb{Z}/n_1 \ldots n_k\mathbb{Z}$ est isomorphe à l'anneau-produit $(\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})$.*

Pour généraliser à des anneaux quelconques, on doit parler de coprimalité.

Définition 1.35. Soit A un anneau et I, J deux idéaux de A. On dit que I, J sont *premiers entre eux* si on a $I + J = A$.

Exemple 1.36.
- Dans $\mathbb{Z}$, les idéaux $m\mathbb{Z}$ et $n\mathbb{Z}$ sont premiers entre eux si et seulement si les entiers m et n sont premiers entre eux.

- Dans $A[X]$, les idéaux (X) et $(X+a)$ sont premiers entre eux si et seulement si on a $a \in A^\times$.
- Dans $\mathbb{R}[X,Y]$, les idéaux (X) et (Y) ne sont pas premiers entre eux, puisque l'idéal $(X)+(Y)$ ne contient que des polynômes sans terme constant.

Si I, J sont deux idéaux de A, on a des projections naturelles $A/IJ \to A/I$ et $A/IJ \to A/J$. En effet, si deux éléments $a, b \in A$ ont la même projection dans A/IJ, il diffèrent par un élément $k \in IJ \subset I \cap J$, donc ils ont la même projection dans A/I et dans A/J. En juxtaposant les deux projections, on a donc une application $A/IJ \to A/I \times A/J$.

Théorème 1.37 (des restes chinois)**.** *Soit A un anneau et $I_1, \dots, I_n$ des idéaux de A deux à deux premiers entre eux. Alors l'application naturelle $f : A/I_1 \dots I_n \to A/I_1 \times \cdots \times A/I_n$ est un isomorphisme d'anneaux.*

Démonstration. Commençons par le cas $n = 2$. On a donc deux idéaux I_1, I_2 tels que $A = I_1 + I_2$. Notons $f : A/I_1I_2 \to A/I_1 \times A/I_2$ la juxtaposition des deux projections naturelles.

Dans ce cas, l'inclusion $I_1I_2 \subset I_1 \cap I_2$ est en fait une égalité. En effet, puisque $I_1 + I_2 = A$, il existe $a_1 \in I_1$ et $a_2 \in I_2$ tels que $a_1 + a_2 = 1$. Pour $x \in I_1 \cap I_2$, on a $x = (a_1 + x_2)x = a_1x + a_2x$. Comme $a_1 \in I_1$ et $x \in I_2$, on a $a_1x \in I_1I_2$, et comme $x \in I_1$ et $a_2 \in I_2$, on a $a_2x \in I_1I_2$. Par conséquent, on a $x \in I_1I_2$.

Montrons que f est injective. Pour cela, prenons $a \in A$ tels que $f(\bar{a}^{I_1I_2}) = (\bar{0}^{I_1}, \bar{0}^{I_2})$. On a alors $a \in I_1$ et $a \in I_2$, donc $a \in I_1 \cap I_2 = I_1I_2$, donc $\bar{a}^{I_1I_2} = \bar{0}^{I_1I_2}$.

Pour la surjectivité de f, prenons $a_1 \in I_1, a_2 \in I_2$ tels que $1 = a_1 + a_2$. Soit x, y dans A. On a alors

$$\begin{aligned} f(\overline{xa_2 + ya_1}^{I_1I_2}) &= (\overline{xa_2 + ya_1}^{I_1}, \overline{xa_2 + ya_1}^{I_2}) \\ &= (\overline{xa_2 + xa_1 + ya_1}^{I_1}, \overline{xa_2 + ya_1 + ya_2}^{I_2}) \\ &= (\overline{x + ya_1}^{I_1}, \overline{xa_2 + y}^{I_2}) \\ &= (\bar{x}^{I_1}, \bar{y}^{I_2}) \end{aligned}$$

Le cas général se déduira par une récurrence sur $n \geqslant 2$, après qu'on ait démontré le lemme suivant:

Lemme 1.38. *Si $I_1, \dots, I_n$ sont des idéaux de A deux à deux premiers entre eux, alors pour tous $j < k$, les idéaux $I_1 \dots I_j$ et I_k sont premiers entre eux.*

Preuve du lemme. Pour tout i entre 1 et j, on a $I_i + I_k = A$, donc il existe $a_i \in I_i$ et $b_i \in I_k$ tels que $1 = a_i + b_i$. On a alors $1 = (a_1 + b_1) \dots (a_j + b_j)$. En développant, on fait apparaître un premier terme $a_1 \dots a_j$ additionné à des termes qui contiennent tous au moins un facteur b_i. On a alors écrit 1 comme somme d'un élément de $I_1 \dots I_j$ et de $2^j - 1$ termes dans I_k, ce qui montre l'égalité $I_1 \dots I_j + I_k = A$. □

Pour conclure la preuve du théorème chinois par récurrence, il suffit d'appliquer le cas $n = 2$ à $I_1 \dots I_{k-1}$ et I_k, qui sont bien premiers entre eux d'après le lemme. □

1.5. **Caractéristique.** Soit A un anneau commutatif. Alors il existe un unique morphisme d'anneaux $f_\mathbb{Z} : \mathbb{Z} \to A$, défini par $f_\mathbb{Z}(1) = 1_A$. Pour $n \in \mathbb{Z}$ et $a \in A$, on peut alors définir sans ambiguïté na comme $f_\mathbb{Z}(n)a$.

De plus $\ker(f_{\mathbb{Z}})$ est un idéal de $\mathbb{Z}$, et donc est de la forme $n_A\mathbb{Z}$ pour un entier $n_A \in \mathbb{N}$.

Définition 1.39. Soit A un anneau, alors l'unique entier $n_A \in \mathbb{N}$ tel que $\ker(f_{\mathbb{Z}}) = (n_A)$ est appelé la *caractéristique* de A.

Dans ce cas, A contient un sous-anneau isomorphe à $\mathbb{Z}/n_A\mathbb{Z}$ (le sous-anneau engendré par 1_A), et pour tout $a \in A$ on a $n_A a = (n_A 1_A)a = 0 \cdot a = 0$.

Si A est intègre, alors nécessairement n_A vaut 0 ou est premier. En effet, si n_A était composé, alors on aurait des diviseurs de 0.

Proposition 1.40. *Soit A un anneau intègre et p_A sa caractéristique. Alors l'application $x \mapsto x^{p_A}$ est un endomorphisme d'anneau.*

Démonstration. Que l'application soit multiplicative est évident, puisque A est supposé commutatif. Quant à l'additivité, pour $x, y \in A$ on a

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

Comme p_A divise $\binom{p_A}{k}$ pour tout k entre 1 et p_A-1, toute la somme centrale est nulle, donc l'élévation à la puissance p_A est bien un morphisme de groupe (additif), et donc un morphisme d'anneau. □

1.6. **Polynomes.** [1] Commençons par un rappel.

Définition 1.41. Soit A un anneau, et $P(X) = \sum_{i=0}^{d} a_i X^i \in A[X]$ avec $a_d \neq 0$ un polynome non nul. Alors d est appelé le *degré* de P, noté $\deg(P)$, et a_d est appelé le *coefficient dominant* de P, noté $\mathrm{dom}(P)$. Si P est le polynome nul, par convention son degré est $-\infty$.

Proposition 1.42 (transfert de l'intégrité)**.** *Si A est un anneau intègre, alors l'anneau $A[X]$ est intègre.*

Démonstration. Soit $P(X) = \sum_{i=0}^{m} a_i X^i$ et $Q(X) = \sum_{i=0}^{n} b_i X^i$ deux polynomes de degrés m et n respectivement. Alors on a $\mathrm{dom}(PQ) = a_m b_n \neq 0$, donc $PQ \neq 0$. □

La proposition est fausse dans un anneau non intègre, comme le montre l'exemple du polynome $2X \in (\mathbb{Z}/4\mathbb{Z})[X]$ dont le carré est $4X^2 = 0$.

Définition 1.43. Soit A un anneau, $P \in A[X]$ et $a \in A$. On dit que a est *racine* de P si on a $P(a) = 0$.

Lemme 1.44. *Pour $P \in A[X]$, un élément $a \in A$ est racine de P si et seulement si $X - a$ divise $P(X)$ dans $A[X]$.*

[1] La présence d'un accent circonflexe semble s'être imposée, bien que la raison en soit douteuse, voir [http://books.cedram.org/MALSM/SMA_1937-1938__5__K_0.pdf, Note 3 de Michèle Audin]

Démonstration. Pour le sens direct, on peut écrire $P(X)$ comme un polynome en $X-a$, c'est-à-dire qu'il existe $a_0,\dots,a_d \in A$ tels que $P(X)=\sum_{i=0}^{d} a_i(X-a)^i$. L'hypothèse $P(a)=0$ implique $a_0=0$, d'où $P(X)=(X-a)(\sum_{i=0}^{d-1} a_{i+1}(X-a)^i)$.

Pour le sens indirect, s'il existe $Q\in A[X]$ tel que $P(X)=(X-a)Q(X)$, il suffit d'évaluer en a pour voir que a est racine. □

Exemple 1.45.
- Dans $\mathbb{Z}[X]$, le polynome X^2-1 a pour racine 1 et -1. Il se factorise $X^2-1=(X-1)(X+1)$.
- Dans $(\mathbb{Z}/8\mathbb{Z})[X]$, ce même polynome X^2-1 a quatre racines, à savoir $1,3,5$ et 7. Il se factorise des deux façons $X^2-1=(X-1)(X-7)=(X-3)(X-5)$.

Définition 1.46. Soit $P\in A[X]$ est $a\in A$ une racine de P. La *multiplicité* de a est le plus plus grand entier m tel que $(X-a)^m$ divise $P(X)$.

Pour $P\in A[X]$, si un élément $a\in A$ est de multiplicité au moins m, alors on a $P(a)=P'(a)=\cdots=P^{(m-1)}(a)=0$. La réciproque n'est pas vraie. En effet, dans un anneau de caractéristique finie $n\in\mathbb{N}$, on a $P^{(n)}=0$ pour tout polynome, et donc en particulier $P^{(n)}(a)=0$ pour tout a, que a soit racine de multiplicité au moins $n+1$ ou pas.

Proposition 1.47. *Soit $P\in A[X]$. Si A est intègre, alors la somme des multiplicités des racines de P est inférieure ou égale à $\deg(P)$.*

L'énoncé est faux si A n'est pas intègre, comme le montre l'exemple 1.45 de X^2-1 dans $(\mathbb{Z}/8\mathbb{Z})[X]$.

Démonstration. Si a est racine de multiplicité m, alors il existe $Q\in A[X]$ de degré $\deg(P)-m$ tel que $P(X)=(X-a)^mQ(X)$. Si b est une racine de P, alors on a $P(b)=(b-a)^mQ(b)=0$. Par intégrité, on a donc $a=b$ ou $Q(b)=0$. On conclut alors par récurrence. □

Voici une application, particulièrement importante en ce qui concerne les corps finis.

Proposition 1.48. *Si A est un anneau intègre et $(G,\cdot)$ un sous-groupe (multiplicatif) fini de $(A^\times,\cdot)$. Alors G est cyclique.*

Encore une fois, on voit que l'énoncé est faux pour l'anneau non intègre $\mathbb{Z}/8\mathbb{Z}$ dont le groupe des unités est le groupe de cardinal 4 non cyclique.

Pour démontrer la proposition, on a besoin de la fonction suivante, fondamentale en théorie des nombres:

Définition 1.49. L'*indicatrice d'Euler* est la fonction $\varphi:\mathbb{N}^*\to\mathbb{N}$ qui à un entier n associe le nombre d'éléments d'ordre exactement n dans le groupe additif $\mathbb{Z}/n\mathbb{Z}$.

Pour $n\geqslant 2$, on voit que $\varphi(n)$ est le nombre d'entiers strictement compris entre 0 et n qui sont premiers avec n. En particulier on a $\varphi(n)\leqslant n-1$, avec égalité si et seulement si n est premier. Plus généralement, le théorème de Lagrange appliqué au groupe $\mathbb{Z}/n\mathbb{Z}$ implique l'égalité

$$\sum_{d|n}\varphi(d)=n\ .$$

Démonstration de la proposition 1.48. Soit $n = \mathrm{card}(G)$. On veut montrer que G contient au moins un élément d'ordre n.

Par le théorème de Lagrange, tout élément $g \in G$ est racine du polynome $X^n - 1$.

Définissons $\psi_G : \mathbb{N}^* \to \mathbb{N}$ comme cousine (adaptée à G) de l'indicatrice d'Euler qui à un entier m associe le nombre d'éléments d'ordre exactement m dans G. Par le théorème de Lagrange, si k ne divise pas n on a $\psi_G(k) = 0$, et d'autre part on a $\sum_{d|n} \psi_G(d) = n$.

Si pour tout d divisant n on a $\psi_G(d) \leqslant \varphi(d)$, alors l'égalité $\sum_{d|n} \psi_G(d) = n = \sum_{d|n} \varphi(d)$ implique $\psi_G(d) = \varphi(d)$ pour tout d divisant n, et en particulier $\psi_G(n) = \varphi(n) > 0$. Par conséquent G contient un élément d'ordre n, et donc est cyclique.

Inversement, s'il existe d divisant n tel que $\psi_G(d) > \varphi(d)$, en choisissant un tel d minimal, on a $\sum_{d'|d} \psi_G(d') > \sum_{d'|d} \varphi(d') = d$. Cela signifie qu'il y a plus que d éléments dans G dont l'ordre divise d, et donc que le polynome $X^d - 1$ a strictement plus que d racines, ce qui contredit la proposition 1.47. □

1.7. **Localisation et corps des fractions.** Un corps est un cas particulier d'anneau intègre, et en particulier tout sous-anneau d'un corps est intègre. Réciproquement, partant d'un anneau, on peut chercher à rendre inversible certains éléments (voire tous pour un anneau intègre).

Théorème 1.50 (de *localisation*)**.** *Soit A un anneau et $S \subset A \setminus \{0\}$ une partie stable par multiplication. Alors il existe un anneau A_S et un morphisme d'anneaux $\ell_S : A \to A_S$ tels que*

- *$\ell_S(S) \subset A_S^\times$;*
- *pour tout morphisme d'anneau $f : A \to B$, si $f(S) \subset B^\times$, alors il existe un morphisme $g : A_S \to B$ tel que $f = g \circ \ell_S$.*

La première propriété est celle qui rend inversible les éléments de S. Le seconde est une propriété de minimalité qui assure l'unicité de A_S ; c'est un exemple de propriété *universelle*: tout anneau B où S est rendu inversible "contient" A_S. Comme un anneau ne peut être unique qu'à isomorphisme près, on exprime cela avec des morphismes. L'anneau A_S est appelé anneau *localisé* de A en S, ou anneau des *fractions* de A associé à S. En particulier si A est intègre et $S = A \setminus \{0\}$, alors A_S est un corps, appelé *corps des fractions de A*, noté $\mathrm{Frac}(A)$.

Exemple 1.51.
- On a $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.
- On a $\mathrm{Frac}(\mathbb{C}[X]) = \mathbb{C}(X)$, le corps des fractions rationnelles en une indéterminée.
- Pour $A = \mathbb{Z}$ et S l'ensemble des puissances de 10 (qui est bien un ensemble stable par multiplication), le localisé de $\mathbb{Z}$ en S est l'anneau $\mathbb{D}$ des nombres décimaux, qu'on peut aussi décrire comme $\mathbb{Z}[\frac{1}{10}]$.

Démonstration du théorème 1.50. Pour l'existence, on considère l'ensemble $A \times S$ auquel on pense comme les quotients d'un élément de A par un élément de S. On définit des lois d'addition et de multiplication par $(a, s) + (a', s') := (as' + a's, ss')$ et $(a, s) \cdot (a', s') := (aa', ss')$. (On remarque que la définition repose de manière cruciale sur la stabilité de S par multiplication.)

On considère alors la relation $\sim$ sur $A \times S$ définie par $(a, s) \sim (a', s')$ s'il existe $t \in S$ tel que $tas' = ta's$ (lorsque A est intègre, on peut se passer de ce t). On vérifie que c'est une relation d'équivalence sur $A \times S$. En effet, pour la transitivité, si on a $(a, s) \sim (a', s')$ et $(a', s') \sim (a'', s'')$, alors il existe $t, t' \in S$ tels que $tas' = ta's$ et $t'a's'' = t'a''s'$, d'où $(tt's')as'' = (tas')t's'' = (ta's)t's'' = (t'a's'')ts = (t'a''s')ts = (tt's')a''s$, donc $(a, s) \sim (a'', s'')$. On définit A_S comme le quotient $A \times S / \sim$. Il faut vérifier que les lois de composition passent au quotient: si on a $(a', s') \sim (a'', s'')$ c'est-à-dire $ta's'' = ta''s'$, alors on a $t(as' + a's)ss'' - t(as'' + a''s)ss' = 0$, donc on a bien $(a, s) + (a', s') \sim (a, s) + (a'', s'')$, et $taa'ss'' = taa''ss'$, donc $(a, s) \cdot (a', s') \sim (a, s) \cdot (a'', s'')$. Ainsi $A_S := A \times S / \sim$ est bien muni d'une structure d'anneau. On remarque que le neutre multiplicatif est la classe des éléments (s, s), pour $s \in S$.

Pour ce qui est de définir $\ell_S : A \to A_S$, on choisit un élément $s_0 \in S$ et on pose $\ell_S(a) = \overline{(as_0, s_0)}$, et on voit que c'est un morphisme. Vérifions qu'alors on a $\ell_S(S) \subset A_S^\times$. En effet, pour $s \in S$, on a $\ell_S(s) = \overline{(ss_0, s_0)}$, d'où $\ell_S(s) \cdot \overline{(s_0, ss_0)} = \overline{(ss_0^2, ss_0^2)}$ qui est le neutre multiplicatif.

Enfin, si $f : A \to B$ est un morphisme d'anneaux tel que $f(S) \subset B^\times$, pour l'étendre à A_S, il n'y a pas le choix, il faut définir $g(\overline{(a, s)}) = f(a)f(s)^{-1}$. On vérifie que c'est bien défini et qu'on a $f = g \circ \ell_S$. □

1.8. **Anneaux principaux.** On a précédemment souligné l'importance des idéaux. On considère maintenant les anneaux dans lesquels ceux-ci sont les plus simples possibles:

Définition 1.52. Un anneau A est dit *principal* s'il est intègre et si tout idéal est principal (*i.e.,* monogène).

Exemple 1.53.
- $\mathbb{Z}$ est principal puisque tous ses idéaux sont de la forme (n).
- Si K est un corps, $K[X]$ est principal, on va rappeler ci-dessous pourquoi.
- $\mathbb{Z}[X]$ n'est pas principal. En effet, l'idéal $(2, X)$ n'est pas principal.
- En général $K[X, Y]$ n'est pas principal. En effet, l'idéal (X, Y) n'est pas principal.

Pour a, b deux éléments quelconques d'un anneau principal, les idéaux (a, b) et $(a) \cap (b)$ sont monogènes.

Définition 1.54. Soit A un anneau principal, $a, b \in A$. Alors un élément d tel que $(a, b) = (d)$ est appelé *plus grand diviseur commun* de a et b, noté $\mathrm{pgcd}(a, b)$; un élément m tel que $(a) \cap (b) = (m)$ est appelé *plus petit multiple commun* de a et b, noté $\mathrm{ppcm}(a, b)$.

Les notations sont ambigües ici puisque d et m ne sont en fait définis qu'à une unité près, donc n'est en général pas uniques.

Dans ce contexte, puisque $d \in (a, b)$, il existe $x, y \in A$ tels que $d = ax + by$. C'est l'*identité de Bézout*.

Les noms pgcd et ppcm sont justifiés par l'énoncé suivant (qui peut être pris[2] comme définition à la place de 1.54):

Proposition 1.55. *Pour A principal et $a, b \in A$, un élément $d \in A$ est un pgcd de a et b si et seulement s'il vérifie*

[2] voir [Berhuy, XVII.1.9]

- $d|a$ *et* $d|b$ *;*
- $\forall c \in A$*, si* $c|a$ *et* $c|b$*, alors* $c|d$*.*

De même, un élément $m \in A$ *est un ppcm de* a *et* b *si et seulement s'il vérifie*

- $a|m$ *et* $b|m$ *;*
- $\forall c \in A$*, si* $a|c$ *et* $b|c$*, alors* $m|c$*.*

Démonstration. Pour le pgcd et le sens direct, si $d = \mathrm{pgcd}(a,b)$, alors on a $a \in (d)$ et $b \in (d)$, donc $d|a$ et $d|b$. Ensuite, si on a $c|a$ on déduit l'existence de $u \in A$ tel que $a = cu$, et si $c|b$ il existe $v \in A$ tel que $b = cv$. Alors l'identité de Bézout $\mathrm{pgcd}(a,b) = ax + by$ donne $\mathrm{pgcd}(a,b) = c(ux + vy)$, et donc $c|\mathrm{pgcd}(a,b)$.

Pour le pgcd et le sens indirect, si on a $d|a$ et $d|b$, alors $a \in (d)$ et $b \in (d)$, donc $(a,b) \subset (d)$. Si l'inclusion était stricte, il existerait $c \in (d)$ tel que $c \notin (a,b)$, ce qui contredirait le second point.

Pour le ppcm et le sens direct, si $m = \mathrm{ppcm}(a,b)$, alors on a $m \in (a) \cap (b) \subset (a)$, donc $a|m$. De même on a $b|m$. Ensuite, si on a $a|c$ et $b|c$, alors on a $c \in (a)$ et $c \in (b)$, donc $c \in (a) \cap (b)$, d'où $c \in (m)$, et donc $m|c$.

Pour le ppcm et le sens indirect, si on a $a|m$ et $b|m$, alors on a $m \in (a)$ et $m \in (b)$, donc $m \in (a) \cap (b)$, d'où $(m) \subset (a) \cap (b)$. Si l'inclusion était stricte, il existerait $c \in (a) \cap (b)$ tel que $c \notin (m)$, ce qui contredirait le second point. □

On a montré en 1.22 que dans un anneau intègre tout élément premier est irréductible. Voici la réciproque pour les anneaux principaux.

Proposition 1.56. *Soit* A *un anneau principal. Alors tout élément de* A *irréductible est premier.*

Remarquons que cette proposition implique que $\mathbb{Z}[\sqrt{-5}]$ n'est pas principal. En effet, on a déjà mentionné que les éléments $2, 3, 1+\sqrt{-5}$ et $1-\sqrt{-5}$ y sont irréductibles mais pas premiers. Pour ce qui est d'un idéal non principal, on peut alors trouver $(2, 1+\sqrt{-5}) = \{a + b\sqrt{-5} \mid a + b \text{ pair}\}$.

Démonstration. Soit $x \in A$ irréductible. Supposons qu'on a $x|ab$, avec $a, b \in A$. On veut montrer qu'on a alors $x|a$ ou $x|b$.

Par définition il existe $y \in A$ tel que $ab = xy$. Considérons l'idéal $I = (b, x)$. Comme il est principal, il existe $c \in A$ tel que $I = (c)$. En particulier il existe $z \in A$ tel que $x = cz$. Comme x est supposé irréductible, on a ou bien $z \in A^\times$, ou bien $c \in A^\times$.

- Dans le premier cas, on a alors $I = (b, x) = (c) = (cz) = (x)$, donc $x|b$.
- Dans le second cas, on a $I = (b, x) = A$, donc il existe $d, e \in A$ tels que $bd + xe = 1$, donc $a = abd + axe = xyd + axe = x(yd + ae)$, donc en particulier $x|a$.

□

1.9. **Anneaux euclidiens.** Montrer qu'un anneau est principal n'est pas forcément chose aisée. Un contexte un peu plus fort rend les choses plus faciles:

Définition 1.57. Soit A un anneau. Un *stathme euclidien* est une application $N : A\setminus\{0\} \to \mathbb{N}$ telle que $\forall a \in A, b \in A \setminus \{0\}, \exists q, r \in A, a = qb + r$, avec $r = 0$ ou $N(r) < N(b)$.

Un anneau A est dit *euclidien* s'il est intègre et s'il admet un stathme euclidien.

Exemple 1.58.
- L'anneau $\mathbb{Z}$ est euclidien, avec le stathme $N(a) = |a|$.
- Pour K un corps, l'anneau $K[X]$ est euclidien, avec le stathme $N(P) = \deg(P)$.

Théorème 1.59. *Si A est un anneau euclidien, alors A est principal.*

Ce théorème implique en particulier que pour K un corps, $K[X]$ est principal, puisqu'euclidien.

Démonstration. Soit A euclidien et N un stathme sur A. Soit I un idéal non nul de A. Alors l'ensemble $\{N(a)\,;\, a \in I \setminus \{0\}\}$ est un sous-ensemble non vide de $\mathbb{N}$. Il admet donc un plus petit élément qui est de la forme $N(b)$, avec $b \in I$. Montrons qu'on a $I = (b)$.

Soit a un élément de I quelconque. Alors il existe $q, r \in A$ tels que $a = qb + r$, avec $r = 0$ ou $N(r) < N(b)$. Comme $a, qb \in I$, on a $r \in I$, et donc par minimalité de $N(b)$, on a $r = 0$, et donc $a = qb$. □

Dans un anneau euclidien, on peut calculer le pgcd de deux éléments avec l'algorithme d'Euclide étendu: partant de deux éléments a, b avec $N(a) \geqslant N(b)$, on pose $r_0 = a$ et $r_1 = b$, puis on calcule récursivement r_{i+2} le reste de la division euclidienne de r_i par r_{i+1} (c'est-à-dire qu'on trouve q_{i+2}, r_{i+2} tels que $r_i = q_{i+2}r_{i+1} + r_{i+2}$ et $N(r_{i+2}) < N(r_{i+1})$. Comme la suite $(N(r_i))_{i\geqslant 0}$ est entière et strictement décroissante, elle termine par un dernier reste r_n non nul. Comme on a à chaque étape $(r_i, r_{i+1}) = (r_{i+1}, r_{i+2})$, on a $(r_n) = (a, b)$, et donc r_n est un pgcd de a et b. Si on a garde la trace des quotients q_i à chaque étape, on peut aussi reconstituer l'identité de Bézout, c'est-à-dire trouver x, y tels que $\mathrm{pgcd}(a, b) = ax + by$. En effet, l'identité $r_i = q_{i+2}r_{i+1} + r_{i+2}$ se réécrit $\left(\begin{smallmatrix} r_{i+1} \\ r_{i+2} \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -q_{i+2} \end{smallmatrix}\right)\left(\begin{smallmatrix} r_i \\ r_{i+1} \end{smallmatrix}\right)$, d'où par récurrence $\left(\begin{smallmatrix} 0 \\ r_n \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -q_n \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & -q_{n_1} \end{smallmatrix}\right) \ldots \left(\begin{smallmatrix} 0 & 1 \\ 1 & -q_2 \end{smallmatrix}\right)\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$. [3]

Il existe des anneaux principaux non euclidiens, mais ce n'est pas si facile d'en exhiber. On peut citer $\mathbb{R}[X, Y]/(X^2 + Y^2 + 1)$ ou $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ [4] .

1.10. **Anneaux factoriels.** La notion d'anneau principal souffre d'un défaut important: elle ne se transfère pas. Ainsi l'anneau $\mathbb{Z}[X]$ n'est-il pas principal. On va maintenant affaiblir la notion d'anneau principal (de façon à englober plus d'anneaux), tout en préservant un certain nombre de propriétés qui permettent de faire de l'arithmétique. On a vu la notion d'élément irréductible dans un anneau (dont on rappelle que dans les anneaux principaux elle coïncide avec la notion d'élément premier). L'exemple de $\mathbb{Z}$ incite à décomposer tout élément comme produit d'éléments irréductibles. Pour A un anneau, on considère donc les propriétés suivantes:

(*existence*) Tout élément de A est produit d'irréductibles, soit

$$\forall a \in A \setminus (A^\times \cup \{0\}), \exists p_1, \ldots, p_r \text{ irreductibles}, a = p_1 \ldots p_r \,.$$

(*unicité*) Si un élément de A est produit d'irréductibles, cette décomposition est unique à multiplication par des unités et permutation des facteurs près, soit

$$\forall a \in A \setminus (A^\times \cup \{0\}), \forall p_1, \ldots, p_r, q_1, \ldots, q_s \text{ irreductibles},$$

[3] Les éléments de $\mathrm{GL}_2(\mathbb{Z}) = \{M \in \mathcal{M}_2(\mathbb{R}) \mid \det(M) = \pm 1\}$ correspondent à l'ensemble de relations de Bézout possibles pour un pgcd égal à 1. La terminaison de l'algorithme d'Euclide implique donc le résultat suivant : les matrices de la forme $\left(\begin{smallmatrix} 0 & 1 \\ 1 & q \end{smallmatrix}\right)$ avec $q \in \mathbb{Z}$ engendrent le groupe $\mathrm{GL}_2(\mathbb{Z})$.

[4] voir [Perrin, section II.5 et exercice II.5.1]

$$a = p_1 \dots p_r = q_1 \dots q_s \Rightarrow r = s \wedge \exists \pi \in S_n, a_1, \dots, a_r \in A^\times, \forall i \in [\![1; r]\!], p_i = a_i q_{\pi(i)} .$$

Définition 1.60. Un anneau A est dit *factoriel*[5] s'il est intègre et satisfait les propriétés ci-dessus d'existence et d'unicité de décomposition en irréductibles.

Exemple 1.61. Dans $\mathbb{Z}$ les irréductibles sont plus ou moins les nombres premiers, et le théorème de décomposition en facteurs premier dit exactement que $\mathbb{Z}$ est factoriel.

Exemple 1.62. L'anneau $\mathbb{Z}[X]$ est factoriel. En effet, les unités sont juste 1 et -1, donc en particulier des polynomes de degré 0. On peut alors montrer l'existence de la décomposition en produit d'irréductibles par récurrence sur le degré: pour $P \in \mathbb{Z}[X]$, ou bien il existe Q, R de degrés strictement inférieur à $\deg(P)$ tels que $P = QR$, et on a l'existence par hypothèse de récurrence, ou bien de tels Q, R n'existent pas et alors P est irréductible. L'unicité n'est pas triviale et sera montrée à l'aide de la notion de *contenu* à la section suivante.

Exemple 1.63. Plus généralement, on verra à la section suivante que si A est factoriel, alors l'anneau $A[X]$ l'est aussi et on peut en déterminer les irréductibles.

Exemple 1.64. Dans $\mathbb{Z}[\sqrt{-5}]$, on peut voir qu'il y existence de la décomposition (par exemple en considérant la norme), mais pas unicité, comme le montre (encore !) l'exemple de $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Ainsi $\mathbb{Z}[\sqrt{-5}]$ n'est pas factoriel.

Exemple 1.65. Si on considère l'anneau des entiers algébriques, c'est-à-dire le sous-anneau de $\mathbb{C}$ composés des racines complexes de polynomes unitaires à coefficients dans $\mathbb{Z}$ (dont on montrera plus tard que c'est bien un anneau), on peut voir qu'il s'agit d'un anneau où il n'y a pas d'existence. En fait, c'est un anneau qui ne contient aucun irréductible (bien qu'il soit loin d'être un corps), puisque si a est un entier algébrique, on montre que $\sqrt{a}$ l'est aussi, et on a $a = \sqrt{a} \cdot \sqrt{a}$ qui n'est donc pas irréductible.

En général, quand dans un anneau factoriel on décompose un élément a en produits d'irréductibles, on regroupe les irréductibles qui sont associés en les puissances d'un même éléments, de sorte qu'on écrit $a = up_1^{e_1} \dots p_r^{e_r}$ avec u inversible, $p_1, \dots, p_r$ irréductibles deux à deux non associées, et $e_1, \dots, e_r$ des entiers (strictement) positifs. Dans ce cas, les diviseurs de a sont exactement les nombres de la forme $vp_1^{f_1} \dots p_r^{f_r}$, avec v unité et $f_1 \leqslant e_1, \dots, f_r \leqslant e_r$ des entiers naturels positifs ou nuls.

Comme dit plus haut, la notion d'anneau factoriel généralise celle d'anneau principal :

Théorème 1.66. *Si A est un anneau principal, alors A est factoriel.*

On a donc les inclusions suivantes:

$$\{\text{euclidiens}\} \subset \{\text{principaux}\} \subset \{\text{factoriels}\} \subset \{\text{integres}\}$$

Toutes les inclusions sont strictes. Par exemple,

- $\mathbb{Z}$ et $K[X]$ (pour K un corps) sont des exemples d'anneaux euclidiens;
- $\mathbb{R}[X, Y]/(X^2 + Y^2 + 1)$ et $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ sont des anneaux principaux non euclidiens;

[5]Le terme anglophone est *unique factorisation domain* qui a l'avantage de bien rappeler la propriété caractéristique.

- $\mathbb{Z}[X]$ et $A[X,Y]$ (pour A un anneau factoriel) sont des anneaux factoriels non principaux;
- $\mathbb{Z}[\sqrt{-5}]$ est un anneau intègre non factoriel.

Preuve du théorème 1.66. On commence par

(*existence*) Soit $a \in A$. Montrons par l'absurde que a admet une décomposition en produits d'irréductibles. Supposons donc que a n'admet pas de décomposition en produit d'irréductibles. Puisque a n'est pas irréductible, il existe $a_1, b_1 \in A$ qui ne sont pas des unités et tels que $a = a_1 b_1$. Alors par hypothèse et quitte à permuter les rôles, a_1 n'admet pas de décomposition en produit d'irréductibles. On itère alors: on obtient une suite infinie $a = a_1 b_1, a_1 = a_2 b_2, a_2 = a_3 b_3, \ldots$, où pour tout $i \in \mathbb{N}^*$ on a $a_{i+1} | a_i$ et a_i n'admet pas de décomposition en produits d'irréductibles. Alors on a la suite d'inclusions d'idéaux infinie $(a_1) \subset (a_2) \subset (a_3) \subset \ldots$. L'ensemble $I = \cup_{i \geqslant 1}(a_i)$ est alors un idéal. Comme A est principal, I l'est, donc il existe $f \in A$ tels que $I = (f)$. Alors puisque f est dans l'union, il existe $n \in \mathbb{N}$ tel que $f \in (a_n)$, et alors $(a_{n+1}) = (a_n)$ (et même la suite d'inclusions stationne à partir de là). Mais alors b_{n+1} est une unité, ce qui fournit une contradiction. [6]

Et maintenant

(*unicité*) Soit $a \in A$ et supposons qu'on a $a = p_1 \ldots p_r = q_1 \ldots q_s$ avec $p_1, \ldots, p_r, q_1, \ldots, q_s$ irréductibles. Comme A est principal et p_1 irréductible, p_1 est premier. Comme p_1 divise le produit $q_1 \ldots q_s$, quitte à permuter les indices, p_1 divise q_1. Comme q_1 est irréductible, il existe une unité a_1 telle que $p_1 = a_1 q_1$. De $a_1 p_1 p_2 \ldots p_r = a_1 q_1 q_2 \ldots q_s$ on déduit $a_1 p_2 \ldots p_r = q_2 \ldots q_s$. On conclut alors par récurrence sur $\min(r, s)$. □

On a montré en 1.56 que dans les anneaux principaux, les éléments irréductibles sont premiers. C'est encore vrai dans les anneaux factoriels:

Proposition 1.67. *Soit A un anneau factoriel. Alors tout élément de A irréductible est premier.*

Démonstration. Soit $x, a, b \in A$ tels que $x | ab$ et x est irréductible. Alors il existe $c \in A$ tel que $ab = xc$. On décompose a, b, c en produits d'irréductibles sous la forme $a = p_1 \ldots p_r, b = q_1 \ldots q_s$ et $c = \ell_1 \ldots \ell_t$. On a alors $x\ell_1 \ldots \ell_t = p_1 \ldots p_r q_1 \ldots q_s$. Par unicité x doit coïncider (à une unité près) avec un élément p_i ou q_i, et donc on a $x | a$ ou $x | b$. □

Les notions de pgcd et de ppcm introduites pour les anneaux principaux se généralisent dans les anneaux factoriels.

Définition 1.68. Soit A un anneau factoriel, $a, b \in A$ deux éléments qui se décomposent en irréductibles sous la forme $a = p_1^{e_1} \ldots p_r^{e_r} u$ et $b = p_1^{f_1} \ldots p_r^{f_r} v$, avec $p_1, \ldots p_r$ irréductibles, $e_1, \ldots e_r, f_1, \ldots f_r$ des entiers naturels (possiblement nuls), et u, v des unités de A. Alors on pose $\mathrm{pgcd}(a, b) = p_1^{\min(e_1, f_1)} \ldots p_r^{\min(e_r, f_r)}$ et $\mathrm{ppcm}(a, b) = p_1^{\max(e_1, f_1)} \ldots p_r^{\max(e_r, f_r)}$.

[6] Quand on verra la notion d'anneau noethérien, on verra que par le même argument, dans les anneaux noethériens, toute suite croissante d'idéaux stationne. Donc la preuve ci-dessus se transportera pour montrer qu'on a toujours existence de la décomposition dans les anneaux noethériens. Par contre la preuve de l'unicité est spécifique aux anneaux principaux.

Dans un anneau principal, on vérifie grâce à la proposition 1.55 que la définition ci-dessus coïncide avec la définition 1.54.

Dans un anneau factoriel non principal, on a $(\mathrm{ppcm}(a,b)) = (a) \cap (b)$ comme dans le cas principal, mais en revanche on a une inclusion $(a,b) \subset (\mathrm{pgcd}(a,b))$ qui peut être stricte. En fait, cette dernière inclusion est une égalité si et seulement on dispose d'une identité de Bézout donnée par deux élément $x, y \in A$ tels que $\mathrm{pgcd}(a,b) = ax + by$.

Exemple 1.69. Dans $K[X,Y]$ (dont on montrera qu'il est factoriel), on a $\mathrm{pgcd}(X,Y) = 1$, et l'inclusion $(X,Y) \subset (1) = K[X,Y]$ est stricte. En effet, il n'existe pas (pour des raisons de degré par exemple) de polynomes $P, Q \in K[X,Y]$ tels que $1 = XP(X,Y) + YQ(X,Y)$.

La définition 1.68 s'étend directement pour définir le pgcd et le ppcm d'un nombre fini quelconque d'éléments.

1.11. **Polynomes dans les anneaux factoriels.** On rappelle que si un anneau A est intègre, il existe un corps canonique dans lequel A se plonge, à savoir son corps des fractions $\mathrm{Frac}(A)$. Si A est factoriel, il est en particulier intègre, et on peut aussi plonger $A[X]$ dans $\mathrm{Frac}(A)[X]$. Comme ce dernier anneau est euclidien, il est plus facile à manipuler. Ce qui permet de remonter les polynomes de $\mathrm{Frac}(A)[X]$ vers $A[X]$ est la notion de contenu :

Définition 1.70. Soit A un anneau factoriel. Pour $P(X) = \sum_{i=0}^{d} a_i X^i \in A[X]$ un polynome, on définit son *contenu* par

$$\mathrm{cont}(P) := \mathrm{pgcd}(a_0, \ldots, a_d) \,.$$

On dit que P est *primitif* si on a $\mathrm{cont}(P) = 1$.

Notons que si P (vu comme élément de l'anneau $A[X]$) est premier, alors il est primitif. En effet, démontrons la contraposée : si P n'est pas primitif, alors $\mathrm{cont}(P)$ n'est pas inversible et on a $P = \mathrm{cont}(P) \cdot \frac{P}{\mathrm{cont}(P)}$. Les deux éléments $\mathrm{cont}(P)$ et $\frac{P}{\mathrm{cont}(P)}$ divisent tous deux P sans être des unités, donc P n'est pas premier.

En revanche un polynome primitif n'est pas nécessairement premier, comme le montre $X^2 - 1 = (X-1)(X+1)$.

Lemme 1.71 (de Gauss)**.** *Soit A un anneau factoriel et $P, Q \in A[X]$, alors on a* $\mathrm{cont}(PQ) = \mathrm{cont}(P)\mathrm{cont}(Q)$.

Démonstration. Si on note $P(X) = \sum_{i=0}^{d} a_i X^i$ et $Q(X) = \sum_{i=0}^{e} b_i X^i$, alors pour tout i l'élément $\mathrm{cont}(P)$ divise a_i et $\mathrm{cont}(Q)$ divise b_i. Par la formule de convolution définissant les coefficients de PQ, $\mathrm{cont}(P)\mathrm{cont}(Q)$ divise chacun des coefficients de PQ, d'où $\mathrm{cont}(P)\mathrm{cont}(Q) | \mathrm{cont}(PQ)$.

Pour montrer la division réciproque $\mathrm{cont}(PQ) | \mathrm{cont}(P)\mathrm{cont}(Q)$, on considère les polynomes $\hat{P} := \frac{P}{\mathrm{cont}(P)}$ et $\hat{Q} := \frac{Q}{\mathrm{cont}(Q)}$ dans $A[X]$. Ils vérifient $\mathrm{cont}(\hat{P}) = \mathrm{cont}(\hat{Q}) = 1$, c'est-à-dire qu'ils sont primitifs. On veut montrer que $\hat{P}\hat{Q}$ est lui aussi primitif. Pour cela, on fixe $p \in A$ un élément premier quelconque. On veut montrer que la classe de $\hat{P}\hat{Q}$ dans $(A/(p))[X]$ est non triviale.

L'hypothèse $\mathrm{cont}(\hat{P}) = 1$ implique que la classe de $\hat{P}(X)$ dans $(A/(p))[X]$ est non nulle. De même la classe de $\hat{Q}(X)$ dans $(A/(p))[X]$ est non nulle. Par la proposition 1.30 l'anneau $A/(p)$ est intègre. Par la proposition de transfert de l'intégrité 1.42 l'anneau $(A/(p))[X]$ l'est aussi. Par intégrité, la classe du produit $\hat{P}\hat{Q}$ dans $(A/(p))[X]$ est non nulle, ce qui

signifie que p ne divise pas $\mathrm{cont}(\hat{P}\hat{Q})$. Comme c'est le cas pour tout p premier, on a bien $\mathrm{cont}(\hat{P}\hat{Q}) = 1$. □

Corollaire 1.72. *Soit A un anneau factoriel. Soit $P, Q \in \mathrm{Frac}(A)[X]$ unitaires et tels que le produit PQ est dans $A[X]$. Alors P et Q sont dans $A[X]$.*

La condition "unitaires" sert à normaliser. En effet, on a $2X \cdot \frac{X}{2} = X^2 \in \mathbb{Z}[X]$, alors que $\frac{X}{2}$ n'est pas dans $\mathbb{Z}[X]$.

Démonstration. Décomposons les coefficients de P sous formes de fractions irréductibles a_i/b_i, et notons m le ppcm des dénominateurs b_i. Alors mP est dans $A[X]$ et on affirme que son contenu vaut 1. En effet, comme mP est de coefficient dominant m, son contenu divise m. Si p est un diviseur premier de m qui apparait à la puissance d dans m, il existe un dénominateur b_i divisible par p^d tandis que p ne divise pas a_i. Alors le coefficient $\frac{ma_i}{b_i}$ n'est pas divisible par p, et donc p ne divise pas $\mathrm{cont}(mP)$. De la même façon si on note n le ppcm des dénominateurs des coefficients de Q, alors nQ est dans $A[X]$ et de contenu 1.

Par le lemme de Gauss on a $\mathrm{cont}(mnPQ) = \mathrm{cont}(mP)\mathrm{cont}(nQ) = 1$. Comme PQ est dans $A[X]$, son contenu est dans A, ce qu'on peut (tautologiquement) écrire $1|\mathrm{cont}(PQ)$. Mais on a alors $mn|\mathrm{cont}(mnPQ) = 1$. Par conséquent m et n sont des unités, donc P et Q sont dans $A[X]$. □

Corollaire 1.73. *Soit $P \in A[X]$ unitaire. Si P est irréductible dans $A[X]$, alors il l'est dans $\mathrm{Frac}(A)[X]$.*

Démonstration. En effet, si P était égal à un produit P_1P_2 avec $P_1, P_2 \in \mathrm{Frac}(A)[X]$, quitte à les multiplier par des constantes on pourrait rendre P_1 et P_2 unitaires, et par le corollaire précédent, on aurait alors $P_1, P_2 \in A[X]$. □

Exemple 1.74. Les polynomes $X^3 - 2$ et $X^3 - 2X + 3$ n'ont pas de racine entière, ils sont donc irréductibles sur $\mathbb{Z}$, et donc sur $\mathbb{Q}$.

Plus généralement, on a un théorème de transfert pour les anneaux factoriels, avec en plus de l'information sur les irréductibles.

Théorème 1.75 (transfert de la factorialité)**.** *Soit A un anneau factoriel. Alors $A[X]$ est factoriel, et les éléments irréductibles de $A[X]$ sont*

- *les éléments irréductibles de A;*
- *les polynomes primitifs de $A[X]$ qui sont irréductibles dans $\mathrm{Frac}(A)[X]$.*

Démonstration. Commençons par montrer que les éléments mentionnés dans l'énoncé sont irréductibles dans $A[X]$.

Si $a \in A$ est un élément irréductible, il reste irréductible dans $A[X]$. En effet, si on avait $a = PQ$, on aurait $\deg(P) = \deg(Q) = 0$, et on est ramené à l'irréductibilité dans A.

Ensuite, soit $P \in A[X]$ primitif et irréductible dans $\mathrm{Frac}(A)[X]$. Supposons qu'on puisse écrire $P = P_1P_2$ avec $P_1, P_2 \in A[X]$. Alors, par irréductibilité dans $\mathrm{Frac}(A)[X]$, l'un des facteurs, disons P_1, est dans $\mathrm{Frac}(A) \cap A[X] = A$. Comme on a $\mathrm{cont}(P) = \mathrm{cont}(P_1)\mathrm{cont}(P_2) = 1$, on a $\mathrm{cont}(P_1) = 1$, donc P_1 est une constante inversible de A, et donc P est irréductible dans $A[X]$.

Il reste à démontrer l'existence et l'unicité de la décomposition de tout polynome en un produit d'éléments des deux types décrits ci-dessus. Commençons par l'existence, et le fait qu'il n'y a pas d'autre irréductible.

Soit $P \in A[X]$ quelconque. Comme $\mathrm{Frac}(A)[X]$ est principal, donc factoriel, on peut décomposer $P = P_1 \dots P_r$ dans $\mathrm{Frac}(A)[X]$. Quitte à multiplier chaque polynome par un élément de $\mathrm{Frac}(A)$, on transforme l'écriture précédent en une décomposition $P = (\frac{a}{b})P_1 \dots P_r$, où chaque polynome P_i est dans $A[X]$ et primitif, et a, b sont deux éléments de A premiers entre eux. Dans $A[X]$, on peut écrire $bP = aP_1 \dots P_r$, d'où $b\mathrm{cont}(P) = a\mathrm{cont}(P_1) \dots \mathrm{cont}(P_r) = a$, d'où $\mathrm{cont}(P) = \frac{a}{b}$. Comme $P \in A[X]$, son contenu est dans A, d'où $b = 1$. On a alors $P = \mathrm{cont}(P)P_1 \dots P_r$. Il suffit de décomposer $\mathrm{cont}(P)$ en produits d'irréductibles de A pour avoir la décomposition de P comme produit des éléments annoncés. Cela montre aussi que si P se décomposait dans $\mathrm{Frac}(A)[X]$, il se décompose de la même façon dans $A[X]$, donc il n'y a pas d'autre irréductible que ceux qui sont mentionnés.

Reste à démontrer l'unicité de la décomposition. Notons d'abord que si on a $P = a_1 \dots a_s P_1 \dots P_r$ avec $a_1, \dots, a_s \in A$ irréductibles et $P_1, \dots, P_r \in A[X]$ primitifs et irréductibles dans $\mathrm{Frac}(A)[X]$, alors $\mathrm{cont}(P) = a_1 \dots a_s$ est une décomposition de $\mathrm{cont}(P)$ dans A. Comme A est factoriel, celle-ci est unique (à permutation et unités près). Enfin $P_1 \dots P_r = \frac{P}{\mathrm{cont}(P)}$ est une décomposition en irréductibles dans $\mathrm{Frac}(A)[X]$, laquelle est aussi unique à multiplication par des éléments de $\mathrm{Frac}(A)^*$ près. □

1.12. **Polynomes irréductibles.** La question de l'irréductibilité des polynomes étant cruciale pour la suite, on présente quelques critères pour y répondre.

Sur les corps, les polynomes primitifs de degré 1 sont évidemment irréductibles. Ensuite, un polynome de degré 2 ou 3 est irréductible si et seulement si il n'a pas de racine.

Exemple 1.76. Le polynome $X^2 + X + 1$ est irréductible sur le corps à deux éléments $\mathbb{F}_2$, puisque ni 0 ni 1 n'en sont racine.

Voici un premier critère moins trivial.

Théorème 1.77. *(réduction modulo idéal premier) Soit A un anneau factoriel, I un idéal premier de A, et $P \in A[X]$ primitif non constant. Si*

- *le coefficient dominant $\mathrm{dom}(P)$ n'est pas dans I,*
- *le projeté $\bar{P}$ de P dans $(A/I)[X]$ est irréductible,*

alors le polynome P est irréductible dans $A[X]$ (et donc dans $\mathrm{Frac}(A)[X]$).

Exemple 1.78.

- $X^2 + X + 1$ étant irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$, il l'est aussi sur $\mathbb{Z}[X]$, et donc sur $\mathbb{Q}[X]$.
- $X^3 + 9X^2 + 5X + 22$ étant irréductible dans $(\mathbb{Z}/3\mathbb{Z})[X]$, il l'est aussi sur $\mathbb{Z}[X]$, et donc sur $\mathbb{Q}[X]$.
- Pour p un entier premier, $X^p - X - 1$ est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$, donc il l'est aussi sur $\mathbb{Z}[X]$, et donc sur $\mathbb{Q}[X]$.
- $X^5 + XY^2 + Y^2 + Y - 1$ est irréductible sur $\mathbb{Z}[X, Y]$.

Attention, la réciproque est fausse. On peut par exemple voir (ce n'est pas trivial) que $X^4 + 1$ est réductible dans tout $(\mathbb{Z}/p\mathbb{Z})[X]$, mais pas sur $\mathbb{Z}$.

Démonstration. Rappelons (proposition 1.30) que l'hypothèse I premier est équivalente à A/I intègre.

Supposons qu'on a $P(X) = B(X)C(X)$. On veut montrer que B ou C est une constante inversible de A. En projetant dans A/I, on a $\bar{P} = \bar{B}\bar{C}$. Comme $\mathrm{dom}(P)$ n'est pas dans I, on en déduit que $\bar{P}$ est de même degré que P, et donc $\bar{B}$ et $\bar{C}$ sont de même degré que B et C respectivement. Or $\bar{P}$ est irréductible, donc $\bar{B}$ ou $\bar{C}$ est une constante inversible de A/I, donc de degré 0. Par conséquent, B ou C est une constante, disons B. Enfin, P est supposé primitif, donc de contenu 1. Par le lemme de Gauss, B et C sont aussi de contenu 1, donc B est une constante inversible. □

Le critère suivant est un cousin, au sens où la preuve est très proche.

Théorème 1.79 (Critère d'Eisenstein)**.** *Soit A un anneau factoriel, p un élément premier de A. Soit $Q(X) = X^d + \sum_{i=0}^{d-1} q_i X^i \in A[X]$ un polynome dont tous les coefficients (à part le dominant) sont divisibles par p et dont le coefficient q_0 n'est pas divisible par p^2. Alors Q est irréductible dans $\mathrm{Frac}(A)[X]$ (et donc dans $A[X]$).*

Exemple 1.80.
- $X^3 + 2X^2 + 6X + 10$ est irréductible sur $\mathbb{Z}$ (et donc sur $\mathbb{Q}$).
- Pour $d \geqslant 1$ un entier et p premier, le polynome $X^d + p$ est irréductible.
- Pour $p \in \mathbb{N}$ un entier premier, le polynome $Q_p(X) := X^{p-1} + X^{p-2} + \cdots + X + 1 = \frac{X^p - 1}{X - 1}$ est irréductible sur $\mathbb{Z}$, et donc sur $\mathbb{Q}$. En effet, on a $Q_p(X+1) = \dfrac{(X+1)^p - 1}{X} = X^{p-1} + \dfrac{\sum_{k=1}^{p-1} \binom{p}{k} X^k}{X} + \dfrac{1-1}{X} = X^{p-1} + \sum_{k=0}^{p-2} \binom{p}{k+1} X^k$. Et comme p divise $\binom{p}{k+1}$ pour tout k entre 0 et $p-2$, et que p^2 ne divise pas $\binom{p}{1} = p$, le polynome $Q_p(X+1)$ est irréductible, et donc Q_p l'est.

Démonstration. Comme son coefficient dominant vaut 1, Q est primitif, donc il suffit se démontrer l'irréductibilité dans $A[X]$. Si on a $Q(X) = B(X)C(X)$, alors en projetant dans $(A/(p))[X]$ on a $X^d = \bar{Q}(X) = \bar{B}(X)\bar{C}(X)$. Comme $(A/(p))[X]$ est intègre, $\bar{B}(X)$ et $\bar{C}(X)$ sont des monomes X^k et X^l, avec $k + l = d$. Si à la fois k et l sont strictement plus grand que 1, alors on a $\bar{B}(0) = \bar{C}(0) = 0$, donc p divise $B(0)$ et $C(0)$, donc p^2 divise $Q(0)$, ce qui contredit l'hypothèse. Donc k ou l est nul, donc B ou C est constant et primitif, ce qui donne l'irréductibilité. □

Un dernier critère à la fois assez élémentaire et très utile en pratique dans le cas particulier des polynomes sur les corps finis est l'algorithme de Berlekamp qui sera vu en DM.

1.13. **Anneaux noethériens.** Rappelons que, dans un anneau, un idéal I est dit de type fini s'il existe des éléments $f_1, \ldots, f_r$ qui l'engendrent : $I = (f_1, \ldots, f_r) = \{\sum_{i=1}^{r} a_i f_i ; a_i \in A\}$.

Définition 1.81. Un anneau A est dit *noethérien*[7] si tous ses idéaux sont de type fini.

Exemple 1.82.
- Les anneaux principaux sont noethériens ($\mathbb{Z}$, $k[X]$, etc).

[7] en hommage à Emmy Noether (1882–1935). Le jour où votre nom deviendra un adjectif, vous aurez réussi votre vie !

- $\mathbb{Z}[\sqrt{-5}]$ est noethérien (cf infra pour la preuve). En fait, ses idéaux sont engendrés par au plus 2 éléments.
- Si A est un anneau noethérien et I un idéal quelconque, alors A/I est noethérien[8].
- L'anneau $K[X_1, \dots]$ des polynomes en une infinité de variables n'est pas noethérien. En effet, l'idéal $(X_1, X_2, \dots)$ des poynomes sans terme constant n'est pas de type fini.
- L'anneau $C^0([0;1], \mathbb{R})$ n'est pas de type fini. En effet, l'idéal des fonctions s'annulant sur un voisinage (indéfini) de 0 n'est pas de type fini.

Contrairement aux anneaux principaux ou factoriels, on ne requiert pas l'intégrité. On a alors

Proposition 1.83. *Soit A un anneau noethérien et I un idéal propre de A. Alors l'anneau-quotient A/I est noethérien.*

Démonstration. On note $\pi : A \to A/I$ le morphisme de projection canonique.

Soit J un idéal de A/I, on veut motrer que J est type fini. On pose $J_0 = \pi^{-1}(J) = \{j \in A \,|\, \pi(j) \in J\}$. Alors J_0 est un idéal de A. En effet, pour $\pi(j_1), \pi(j_2) \in J$ on a $\pi(j_1 \pm j_2) = \pi(j_1) \pm \pi(j_2) \in J$, et pour $a \in A$, $j \in J$ on a $\pi(aj) = \pi(a)\pi(j) \in J$. Comme A est noethérien, J_0 est de type fini, donc il existe $j_1, \dots, j_k \in A$ tels que $J_0 = (j_1, \dots, j_k) = \{\sum_{i=1}^{k} a_i j_i ; a_i \in A\}$. Reste à montrer qu'on a $J = (\pi(j_1), \dots, \pi(j_k))$. Procédons par double-inclusion.

Pour $\subset$, soit $\ell \in J$ et $\ell_0 \in \pi^{-1}(\ell)$. Alors il existe $a_1, \dots, a_k \in A$ tels que $\ell_0 = \sum a_i j_i$, et donc $\ell = \pi(\ell_0) = \sum \pi(a_i)\pi(j_i)$.

Pour $\supset$, puisque $j_i \in J_0 = \pi^{-1}(J)$, on a $\pi(j_i) \in J$, donc l'idéal engendré par les j_i est inclus dans J. □

Remarquons que la preuve précédente passe presque aux anneaux principaux: les idéaux du quotient d'un anneau principal sont principaux, mais l'anneau-quotient n'est pas toujours principal car pas nécessairement intègre.

Dans le même genre, les produits d'anneaux noethériens sont noethériens, ainsi que les localisés d'anneaux noethériens.

En revanche, un sous-anneau d'un anneau noethérien ne l'est pas forcément (penser au cas d'un anneau non noethérien comme sous-anneau de son corps des fractions).

Voici une autre caractérisation de la noethérianité. On rappelle qu'une suite est dite *stationnaire* si elle est constante à partir d'un certain rang.

Proposition 1.84. *Un anneau est noethérien si et seulement si toute suite croissante d'idéaux (pour l'inclusion) est stationnaire.*

Concernant les exemples précédents, on peut remarquer que dans $\mathbb{Z}[\sqrt{-5}]$, si on a une suite croissante d'idéaux, la norme du plus petit élément non nul diminue, donc elle stationne. En revanche, dans $K[X_1, \dots]$, on a la suite croissante $(X_1) \subset (X_1, X_2) \subset \dots$ qui ne stationne jamais.

[8] Cette propriété passe au quotient par des idéaux quelconques, même pas forcément premiers, en particulier car on n'a pas demandé l'intégrité pour être noethérien.

Démonstration. Pour le sens direct, si $I_1 \subset I_2 \subset \dots$ est une suite croissante d'idéaux. Alors $I = \cup_{k\geqslant 0} I_k$ est un idéal. Par hypothèse, il est de type fini, donc il existe $f_1, \dots, f_r$ tels que $I = (f_1, \dots, f_r)$. Chacun de ces éléments $f_1, \dots, f_r$ étant dans un I_k, il existe k_{max} tels que $f_1, \dots, f_r$ sont tous dans $I_{k_{max}}$, donc $I = I_{k_{max}}$, et la suite stationne à partir de k_{max}.

Pour le sens indirect, prouvons plutôt la contraposée : si I est un idéal de A qui n'est pas de type fini, alors on prend $f_1 \in I$ quelconque et l'idéal $I_1 = (f_1)$. Comme I n'est pas de type fini, il n'est pas égal à I_1, donc il existe $f_2 \in I \setminus I_1$. On considère alors $I_2 = (f_1, f_2)$, etc. Alors la suite $I_1 \subset I_2 \subset \dots$ est une suite strictement croissante pour l'inclusion. □

Le dernier argument est proche de ce qu'on avait utilisé pour montrer l'existence d'une décomposition en irréductibles pour les anneaux principaux (Théorème 1.66). On a donc

Proposition 1.85. *Si A est un anneau noethérien, alors tout élément de A admet une décomposition (pas nécessairement unique) en produit d'éléments irréductibles.*

Démonstration. (On recopie presque mot pour mot la partie *existence* de la démonstration du théorème 1.66.) Soit $a \in A$. Montrons par l'absurde que a admet une décomposition en produits d'irréductibles. Supposons donc que a n'admet pas de décomposition en produit d'irréductibles. Puisque a n'est pas irréductible, il existe $a_1, b_1 \in A$ qui ne sont pas des unités et tels que $a = a_1 b_1$. Alors par hypothèse et quitte à permuter les rôles, a_1 n'admet pas de décomposition en produit d'irréductibles. On itère alors: on obtient une suite infinie $a = a_1 b_1, a_1 = a_2 b_2, a_2 = a_3 b_3, \dots$, où pour tout $i \in \mathbb{N}^*$ on a $a_{i+1} | a_i$ et a_i n'admet pas de décomposition en produits d'irréductibles. Alors on a la suite d'inclusions d'idéaux infinie $(a_1) \subset (a_2) \subset (a_3) \subset \dots$. L'ensemble $I = \cup_{i\geqslant 1}(a_i)$ est alors un idéal. Comme A est noethérien, I est de type fini, donc il existe $f_1, \dots, f_r \in A$ tels que $I = (f_1, \dots, f_r)$. Alors puisque $f_1, \dots, f_r$ sont dans I, il existe $n \in \mathbb{N}$ tel que $f_1, \dots, f_r \in (a_n)$, et alors $(a_{n+1}) = (a_n)$ (et même la suite d'inclusions stationne à partir de là). Mais alors b_{n+1} est une unité, ce qui fournit une contradiction. □

Un grand avantage de la notion de noethérianité (qui fait son importance) est qu'elle se transfère aux anneaux de polynomes.

Théorème 1.86 (de la base de Hilbert / transfert de la noethérianité)**.** *Soit A un anneau noethérien. Alors l'anneau $A[X]$ est noethérien.*

Comme le nom du théorème l'indique, la démonstration va fournir un peu plus: si on sait trouver des familles génératrices (qu'on appelle *bases* par abus) pour les idéaux de A, on va trouver des familles génératrices pour les idéaux de $A[X]$.

Démonstration. Soit I un idéal de $A[X]$. On s'intéresse aux coefficients dominants des éléments de I : pour k entier, on définit $I_k := \{a_k \in A \mid \exists P \in I, \deg(P) = k \wedge \mathrm{dom}(P) = a_k\}$. Le fait que I soit un idéal de $A[X]$ implique que pour tout k l'ensemble I_k est un idéal de A, et on a les inclusions $I_0 \subset I_1 \subset \dots$ Comme A est noethérien, par la proposition 1.84, la suite précédente stationne, et donc il existe un entier N tel que $\forall n \geqslant N, I_n = I_N$.

Comme A est noethérien, pour tout entier k, l'idéal I_k est noethérien, donc il existe des éléments $a_{k,1}, \dots, a_{k,m_k} \in A$ tels que $I_k = (a_{k,1}, \dots, a_{k,m_k})$. Par définition de I_k, pour chaque élément de type $a_{k,j}$, il existe $P_{k,j} \in I$ de degré k et tel que $\mathrm{dom}(P_{k,j}) = a_{k,j}$.

On affirme que l'idéal I est engendré par la famille finie $(P_{k,j})_{0\leqslant k\leqslant N, 1\leqslant j\leqslant m_k}$. Prouvons-le par récurrence sur le degré d'un élément $P \in I$.

Si $\deg(P) = 0$, alors P est une constante dans I_0, donc $P \in (P_{0,1}, \dots, P_{0,m_0})$.

Ensuite si $\deg(P) \leqslant N$, alors $\mathrm{dom}(P) \in I_{\deg(P)}$, donc il existe $\lambda_1, \dots, \lambda_{\deg(P)} \in A$ tels que $\mathrm{dom}(P) = \sum \lambda_j a_{\deg(P),j}$. Alors $P - \sum \lambda_i P_{\deg(P),i}$ est de degré strictement inférieur à $\deg(P)$, et donc dans $(P_{k,j})_{0\leqslant k\leqslant N, 1\leqslant j\leqslant m_k}$ par hypothèse de récurrence. Donc P aussi.

Enfin si $\deg(P) > N$, l'argument est presque le même, en remplaçant $I_{\deg(P)}$ par I_N: $\mathrm{dom}(P)$ est dans I_N, donc il existe $\lambda_1, \dots, \lambda_N \in A$ tels que $\mathrm{dom}(P) = \sum \lambda_j a_{N,j}$. Alors $P - \sum \lambda_i P_{N,i} X^{\deg(P)-N}$ est de degré strictement inférieur à $\deg(P)$, et donc dans $(P_{k,j})_{0\leqslant k\leqslant N, 1\leqslant j\leqslant m_k}$ par hypothèse de récurrence. □

On a même plus: si A est noethérien, alors l'anneau des séries formelles $A[[X]]$ l'est aussi. Une série formelle n'ayant pas de coefficients dominant, il faut changer un peu la preuve !

1.14. **Idéaux maximaux et autres Zorneries (bases d'ev).** On a vu que dans un anneau noethérien, toute suite croissante (pour l'inclusion) d'idéaux est stationnaire (proposition 1.84). Étant donné un idéal propre, on peut donc chercher à rajouter des éléments jusqu'à le rendre le plus gros possible. Cela suggère que tout idéal pourrait être inclus dans un idéal maximal. "Rajouter" des éléments nécessite de les choisir — une opération qui semble naturelle, mais repose néanmoins sur l'axiome du choix (AC). Celui-ci est axiome de la théorie des ensembles dont on a souvent envie de se servir mais qui est indépendant des autres axiomes. On note ZF pour l'ensemble des axiomes usuels de Zermelo-Frankel (sans le choix), et ZFC quand on a ajouté AC. [9]

Pour ce qui nous occupe, on utilise plutôt le lemme de Zorn, équivalent à l'axiome du choix[10]. Un ordre (partiel) sur un ensemble E est une relation $\leqslant$ qui est réflexive ($\forall x \in E, x \leqslant x$), anti-symmétrique ($\forall x, y \in E, x \leqslant y \wedge y \leqslant x \Rightarrow x = y$) et transitive ($\forall x, y, z \in E, x \leqslant y \wedge y \leqslant z \Rightarrow x \leqslant z$). Une partie $P \subset E$ est dite *totalement ordonnée* si deux éléments quelconques de P sont comparables ($\forall x, y \in P, x \leqslant y \vee y \leqslant x$). Pour P' une partie quelconque de E, un majorant de P' est un élément $m \in E$ satisfaisant $\forall x \in P, x \leqslant m$. On dit qu'un ensemble E est *inductif* si toute partie non vide totalement ordonnée admet un majorant. Enfin un élément maximal de E est un élément satisfaisant $\forall x \in E, m \leqslant x \Rightarrow m = x$.

Lemme 1.87 (de Zorn)**.** *Tout ensemble inductif non vide admet un élément maximal.*

Voici deux applications du lemme de Zorn, dont la première concerne les idéaux :

Théorème 1.88 (de Krull, 1929)**.** *Tout anneau non nul admet un idéal maximal.*

Démonstration. Soit E l'ensemble des idéaux propres de A, muni de la relation d'inclusion. C'est un ensemble ordonné. Si P est une partie totalement ordonnée de E, alors la réunion $\cup_{I\in P} I$ est un idéal de A qui contient tous les idéaux de P, qui est propre (car l'élément

[9] Notez que comme on ne connait souvent pas les axiomes de ZF, ça peut sembler bizarre de donner autant de place à AC. Une raison est qu'on peut déjà faire beaucoup de choses sans AC, une autre est que AC a des conséquences parfois très surprenantes comme le paradoxe de Banach-Tarski, demandez à J-C Sikorav qui est friand de ce sujet.

[10] voir dans [Lang] pour une démonstration

1 n'appartient à aucun des idéaux de P et donc pas à leur union non plus), et qui est donc un majorant de P. L'ensemble des idéaux propres de A est donc un ensemble ordonné inductif, et par le lemme de Zorn, il admet un élément maximal pour l'inclusion, lequel est alors un idéal maximal de A. □

Voici une seconde application qui n'a rien à voir, mais qui est importante.

Théorème 1.89. *Tout espace vectoriel V non nul admet une base.*

Démonstration. Soit E l'ensemble des familles libres d'éléments de V, muni de la relation d'inclusion. C'est un ensemble ordonné inductif : si $\{L_i\}$ est un ensemble totalement ordonné de familles libres de E, alors leur réunion $\cup_i L_i$ est libre et est donc un majorant des L_i. Il existe donc une famille L maximale pour l'inclusion, dont on va montrer que c'est une base. Soit W le sous-espace de V engendré par L. Si on avait $W \neq V$, alors on pourrait rajouter à L un élément de $V \setminus W$, ce qui contredirait la maximalité de L. □

2. Corps et extensions

2.1. **Exemples de base.**

Définition 2.1. Un *corps* est un anneau dont tout élément non nul est inversible. Un *sous-corps* d'un corps est un sous-ensemble qui forme un corps.

Exemple 2.2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ forment des corps, $\mathbb{Z}$ n'en est pas un,

D'après la proposition 1.30, pour A un anneau et I un idéal, l'anneau-quotient A/I est un corps si et seulement si I est un idéal maximal.

Exemple 2.3. Pour $A = \mathbb{Z}$, on voit que $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est un nombre premier. On note $\mathbb{F}_p$ ce corps.

Lemme 2.4. *Pour K un corps, un idéal I de $K[X]$ est maximal si et seulement il existe un polynome $P \in K[X]$ irréductible tel que $I = (P)$.*

Démonstration. Pour le sens direct, si I est maximal, par principalité il existe P tels que $I = (P)$. Si on a $P = QR$ avec Q, R non constants, on a alors $I = (P) \subset (Q) \subset K[X]$, les deux inclusion étant strictes. Cela contredit la maximalité, donc P est irréductible.

Réciproquement, si I n'est pas maximal, soit P quelconque tel que $I = (P)$. Alors il existe J tel qu'on a $I \subset J \subset K[X]$ avec des inclusions strictes. Par principalité, il existe $Q \in K[X]$ tels que $J = (Q)$. Alors $I \subset J$ implique $Q|P$, donc P n'est pas irréductible. □

Exemple 2.5.
- Les polynomes irréductibles de $\mathbb{R}[X]$ sont de la forme $X - a$ avec $a \in \mathbb{R}$ et $X^2 + a$ avec $a \in \mathbb{R}_+^*$. On trouve que $\mathbb{R}[X]/(X - a)$ pour $a \in \mathbb{R}$ est un corps isomorphe à $\mathbb{R}$, tandis que $\mathbb{R}[X]/(X^2 + a)$ pour $a \in \mathbb{R}_+^*$ est un corps isomorphe à $\mathbb{C}$.
- Pour $A = \mathbb{F}_2[X]$ le polynome $X^2 + X + 1$ est irréductible (car sans racine), donc $\mathbb{F}_2[X]/(X^2 + X + 1)$ est un corps (à 4 éléments).
- Plus généralement, pour $A = \mathbb{F}_p[X]$, il y a $\frac{p(p+1)}{2}$ polynomes unitaires réductibles de degré 2, donc $\frac{p(p-1)}{2}$ polynomes irréductibles de degré 2, ce qui donne autant de corps à p^2 éléments. On montrera qu'ils sont en fait tous isomorphes.
- Si on est capable de montrer que sur $\mathbb{F}_p[X]$, il existe des polynomes irréductibles de tout degré n, alors on est capable de construire des corps à p^n éléments pour tout n. Par un argument de dénombrement, on pourrait y arriver; on donnera une preuve plus directe (mais moins élémentaire).

Définition 2.6. Un *morphisme de corps* est une application $f : K_1 \to K_2$ qui respecte les structures de corps, c'est-à-dire $f(0) = 0, f(1) = 1, f(a - b) = f(a) - f(b)$ et $f(ab^{-1}) = f(a)f(b)^{-1}$.

Lemme 2.7. *Soit $f : A \to B$ un morphisme de corps. Alors f est injectif.*

Démonstration. Cela tient à l'inversibilité: si a est non nul, comme on a $f(a)f(a^{-1}) = 1_B$, on a $f(a) \neq 0_B$. Ainsi $\ker(f)$ est réduit à $\{0_A\}$. □

2.2. **Extensions de corps.**

Si K est un corps et F un sous-corps de K, alors K est muni d'une structure de F-espace vectoriel naturelle.

Définition 2.8. Dans ce contexte, on dit que K est une *extension* de F, ce qu'on note K/F. Le *degré* de l'extension K/F est la dimension de K comme F-espace vectoriel, on la note $[K : F]$. L'extension K/F est dite *finie* si son degré $[K : F]$ est fini.

Si $F \subset K \subset L$ sont des extensions, on dit que K/F est une *sous-extension* de L/F.

Exemple 2.9.
- $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = +\infty$,
- $[\mathbb{F}_2[X]/(X^2 + X + 1) : \mathbb{F}_2] = 2$,

Théorème 2.10 (de la base télescopique)**.** *Si K/F et F/E sont des extensions de corps, alors on a $[K : E] = [K : F][F : E]$. De plus, si $\{f_i\}_{i\in I}$ est une E-base de F et $\{k_j\}_{j\in J}$ est une F-base de K, alors $\{f_i k_j\}_{i\in I, j\in J}$ est une E-base de K.*

Démonstration. Il suffit de vérifier l'énoncé sur les bases, celui sur les dimensions en découle par dénombrement.

Montrons que la famille $\{f_i k_k\}_{i\in I, j\in J}$ est génératrice : si x est un élément de F, il existe des éléments $(y_j)_{j\in J}$ dans F tels que $x = \sum_{j\in J} y_j k_j$. Pour tout $j \in J$, comme y_j est dans F, il existe des éléments $(z_{i,j})_{i\in I}$ dans E tels que $y_j = \sum_{i\in I} z_{i,j} f_i$. On a alors $x = \sum_{i\in I, j\in J} z_{i,j}(f_i k_j)$.

Montrons que la famille $\{f_i k_k\}_{i\in I, j\in J}$ est libre : si $\sum_{i\in I, j\in J} z_{i,j} f_i k_j = 0$, alors $\sum_{j\in J}(\sum_{i\in I} z_{i,j} f_i)k_j = 0$, donc pour tout $j \in J$, on a $\sum_{i\in I} z_{i,j} f_i = 0$, et donc pour tout $i \in I$, $j \in J$ on a $z_{i,j} = 0$. □

Définition 2.11. Soit K un corps, $P \subset K$ une partie. Le *sous-corps* engendré par P est le plus petit sous-corps de K contenant P.

Le sous-corps engendré par $\{1\}$ est appelé *sous-corps premier*.

Rappelons que pour A un anneau, il existe un unique morphisme $f : \mathbb{Z} \to A$, donc le noyau est de la forme $n_A\mathbb{Z}$. L'entier n_A est appelé la caractéristique de A. Lorsque A est intègre, donc en particulier si c'est un corps, sa caractéristique est un nombre premier. On voit que l'image de f est incluse dans le sous-corps premier. On a l'alternative suivante :

Lemme 2.12. *Soit K un corps,*
- *si $\mathrm{car}(K) = p > 0$, alors le sous-corps premier de K est isomorphe à $\mathbb{F}_p$;*
- *si $\mathrm{car}(K) = 0$, alors le sous-corps premier de K est isomorphe à $\mathbb{Q}$.*

Démonstration. Dans le premier cas, il n'y a rien à dire : le sous-corps premier comprend l'image du morphisme $f : \mathbb{Z} \to A$, qui est une copie de l'anneau $\mathbb{Z}/p\mathbb{Z}$. Il se trouve que c'est un corps.

Dans le second cas, l'image du morphisme $f : \mathbb{Z} \to A$ est une copie de l'anneau $\mathbb{Z}$. Le sous-corps premier contient donc cette copie de $\mathbb{Z}$. Comme il s'agit d'un corps, il comprend aussi les inverses de ses éléments. On a donc un morphime de corps $\bar{f} : \mathbb{Q} \to K$ défini par $\bar{f}(a/b) = f(a)f(b)^{-1}$. Comme tout morphisme de corps est injectif (lemme 2.7), l'image de $\bar{f}$ est isomorphe à $\mathbb{Q}$. □

Tout corps est une extension de son sous-corps premier. En particulier si un corps est fini, son sous-corps premier l'est, donc tout corps fini est une extension de $\mathbb{F}_p$ pour un certain p, donc de cardinal p^n pour un certain p premier et n entier.

Un corps de cardinal p^d ne peut être une extension d'un corps de cardinal $p^{d'}$ que si $p^{d'}$ est une puissance de p^d, c'est-à-dire si on a $d|d'$. Dans ce cas, le degré de l'extension est $\frac{d'}{d}$.

2.3. **Éléments algébriques.**

Définition 2.13. Pour K/F une extension et $\alpha \in K \setminus F$ un élément, on note

- $F[\alpha]$ le sous-anneau de K qui est l'image de $F[X]$ par le morphisme d'évaluation ev_α, c'est-à-dire $F[\alpha] = \{P(\alpha); P \in F[X)\}$.
- $F(\alpha)$ le sous-corps de K engendré par F et par α.

Définition 2.14. Soit K/F une extension et $\alpha \in K/F$. On dit que α est *algébrique sur* F s'il existe $P \in F[X]$ non nul tel que $P(\alpha) = 0$.

Un nombre qui n'est pas algébrique sur $\mathbb{Q}$ est dit *transcendant*.

Exemple 2.15.
- $\sqrt{2} \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$ puisqu'il est racine de $X^2 - 2 \in \mathbb{Q}[X]$.
- $\mathrm{i}\sqrt{3} \in \mathbb{C}$ est algébrique sur $\mathbb{Q}$ puisqu'il est racine de $X^2 + 3 \in \mathbb{Q}[X]$.
- e est transcendant (théorème de Hermite, 1873).
- π est transcendant (théorème de von Lindemann, 1882).

Proposition 2.16. *Soit K/F une extension et α un élément de K. Alors les assertions suivantes sont équivalentes :*

(1) *α est algébrique sur K;*
(2) *$F[\alpha]/F$ est une extension finie;*
(3) *$F[\alpha] = F(\alpha)$.*

Démonstration. (1)⇒(2): Soit $P \in F[X]$ non nul tel que $P(\alpha) = 0$. Alors l'application $\mathrm{ev}_\alpha : F[X] \to F[\alpha]$ est linéaire et bien définie. Comme $(P(X)) \subset \ker(\mathrm{ev}_\alpha)$, elle passe au quotient en une application $\overline{\mathrm{ev}}_\alpha : F[X]/(P(X)) \to F[\alpha]$ surjective. Comme l'espace source est une extension finie de F de degré inférieur ou égal à celui de P, l'image $F[\alpha]$ est aussi une extension de F de degré inférieur ou égal à $\deg(P)$.

(2)⇒(3): Montrons que si $F[\alpha]/F$ est finie, alors $F[\alpha]$ est un corps. Pour cela, soit $\beta \in F[\alpha]$ non nul. Alors la multiplication par β est un endomorphisme de $F[\alpha]$ (vu comme F-espace vectoriel), qui est injectif par intégrité. Comme on est en dimension finie, il est alors surjectif, donc il existe $\gamma \in F[\alpha]$ tels que $\beta\gamma = 1$. Ainsi β est inversible, et donc $F[\alpha]$ est un corps. Comme il contient F et α, il s'agit bien de $F(\alpha)$.

(3)⇒(1): Dans $F(\alpha)$, l'élément α a un inverse, donc on a $\frac{1}{\alpha} \in F[\alpha]$. Par conséquent il existe $Q(X) \in F[X]$ tel que $\frac{1}{\alpha} = Q[\alpha]$, soit $\alpha Q(\alpha) - 1 = 0$. En particulier α est annulé par le polynome $XQ(X) - 1 \in F[X]$. □

Si α est algébrique sur F, alors l'ensemble $I_\alpha = \{P(X) \in F[X] \,|\, P(\alpha) = 0\}$ est un idéal de $F[X]$. Or ce dernier est un anneau principal, donc l'idéal I_α est principal.

Définition 2.17. Soit K/F une extension et $\alpha \in K$ algébrique sur F. L'ensemble des polynomes $P(X) \in F[X]$ annulant α est appelé *idéal annulateur* de α. Le générateur unitaire de cet idéal est appelé *polynome minimal de α (sur F)*, noté $P_{\min,\alpha}$, $\mu_{F,\alpha}$, voire μ_α lorsque F est donné par le contexte.

Exemple 2.18.
- Le polynome minimal de $\sqrt{2}$ sur $\mathbb{Q}$ est $X^2 - 2$.
- Le polynome minimal de $\sqrt{2} + \sqrt{3}$ sur $\mathbb{Q}$ est $(X^2 - 5)^2 - 24 = X^4 - 10X + 1$.

Lemme 2.19. *Dans le contexte précédent, le polynome $\mu_{F,\alpha}$ est irréductible sur F.*

Démonstration. Supposons $\mu_\alpha = QR$. Alors en particulier on a $Q(\alpha)R(\alpha) = 0$, donc par intégrité et quitte à permuter on a $Q(\alpha) = 0$, ce qui par minimalité implique que Q est de même degré que μ_α, et donc que R est constant. □

Définition 2.20. Soit K/F une extension et $\alpha \in K$ algébrique sur F. Le *degré* de α est défini comme le degré de son polynome minimal, on le note $\deg_F(\alpha)$.

Lemme 2.21. *Soit K/F une extension et $\alpha \in K$ algébrique sur F. Alors on a $\deg_F(\alpha) = [F[\alpha] : F]$ et $F[X]/(\mu_{F,\alpha}) \simeq F[\alpha]$.*

Démonstration. L'égalité numérique découle de l'isomorphisme en considérant les dimensions comme F-espaces vectoriels.

Quant à l'isomorphisme, on remarque que l'idéal $(\mu_{F,\alpha})$ est inclus dans le noyau du morphisme $\mathrm{ev}_\alpha : F[X] \to F[\alpha]$, donc celui-ci passe au quotient en un morphisme $\overline{\mathrm{ev}}_\alpha : F[X]/(\mu_{F,\alpha}) \simeq F[\alpha]$. Or ce morphisme est injectif par définition de μ_α: si on a $\mathrm{ev}_\alpha(Q(X)) = 0$, alors $Q(X)$ est dans l'idéal annulateur de α, donc Q est un multiple de $\mu_{F,\alpha}$. Comme on est en dimension finie, le morphisme $\overline{\mathrm{ev}}_\alpha$ est donc un isomorphisme. □

Voici une application importante et non triviale du lien entre algébricité et extensions finies (2.16). Il n'est a priori pas trivial que la somme ou le produit de deux nombres algébriques le soient. Et pourtant:

Proposition 2.22. *Soit K/F une extension. Alors l'ensemble des éléments de K algébriques sur F est un sous-corps de K.*

Démonstration. Soit $\alpha, \beta \in K$ algébriques sur F. Alors, en tant qu'espace vectoriel, $F[\alpha,\beta]$ est engendré par la famille $\{\alpha^i\beta^j\}_{0\leqslant i<\deg(\alpha),0\leqslant j<\deg(\beta)}$. En particulier $F[\alpha,\beta]$ est une extension finie de F. Or on a $F \subset F[\alpha-\beta] \subset F[\alpha,\beta]$, donc $F[\alpha-\beta]/F$ est une extension finie. Par conséquent $\alpha-\beta$ est algébrique sur F. De la même façon, on a $F \subset F[\alpha\beta] \subset F[\alpha,\beta]$, donc $F[\alpha\beta]/F$ est une extension finie, et par conséquent $\alpha\beta$ est algébrique sur F.

Ennfin pour α algébrique sur F et non nul, si on note $\mu_\alpha(X) = \sum_{i=0}^d a_i X^i$ son polynome minimal, alors $\sum_{i=0}^d a_i X^{d-i}$ annule $\frac{1}{\alpha}$, qui est donc algébrique sur F. □

Exemple 2.23. Comme $\sqrt{2} + \sqrt[3]{2} \in \mathbb{Q}[\sqrt{2}, \sqrt[3]{2}]$, c'est un nombre algébrique sur $\mathbb{Q}$ de degré au plus 6, et même divisant 6. Or on vérifie que la famille $1, \sqrt{2}+\sqrt[3]{2}, (\sqrt{2}+\sqrt[3]{2})^2$ est $\mathbb{Q}$-libre, donc c'est un nombre de degré exactement 6.

Définition 2.24. L'ensemble des éléments algébriques sur $\mathbb{Q}$ de $\mathbb{C}$ est noté $\bar{\mathbb{Q}}$.

On peut voir que si F est infini, l'ensemble des éléments algébriques sur F forme un corps de même cardinal que F. En particulier $\bar{\mathbb{Q}}$ est un sous-corps dénombrable de $\mathbb{C}$.

On veut définir une notion de produit pour les extensions. Ceci ne peut être fait qu'à l'intérieur d'une extension commune.

Définition 2.25. Soit K/F une extension de corps et $E_1/F, E_2/F$ deux sous-extensions de K/F. Le *compositum* $E_1 \cdot E_2$ est le sous-corps de K engendré par E_1 et E_2.

Proposition 2.26. *Si $E_1/F, E_2/F$ sont deux sous-extensions finies de K/F, alors $E_1 \cdot E_2$ est une extension finie de F. De plus on a $[E_1 \cdot E_2 : F] \leqslant [E_1 : F][E_2 : F]$, avec égalité si $[E_1 : F]$ et $[E_2 : F]$ sont premiers entre eux.*

Exemple 2.27.
- Dans $\mathbb{C}/\mathbb{Q}$, on considère les sous-extensions finies $\mathbb{Q}[\mathrm{i}]/\mathbb{Q}$ et $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$, toutes deux de degré 2. Leur compositum $\mathbb{Q}[\mathrm{i}] \cdot \mathbb{Q}[\sqrt{2}]$ est l'extension $\mathbb{Q}[\mathrm{i}, \sqrt{2}]$ qui est de degré 4 (une $\mathbb{Q}$-base est par exemple $(1, \mathrm{i}, \sqrt{2}, \mathrm{i}\sqrt{2})$). On a ici égalité dans l'inégalité des degrés (bien que 2 et 2 ne soient pas premiers entre eux !).
- Dans $\mathbb{C}/\mathbb{Q}$, on considère les sous-extensions finies $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ et $\mathbb{Q}[\mathrm{j}\sqrt[3]{2}]/\mathbb{Q}$, toutes deux de degré 3. Leur compositum $\mathbb{Q}[\sqrt[3]{2}] \cdot \mathbb{Q}[\mathrm{j}\sqrt[3]{2}]$ est l'extension $\mathbb{Q}[\mathrm{j}, \sqrt[3]{2}]$ qui est de degré 6 (une $\mathbb{Q}$-base est par exemple $(1, \sqrt[3]{2}, \sqrt[3]{4}, \mathrm{j}, \mathrm{j}\sqrt[3]{2}, \mathrm{j}\sqrt[3]{4})$). On a ici inégalité stricte dans l'inégalité des degrés.

Démonstration. Soit A l'anneau engendré par E_1 et E_2, c'est un sous-anneau de K. Vu comme F-espace vectoriel, il est de dimension finie.

Comme E_1/K et E_2/K sont finies, tous les éléments de ces extensions sont algébriques sur F. Par la proposition précédente, tout élément de A est algébrique sur F. En particulier pour tout élément $\alpha \in A$ on a $F[\alpha] \subset A$, donc α est inversible dans A. Ainsi A est un corps, et donc $E_1 \cdot E_2 = A$.

Ensuite, si on note $(b_1, \dots, b_m)$ une F-base de E_1, $(c_1, \dots, c_n)$ une F-base de E_2, alors A est engendrée sur F par la famille $(b_1c_1, \dots, b_mc_n)$, donc A est un F-espace vectoriel de dimension au plus mn.

Enfin, si $[E_1 : F]$ et $[E_2 : F]$ sont premiers entre eux, on a les deux tours d'extensions $F \subset E_1 \subset E_1 \cdot E_2$ et $F \subset E_2 \subset E_1 \cdot E_2$. Par conséquent $[E_1 \cdot E_2 : K]$ est divisible à la fois par $[E_1 : K]$ et par $[E_2 : K]$, donc par leur produit, d'où l'égalité. □

2.4. **Adjonction de racines, corps de rupture, corps de décomposition.** La question qui nous occupe maintenant est : étant donné un corps K et un polynome $P(X) \in K[X]$, peut-on construire des extensions de K dans lesquelles P a une racine? dans lesquelles P est scindé? La réponse est oui, et même il y a unicité si on est un peu plus restrictif.

On rappelle que dans le contexte précédent l'anneau-quotient $K[X]/(P(X))$ est un corps si et seulement si le polynome P est irréductible sur K. Dans ce cas, on a construit une extension (finie) de K dans laquelle le polynome P a une racine. On parle d'*adjonction de racine*. Cette extension n'est pas la seule dans laquelle P a une racine (puisque ce sera le cas dans toute sur-extension), mais elle est néanmoins minimale au sens où toute extension la "contient".

Définition 2.28. Soit K un corps et $P(X) \in K[X]$ un polynome irréductible. Une extension L/K est appelée *corps de rupture* de P sur K, notée parfois $\mathrm{Rupt}_K(P)$ ou $R_K(P)$, s'il existe $\alpha \in L$ tel qu'on a $P(\alpha) = 0$ et $L = K(\alpha)$.

Exemple 2.29.
- $\mathbb{Q}[\sqrt{2}]$ est un corps de rupture de $X^2 - 2$ sur $\mathbb{Q}$.
- $\mathbb{Q}[\sqrt[3]{2}]$ est un corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$.
- $\mathbb{C}$ est un corps de rupture de $X^2 + 1$ sur $\mathbb{R}$.

Remarquons que le polynome $P(X)$ n'est pas toujours scindé —et même souvent pas— dans $\mathrm{Rupt}_K(P)$, comme le montre l'exemple de $X^3 - 2$ qui se factorise en $(X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$ sur $\mathbb{Q}[\sqrt[3]{2}]$.

Pour K un corps et $L_1/K, L_2/K$ deux extensions, un K-isomorphisme $u : L_1 \to L_2$ est un isomorphisme de corps dont la restriction à K est l'identité.

Théorème 2.30 (existence et unicité du corps de rupture)**.** *Soit K un corps et $P(X) \in K[X]$ un polynome irréductible sur K. Alors il existe un corps de rupture de P sur K. Celui-ci est une extension de degré $\deg(P)$ de K, et il est unique à K-isomorphisme près.*

Démonstration. L'existence se fait par adjonction de racine: on considère l'extension $K[X]/(P(X))$, qui est un corps puisque P est supposé irréductible. Soit α l'image de X dans $K[X]/(P(X))$. Alors d'une part on a $P(\alpha) = 0$, et d'autre part α engendre $K[X]/(P(X))$ puisque X engendre (en tant qu'anneau) $K[X]$. L'extension ainsi construite est bien de degré $\deg(P)$.

Pour l'unicité, soit L une extension de K engendrée par une racine α de P. On va montrer que L est isomorphe à $K[X]/(P(X))$. Pour cela, on définit un morphisme d'anneaux $u : K[X] \to L$ par $u(Q(X)) = Q(\alpha)$ pour tout polynome $Q \in K[X]$. Comme on a $P(\alpha) = 0$, l'idéal $(P(X))$ est inclus dans $\ker(u)$, et donc u passe au quotient en un morphisme d'anneaux $\bar{u} : K[X]/(P(X)) \to L$ défini par $\bar{u}(\bar{Q}(X)) = Q(\alpha)$, où Q est un représentant quelconque de la classe $\bar{Q}$. Comme $K[X]/(P(X))$ et L sont des corps, $\bar{u}$ est en fait un morphisme de corps (en effet, on a $\bar{u}(1) = 1$, puis $\bar{u}(1/x)\bar{u}(x) = \bar{u}(1) = 1$, donc $\bar{u}(1/x) = 1/\bar{u}(x)$). En particulier $\bar{u}$ est injectif (lemme 2.7). De plus, comme L est engendré par $\alpha = \bar{u}(X)$, $\bar{u}$ est surjectif, et donc $\bar{u}$ réalise l'isomorphisme annoncé. □

Notons que si le corps de rupture est unique à K-isomorphisme près, l'isomorphisme n'est pas unique. Au contraire, cette non-unicité est la richesse de la théorie de Galois.

Notons que si on ne suppose pas le polynome P irréductible, trouver une extension engendrée par une racine n'est pas un problème (il suffit de choisir un facteur de irréductible P), mais on n'a plus unicité.

Exemple 2.31. Dans $\mathbb{C}$ le polynome $X^3 - 2$ est scindé et a pour racines $\sqrt[3]{2}, \mathrm{j}\sqrt[3]{2}$ et $\mathrm{j}^2\sqrt[3]{2}$. "Le" corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$ est donc $\mathbb{Q}[\sqrt{2}] \simeq \mathbb{Q}[\mathrm{j}\sqrt{2}] \simeq \mathbb{Q}[j^2\sqrt{2}]$. Cela illustre le fait que l'unicité n'est qu'à isomorphisme près.

Exemple 2.32. Les corps finis peuvent être construits comme corps de rupture, pourvu qu'on ait des polynomes irréductibles des bons degré. Par exemple, le polynome $X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$, donc $\mathrm{Rupt}_{\mathbb{F}_2}(X^2 + X + 1)$ est un corps à 4 éléments.

Sur son corps de rupture, un polynome n'est en général pas scindé. On peut demander cela, mais alors il faut des extensions plus grandes.

Définition 2.33. Soit K un corps et $P(X) \in K[X]$ un polynome. Une extension L/K est appelée *corps de décomposition* de P sur K, notée parfois $\mathrm{Dec}_K(P)$ ou $D_K(P)$, si $P(X)$, vu comme polynome de $L[X]$, est scindé, et si l'extension L/K est engendrée par les racines de P dans L.

Exemple 2.34. $\mathbb{Q}[\sqrt[3]{2}, \mathrm{j}]$ est un corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$. En effet, les nombres $\sqrt[3]{2}, \mathrm{j}\sqrt[3]{2}$ et $\mathrm{j}^2\sqrt[3]{2}$ sont dans $\mathbb{Q}[\sqrt[3]{2}, \mathrm{j}]$ et on a $\mathbb{Q}[\sqrt[3]{2}, \mathrm{j}] = \mathbb{Q}[\sqrt[3]{2}, \mathrm{j}\sqrt[3]{2}, \mathrm{j}^2\sqrt[3]{2}]$. C'est une extension de $\mathbb{Q}$ de degré 6.

Théorème 2.35 (Existence et unicité du corps de décomposition)**.** *Soit K un corps et $P(X) \in K[X]$ un polynome sur K. Alors il existe un corps de décomposition de P sur K. Celui-ci est une extension de degré au plus $\deg(P)!$ de K, et il est unique à K-isomorphisme près.*

Notons qu'ici on a unicité, même lorsque P n'est pas irréductible. Tout comme pour le corps de rupture, l'isomorphisme n'est pas unique en général. D'autre part, on n'a pas d'expression exacte du degré en général, juste une borne supérieure factorielle.

Démonstration. Commençons par démontrer l'existence et la borne sur le degré, par récurrence sur $\deg(P)$. On décompose P en facteurs irréductibles. S'ils sont tous de degré 1, alors P est scindé sur K, et donc K est un corps de décomposition. Sinon soit Q un facteur irréductible de P de degré au moins 2. Soit $K' = \mathrm{Rupt}_K(Q)$ et $x_1 \in K'$ tel que $K' = K(x_1)$. Alors il existe $P_1(X) \in K'[X]$ tel que $P(X) = (X - x_1)P_1(X)$. Par hypothèse de récurrence, il existe un corps de décomposition $L = \mathrm{Dec}_{K'}(P_1)$. Alors P_1 est scindé sur L et donc P aussi. En notant $x_2, \dots, x_{\deg(P)}$ les racines de P_1 dans L, on a $L = K'(x_2, \dots, x_{\deg(P)})$, d'où $L = K(x_1)(x_2, \dots, x_{\deg(P)}) = K(x_1, x_2, \dots, x_{\deg(P)})$, donc L est un corps de décomposition de P sur K.

Pour le degré, notons qu'on a $[K' : K] \leqslant \deg(P)$ puisque K' est le corps de rupture d'un facteur irréductible de P, et $[L : K'] \leqslant (\deg(P) - 1)!$ par hypothèse de récurrence. Par le théorème de la base télescopique, on a alors $[L : K] = [L : K'][K' : L] \leqslant (\deg(P) - 1)! \deg(P) = \deg(P)!$.

Pour démontrer l'unicité, on doit renforcer un peu la propriété à démontrer (du fait que la preuve va se faire ajout de racine par ajout de racine, et donc qu'après la première étape, on n'a plus forcément le même corps de base):

Lemme 2.36. *Soit K, K' deux corps et $i : K \to K'$ un isomorphisme, étendu en un isomorphisme d'anneaux $\hat{i} : K[X] \to K'[X]$. Soit $P(X) \in K[X]$, $L = \mathrm{Dec}_K(P)$ et $L' = \mathrm{Dec}_{K'}(\hat{i}(P))$ deux corps de décomposition. Alors il existe un isomorphisme $j : L \to L'$ prolongeant i. De plus j envoie toute racine de P sur une racine de $\hat{i}(P)$.*

Preuve du lemme 2.36. On raisonne encore par récurrence sur le degré $[L : K]$ de l'extension. Pour $[L : K] = 1$, $j = i$ convient.

Pour $[L : K] \geqslant 2$, le polynome P est scindé dans L et a des racines dans $L \setminus K$; soit α d'une d'elles. Alors le polynome minimal $\mu_K(\alpha)$ divise P et est irréductible. Notons d son degré. Le polynome $\hat{i}(\mu_K(\alpha))$ est alors aussi irréductible, de degré d, et divise $\hat{i}(P)$. Comme L' est un corps de décomposition de $\hat{i}(P)$, le polynome $\hat{i}(\mu_K(\alpha))$ admet des racines dans L'; soit α' l'une d'elles. On affirme qu'il existe un isomorphisme $i_1 : K(\alpha) \to K'(\alpha')$ prolongeant i.

En effet, $K(\alpha)$ est un corps de rupture pour $\mu_{K,\alpha}$ sur K, donc il est K-isomorphe à $K[X]/(\mu_{K,\alpha}(X))$. De même, $K'(\alpha')$ est un corps de rupture pour $\hat{i}(\mu_{K,\alpha})$ sur K', donc il est K'-isomorphe à $K'[X]/(\hat{i}(\mu_{K,\alpha})(X))$. Enfin $\hat{i}$ induit un isomorphisme entre $K[X]/(\mu_{K,\alpha}(X))$ et $K'[X]/(\hat{i}(\mu_{K,\alpha})(X))$, d'où l'existence de l'isomorphisme i_1.

Maintenant L et L' sont des corps de décomposition de P et $\hat{i}(P)$ sur $K(\alpha)$ et $K'(\alpha')$ respectivement. Par le théorème de la base télescopique on a $[L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K]$. Comme on a $[K(\alpha) : K] \geqslant 2$, on a $[L : K(\alpha)] < [L : K]$. Par hypothèse de récurrence, on peut donc prolonger l'isomorphisme $i_1 : K(\alpha) \to K'(\alpha')$ en un isomorphisme $j : L \to L'$. Comme i_1 prolongeait i, j le prolonge aussi. □

Il suffit d'appliquer le lemme 2.36 pour $K = K'$ et $i = \mathrm{id}_K$ pour démontrer l'unicité dans le théorème 2.35. □

2.5. **Corps finis.** En guise d'illustration des constructions précédentes, et parce que ce sont des objets fondamentaux, on construit ici les corps finis. Notons que tout ce cours se place dans un cadre commutatif. Il se trouve que même dans un cadre non commutatif, les corps finis le sont toujours (théorème de Wedderburn, 1905).

On a déjà démontré que si K est un corps fini de cardinal q, sa caractéristique est un nombre premier qu'on note p. Son sous-corps premier est alors canoniquement isomorphe à $\mathbb{F}_p$ (lemme 2.12), de sorte K est un $\mathbb{F}_p$-espace vectoriel de dimension finie. Notant n cette dimension, on a $q = p^n$ pour des raisons de cardinal. De plus le groupe multiplicatif K^* est cyclique (proposition 1.48), de cardinal $q-1 = p^n - 1$. Ainsi tout élément de K est racine du polynome $X^q - X$. Comme il s'agit d'un polynome de degré q et qu'il a q racines sur K, on en déduit qu'il est scindé sur K. Enfin, l'application définie par $f(x) = x^p$ est un automorphisme de K (proposition 1.40).

Définition 2.37 (automorphisme de Frobenius)**.** Soit K un corps fini de caractéristique p. L'automorphisme de corps $\mathrm{Fr} : K \to K$ défini par $f(x) = x^p$ est appelé *automorphisme de Frobenius* ou plus simplement *Frobenius*.

Dans ce contexte, pour r un entier naturel, l'application $x \mapsto x^{p^r} = (((x^p)^p)\dots)^p$ est le Frobenius itéré r fois, c'est donc un automorphisme de K.

Théorème 2.38 (existence et unicité des corps finis)**.** *Soit p un nombre premier et $n \in \mathbb{N}^*$ un entier positif. Alors il existe un corps fini de cardinal p^n, et celui-ci est unique à isomorphisme près. En particulier il est isomorphe à $\mathrm{Dec}_{\mathbb{F}_p}(X^{p^n} - X)$.*

Dans ce cadre, on note (abusivement) $\mathbb{F}_{p^n}$ l'unique corps à p^n éléments.

Démonstration. Commençons par l'existence. Comme on a remarqué ci-dessus, le polynome $X^{p^n} - X$ doit être scindé sur un corps de cardinal p^n. On considère alors le corps $K = \mathrm{Dec}_{\mathbb{F}_p}(X^{p^n} - X)$, et le sous-ensemble $k \subset K$ des racines de $X^{p^n} - X$. On affirme que k est un sous-corps de K. En effet, comme $x \mapsto x^{p^n}$ est un automorphisme de K, si x, y sont dans k, alors $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ et $(xy)^{p^n} = x^{p^n} y^{p^n}$, de sorte que $x+y$ et xy sont dans k; on vérifie aussi que si $x \in k^*$, alors $-x$ et $\frac{1}{x}$ sont dans k^*, ce qui prouve que k est un corps. En notant $Q(X) = X^{p^n} - X$, on a $Q'(X) = p^n X^{p^n-1} - 1 = -1$, puisque $p | p^n$. Ainsi Q et Q' sont premiers entre eux, donc toutes les racines de Q sont simples. Comme Q est scindé sur k, on a $|k| = p^n$. Par minimalité du corps de décomposition, on a donc $k = K$, ce qui conclut la preuve de l'existence.

Pour l'unicité, soit K un corps à p^n élements. Par le théorème de Lagrange, tout élément de K est racine de $X^{p^n} - X$, et donc ce polynome a p^n racines distinctes. En considérant le degré, on a en particulier $X^{p^n} - X = \prod_{x \in K}(X - x)$, de sorte que $X^{p^n} - X$ est scindé sur K. En notant $x_1, \dots, x_{p^n}$ les éléments de K, on a (tautologiquement) $K = \mathbb{F}_p(x_1, \dots, x_{p^n})$, de sorte que K est un corps de décomposition de $X^{p^n} - X$ sur son sous-corps premier $\mathbb{F}_p$. On conclut par l'unicité du corps de décomposition (théorème 2.35). □

Notons que, si K est un corps à p^n éléments, comme K^* est un groupe cyclique, il admet des générateurs (qui sont au nombre de $p^n - p^{n-1}$). Soit ξ un tel générateur, alors ξ est un nombre algébrique sur $\mathbb{F}_p$, de degré n. En particulier son polynome minimal $\mu_{\mathbb{F}_p,\xi}$ est un polynome irréductible de degré n. On déduit donc du théorème 2.38

Corollaire 2.39. *Soit p un nombre premier et n un entier naturel, alors il existe des polynomes irréductibles de degré n dans $\mathbb{F}_p[X]$, et pour P_1, P_2 deux tels polynomes, on a $\mathbb{F}_p[X]/(P_1(X)) \simeq \mathbb{F}_p[X]/(P_2(X)) \simeq \mathbb{F}_{p^n}$.*

Notons que l'isomorphisme précédent n'a rien d'évident (c'est pourquoi la notation $\mathbb{F}_{p^n}$ est dangeureuse).

Exemple 2.40.

- Sur $\mathbb{F}_2$, les deux polynomes X^3+X+1 et X^3+X^2+1 sont irréductibles, on a donc $\mathbb{F}_2[X]/(X^3+X+1) \simeq \mathbb{F}_2[X]/(X^3+X^2+1) \simeq \mathbb{F}_8$. En fait sur $\mathbb{F}_2$ on a la décomposition $X^8 - X = X(X+1)(X^3+X+1)(X^3+X^2+1)$.

  Cela peut sembler paradoxal que les corps de ruptures de deux polynomes distincts soient isomorphes. C'est qu'en rajoutant une racine de X^3+X+1, on a en fait rajouté toutes les autres racines de ce polynome, et plus généralement toutes les racines de tous les polynomes irréductibles de degré 3.

  On peut même détailler un peu plus: si on prend α une racine de X^3+X+1, c'est un générateur de $\mathbb{F}_8^*$. Donc la famille $1, \alpha, \alpha^2$ est une base de $\mathbb{F}_8$ comme $\mathbb{F}_2$-espace vectoriel. Aussi, on peut décomposer les puissances de α (qui parcourent tout $\mathbb{F}_8^*$) dans cette base: on a α, α^2, $\alpha^3 = \alpha + 1$, $\alpha^4 = \alpha^2 + \alpha$, $\alpha^5 = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$, $\alpha^6 = \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1, \alpha^7 = 1$. On peut alors calculer les polynomes minimaux de tous ces éléments: pour 0 on trouve X, pour 1 on trouve $X-1$, pour α on trouve X^3+X+1. Pour α^2 ne voit pas de relation entre $\alpha^4 = \alpha^2 + \alpha, \alpha^2$ et 1 on doit alors aller à $\alpha^6 = \alpha^2 + 1$, et on trouve $\alpha^6 + \alpha^2 + 1 = 0$ donc le polynome minimal de α^2 est X^3+X+1. De la même façon pour α^3 on ne voit pas de relation entre $\alpha^6 = \alpha^2 + \alpha + 1, \alpha^3 = \alpha + 1$ et 1. Mais on trouve $\alpha^9 + \alpha^6 + 1 = 0$, donc le polynome minimal de α^3 est X^3+X^2+1. En continuant de la sorte on trouve que trois éléments ont pour polynome minimal X^3+X+1, à savoir α, α^2 et α^4, et trois éléments ont pour polynome minimal X^3+X^2+1, à savoir α^3, α^5 et α^6. Cela sera expliqué avec le théorème 2.46.
- De même on peut décomposer $X^{16} - X$ sur $\mathbb{F}_2$: on a $X^{16} - X = X(X+1)(X^2+X+1)(X^4+X^3+X^2+X+1)(X^4+X+1)(X^4+X^3+1)$. La racine de X est l'élément 0, la racine de $X+1$ est l'élément 1, de sorte que les racines de $X^2 - X$ sont le sous-corps premier. Les racines de $X(X+1)(X^2+X+1) = X^4 - X$ correspondent à un sous-corps de cardinal 4 (cf infra). Enfin les racines des trois autres polynomes irréductibles correspondent à des générateurs du groupe multiplicatif $\mathbb{F}_{16}^*$.

L'exemple précédent de $\mathbb{F}_{16}$ suggère qu'un corps K de cardinal p^n peut contenir des sous-corps de cardinal p^d pour certains d. Par exemple pour $d = 1$, c'est le sous-corps premier. Si k est un sous-corps de cardinal p^d, alors K est une extension de k donc en particulier p^n est une puissance de p^d. Ceci n'est possible que si $d|n$.

Proposition 2.41. *Soit p un entier premier et $d \leqslant n$ deux entiers positifs. Alors $\mathbb{F}_{p^n}$ contient un sous-corps de cardinal p^d si et seulement on a $d|n$. Dans ce cas, le sous-corps de cardinal p^d est unique, il s'agit de l'ensemble des racines du polynome $X^{p^d} - X$.*

Démonstration. Si $k \subset \mathbb{F}_{p^n}$ est un sous-corps de cardinal p^d, alors d'après le théorème de Lagrange, tous ses éléments sont racines de $X^{p^d} - X$. Comme un tel polynome a au plus p^d

racines, si un tel sous-corps existe, il est unique. Reste à montrer que ce polynome admet bien p^d racines sur $\mathbb{F}_{p^n}$.

C'est ici qu'on va utiliser l'hypothèse $d|n$. Sa nécéssité a été établie avant la proposition. Maintenant remarquons que $d|n$ implique $p^d - 1|p^n - 1$. En effet, modulo $p^d - 1$ on a $p^n \equiv (p^d)^{\frac{n}{d}} \equiv 1^{\frac{n}{d}} \equiv 1 \mod p^d - 1$. En notant $k = \frac{p^n-1}{p^d-1}$, on a alors $X^{p^n} - X = X(X^{p^n-1} - 1) = X((X^{p^d-1})^k - 1) = X(X^{p^d-1} - 1)((X^{p^d-1})^{k-1} + (X^{p^d-1})^{k-2} + \cdots + (X^{p^d-1}) + 1)$, de sorte que $X^{p^d} - X$ divise $X^{p^n} - X$. Comme le polynome $X^{p^n} - X$ est scindé sur $\mathbb{F}_{p^n}$, le polynome $X^{p^d} - X$ l'est aussi, et donc il admet bien p^d racines sur $\mathbb{F}_{p^n}$. □

On peut alors complètement décomposer $X^{p^n} - X$ sur $\mathbb{F}_p$, en combinant les éléments précédents:

Théorème 2.42. *Soit p un nombre premier et $n \geqslant 2$ en entier. Soit $P_1, \ldots, P_k \in \mathbb{F}_p[X]$ l'ensemble des polynomes unitaires irréductibles sur $\mathbb{F}_p$ dont le degré divise n. Alors dans $\mathbb{F}_p[X]$ on a la décomposition*

$$X^{p^n} - X = \prod_{j=1}^{k} P_j(X).$$

Démonstration. Notons $X^{p^n} - X = \prod_{j=1}^{\ell} Q_j(X)$ la décomposition en irréductibles de $X^{p^n} - X$ dans $\mathbb{F}_p[X]$, qu'on normalise pour être tous unitaires. Comme $X^{p^n} - X$ est premier avec son polynome dérivé -1, il n'y a aucun facteur multiple dans cette décomposition.

Comme $\mathbb{F}_{p^n}$ est un corps de décomposition de $X^{p^n} - X$, pour tout j il existe $\alpha_j \in \mathbb{F}_{p^n}$ tel que $Q_j(\alpha_j) = 0$. On a alors les extensions $\mathbb{F}_{p^n}/\mathbb{F}_p(\alpha_j)$ et $\mathbb{F}_p(\alpha_j)/\mathbb{F}_p$. En notant $d_j = \deg(Q_j)$, on a alors $|\mathbb{F}_p(\alpha_j)| = p^{d_j}$, d'où $d_j|n$. Ainsi la famille des Q_j est incluse dans la famille des P_j.

Réciproquement, si P est un polynome unitaire irréductible sur $\mathbb{F}_p$ de degré d divisant n, alors le corps de rupture $\mathbb{F}_p[X]/(P)$ est isomorphe à $\mathbb{F}_{p^d}$, qui est lui-même inclus dans $\mathbb{F}_{p^n}$ par la proposition précédente. Donc $\mathbb{F}_{p^n}$ contient une racine, disons α, de P. Ainsi $P(X) = \mu_{\mathbb{F}_p,\alpha}(X)$ divise $X^{p^n} - X$, donc P apparait bien dans la décomposition de $X^{p^n} - X$ en irréductibles. □

Si on note $m_n(p)$ le nombre de polynomes irréductibles unitaires dans $\mathbb{F}_p[X]$ de degré n, en considérant les degrés dans le théorème précédent on trouve $p^n = \sum_{d|n} dm_d(p)$. On en déduit d'une part $m_n(p) \leqslant \frac{p^n}{n}$ et d'autre part $p^n - nm_n(p) \leqslant \sum_{d|n} p^d \leqslant \sum_{d\leqslant\frac{n}{2}} p^d < p^{\frac{n}{2}}$, d'où $m_n(p) \sim \frac{p^n}{n}$. Non seulement il y a des polynomes irréductibles, mais il y en a beaucoup: parmi les p^n polynomes unitaires de degré n, une proportion en gros $\frac{1}{n}$ d'entre eux sont irréductibles.

2.6. **Automorphismes des corps finis.** L'automorphisme de Frobenius a joué un rôle dans la construction des corps finis dans la section précédente. On peut dire plus de cet automorphisme et de ces puissances. Cela donne en retour des informations sur la structure des corps finis.

Lemme 2.43. *Soit p un nombre premier et $n \geqslant 2$ un entier. Alors un élément $x \in \mathbb{F}_{p^n}$ vérifie $\mathrm{Fr}(x) = x$ si et seulement x appartient au sous-corps premier de $\mathbb{F}_{p^n}$.*

Démonstration. Notons que 1 est point fixe de Fr. Comme Fr est un automorphisme, on a $\mathrm{Fr}(1+1+\cdots+1) = \mathrm{Fr}(1)+\mathrm{Fr}(1)+\cdots+\mathrm{Fr}(1) = 1+1+\cdots+1$. Donc tous les éléments du sous-corps premier sont points fixes de Fr, ce qui fait déjà au moins p points fixes pour Fr.

Or un élément $x \in K$ est point fixe de Fr si et seulement s'il est racine du polynome $P(X) = X^p - X$. Comme K est intègre et P de degré p, il a au plus p racines. Donc Fr ne peut avoir d'autre point fixe que les éléments du sous-corps premier. □

La première partie de la preuve précédente rappelle que pour tout nombre premier p et pour tout entier x, on a $x^p \equiv x \mod p$.

Plus généralement on a

Lemme 2.44. *Soit p un nombre premier, $n \geqslant 2$ un entier et d un entier divisant n. Alors élément $x \in \mathbb{F}_{p^n}$ vérifie $\mathrm{Fr}^{(d)}(x) = x$ si et seulement si x appartient au sous-corps $\mathbb{F}_{p^d}$ de $\mathbb{F}_{p^n}$.*

Démonstration. La preuve est presque la même que le lemme précédent: l'équation $\mathrm{Fr}^{(d)}(x) = x$ se réécrit $x^{p^d} = x$, ce qui correspond bien aux éléments de $\mathbb{F}_{p^d}$. □

Voyons maintenant une propriété des polynomes qui relie les coefficients à l'invariance par le Frobenius.

Lemme 2.45. *Soit p un nombre premier et $n \geqslant 2$ un entier. Soit $Q \in \mathbb{F}_{p^n}[X]$. Alors Q est dans $\mathbb{F}_p[X]$ si et seulement si on a $Q(X^p) = Q(X)^p$.*

Démonstration. Notons $Q(X) = \sum a^i X^i$ avec $a_i \in \mathbb{F}_{p^n}$. Alors on a $Q(X^p) = \sum a_i X^{ip}$ et $Q(X)^p = (\sum a_i X^i)^p = \sum a_i^p X^{ip}$, la dernière égalité provenant du fait que Fr est un automorphisme de corps. On a donc $Q(X^p) = Q(X)^p$ si et seulement on a $a_i = a_i^p$ pour tout i, c'est-à-dire si et seulement si $a_i \in \mathbb{F}_p$ pour tout i. □

En particulier, on voit que pour $Q \in \mathbb{F}_p[X]$, si α est racine de Q, alors toute l'orbite de α sous l'action du Frobenius est racine de Q. On a maintenant une factorisation des polynomes irréductibles sur $\mathbb{F}_p$ dans $\mathbb{F}_{p^n}$. En effet, rappelons que tout polynome irréductible de degré n est un facteur de $X^{p^n} - X$ (théorème 2.42), et donc le polynome minimal d'un élément de $\mathbb{F}_{p^n}$.

Théorème 2.46. *Soit p un nombre premier et $n \geqslant 2$ un entier. Soit $\alpha \in \mathbb{F}_{p^n}$, $\mu_{\mathbb{F}_p,\alpha}$ son polynome minimal sur $\mathbb{F}_p$, et r son degré. Alors on a $r = \min\{s \mid \alpha^{p^s} = \alpha\}$, pour tous i, j distincts entre 0 et $r-1$ on a $\alpha^{p^i} \neq \alpha^{p^j}$, et on a $\mu_{\mathbb{F}_p,\alpha}(X) = \prod_{i=0}^{r-1}(X - \alpha^{p^i})$.*

Démonstration. Comme α est dans $\mathbb{F}_{p^n}$, on a $\mathrm{Fr}^{(n)}(\alpha) = \alpha$, et donc il existe $r > 0$ minimal tel que $\mathrm{Fr}^{(r)}(\alpha) = \alpha$. Comme Fr est un automorphisme (donc bijectif), cela implique $\mathrm{Fr}^{(i)}(\alpha) \neq \mathrm{Fr}^{(j)}(\alpha)$ pour tous i, j distincts entre 0 et r. Par le lemme 2.44, r est aussi le plus petit entier $d|n$ tel que $\alpha \in \mathbb{F}_{p^d}$. En particulier, c'est le degré de α sur $\mathbb{F}_p$.

Enfin comme $\mu_{\mathbb{F}_p,\alpha}$ est à coefficients dans $\mathbb{F}_p$, on a $\mu_{\mathbb{F}_p,\alpha}(X^p) = (\mu_{\mathbb{F}_p,\alpha}(X))^p$, donc l'ensemble des racines de $\mu_{\mathbb{F}_p,\alpha}$ est stable par Fr. En particulier, $\{\alpha^{p^i}\,;\, 0 \leqslant i \leqslant r-1\}$ est inclus dans les racines de $\mu_{\mathbb{F}_p,\alpha}$. Posons $Q(X) = \prod_{i=0}^{r-1}(X - \alpha^{p^i}) \in \mathbb{F}_{p^n}[X]$, qui est un diviseur de $\mu_{\mathbb{F}_p,\alpha}$ par la remarque précédente. Alors on a $Q(X^p) = \prod_{i=0}^{r-1}(X^p - \alpha^{p^i}) = (X^p - \alpha)\prod_{i=1}^{r-1}(X - \alpha^{p^{i-1}})^p = (X^p - \alpha^{p^s})\prod_{i=0}^{r-2}(X - \alpha^{p^i})^p = (X - \alpha^{p^{s-1}})^p \prod_{i=0}^{r-2}(X - \alpha^{p^i})^p = \prod_{i=0}^{r-1}(X - \alpha^{p^i})^p = (Q(X))^p$. Par le

lemme précédent, $Q(X)$ est donc dans $\mathbb{F}_p[X]$. Comme il divise $\mu_{\mathbb{F}_p,\alpha}(X)$ et que celui-ci est irréductible, on a alors $Q = \mu_{\mathbb{F}_p,\alpha}$, et donc $\mu_{\mathbb{F}_p,\alpha}(X) = \prod_{i=0}^{r-1}(X - \alpha^{p^i})$. □

Pour résumer les théorèmes 2.42 et 2.46: tout polynome irréductible sur $\mathbb{F}_p$ dont le degré d divise n apparait comme facteur de $X^{p^n} - X$ avec multiplicité 1. Il a alors d racines dans $\mathbb{F}_{p^n}$, qui correspondent à exactement une orbite de longueur d sous l'action du Frobenius.

On a vu que dans un corps fini, le Frobenius est un automorphisme. Il se trouve qu'à puissances près, c'est le seul:

Théorème 2.47. *Soit p premier et $n \geqslant 2$ entier. Alors les automorphismes de corps de $\mathbb{F}_{p^n}$ sont de la forme $\mathrm{Fr}^{(k)}$, avec $0 \leqslant k \leqslant n-1$. Ils forment un groupe isomorphe à $\mathbb{Z}/n\mathbb{Z}$, engendré par Fr.*

Démonstration. Soit f un automorphisme de $\mathbb{F}_{p^n}$. Considérons un générateur ξ du groupe multiplicatif $\mathbb{F}_{p^n}^*$. Notons que f est entièrement déterminé par $f(\xi)$ puisque tout élément non nul de $\mathbb{F}_{p^n}$ est de la forme ξ^i et qu'alors on a $f(\xi^i) = f(\xi)^i$. Il suffit donc de montrer que $f(\xi)$ est de la forme $\mathrm{Fr}^{(k)}(\xi)$ pour démontrer la première partie de l'énoncé.

Soit $\mu_{\mathbb{F}_p,\xi}(X) \in \mathbb{F}_p[X]$ le polynome minimal de ξ sur $\mathbb{F}_p$. Par le théorème précédent, $\mu_{\mathbb{F}_p,\xi}(X)$ est un polynome irréductible de degré n dont les racines sont les $\mathrm{Fr}^{(k)}(\xi)$, avec $0 \leqslant k \leqslant n-1$.

Comme on a $f(1) = 1$, f est l'identité sur le sous-corps premier. En notant $\mu_{\mathbb{F}_p,\xi}(X) = \sum a_i X^i$, on a $\mu_{\mathbb{F}_p,\xi}(f(X)) = \sum a_i (f(X)^i = \sum f(a_i) f(X)^i = f(\sum a_i X^i) = f(\mu_{\mathbb{F}_p,\xi}(X))$. On a alors $\mu_{\mathbb{F}_p,\xi}(f(\xi)) = f(\mu_{\mathbb{F}_p,\xi}(\xi)) = 0$, ce qui implique que $f(\xi)$ est racine de $\mu_{\mathbb{F}_p,\xi}$, et donc que $f(\xi)$ est bien de la forme $\mathrm{Fr}^{(k)}(\xi)$ avec $0 \leqslant k \leqslant n-1$.

La seconde partie du théorème est immédiate. □

2.7. **Clôture algébrique.**

Définition 2.48. Soit K/F est une extension de corps. On dit que c'est une extension *algébrique* si tout élément $\alpha \in K$ est algébrique sur $\mathbb{F}$.

Exemple 2.49.
- Une extension finie est algébrique.
- L'extension $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots)$ est algébrique, mais pas finie.

Lemme 2.50 (Transitivité de l'algébricité)**.** *Soit L/K et K/F deux extensions algébriques. Alors l'extension L/F est algébrique.*

Démonstration. Soit $\alpha \in L$. On veut montrer que α est algébrique sur F, c'est-à-dire que l'extension $F(\alpha)/F$ est finie. Comme L/K algébrique, α est algébrique sur K, et en particulier il existe $P(X) \in K[X]$ annulant α. Notons $a_0, \dots, a_n \in K$ les coefficients de P. Ce sont tous des éléments de K, qui sont donc algébriques sur F, de sorte que l'extension $F(a_0, \dots, a_n)/F$ est aussi finie. Or l'extension $F(a_0, \dots, a_n)(\alpha)/F(a_0, \dots, a_n)$ est finie (de degré au plus n), donc par le théorème de la base télescopique, l'extensions $F(a_0, \dots, a_n, \alpha)/F$ est finie. Comme $F(\alpha)/F$ en est une sous-extension, elle est aussi finie. □

Définition 2.51. Un corps K est dit *algébriquement clos* si tout polynome $P \in K[X]$ a une racine dans K.

Tout polynome sur un corps algébriquement corps est alors scindé.

Remarque 2.52. Si K est algébriquement clos et si L/K est une extension algébrique, alors L coïncide avec K. En effet, tout élément de L est algébrique sur K, donc racine d'un polynome de $K[X]$, et donc dans K.

Théorème 2.53 (D'Alembert-Gauss)**.** *Le corps $\mathbb{C}$ est algébriquement clos.*

Le théorème a été énoncé par D'Alembert, et Gauss en a proposé une preuve. Celle-ci était très élégante, mais en fait incomplète. Pour $P(X) \in \mathbb{C}[X]$ de degré n, l'idée est d'analyser les ensembles $C_{\Im} := \{z \in \mathbb{C} \mid \Re(P(z)) = 0\}$ et $C_{\Re} := \{z \in \mathbb{C} \mid \Im(P(z)) = 0\}$: il s'agit[11] de deux collections de n courbes immergées dans $\mathbb{C}$. Au voisinage de l'infini, elle alternent (car le comportement y est dicté par le terme dominant z^n). Alors par des considérations topologiques, la multicourbe $C_{\Im}$ doit couper la multicourbe $C_{\Re}$. Au point d'intersection, P s'annule; on a ainsi trouvé une racine.

Démonstration. Soit $P(X) \in \mathbb{C}[X]$ un polynome non constant, dont on note d le degré. On considère la fonction $N : \mathbb{C} \to \mathbb{R}$ définie par $N(z) = |P(z)|$. Au voisinage de l'infini, N est équivalente à z^d, et en particulier tend vers $+\infty$. Par conséquent N admet un minimal global, qu'on note z_0. Si on a $P(z_0) = 0$, on a trouvé une racine. Sinon on cherche une contradiction. En développant P au voisinage de z_0, on a $P(z) = P(z_0)(1 + b_m(z - z_0)^m + O((z - z_0)^{m+1})$, où b_m est un complexe non nul, qu'on écrit sous le forme $r_m e^{i\theta_m}$, avec $r_m \neq 0$. Pour $\varepsilon \in \mathbb{R}_+$, on considère le complexe $z_\varepsilon = z_0 + \varepsilon e^{i(-\theta_m+\pi)/m}$. On a alors

$$N(z_\varepsilon) = |P(z_0)|(1 - r_m\varepsilon^m + O(\varepsilon^{m+1}))|.$$

Pour ε assez petit, on a alors $N(z_\varepsilon) < N(z_0)$, une contradiction. □

Définition 2.54. Soit extension L/K est une *clôture algébrique* de K si L est algébriquement clos et L/K est une extension algébrique.

Corollaire 2.55 (du théorème de D'Alembert-Gauss)**.** *$\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.*

Attention, en revanche $\mathbb{C}$ n'est pas une clôture algébrique de $\mathbb{Q}$, puisque $\mathbb{C}$ contient des nombres transcendants sur $\mathbb{Q}$.

Proposition 2.56. *Si L/K est une extension et si L est algébriquement clos, alors l'ensemble $\bar{K}$ des éléments de L qui sont algébriques sur K est une clôture algébrique de K.*

Ainsi, l'ensemble $\bar{\mathbb{Q}}$ des nombres complexes qui sont algébriques sur $\mathbb{Q}$ est une clôture algébrique de $\mathbb{Q}$.

Démonstration. On a vu avec la proposition 2.22 que l'ensemble $\bar{K}$ est un corps. Par définition tous les éléments de $\bar{K}$ sont algébriques sur K, donc $\bar{K}/K$ est algébrique. Enfin si P est un polynome à coefficients dans $\bar{K}$, alors P est scindé dans L, donc il existe $\alpha_1, \ldots, \alpha_n \in L$ tels que $P(X) = (X - \alpha_1)\ldots(X - \alpha_n)$. Par le lemme 2.50, les éléments $\alpha_1, \ldots, \alpha_n$ sont algébriques sur $\bar{K}$, donc par le même lemme sur K, et donc ils appartiennent à $\bar{K}$. Ainsi P est scindé sur $\bar{K}$, et donc $\bar{K}$ est algébriquement clos. □

[11] C'est à démontrer, et c'est là que la preuve de Gauss est incomplète.

Théorème 2.57 (Steinitz)**.** *Tout corps admet une clôture algébrique, unique à isomorphisme près.*

Démonstration. (existence) Soit K un corps. L'idée est, comme pour la construction du corps de décomposition, de construire une extension dans laquelle tous les polynomes ont une racine, puis d'itérer à partir de l'extension obtenue. On commence donc par construire une extension algébrique E_1/K dans laquelle tous les polynomes de $K[X]$ sont scindés [12]. Pour cela, on introduit l'ensemble $\mathrm{Pol}_K \subset K[X]$ des polynomes non constants à coefficients dans K. Pour chaque élément $P \in \mathrm{Pol}_K$ on introduit une variable formelle X_P, et on considère l'anneau de polynomes $A := K[X_P]_{P\in\mathrm{Pol}_K}$ en une infinité de variables. On considère l'idéal $I := (P(X_P))_{P\in\mathrm{Pol}_K}$. On voudrait considérer l'anneau A/I dans lequel chacun des polynomes non constants à coefficients dans K a une racine, et dire que c'est un corps. Pour cela il faut vérifier d'une part que $A \neq I$ et que I est maximal. Le premier point est vrai, mais le second pas nécessairement : on s'en sort plutôt avec un idéal maximal.

Montrons donc que I n'est pas égal à A entier. Si c'était le cas, 1 serait dans I, donc on aurait des polynomes $P_1, \dots, P_n \in \mathrm{Pol}_K$ et des éléments $a_1, \dots, a_n \in A$ tels que $1 = \sum_k a_k P_k(X_{P_k})$. Dans cette somme, les coefficients $a_k \in A$ sont aussi des polynomes, et seul un nombre fini de variables apparait. Récursivement, en partant de $K_0 = K$, pour chaque variable X_{P_k} on construit alors une extension finie K_k/K_{k-1} dans laquelle P_k a une racine α_{P_k}. En évaluant en $X_{P_k} = \alpha_{P_k}$, on trouve alors $1 = 0$, une contradiction. Ainsi I est un idéal propre.

Par le théorème de Krull, il existe un idéal maximal I_m contenant I. On considère alors le corps $E_1 := A/I_m$. C'est une extension algébrique de K. Puisqu'on a quotienté par un idéal contenant I, dans E_1 tous les polynomes $P \in \mathrm{Pol}_K$ ont une racine dans E_1, et donc sont scindés dans E_1.

On peut alors itérer la construction: on construit pour tout $n \in \mathbb{N}^*$ une extension E_{n+1} de E_n comme on a construit E_1 à partir de K. On obtient une suite d'extensions algébriques de corps, telles que tout polynome non constant à coefficient dans E_n est scindé dans E_{n+1}.

On considère alors $E = \cup_{n\in\mathbb{N}^*} E_n$, donc on vérifie que c'est un corps, qui est aussi une extension algébrique de K. Enfin, E est algébriquement clos puisque si P est à coefficients dans E, il est à coefficients dans E_n pour un certain entier n, donc scindé dans E_{n+1}, et donc dans E.

L'unicité repose sur deux lemmes de puissances croissantes, mais l'idée est proche de celle qu'on a utilisé pour l'unicité des corps de rupture et de décomposition.

Définition 2.58. Soit L/K une extension et $\alpha \in L$ un élément algébrique. Les *conjugués*[13] de α dans L sont les éléments de L qui sont racines du polynome minimal $\mu_{K,\alpha}$.

Lemme 2.59. *Soit K un corps, L/K une extension, F un corps algébriquement clos, et $\sigma : K \to F$ un morphisme de corps, étendu en un morphisme d'anneaux $\hat{\sigma} : K[X] \to F[X]$. Soit $\alpha \in L$ un élément algébrique sur K, alors il y a bijection entre les prolongements $\tau : K(\alpha) \to F$ de σ et les conjugués de α dans L.*

[12] un "corps de décomposition" commun pour tous les polynomes de $K[X]$

[13] on précise parfois *conjugué algébrique*

Démonstration. L'argument est proche de celui utilisé pour l'unicité des corps de rupture et de décomposition (lemme 2.36). On rappelle que $\mu_{K,\alpha}(X) \in K[X]$ désigne le polynome minimal de α. Un prolongement $\tau : K(\alpha) \to F$ de σ est déterminé par l'élément $\tau(\alpha) \in L$ et celui-ci doit être une racine de $\hat{\sigma}(\mu_{K,\alpha})$.

Réciproquement, si $\beta \in L$ est une racine de $\hat{\sigma}(\mu_{K,\alpha})$, alors le morphisme $\hat{\tau} : K[X] \to L$ défini par $\hat{\tau}(Q(X)) = \hat{\sigma}(Q)(\beta)$ est bien défini (c'est l'évaluation en β du morphisme $\hat{\sigma}$), et s'annule sur l'idéal $(\mu_{K,\alpha})$. Par conséquent il passe au quotient en un morphisme $\tau : K[X]/(\mu_{K,\alpha}) \to L$. Or on a $K[X]/(\mu_{K,\alpha}) \simeq K(\alpha)$, d'où le résultat. □

Lemme 2.60 (Prolongement des morphismes)**.** *Soit K un corps, L/K une extension algébrique, F un corps algébriquement clos. Alors tout morphisme $\sigma : K \to F$ s'étend à L.*

Démonstration. On veut appliquer le lemme précédent à tous les éléments de L... mais ils sont (trop?) nombreux ! On fait donc une zornerie : Soit $S = \{(E, \tau) \,|\, K \subset E \subset L \text{ et } \tau : E \to F \text{ prolonge } \sigma\}$. On veut montrer qu'il existe un élément de la forme (L, τ_L) dans S. On ordonne S avec la relation $(E, \tau) \leqslant (E', \tau')$ si on a $E \subset E'$ et τ' prolonge τ. Si $P \subset S$ est une famille totalement ordonnée, alors $E_P := \cup_{E \in P} E$ est un majorant de P. Par conséquent l'ensemble S muni de la relation $\leqslant$ est ordonné inductif. Par le lemme de Zorn, il admet un élément maximal (E, τ). Si on avait $E \neq L$, alors on aurait un élément $\alpha \in L \setminus E$ algébrique sur K, donc par le lemme précédent on pourrait étendre τ à $E(\alpha)$, ce qui contredit la maximalité. D'où $E = L$. □

On peut maintenant prouver l'unicité de la clôture algébrique: Soit K un corps, L et F deux clôtures algébriques, et $\sigma : K \to F$ l'inclusion. Par le lemme précédent, on peut prolonger σ en $\tau : L \to F$. L'image $\tau(L) \subset F$ est un corps algébriquement clos. L'extension F/K étant algébrique, l'extension $F/\tau(L)$ l'est aussi. Par la remarque 2.52 on a $F = \tau(L)$, donc τ est donc un morphisme de corps surjectif. En particulier F et L sont isomorphes. □

Exemple 2.61. Par le théorème de Steinitz, pour tout premier p et tout entier $n \geqslant 1$, le corps $\mathbb{F}_{p^n}$ admet une clôture algébrique. Pour $n \geqslant 2$, le corps $\mathbb{F}_{p^n}$ est une extension algébrique de $\mathbb{F}_p$, par conséquent sa clôture est isomorphe à celle de $\mathbb{F}_p$.

Il se trouve qu'on peut construire une telle clôture algébrique : si en général $m \leqslant n$ n'implique pas $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$, on a néanmoins $\mathbb{F}_{p^{m!}} \subset \mathbb{F}_{p^{n!}}$. On considère alors $\cup_{n \in \mathbb{N}} F_{p^{n!}}$ qui est un corps bien défini. C'est une extension algébrique de $\mathbb{F}_p$ et tous les polynomes de $\mathbb{F}_p$ y sont scindés. Avec un peu de travail, on montre que $\cup_{n \in \mathbb{N}} F_{p^{n!}}$ est algébriquement clos, et donc c'est la clôture algébrique $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$, et de tous les $\mathbb{F}_{p^n}$ avec $n \geqslant 1$.

Notons la conséquence des lemmes 2.59 et 2.60 suivante.

Corollaire 2.62. *Si L/K est une extension algébrique et F une clôture algébrique de L (et donc de K). Soit $\alpha \in L$. Alors les conjugués de α dans F sont les éléments de la forme $f(\alpha)$, où f parcourt les morphismes K-linéaires de L dans F.*

Démonstration. En effet, si f est un morphisme K-linéaire de L dans F, nécessairement $f(\alpha)$ est un conjugué de α. Le lemme 2.59 assure qu'il existe bien un morphisme de $K(\alpha) \to F$ tel que $f(\alpha) = \alpha$ et le lemme 2.60 assure qu'on peut étendre ce morphisme à L. □

3. Théorie de Galois

Partant du polynome $X^2 + bX + c$, on dispose d'une formule pour les racines, à savoir $\frac{-b\pm\sqrt{b^2-4c}}{2}$). En particulier, si b et c vivent dans un corps K, les racines vivent dans l'extension quadratique $K(\sqrt{b^2-4c})$.

De la même façon, pour l'équation X^3+pX+q, les formules de Cardano-Tartaglia donnent les racines $\mathrm{j}^k\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}}+\mathrm{j}^{-k}\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}}$, avec $k=0,1,2$ et j racine troisième de l'unité. En particulier, si p et q vivent dans K, les racines vivent dans une extension de degré au plus 6.

On veut comprendre d'où viennent ces formules, et comprendre quand peut-on les généraliser (ou pas). L'énoncé suivant, que l'on démontrera, est une telle réponse. Il s'agit d'en comprendre les termes.

Théorème 3.1. *Soit K un corps de caractéristique nulle, et $P(X)\in K[X]$ non constant. Alors les assertions suivantes sont équivalents:*

(1) *le polynome P est résoluble par radicaux;*
(2) *le corps $\mathrm{Dec}_K(P)$ est contenu dans une extension résoluble de K;*
(3) *le groupe de Galois $\mathrm{Gal}_K(P)$ est résoluble.*

3.1. Groupe de Galois et extensions galoisiennes finies.

Rappelons que les automorphismes d'une structure algébrique forment toujours un groupe.

Définition 3.2. Étant donné une extension L/K, on appelle K-automorphisme de L un automorphisme de corps de L dont la restriction à K est l'identité. Le groupe des K-automorphismes de K est appelé *groupe de Galois* de L/K, noté $\mathrm{Gal}(L/K)$.

C'est un sous-groupe des automorphismes de L.

Exemple 3.3.
(1) $\mathrm{Gal}(\mathbb{C}/\mathbb{R})=\{\mathrm{id}_{\mathbb{C}}, z\mapsto\bar{z}\}\simeq\mathbb{Z}/2\mathbb{Z}$
(2) $\mathrm{Gal}(\mathbb{Q}[\sqrt{2}]/\mathbb{Q})=\{\mathrm{id}, a+b\sqrt{2}\mapsto a-b\sqrt{2}\}\simeq\mathbb{Z}/2\mathbb{Z}$
(3) $\mathrm{Gal}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q})=\{\mathrm{id}\}$
(4) $\mathrm{Gal}(\mathbb{Q}[\sqrt[3]{2},\mathrm{j}]/\mathbb{Q})=\langle(\sqrt[3]{2}\mapsto\sqrt[3]{2},\mathrm{j}\mapsto\bar{\mathrm{j}}),(\sqrt[3]{2}\mapsto\mathrm{j}\sqrt[3]{2},\mathrm{j}\mapsto\mathrm{j}),\rangle\simeq\mathcal{S}_3$
(5) $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)=\langle\mathrm{Fr}\rangle\simeq\mathbb{Z}/n\mathbb{Z}$
(6) $\mathrm{Gal}(\mathbb{R}/\mathbb{Q})=\{\mathrm{id}\}$ (exercice)

Théorème 3.4. *Soit L/K une extension finie. Alors on a $|\mathrm{Gal}(L/K)|\leqslant[L:K]$.*

Définition 3.5. On appelle *extension galoisienne* toute extension finie L/K telle que $|\mathrm{Gal}(L/K)|=[L:K]$.

Exemple 3.6.
(1) $\mathbb{C}/\mathbb{R},\mathbb{Q}[\sqrt{2}]/\mathbb{Q},\mathbb{Q}[\sqrt[3]{2},\mathrm{j}]/\mathbb{Q},\mathbb{F}_{p^n}/\mathbb{F}_p$ sont des extensions galoisiennes finies.
(2) $\mathbb{Q}[\sqrt[3]{2}/\mathbb{Q}]$ est finie mais pas galoisienne.

Démonstration. On raisonne par l'absurde. Si $n=[L:K]$ et $|\mathrm{Gal}(L/K)]>n$. Alors il existe des K-automorphismes de L distincts, disons $\sigma_1,\dots,\sigma_{n+1}$. Soit $x_1,\dots,x_n$ une base de L comme K-espace vectoriel. Pour des raisons de dimension, il existe alors une relation

linéaire non triviale, c'est-à-dire des éléments $\lambda_1, \dots, \lambda_{n+1}$ de K non tous nuls tels que pour tout i entre 1 et n on a $\sum_{j=1}^{n+1} \lambda_j \sigma_j(x_i) = 0$. Comme les σ_j sont des automorphismes, ils sont en particulier linéaires, donc pour tout $x \in L$ on a la relation $\sum_{j=1}^{n+1} \lambda_j \sigma_j(x) = 0$.

On voit donc que l'ensemble des relations linéaires satisfaites par tous les éléments de L est non vide, et on peut choisir une relation qui soit de taille r minimale; quitte à permuter les indices, on la note

$$\forall x \in L, \sum_{j=1}^{r} \mu_j \sigma_j(x) = 0,$$

avec $\mu_1, \dots, \mu_r \in K$ non nuls.

En écrivant la relation pour un élément xy, on a $\sum_{j=1}^{r} \mu_j \sigma_j(xy) = 0$, qui peut se réécrire

$$\forall x, y \in L, \sum_{j=1}^{r} \mu_j \sigma_j(x) \sigma_j(y) = 0.$$

En fixant y tel que $\sigma_r(y)$ n'est pas égal à $\sigma_j(y)$ pour un certain j, et en combinant cette dernière relation avec la précédente multipliée par $\sigma_r(y)$, on obtient

$$\forall x \in L, \sum_{j=1}^{r} \mu_j (\sigma_j(y) - \sigma_r(y)) \sigma_j(x) = 0.$$

Le coefficient $\mu_r(\sigma_r(y) - \sigma_r(y))$ étant nul, cette dernière relation est en fait de longueur strictement plus petite que r, une contradiction. □

3.2. **Énoncé de la correspondance de Galois finie.** Anticipons un peu: le but qu'on a en tête est le suivant.

Théorème 3.7 (Correspondance de Galois finie)**.** *Soit L/K une extension galoisienne finie et $G = \mathrm{Gal}(L/K)$ le groupe de Galois correspondant.*

1. *L'application qui à un sous-groupe H de G associe l'ensemble L^H est éléments de L fixés par H établit une bijection entre les sous-groupes de G et les sous-extensions de L/K.*
2. *L'application-réciproque associe à une sous-extension $L/L'/K$ l'ensemble des éléments de $\mathrm{Gal}(L/K)$ qui laissent les éléments de L' fixes.*
3. *Pour tout sous-groupe H de G, l'extension L/L^H est galoisienne de groupe de Galois H.*
4. *Pour tout sous-groupe H de G, l'extension L^H/K est galoisienne si et seulement si H est distingué*[14] *dans G. Dans ce cas, on a $\mathrm{Gal}(L^H/K) = G/H$.*

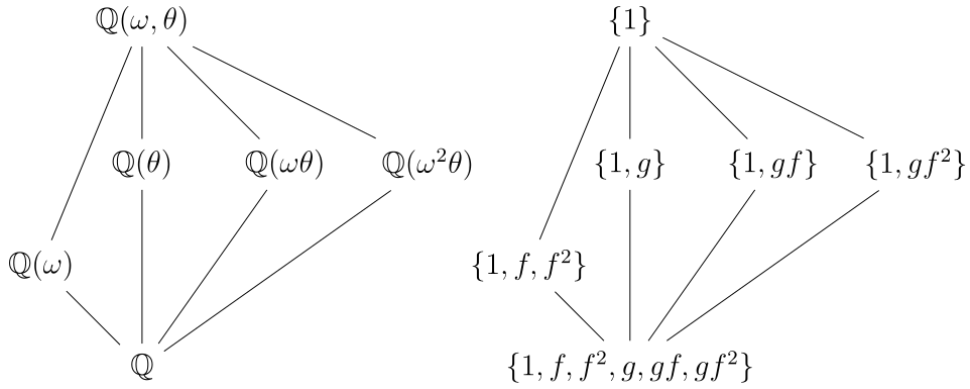
Exemple 3.8. Considérons l'extension $\mathbb{Q}(\mathrm{j}, \sqrt[3]{2})/\mathbb{Q}$, dont on a vu en 3.3 qu'elle est de degré 6, de groupe de Galois $\mathcal{S}_3$. Plus précisément, le groupe de Galois est engendré par la conjugaison complexe g (qui est d'ordre 2), et la "rotation" f (d'ordre 3) qui fixe j, mais permute les racines $X^3 - 2$ selon le cycle $\sqrt[3]{2} \mapsto \mathrm{j}\sqrt[3]{2} \mapsto \mathrm{j}^2\sqrt[3]{2} \mapsto \sqrt[3]{2}$.

[14] *normal* en anglais

Le groupe $\mathcal{S}_3$ a 4 sous-groupes non triviaux: les 3 sous-groupes à deux éléments contenant les transpositions g, gf et gf^2, et le sous-groupe $\mathcal{A}_3$ engendré par f qui est distingué dans $\mathcal{S}_3$.

Côté corps, l'extension $\mathbb{Q}(\mathrm{j}, \sqrt[3]{2})/\mathbb{Q}$ a 4 extensions intermédiaires: les 3 sous-extensions $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}, \mathbb{Q}(\mathrm{j}\sqrt[3]{2})/\mathbb{Q}, \mathbb{Q}(\mathrm{j}^2\sqrt[3]{2})/\mathbb{Q}$ de degré 3, et la sous-extension $\mathbb{Q}(\mathrm{j})/\mathbb{Q}$ de degré 2. On vérifie par exemple que $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ correspond bien aux éléments fixés par la conjugaison c, tandis que les deux autres aux éléments fixés par $c\sigma$ et $c\sigma^2$. De même $\mathbb{Q}(\mathrm{j})/\mathbb{Q}$ correspond aux éléments fixés par le 3-cycle σ (et ses puissances).

Voici[15] le treillis des sous-extensions (à gauche), où $\omega = \mathrm{j}$ et $\theta = \sqrt[3]{2}$, et celui des sous-groupes (à droite). Noter que la correspondance renverse les inclusions.



On vérifie que $\mathbb{Q}(\mathrm{j})/\mathbb{Q}$ est normale, puisque c'est le corps de décomposition de X^2+X+1. Cela correspond au fait que $\mathcal{A}_3$ est distingué dans $\mathcal{S}_3$.

En revanche, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n'est pas normale (tout comme $\mathbb{Q}(\mathrm{j}\sqrt[3]{2})/\mathbb{Q}$ et $\mathbb{Q}(\mathrm{j}^2\sqrt[3]{2})/\mathbb{Q}$), puisque X^3-2 y admet une racine mais n'est pas scindé; on peut aussi rappeler que son groupe d'automorphisme est trivial alors que c'est une extension de degré 3. Cela correspond au fait que les groupes engendrés par une transposition ne sont pas distingués dans $\mathcal{S}_3$ (il sont en fait conjugués les uns aux autres: ce sont les 2-Sylow de $\mathcal{S}_3$).

3.3. **Extensions normales.** Pour démontrer la correspondance de Galois finie, on a besoin de propriétés supplémentaires des extensions galoisiennes finies, c'est-à-dire des extensions qui ont le plus possible d'automorphismes.

Si L/K est une extension monogène de degré n, elle est de la forme $K(\alpha_1)$ avec α_1 algébrique sur K de degré n, et L est un corps de rupture du polynome μ_{K,α_1}. Selon les situations, L contient, ou pas, des conjugués de α_1, disons $\alpha_1,\dots,\alpha_k$, avec $k \leqslant n$. Alors, en vertu du corollaire 2.62, on a $|\mathrm{Gal}(L/K)| = k$. En effet un K-automorphisme $f : L \to L$ est défini par l'image $f(\alpha_1)$, qui est l'un des α_i. En particulier l'extension L/K est galoisienne si $k = n$, c'est-à-dire si μ_{K,α_1} est scindé à racines simples sur L.

Définition 3.9. On dit qu'une extension algébrique L/K est *normale* si pour tout $P(X) \in K[X]$ irréductible, si P a une racine dans L, alors P est scindé dans L.

Exemple 3.10.
- $\mathbb{Q}[\sqrt[3]{2}, \mathrm{j}]/\mathbb{Q}$ est normale.

[15] image tirée de wikipedia

- pour tout K, la clôture algébrique de K est une extension normale.
- $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ n'est pas normale.
- Toute extension quadratique est normale. En effet, si on a $[L : K] = 2$, si $P(X) \in K[X]$ est irréductible, et si P a une racine α dans L, alors on vérifie que $-b - \alpha$ est dans L est aussi racine : on a $P(X) = (X - \alpha)(X + b + \alpha)$, donc P est scindé dans L.

La définition suivante généralise 2.33 de façon directe.

Définition 3.11. Soit K un corps et $\{P_i\}_{i\in I} \subset K[X]$ une famille de polynomes. Un *corps de décomposition* de $\{P_i\}_{i\in I}$ est une extension E/K telle que

- pour tout $i \in I$, P_i est scindé dans E, de racines notées $\alpha_{i1}, \dots, \alpha_{in_i}$,
- $E = K(\alpha_{ij})_{i\in I, 1\leqslant j\leqslant n_i}$.

On le note $\mathrm{Dec}_K(\{P_i\}_{i\in I})$.

Théorème 3.12. *Soit K un corps, $\bar{K}/K$ une clôture algébrique, et L/K une sous-extension de $\bar{K}/K$. Alors les assertions suivantes sont équivalentes:*

(1) *l'extension L/K est normale (c'est-à-dire que tout polynome qui a une racine dans L a toutes ses racines dans L),*
(2) *pour tout plongement K-linéaire $\sigma : L \to \bar{K}$ on a $\sigma(L) = L$,*
(3) *il existe une famille $(P_i)_{i\in I} \subset K[X]$ telle que $L = \mathrm{Dec}_K(\{P_i\}_{i\in I})$.*

Le critère (2) est parfois pris comme définition de la normalité. Comme on le verra, il explique le terme *normal*, en vertu de son lien avec la théorie des groupes.

Démonstration. (2) $\Rightarrow$ (1): Soit $P \in K[X]$ irréductible et unitaire, et $\alpha \in L$ une racine de P. Alors on a $P = \mu_{K,\alpha}$. Soit β une racine de P dans $\bar{K}$; on veut montrer que β est dans L. Par le lemme 2.59 il existe un plongement K-linéaire $\sigma = K(\alpha) \to L$ qui envoie α sur β, et par le prolongement des morphismes 2.60 on peut étendre σ en $\bar{\sigma} : L \to \bar{K}$. Comme on a $\bar{\sigma}(L) = L$, on a $\beta \in \bar{\sigma}(L) = L$.

(1) $\Rightarrow$ (3): Soit $\alpha \in L$. Comme L/K est algébrique, que α est algébrique sur L, α est algébrique sur K. Soit $\mu_{K,\alpha} \in K[X]$ son polynome minimal. Alors les conjugués de α sont dans L. Donc $\mathrm{Dec}(\mu_{K,\alpha}) \subset L$, et donc $L = \mathrm{Dec}(\{\mu_{K,\alpha}\}_{\alpha\in L})$.

(3) $\Rightarrow$ (2): Pour tout $i \in I$, on note $\alpha_{i1}, \dots, \alpha_{in_i}$ les racines de P_i dans $\bar{K}$. On a $L = K(\alpha_{ij})_{i\in I, 1\leqslant j\leqslant n_i}$. Pour tout plongement K-linéaire $\sigma : L \to K$ et pour tous i, j, l'élément $\sigma(\alpha_{ij}) \in \bar{K}$ doit être une racine de P_i. Par conséquent pour tout $i \in I$, σ induit une permutation de la famille $(\alpha_{ij})_{1\leqslant j\leqslant n_i}$. Ainsi on a $\sigma(K(\alpha_{i1}, \dots, \alpha_{in_i})) = K(\alpha_{i1}, \dots, \alpha_{in_i})$, et donc $\sigma(L) = L$. □

Remarque 3.13. Si les extensions E/K et F/K sont normales, alors $(E \cap F)/K$ et EF/K sont normales, cela découle de la définition.

Si l'extension F/K est normales et que E/K est une sous-extension, alors F/E est normale, par le point (3). En revanche E/K ne l'est pas : penser au corps de rupture comme sous-extension d'un corps de décomposition.

Remarque 3.14. Si L/K est une extension algébrique, comme dans la preuve de l'implication (1) $\Rightarrow$ (3), on peut considérer la famille $\{\mu_{K,\alpha}\}_{\alpha\in L}$. Le corps de décomposition de cette famille sur K est alors une extension normale de K, et on peut vérifier que c'est la plus petite qui

contienne L. On l'appelle alors *clôture normale de L*. On peut montrer qu'elle est unique à isomorphisme près.

3.4. **Extensions séparables.** Pour démontrer la correspondance de Galois, on a besoin d'éléments supplémentaires, et en particulier d'autres caractérisations du caractère galoisien d'une extension.

Comme expliqué au début de la section sur la normalité, pour qu'une extension monogène $K(\alpha_1)/K$ soit galoisienne, le polynome minimal de α_1 doit être scindé à racines simples. Le caractère scindé correspond à la notion de normalité introduite précédemment. Quant à la simplicité des racines, elle correspond à la séparabilité. Il est désormais commode de supposer qu'un corps et les extensions algébriques qu'on considère sont plongées dans une clôture algébrique.

Définition 3.15. Soit K un corps et $\bar{K}$ une clôture algébrique. Soit L/K une extension finie, avec $L \subset \bar{K}$.

Un polynome $P(X) \in K[X]$ est dit *séparable* sur K si ses racines dans $\bar{K}$ sont simples.

Un élément $\alpha \in L$ est dit *séparable* sur K si son polynome minimal $\mu_{K,\alpha}(X) \in K[X]$ l'est.

L'extension L/K est dite *séparable* si tous les éléments de L sont séparables sur K.

Le critère suivant montre qu'il n'y a pas besoin d'aller dans la clôture algébrique pour tester la séparabilité:

Lemme 3.16. *Dans le contexte précédent, un polynome $P(X) \in K[X]$ est séparable si et seulement si les polynomes P et P' sont premiers entre eux.*

Un élément $\alpha \in L$ est séparable sur K si et seulement si la dérivée de son polynome minimal $\mu'_{K,\alpha}$ est non nulle.

Démonstration. Soit n le degré de $P(X) \in K[X]$. Factorisons $P(X)$ dans $\bar{K}[X]$ sous la forme $\prod_{i=1}^{n}(X-\alpha_i)$. Alors on a $P'(X) = \sum_{i=1}^{n}\prod_{j\neq i}(X-\alpha_j)$.

Si P est séparable, alors les α_i sont tous distincts. En particulier, pour i_0 fixé, $X-\alpha_{i_0}$ divise tous les termes de la somme $\sum_{i=1}^{n}\prod_{j\neq i}(X-\alpha_j)$ sauf 1, et donc $X-\alpha_{i_0}$ ne divise pas $P'(X)$. Par conséquent $PX)$ et $P'(X)$ sont premiers entre eux.

Inversement, si $P(X)$ et $P'(X)$ ne sont pas premiers entre eux, ils ont un diviseur commun dans $\bar{K}[X]$ de la forme $X-\beta$. Nécessairement β est une racine de $P(X)$, donc de la forme α_{i_0}, et de $P'(X)$. De l'expression $P'(X) = \sum_{i=1}^{n}\prod_{j\neq i}(X-\alpha_j)$ on déduit qu'il existe $i_1 \neq i_0$ tel que $\alpha_{i_0} = \alpha_{i_1}$, et donc $P(X)$ n'est pas à racines simples dans $\bar{K}[X]$.

Enfin pour $\alpha \in L$, le polynome minimal $\mu_{K,\alpha}$ est irréductible. Sa dérivée est un polynome $\mu'_{K,\alpha}$ de degré strictement plus petit que $\deg(\alpha)$. Le seul polynome premier avec $\mu_{K,\alpha}$ et de degré strictement plus petit est le polynome nul. Ainsi α est séparable si et seulement si $\mu_{K,\alpha}$ et $\mu'_{K,\alpha}$ sont premiers entre eux, et donc si et seulement $\mu'_{K,\alpha}$ est non nul. □

Exemple 3.17. Si K est de caractéristique nulle et L une extension finie, tous les éléments de L sont séparables sur K. En effet, soit $\alpha \in L^*$ de degré $n \geqslant 1$. Alors $\mu_{K,\alpha}$ est irréductible de degré n, donc $\mu'_{K,\alpha}$ est de degré $n-1$ (c'est ici qu'on utilise la nullité de la caractéristique) et non nul. Comme $\mu_{K,\alpha}$ n'a aucun diviseur de degré $< n$, il est premier avec $\mu'_{K,\alpha}$.

Exemple 3.18. Considérons $K = \mathbb{F}_p(x^p)$ le corps des fractions rationnelles en une indéterminée x^p, et l'extension $L = \mathbb{F}_p(x)$ corps des fractions rationnelles en l'indéterminée x. En

particulier on a $L = F[x]$, et L/K est une extension de degré p. Le polynome minimal de x est $\mu_{K,x}(X) = X^p - x^p \in \mathbb{F}_p(x^p)[X]$. On a $\mu'_{K,x}(X) = 0$, donc $\mu_{K,x}$ et $\mu'_{K,x}$ ne sont pas premiers entre eux, et donc x n'est pas séparable sur $\mathbb{F}_p[x^p]$. On peut le voir aussi en remarquant qu'on a $\mu_{K,x}(X) = X^p - x^p = (X-x)^p$, et donc que $\mu_{K,x}$ n'est pas à racines simples. L'extension $\mathbb{F}_p(x^p)/\mathbb{F}_p(x)$ n'est par conséquent pas séparable.

Remarque 3.19. Soit $L/K/F$ une tour d'extension. Si L/F est séparable, alors K/F et L/K le sont aussi.

Définition 3.20. Un corps K est dit *parfait* si toute extension finie de K est séparable.

Théorème 3.21. *Soit K un corps.*

- *Si K est de caractéristique nulle, alors K est parfait.*
- *Si K est de caractéristique p finie, alors K est parfait si et seulement si l'autormorphisme $\mathrm{Fr} : x \mapsto x^p$ est surjectif.*

Démonstration. Le cas $\mathrm{car}(K) = 0$ est l'exemple 3.17.

Supposons $\mathrm{car}(K) = p > 0$ et K parfait. Soit $\alpha \in K$. On veut montrer que α a une racine p-ième. Soit L une extension de K dans laquelle $X^p - \alpha$ a une racine y. Alors $\mu_{K,y}(X)$ divise $X^p - \alpha = X^p - y^p = (X-y)^p$. Par perfection, $\mu_{K,y}$ est à racines simples, donc $\mu_{K,y}(X) = X - y$, donc y est dans K. Ainsi α a une racine p-ième, et donc l'automorphisme de Frobenius est surjectif dans K.

Réciproquement, supposons $\mathrm{car}(K) = p > 0$ et $\mathrm{Fr} : x \mapsto x^p$ surjectif. Soit L/K une extension finie et $\alpha \in L$. On veut montrer que α est séparable. Si on a $\mu_{K,\alpha}(X) \neq 0$, alors $\mu_{K,\alpha}$ et $\mu'_{K,\alpha}$ sont premiers entre eux (par le même argument que dans l'exemple 3.17), donc les racines de $\mu_{K,\alpha}$ sont simples.

Reste le cas $\mu'_{K,\alpha}(X) = 0$. Montrons qu'il ne peut se produire sous nos hypothèses. On affirme que dans ce cas il existe $Q(X) \in K[X]$ tel que $\mu_{K,\alpha}(X) = Q(X^p)$. En effet, si on a note $\mu_{K,\alpha}(X) = \sum_i a_i X^i$, alors on a $\mu'_{K,\alpha}(X) = \sum_i i a_i X^{i-1}$. Donc pour tout i on a $i a_i = 0$. Ainsi les seuls a_i qui peuvent ne pas être nuls sont ceux pour lesquels i est nul (dans K), c'est-à-dire i multiple de p. Ainsi on a $\mu_{K,\alpha}(X) = \sum_{p|i} a_i X^i = \sum_i a_{i/p} (X^p)^i$. Donc $Q(X) = \sum_i a_{i/p} X^i$ marche. Maintenant, comme Fr est supposé surjectif, pour tout i il existe r_i tel que $r_i^p = a_{i/p}$. On a alors $Q(X^p) = \sum_i a_{i/p} (X^p)^i = \sum_i (r_i X^i)^p = (\sum_i r_i X^i)^p = R(X)^p$. Ainsi on a $\mu_{K,\alpha}(X) = R(X)^p$ qui n'est pas irréductible, une contradiction. □

Voici une propriété remarquable des extensions séparables:

Théorème 3.22 (de l'élément primitif)**.** *Soit L/K une extension finie séparable. Alors il existe $\alpha \in L$ tel que $L = K(\alpha)$.*

Exemple 3.23.

- Pour $K = \mathbb{F}_p$ et $L = \mathbb{F}_{p^n}$, on sait par exemple que L^* est cyclique, donc tout générateur de L^* est un générateur de l'extension L/K. Un autre argument est que L est corps de décomposition des polynomes irréductibles de $\mathbb{F}_p$ de degré n, et l'extension L/K est engendré par une racine quelconque d'un tel polynome.
- On vérifie que l'extension $\mathbb{Q}[\mathrm{i}, \sqrt{2}]/\mathbb{Q}$ est engendré par $\mathrm{i} + \sqrt{2}$.

Démonstration. Si K est fini, L aussi, donc L^* est cyclique, donc le théorème est vrai.

Si K est infini et L/K finie, alors L/K est de type fini, c'est-à-dire qu'il existe $\alpha_1, \dots, \alpha_k \in L$ tels que $L = K(\alpha_1, \dots, \alpha_k)$. Si $k = 1$ il n'y a rien à dire. Traitons le cas $k = 2$, par une récurrence directe, les autres cas s'en déduisent.

On considère donc une extension bigène $K(x, y)/K$ et les polynomes minimaux $\mu_{K,x}$ et $\mu_{K,y}$. Soit F une extension telle $\mu_{K,x}$ et $\mu_{K,y}$ sont scindés sur F. On note $x = x_1, \dots, x_r$ et $y = y_1, \dots, y_s$ leurs racines dans F qui, par séparabilité, sont distinctes. On affirme qu'il existe $t \in K^*$ tel que pour tous i, j satisfaisant $1 \leqslant i \leqslant r$ et $1 \leqslant j \leqslant s$ on a $x + ty = x_i + ty_i$ si et seulement $i = j = 1$. En effet, l'équation $x + ty = x_i + ty_j$ est équivalente à $t = \frac{x - x_i}{y - y_j}$. Comme K est infini, il suffit de prendre t différent de tous ces quotients. On pose alors $z = x + ty$.

On va montrer l'égalité $K(x, y) = K(z)$. Comme on a évidemment $K(z) \subset K(x, y)$, il suffit de vérifier $x, y \in K(z)$. Maintenant y est racine de son polynome minimal $\mu_{K,y}(X) \in K[X] \subset K(z)[X]$ et on vérifie qu'il est aussi racine de $\mu_{K,x}(z - tX) \in K(z)[X]$. En posant $Q(X) = \operatorname{pgcd}(\mu_{K,y}(X), \mu_{K,x}(z - tX)) \in K(z)[X]$, on en déduit que y en est racine. Comme Q divise $\mu_{K,y}(X)$, il est scindé à racines simples sur F et ses racines sont inclues dans $y_1, \dots, y_s$. Supposons qu'il a une racine y_j avec $j \neq 1$, alors on a $\mu_{K,z}(z - ty_j) = 0$, donc il existe i tel que $z - ty_j = x_i$, ce qui contredit l'inégalité $z \neq x_i + ty_j$. Par conséquent Q est de degré 1, c'est le monome $X - y$. On a donc $X - y \in K(z)[X]$, et donc $y \in K(z)$. Comme on a $x = z - ty$, on a également $x \in K(z)$. □

Rappelons qu'étant donné une extension finie L/K, on s'intéresse au groupe $\operatorname{Gal}(L/K)$ des automorphismes de L fixant K. D'après le théorème 3.4, ce groupe est de cardinal au plus $[L : K]$, et les extensions galoisiennes correspondent au cas d'égalité.

En plongeant K et L dans une clôture algébrique commune, notée $\bar{K}$, et par le lemme de prolongement des morphismes 2.60, tout K-automorphisme de L se prolonge en un K-automorphisme de $\bar{K}$. Autrement dit, un K-automorphisme de L est la restriction à L d'un K-automorphisme de $\bar{K}$ fixant L.

Proposition 3.24. *Soit K un corps de clôture algébrique $\bar{K}$ et soit L/K une sous-extension finie. Alors il y a au plus $[L : K]$ plongements K-linéaires de L dans $\bar{K}$, avec égalité si et seulement L/K est séparable.*

Démonstration. Si L est de la forme $K(\alpha)$, alors comme on a $[K(\alpha) : K] = \deg(\mu_{K,\alpha})$, le lemme 2.59 affirme que le nombre de prlongements K-linéaires de L dans $\bar{K}$ est le nombre de racines de $\mu_{K,\alpha}$. Ce nombre est inférieur ou égal au degré de α, avec égalité si $\mu_{K,\alpha}$ est scindé sur L, ce qui correspond à la séparabilité de α.

Si $L = K(\alpha_1, \dots, \alpha_n)$, alors un plongement $\sigma_i = K(\alpha_1, \dots, \alpha_i) \to \bar{K}$ s'étend en au plus $[K(\alpha_1, \dots, \alpha_{i+1}) : K(\alpha_1, \dots, \alpha_i)]$ plongements $\sigma_{i+1} : K(\alpha_1, \dots, \alpha_{i+1}) \to \bar{K}$, avec égalité si et seulement si α_{i+1} est séparable. Par une récurrence immédiate, on a l'inégalité, et l'égalité si l'extension est séparable.

Maintenant si L/K n'est pas séparable, il existe un élément $\alpha \in L$ non séparable sur K. Dans ce cas, $\sigma : K \to \bar{K}$ se prolonge en strictement moins que $[K(\alpha) : K]$ plongements $\bar{\sigma} : K(\alpha) \to \bar{K}$. Cela donne une inégalité stricte dans la récurrence. □

Corollaire 3.25 (transitivité de la séparabilité)**.** *Si $M/L/K$ sont des extensions finies, alors M/L et L/K sont séparables si et seulement si M/L est séparable.*

Démonstration. Le nombre de plongements K-linéaires de M dans $\bar{K}$ est majoré par $[M : L][L : K] = [M : K]$, avec égalité si et seulement si chacune des deux extensions est séparable. □

Corollaire 3.26. *Soit L/K finie et $x \in L$. Alors x est séparable sur K si et seulement si $K(x)/K$ est séparable.*

Démonstration. Supposons x séparable sur K. Soit $\bar{K}$ une clôture algébrique de L (et donc de K). Alors $\mu_{K,x}$ a $\deg(x)$ racines dans $\bar{K}$, et donc le plongement de K dans $\bar{K}$ s'étend en exactement $\deg(x)$ plongements de $K(x)$ dans $\bar{K}$. Par la proposition, $K(x)/K$ est séparable.

L'implication-réciproque est évidente. □

Corollaire 3.27. *Soit L/K une extension séparable et $\bar{K}$ une clôture algébrique. Alors on a $K = \{x \in L \,|\, \forall \sigma \in \mathrm{Hom}_K(L, \bar{K}), \sigma(x) = x\}$.*

Démonstration. Par définition des morphismes K-linéaires de L dans $\bar{K}$, on a $K \subset \{x \in L \,|\, \forall \sigma \in \mathrm{Hom}_K(L, \bar{K}), \sigma(x) = x\}$.

Maintenant, si y est un élément de $L \setminus K$, le polynome minimal $\mu_{K,y}$ est de degré > 1. Par séparabilité, il contient donc des racines dans $\bar{K}$ différentes de y. Par la proposition, il existe alors un morphisme K-linéaire σ tel que $\sigma(y) = z$, et donc $y \notin \{x \in L \,|\, \forall \sigma \in \mathrm{Hom}_K(L, \bar{K}), \sigma(x) = x\}$. □

3.5. **Extensions galoisiennes finies : différentes caractérisations.** On rappelle qu'étant donné une extension L/K, le groupe de Galois $\mathrm{Gal}(L/K)$ est le groupe des automorphismes K-linéaires de L. On a $|\mathrm{Gal}(L/K)| \leqslant [L : K]$. Aussi, si l'extension L/K est finie, elle est dite galoisienne finie si on a l'égalité $|\mathrm{Gal}(L/K)| = [L : K]$.

Rappelons aussi si $\bar{K}$ est une clôture algébrique de L et de K, un plongement de L/K est un morphisme K-linéaire $\sigma : L \to \bar{K}$. On note $\mathrm{Hom}_K(L, \bar{K})$ l'ensemble des plongements de L dans $\bar{K}$. Alors par le prolongement des morphismes, tout élément du groupe de Galois $\mathrm{Gal}(L/K)$ se prolonge en un plongement, donc on a $\mathrm{Gal}(L/K) \subset \mathrm{Hom}_K(L, \bar{K})$.

Voici une autre caractérisation des extensions galoisiennes (qui est prise comme définition quand on sort du cas fini):

Proposition 3.28. *Soit L/K une extension finie. Alors L/K est galoisienne finie si et seulement si elle est normale et séparable.*

Démonstration. Notons $\bar{K}$ une cloture algébrique de L (et de K).

On a l'inclusion $\mathrm{Gal}(L/K) \subset \mathrm{Hom}_K(L, \bar{K})$, d'où $|\mathrm{Gal}(L/K)| \leqslant |\mathrm{Hom}_K(L, \bar{K})|$. De plus, par la caractérisation des extensions normales (théorème 3.12), on a égalité si et seulement si L/K est normale.

D'autre part, par la proposition 3.24, on a $|\mathrm{Hom}_K(L, \bar{K})| \leqslant [L : K]$, avec égalité si et seulement si L/K est séparable.

On obtient la conclusion en combinant les deux inégalités et leurs cas d'égalité. □

Proposition 3.29. *Soit L/K une extension finie. Alors L/K est galoisienne et seulement si L est le corps de décomposision d'un polynome séparable $P(X) \in K[X]$.*

Démonstration. $\Rightarrow$ Comme L/K est séparable, par le théorème de l'élément primitif 3.22, il existe $\alpha \in L$ tel que $L = K(\alpha)$. Par séparabilité encore, le polynome minimal $\mu_{K,\alpha}$ est

séparable sur K. Comme L/K est normale, toutes les racines de $\mu_{K,\alpha}$ sont dans L, donc $L = \mathrm{Dec}_K(\mu_{K,\alpha})$.

$\Leftarrow$ Si $L = \mathrm{Dec}_K(P)$ avec $P(X) \in K[X]$ séparable, par la caractérisation des extensions normales (théorème 3.12), l'extension L/K est normale. Notons $\alpha_1, \ldots, \alpha_n$ les racines (distinctes par séparabilité) de P dans L, on a alors $L = K(\alpha_1, \ldots, \alpha_n)$. Les α_i sont donc séparables, donc chacune des extensions $K(\alpha, \ldots, \alpha_{k+1})/K(\alpha, \ldots, \alpha_k)$ est séparable. Par la transitivité de la séparabilité (corollaire 3.25) l'extension L/K est séparable. □

Pour H un sous-groupe du groupe d'automorphisme d'un corps L, on note L^H le sous-groupe constitué des points fixes de L sous l'action de H, c'est-à-dire

$$L^H := \{x \in L \,|\, \forall h \in H, h.x = x\}.$$

Le corollaire 3.27 implique alors

Lemme 3.30. *Si L/K est galoisienne finie, alors on a $K = L^{\mathrm{Gal}(L/K)}$.*

L'implication-réciproque est aussi vraie, elle découle de l'énoncé plus général suivant:

Lemme 3.31 (d'Artin)**.** *Soit L est corps quelconque et H un sous-groupe fini des automorphismes de L. Alors l'extension L/L^H est galoisienne et on a $\mathrm{Gal}(L/L^H) = H$.*

Notons d'abord le résultat technique suivant

Lemme 3.32. *Soit L/K séparable. S'il existe un entier d tel que tout élément $x \in L$ est de degré au plus d sur K, alors L/K est finie, et de degré au plus d.*

Démonstration. Soit $x \in L$ de degré maximal (disons d, quitte à changer le choix de d). Alors, par le théorème de l'élément primitif, pour tout élément $y \in L$, l'extension $K(x, y)/K$ est de la forme $K(z)$, donc de degré au plus d, et donc on a $K(x, y) = K(x)$, d'où $L = K(x)$. □

Démonstration du lemme d'Artin. Notons $d = |H|$. Soit $\alpha \in L$ et $O_\alpha = H.\alpha$ son orbite sous l'action de H. Posons $Q_\alpha(X) = \prod_{y \in O_\alpha}(X - y)$. Alors bien sûr Q_α annule α. D'autre part, pour h un élément de H quelconque, h permute les éléments de O_α, donc h laisse Q_α invariant. Par conséquent les coefficients de Q_α sont invariants sous l'action de H, donc $Q_\alpha(X)$ est dans $L^H[X]$. Par conséquent α est séparable sur L^H, et on a $[L^H(\alpha) : L^H] \leqslant d$. Par le lemme précédent on a alors $[L/L^H] \leqslant d$. Comme H agit par automorphismes sur L/L^H, cette extension a au moins d automorphismes, d'où finalement exactement d automorphismes. On a alors $[L : L^H] = d$, et l'extension est galoisienne. □

En combinant tous les résultats de cette section, on a alors:

Théorème 3.33. *Soit L/K une extension finie. Les assertions suivantes sont équivalentes:*

(1) *L/K est galoisienne;*
(2) *L/K est normale et séparable;*
(3) *L est le corps de décomposision d'un polynome de $K[X]$ séparable;*
(4) *$K = L^{\mathrm{Gal}(L/K)}$.*

Démonstration. (1)⇔(2) est la proposition 3.28.

(2)⇔(3) est la proposition 3.29.

(1)⇒(4) est le lemme 3.30.

(4)⇒(1) : si on a $L^{\mathrm{Gal}(L/K)} = K$, alors on a $L/K = L/L^{\mathrm{Gal}(L/K)}$. Par le lemme d'Artin 3.31 cettte dernière extension est galoisienne de groupe de Galois $\mathrm{Gal}(L/K)$. □

3.6. **Preuve de la correspondance de Galois.** On peut maintenant combiner tous les éléments rassemblés pour démontrer la correspondance de Galois. Introduisons (ou rappelons) quelques notations: soit L/K une extension finie, de groupe de Galois $\mathrm{Gal}(L/K)$; on note $\mathcal{G}_{L/K}$ l'ensemble des sous-groupes de $\mathrm{Gal}(L/K)$, ordonné par inclusion; on note $\mathcal{E}_{L/K}$ l'ensemble des sous-extensions de L/K, ordonné par inclusion. On note $\Phi_{L/K} : \mathcal{G}_{L/K} \to \mathcal{E}_{L/K}$ l'application qui à un sous-groupe H de $\mathrm{Gal}(L/K)$ associe la sous-extension L^H/K. Enfin, on note $\Psi_{L/K} : \mathcal{E}_{L/K} \to \mathcal{G}_{L/K}$ l'application qui à une sous-extension L'/K de L/K associe le sous-groupe des éléments de $\mathrm{Gal}(L/K)$ qui fixent L' point par point; ce dernier s'identifie naturellement à $\mathrm{Gal}(L/L')$.

Des définitions découle directement (et sans utiliser aucune propriété telle que normalité ou séparabilité):

Lemme 3.34. *Soit L/K une extension finie. Les deux applications $\Phi_{L/K}$ et $\Psi_{L/K}$ sont décroissantes pour l'inclusion : si on a $H_1 \subset H_2$, alors on a $\Phi_{L/K}(H_1) \supset \Phi_{L/K}(H_2)$, et si on a $L_1 \subset L_2$, alors on a $\Psi_{L/K}(L_1) \supset \Psi_{L/K}(L_2)$.*

D'autre part on a $H \subset (\Psi_{L/K} \circ \Phi_{L/K})(H)$ et $L' \subset (\Phi_{L/K} \circ \Psi_{L/K})(L')$.

Démonstration. La décroissante est claire.

Pour $H < G$ quelconque, on a $(\Psi_{L/K} \circ \Phi_{L/K})(H) = \{g \in \mathrm{Gal}(L/K) \,|\, \forall x \in L^H, g.x = x\}$. Par construction de L^H, si h est dans H, alors il fixe tous les éléments de L^H, donc on a $H \subset (\Psi_{L/K} \circ \Phi_{L/K})(H)$.

Pour L'/K une sous-extension de L/K quelconque, on a $(\Phi_{L/K} \circ \Psi_{L/K})(L') = \{x \in L \,|\, \forall g \in \mathrm{Gal}(L/L'), g.x = x\}$. Comme les éléments de $\mathrm{Gal}(L/L')$ fixent L' point par point, on a bien $L' \subset (\Phi_{L/K} \circ \Psi_{L/K})(L')$. □

La correspondance de Galois 3.7 peut alors se réécrire sous la forme suivante (en réunissant les deux premiers items).

Proposition 3.35 (Réécriture de la correspondance de Galois finie)**.** *Soit L/K une extension galoisienne finie et $G = \mathrm{Gal}(L/K)$ le groupe de Galois correspondant.*

1. *Les applications $\Phi_{L/K} : \mathcal{G}_{L/K} \to \mathcal{E}_{L/K}$ et $\Psi_{L/K} : \mathcal{E}_{L/K} \to \mathcal{G}_{L/K}$ sont bijectives et réciproques l'une de d'autre.*
2. *Pour tout sous-groupe H de G, l'extension L/L^H est galoisienne de groupe de Galois H.*
3. *Pour tout sous-groupe H de G, l'extension L^H/K est galoisienne si et seulement si H est distingué dans G. Dans ce cas, on a $\mathrm{Gal}(L^H/K) = G/H$.*

Démonstration. (1) Soit $L'/K \in \mathcal{E}_{L/K}$. Comme L/K est galoisienne finie, c'est le corps de décomposition d'un polynome de $K[X]$ séparable, et comme un tel polynome est dans $L'[X]$, l'extension L/L' est aussi galoisienne finie. Par le point (4) de la caractérisation des extensions galoisiennes, on a $L' = L^{\mathrm{Gal}(L/L')}$, c'est-à-dire $L' = (\Phi_{L/K} \circ \Psi_{L/K})(L')$.

Soit $H \in \mathcal{G}_{L/K}$ un sous-groupe de $\mathrm{Gal}(L/K)$. Par le lemme d'Artin 3.31, on a $\mathrm{Gal}(L/L^H) = H$, c'est-à-dire $(\Psi_{L/K} \circ \Phi_{L/K})(H) = H$.

(2) est (encore!) le lemme d'Artin 3.31.

(3) Comme sous-extension d'une extension séparable, l'extension L^H/K est séparable. Elle est donc galoisienne si et seulement si elle est normale, c'est-à-dire si $g(L^H) = L^H$ pour tout $g \in \mathrm{Gal}(L/K)$. Or $g(L^H) = L^{gHg^{-1}}$, donc L^H/K est normale si et seulement H est distingué dans $\mathrm{Gal}(L/K)$.

Dans ce cas, tout élément $g \in \mathrm{Gal}(L/K)$ se restreint à L^H, et on a une application bien définie $\pi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(L^H/K)$. Son noyau $\ker(\pi)$ est constitué des éléments de $\mathrm{Gal}(L/K)$ qui agissent trivialement sur L^H, c'est-à-dire le gorupe $\mathrm{Gal}(L/L^H) = H$. On a donc bien $\mathrm{Gal}(L^H/K) = H$. □

3.7. **Extensions cycliques et de Kummer.** Allons vers les questions de résolubilité, en étudiant d'abord les extensions dont le groupe de Galois est cyclique. On rappelle qu'une racine primitive n-ième de l'unité est un élément ξ satisfaisant $\xi^n = 1$ et $\xi^k \neq 1$ pour tout $k < n$.

Proposition 3.36. *Soit K un corps et n un entier non multiple de $\mathrm{car}(K)$. Soit L/K une extension et $\xi \in L$ une racine primitive n-ième de l'unité. Alors $K(\xi)/K$ est galoisienne finie et $\mathrm{Gal}(K(\xi)/K)$ est abélien. Si $\xi \notin K$, alors $\mathrm{Gal}(K(\xi)/K)$ est isomorphe à un sous-groupe du groupe mutliplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Démonstration. Si $\xi \in K$, il n'y a rien à montrer. Sinon $K(\xi)/K$ est corps de décomposition de $X^n - 1$. Comme $\mathrm{car}(K)$ ne divise pas n, ce polynome est séparable. Donc l'extension $K(\xi)/K$ est galoisienne finie. Un élément $g \in \mathrm{Gal}(K(\xi)/K)$ est déterminé par l'image $g(\xi)$ qui est une racine primitive n-ième de l'unité, d'où l'existence d'un élément $i(g) \in \{1, \dots, n\}$ premier avec n tel que $g(\xi) = \xi^{i(g)}$. En considérant la classe $\overline{i(g)} \in \mathbb{Z}/n\mathbb{Z}$, on obtient un morphisme $\bar{i} : \mathrm{Gal}(K(\xi)/K) \to (\mathbb{Z}/n\mathbb{Z})^\times, g \mapsto \overline{i(g)}$. (En effet, on a $gg'(\xi) = g(\xi^{i(g')}) = (\xi^{i(g')})^{i(g)} = \xi^{i(g)i(g')}$.) Ce morphisme $\bar{i}$ est clairement injectif. □

Exemple 3.37.

- L'extension $\mathbb{Q}(e^{i2\pi/n})/\mathbb{Q}$ est galoisienne. Lorsque n est premier, son groupe de Galois est alors $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathbb{Z}/(n-1)\mathbb{Z}$. Les éléments de $\mathrm{Gal}(\mathbb{Q}(e^{i2\pi/n})/\mathbb{Q})$ sont de la forme $e^{i2\pi/n} \mapsto (e^{i2\pi/n})^k = e^{i2k\pi/n}$, pour $k \in \{1, \dots, n-1\}$.
- Soit p premier et $n \geqslant 2$. Alors $p^n - 1$ est premier avec p. Soit $\alpha \in \bar{\mathbb{F}}_p$ une racine primitive de $X^{p^n-1} - 1$. Alors $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ est galoisienne de groupe de Galois $\mathbb{Z}/n\mathbb{Z}$. Ce dernier est bien un sous-groupe de $(\mathbb{Z}/(p^n-1)\mathbb{Z})^\times$ (c'est le sous-groupe engendré par $\bar{p}$), mais un sous-groupe strict.

Proposition 3.38. *On suppose que K contient une racine primitive n-ième de l'unité ξ. Soit $a \in K^*$ et $\alpha \in \bar{K}$ une racine du polynome $X^n - a$. Alors $K(\alpha)/K$ est galoisienne finie, et $\mathrm{Gal}(K(\alpha)/K)$ est cyclique d'ordre d, avec $d|n$ et $\alpha^d \in K$.*

Démonstration. Si $\alpha \in K$ il n'y a rien à dire. Sinon puisque ξ est dans K, toutes ses puissances aussi, donc toutes les racines n-ièmes de l'unité sont dans K. Comme α est racine de $X^n - a$, les autres racines sont alors les $\xi^k\alpha$, avec $k = 0, \dots, n-1$. Ainsi $K(\alpha)$ est corps de décomposition de $X^n - a$. Comme $X^n - a$ est séparable, l'extension $K(\alpha)/K$ est galoisienne finie. Soit $g \in \mathrm{Gal}(K(\alpha)/K)$. Alors g est caractérisé par $g(\alpha)$ qui est une racine

de $X^n - a$, donc de la forme $\xi^{i(g)}\alpha$, pour un certain entier $i(g) \in \{0, \dots, n-1\}$. L'application $\overline{i} : \mathrm{Gal}(K(\alpha)/K) \to \mathbb{Z}/n\mathbb{Z}, g \mapsto \overline{i(g)}$ est alors un morphisme de groupe. En effet, on a $gg'(\alpha) = g(\xi^{i(g')}\alpha) = \xi^{i(g')}g(\alpha) = \xi^{i(g)+i(g')}\alpha$. De plus $\overline{i}$ est clairement injectif. Ainsi $\mathrm{Gal}(K(\alpha)/K)$ s'identifie à un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$, donc de la forme $\mathbb{Z}/d\mathbb{Z}$ avec $d|n$.

Soit g_1 un générateur de ce groupe, et i_1 tel que $g_1(\alpha) = \alpha\xi^{i_1}$, alors on a $\alpha = g_1^{(d)}(\alpha) = g_1^{(d-1)}(\alpha\xi^{i_1}) = \cdots = \alpha\xi^{di_1}$, d'où $\xi^{di_1} = 1$. D'autre part on a $g_1(\alpha^d) = (g_1(\alpha))^d = (\alpha\xi^{i_1})^d = \alpha^d\xi^{di_1} = \alpha^d$. Donc α^d est invariant par l'action du groupe de Galois, d'où $\alpha^d \in K$. □

Ce qui est remarquable, c'est que la réciproque est vraie:

Proposition 3.39. *Soit K un corps contenant une racine primitive n-ième de l'unité ξ. Si L/K est une extension galoisienne finie de groupe de Galois $\mathbb{Z}/n\mathbb{Z}$, alors il existe $\alpha \in L$ satisfaisant $L = K(\alpha)$ et $\alpha^n \in K$ (ce qu'on peut abréger en écrivant $L = K(\sqrt[n]{a})$, où $a = \alpha^n$).*

Démonstration. Soit g un générateur de $\mathrm{Gal}(L/K)$. Pour $t \in L$, on pose $\alpha(t) = t + \xi g(t) + \cdots + \xi^{n-1}g^{(n-1)}(t)$. Si pour tout t, $\alpha(t)$ était nul, on aurait une relation linéaire non triviale entre les éléments $\mathrm{id}, g, \dots, g^{(n-1)}$ du groupe de Galois $\mathrm{Gal}(L/K)$, ce qui est contredit par la preuve du théorème 3.4. Ainsi on peut trouver $t \in L$ tel que $\alpha(t) \neq 0$. Alors on a $g(\alpha(t)) = \xi^{-1}\alpha(t)$, et donc $g(\alpha(t)^n) = \xi^{-n}\alpha(t)^n = \alpha(t)^n$, de sorte que $\alpha(t)^n$ est invariant par le groupe de Galois, et donc dans K. Enfin, $\mathrm{Gal}(L/K)$ agit librement sur $K(\alpha(t))/K$, donc on a $[K(\alpha(t)) : K] \geqslant n$, de sorte que finalement $L = K(\alpha(t))$. □

Définition 3.40. Soit K un corps, n un entier tel que K contienne une racine n-ième de l'unité. Une extension galoisienne finie L/K de groupe de Galois $\mathbb{Z}/n\mathbb{Z}$ est appelée *extension de Kummer*.

Par la proposition précédente, une extension de Kummer est de la forme $K(\alpha)$, pour un élément $\alpha \in L$ satisfaisant $\alpha^n \in K$.

3.8. **Résolubilité.** Il s'agit de relier la notion "intuitive" d'expression des racines d'un polynome en termes d'extraction de racine (d'où le nom d'extension radicale) à la notion découverte par Galois de résolubilité d'un groupe.

Définition 3.41. Une extension L/K est dite *radicale élémentaire* s'il existe $\alpha \in L$ et $n \in \mathbb{N}^*$ tels que $L = K(\alpha)$ et $\alpha^n \in K$.

Une extension L/K est dite *radicale* s'il existe une tour d'extensions $K = L_0 \subset L_1 \subset \cdots \subset L_r = L$ telles que pour tout $0 \leqslant i < r$ l'extension L_{i+1}/L_i est radicale élémentaire.

Autrement dit L/K est radicale s'il existe une tour $K = L_0 \subset L_1 \subset \cdots \subset L_r = L$ et pour tout i il existe $\alpha_{i+1} \in L_{i+1}$ et un entier n_{i+1} tels que $L_{i+1} = L_i(\alpha_{i+1})$ et $\alpha_{i+1}^{n_{i+1}} \in L_i$.

Noter que la différence entre extension radicale élémentaire et extension de Kummer réside dans le fait que K contienne, ou pas, une racine n-ième de l'unité.

Remarque 3.42. Si L/K est une extension radicale et E/K une extension quelconque, alors EL/E est radicale. En effet, si $K = L_0 \subset L_1 \subset \cdots \subset L_r = L$ est une suite avec $L_{i+1} = L_i(\alpha_{i+1})$, alors on a la suite $E = EL_0 \subset EL_1 \subset \cdots \subset EL_r = EL$ qui satisfait $EL_{i+1} = EL_i(\alpha_{i+1})$.

En particulier, le compositum de deux extensions radicales est une extension radicale.

Exemple 3.43.
- Une extension cyclotomique est radicale (et même élémentaire).

- Une extension quadratique sur un corps de caractéristique nulle est radicale.
- L'extension $\mathbb{Q}(\sqrt[3]{2}, \mathrm{j})/\mathbb{Q}$ est radicale non élémentaire. En effet, on a $\mathbb{Q} \subset \mathbb{Q}(\mathrm{j}) \subset \mathbb{Q}(\mathrm{j}, \sqrt[3]{2})$, et les deux extensions $\mathbb{Q}(\mathrm{j})/\mathbb{Q}$ et $\mathbb{Q}(\sqrt[3]{2}, \mathrm{j})/\mathbb{Q}(\mathrm{j})$ sont radicales élémentaires.

Définition 3.44. Soit K un corps de caractéristique nulle et $\bar{K}$ sa clôture algébrique.

On dit qu'un élément α de $\bar{K}$ est *exprimable par radicaux (sur K)* s'il existe une extension radicale L/K contenant α.

On dit qu'un polynome $P(X) \in K[X]$ est *résoluble par radicaux (sur K)* si toutes ses racines dans $\bar{K}$ sont exprimables par radicaux.

Exemple 3.45. Le nombre $3 - \sqrt[3]{2 + \mathrm{i}\sqrt{1 - \sqrt[5]{17}}}$ est exprimable par radicaux sur $\mathbb{Q}$, puisque dans l'extension $\mathbb{Q}(\sqrt[3]{2 + \mathrm{i}\sqrt{1 - \sqrt[5]{17}}})/\mathbb{Q}$, et que celle-ci est le dernière étage de la tour $\mathbb{Q}(\sqrt[3]{2 + \mathrm{i}\sqrt{1 - \sqrt[5]{17}}})/\mathbb{Q}(\mathrm{i}\sqrt{1 - \sqrt[5]{17}})/\mathbb{Q}(\sqrt[5]{17})/\mathbb{Q}$, dont tous les étages sont radicaux élémentaires.

Exemple 3.46. Le polynome $X^4 - 2$ est résoluble par radicaux sur $\mathbb{Q}$ puisque ses racines sont toutes dans l'extension $\mathbb{Q}(\sqrt[4]{2}, \mathrm{i})/\mathbb{Q}$, laquelle est le dernière étage de la tour d'extensions $\mathbb{Q}(\sqrt[4]{2}, \mathrm{i})/\mathbb{Q}(\mathrm{i})/\mathbb{Q}$, dont tous les étages sont radicaux élémentaires.

Exemple 3.47. Le polynome $X^2 + X + 1$ est résoluble par radicaux sur $\mathbb{F}_2$ puisque ses racines sont toutes dans l'extension $\mathbb{F}_2(\mathrm{j})$, où j est une racine troisième de l'unité (puisque $(X + 1)(X^2 + X + 1) = X^3 - 1$ sur $\mathbb{F}_2$). Notons ici que $X^2 + X + 1$ n'est pas résoluble si on se restreint à des radicaux carrés (c'est-à-dire de degré 2).

Remarque 3.48. La notion de radicalité étant stable par compositum, on voit qu'un polynome est résoluble par radicaux si et seulement si son corps de décomposition est contenu dans une extension radicale.

Remarque 3.49. Ne supposant pas que K contient des racines n-ième de l'unité pour tout n, l'expression d'un élément α résoluble contient des ambiguïtés, comme dans l'exemple 3.45. En caractéristique nulle, celles-ci peuvent être levées sans peine en rajoutant une racine de l'unité (du bon ordre) dans le corps et dans l'expression de α. Cela ne change pas le caractère radical de l'extension: si L/K est radicale avec la tour $K = L_0 \subset L_1 \subset \cdots \subset L_r = L$, où pour tout i on a $L_{i+1} = L_i(\alpha_{i+1})$ et $\alpha_{i+1}^{n_{i+1}} \in L_i$, alors en posant $n = \mathrm{ppcm}(n_i)$ (ou plus simplement $n = [L : K]$ qui en est un multiple) et ξ une racine n-ième de 1 dans $\bar{K}$, on a (comme en 3.42)

$$K = L_0 \subset L_0(\xi) \subset L_1(\xi) \subset \cdots \subset L_r(\xi),$$

de sorte que $L(\xi)/K$ est radicale.

Dans ce cadre, et en vertu de la proposition 3.38, chaque extension $L_{i+1}(\xi)/L_i(\xi)$, ainsi que $L_0(\xi)/L_0$, est galoisienne de groupe de Galois abélien.

Définition 3.50. Soit G un groupe. On dit que G est *résoluble* s'il existe une suite de sous-groupes $\{1\} = G_r \triangleleft G_{r-1} \triangleleft \cdots \triangleleft G_0 = G$ telle que pour tout i, le sous-groupe G_{i+1} est distingué dans G_i et le quotient G_i/G_{i+1} est abélien. Une telle suite est appelée *suite de résolubilité*.

Exemple 3.51. Le groupe $\mathcal{S}_3$ est résoluble (mais pas abélien). En effet, on a $\{1\} \triangleleft \mathcal{A}_3 \triangleleft \mathcal{S}_3$, et les quotients $\mathcal{A}_3/\{1\} \simeq \mathbb{Z}/3\mathbb{Z}$ et $\mathcal{S}_3/\mathcal{A}_3 \simeq \mathbb{Z}/2\mathbb{Z}$ sont abéliens.

Aussi, le groupe $\mathcal{S}_4$ est aussi résoluble non abélien. En effet, on a $\{1\} \triangleleft V_4 \triangleleft \mathcal{A}_4 \triangleleft \mathcal{S}_4$, où V_4 est le sous-groupe de cardinal 4 contenant l'identité et les doubles-transpositions. Les quotients $V_4/\{1\} \simeq (\mathbb{Z}/2\mathbb{Z})^2$, $\mathcal{A}_4/V_4 \simeq \mathbb{Z}/3\mathbb{Z}$ et $\mathcal{S}_4/\mathcal{A}_4 \simeq \mathbb{Z}/2\mathbb{Z}$ sont abéliens.

Pour tout $n \geqslant 5$, le groupe $\mathcal{A}_n$ n'est pas résoluble. En effet il est simple, c'est-à-dire qu'il n'admet aucun sous-groupe distingué, et non abélien.

Remarque 3.52. On peut se demander s'il existe une suite de composition "minimale" qui trivialise un groupe le plus rapidement possible. C'est le cas: un groupe G est résoluble si et seulement la suite $D^{(n)}(G)$ stationne à $\{1\}$, où $D(G)$ désigne le groupe dérivé de G. Le quotient $G/D(G)$ est le plus gros quotient abélien de G au sens de l'inclusion.

On va utiliser le résultat suivant, dont la démonstration ne pose pas de difficulté particulière.

Lemme 3.53. *Soit G un groupe,*

(1) *si G est résoluble, alors tout sous-groupe de G l'est;*
(2) *si G est résoluble, alors tout quotient de G l'est;*
(3) *pour tout sous-groupe distingué H de G, le groupe G est résoluble si et seulement H et G/H le sont.*

Démonstration. (1) Si G admet la suite de décomposition $\{1\} = G_r \triangleleft G_{r-1} \triangleleft \cdots \triangleleft G_0 = G$, et H est un sous-groupe de G, alors H admet la suite $\{1\} = (G_r \cap H) \triangleleft (G_{r-1} \cap H) \triangleleft \cdots \triangleleft (G_0 \cap H) = H$.

(2) De même, G/H admet la suite $\{1\} = \langle G_r, H\rangle/H \triangleleft \langle G_{r-1}, H\rangle/H \triangleleft \cdots \triangleleft \langle G, H\rangle/H = G/H$.

(3) Le sens direct découle des deux items précédents. Quant au sens indirect, on compose les suites de résolubilité: si on a $\{1\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_r = H$ avec H_{i+1}/H_i abélien, et $\{1\} = F_0 \triangleleft F_1 \triangleleft \cdots \triangleleft F_s = G/H$ avec F_{i+1}/F_i abélien, alors on a $\{1\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_r = H \triangleleft HF_0 \triangleleft HF_1 \triangleleft \cdots \triangleleft HF_s = G$.

□

Exemple 3.54. Pour $n \geqslant 5$, le groupe $\mathcal{S}_n$ n'est pas résoluble. En effet, il admet $\mathcal{A}_n$ pour sous-groupe distingué, et ce dernier n'est pas résoluble.

Exemple 3.55. Soit p un nombre premier. Tout p-groupe (c'est-à-dire groupe dont le cardinal est une puissance de p) est résoluble. Cela provient du fait que le centre d'un p-groupe est toujours non trivial, ce qui permet à l'aide de l'item (3) du lemme précédent de faire une récurrence.

On peut alors transposer les propriétés des groupes résolubles aux extensions:

Définition 3.56. Une extension finie L/K est dite *résoluble* si elle est galoisienne et si son groupe de Galois est résoluble.

Exemple 3.57. Si L/K est une extension galoisienne finie de degré p^n, alors L/K est résoluble, puisque son groupe de Galois est un p-groupe fini.

Lemme 3.58. *Soit K un corps, L/K une extension galoisienne finie, et L'/K une sous-extension.*

(1) *Si L/K est résoluble, alors L/L' est résoluble.*
(2) *Si L/K est résoluble et L'/K galoisienne, alors L'/K est résoluble.*
(3) *Si L'/K est galoisienne, alors L/K est résoluble si et seulement si L/L' et L'/K sont résolubles.*
(4) *Si L/K est résoluble et E/K une extension quelconque, alors EL/E est résoluble.*

Démonstration. Les trois premières propriétés découlent de la correspondance de Galois finie 3.7 et du lemme 3.53. Pour (4), notons déjà que EL/E est galoisienne finie. En effet, si $L = \mathrm{Dec}_K(P)$, alors $EL = \mathrm{Dec}_E(P)$. De plus $\mathrm{Gal}(EL/E)$ est un sous-groupe de $\mathrm{Gal}(L/K)$. En effet, on vérifie que l'application de restriction : $\mathrm{Gal}(EL/E) \to \mathrm{Gal}(L/K), \sigma \mapsto \sigma|_L$ est un morphisme injectif. Comme $\mathrm{Gal}(L/K)$ est résoluble, $\mathrm{Gal}(EL/E)$ aussi. □

On veut maintenant montrer qu'extensions radicales et extensions résolubles sont presque la même chose. Noter qu'une extension résoluble est galoisienne par définition, ce qui n'est pas le cas d'une extension radicale. C'est (en partie) pourquoi on n'a pas stricte égalité entre les deux notions, mais des inclusions.

Lemme 3.59. *Soit K de caractéristique nulle et L/K résoluble. Soit $n = [L : K]$ et ξ une racine primitive n-ième de l'unité dans $\bar{K}$. Alors l'extension $L(\xi)/K$ est radicale.*

En particulier tout élément de L est exprimable par radicaux sur K.

Démonstration. Comme L/K est résoluble, $L(\xi)/K(\xi)$ l'est par le lemme précédent, et $\mathrm{Gal}(L(\xi)/K(\xi))$ est un sous-groupe de $\mathrm{Gal}(L/K)$. Comme $K(\xi)/K$ est radicale, il suffit de montrer que $L(\xi)/K(\xi)$ l'est.

Posons $G = \mathrm{Gal}(L(\xi)/K(\xi))$. Soit $\{1\} = G_r \triangleleft G_{r-1} \triangleleft \cdots \triangleleft G_0 = G$ une suite de résolution. Quitte à en allonger la longueur, on peut supposer que chaque quotient G_{i+1}/G_i est cyclique (et non juste abélien). On pose $L_i = L(\xi)^{G_i}$. Alors on a $K(\xi) = L_0 \subset L_1 \subset \cdots \subset L_r = L(\xi)$. Par le lemme d'Artin 3.31, on a $\mathrm{Gal}(L(\xi)/L_{i+1}) = G_{i+1} \triangleleft G_i = \mathrm{Gal}(L(\xi)/L_i)$. Par la correspondance de Galois, L_{i+1}/L_i est galoisienne et $\mathrm{Gal}(L_{i+1}/L_i) \simeq G_i/G_{i+1}$ est abélien. Notons aussi que $[L_{i+1} : L_i]$ divise n. La proposition 3.39 s'applique alors, et implique que L_{i+1}/L_i est radicale élémentaire. □

Passons à la réciproque, à savoir que toute extension radicale est contenue dans une extension résoluble, qu'on démontrera par récurrence. On commence par renforcer la proposition 3.38 :

Lemme 3.60. *Soit K de caractéristique nulle et E/K galoisienne finie. Soit F/E de la forme $L = E(\alpha)$, avec $\alpha^n \in E$. Alors F est contenue dans une extension galoisienne finie L/K telle que L/E est résoluble.*

Démonstration. Soit $a = \alpha^n \in E$. On pose $P(X) = \prod_{\sigma \in \mathrm{Gal}(E/K)}(X^n - \sigma(a)) \in E[X]$. Alors P est invariant par l'action de $\mathrm{Gal}(E/K)$, donc ses coefficients aussi, et donc $P(X)$ est dans $K[X]$. Aussi l'extension $\mathrm{Dec}_K(P)/K$ est normale par construction, et séparable car K parfait, donc galoisienne finie.

Notons $\alpha_1, \ldots, \alpha_m$ les racines de P dans $\bar{K}$, et soit ξ une racine n-ième de 1 dans $\bar{K}$. On considère $E(\xi)/E$ qui est galoisienne de groupe de Galois abélien. Soit L l'extension $E(\xi, \alpha_1, \ldots, \alpha_m)/K$. C'est le compositum des extensions normales E/K, $K(\xi)/K$ et $\mathrm{Dec}_K(P)/K$,

donc L/K est normale, et donc galoisienne finie puisque K est parfait. De plus on a $F = E(\alpha) \subset L$.

Reste à voir que L/E est résoluble. Par la proposition 3.38 chaque extension $E(\xi, \alpha_i)/E(\xi)$ est galoisienne finie, de groupe de Galois cyclique, donc a fortiori résoluble. De plus $E(\xi)/E$ est abélienne, donc résoluble. Par le lemme 3.58, le compositum L/E est résoluble. □

Lemme 3.61. *Soit K de caractéristique nulle. Alors toute extension radicale F/K est contenue dans une extension résoluble L/K*

Démonstration. On fait une récurrence à partir du lemme précédent. L'emboitement vient du lemme 3.58 (3). □

En combinant les lemmes 3.59 et 3.61, on a alors

Théorème 3.62 (annoncé comme théorème 3.1)**.** *Soit K un corps de caractéristique nulle, et $P(X) \in K[X]$ non constant. Alors les assertions suivantes sont équivalentes:*

(1) *le polynome P est résoluble par radicaux sur K;*
(2) *le groupe de Galois $\mathrm{Gal}_(\mathrm{Dec}_K(P)/K)$ est résoluble.*

Pour montrer qu'il existe des polynomes non résolubles par radicaux, il suffit donc de trouver des polynomes dont le groupe de Galois n'est pas résoluble. C'est par exemple le cas de $X^5 - X - 1$ dont le groupe de Galois sur $\mathbb{Q}$ est le groupe de permutations $\mathcal{S}_5$ tout entier (ce qui n'est pas trivial à démontrer).

3.9. **Formules en degré 3.** Comment retrouver à partir de la correspondance de Galois et de la section précédente les formules de Cardano pour la résolution des équations de degré 3?

On part d'un corps K dont on suppose (quitte à la rajouter) qu'il contient une racine sixième de l'unité ξ (en fait, on utilisera $\mathrm{j} = \xi^2$ et $\mathrm{i} = \xi^3$). On prend trois éléments s_1, s_2, s_3 d'une extension de K et on note $F = K(s_1, s_2, s_3)$. On considère le polynome $P(X) = X^3 - s_1X^2 + s_2X - s3 \in F[X]$, et on note $\alpha_1, \alpha_2, \alpha_3$ ses racines dans $\bar{F}$. On considère l'extension $L = K(\alpha_1, \alpha_2, \alpha_3)/K(s_1, s_2, s_3) = F$. Comme on a $P(X) = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$, on a

$$s_1 = \alpha_1 + \alpha_2 + \alpha_3, \quad s_2 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1, \quad s_3 = \alpha_1\alpha_2\alpha_3.$$

Classiquement, quitte à faire un changement de variable $X = X - s_1/3$, on peut supposer $s_1 = 0$, ce qui simplifie les expressions.

L'extension $K(\alpha_1, \alpha_2, \alpha_3)/K(s_1, s_2, s_3)$ est corps de décomposition de P, donc galoisienne finie. Son groupe de Galois agit librement sur $\{\alpha_1, \alpha_2, \alpha_3\}$ par permutations, de sorte que $\mathrm{Gal}(K(\alpha_1, \alpha_2, \alpha_3)/K(s_1, s_2, s_3))$ est (un sous-groupe de) $\mathcal{S}_3$.

On a la suite de résolution $\{1\} \triangleleft \mathcal{A}_3 \triangleleft \mathcal{S}_3$, avec quotients cycliques, qui correspond à la tour d'extensions $F = K(s_1, s_2, s_3) = K(\alpha_1, \alpha_2, \alpha_3)^{\mathcal{S}_3} \subset K(\alpha_1, \alpha_2, \alpha_3)^{\mathcal{A}_3} \subset K(\alpha_1, \alpha_2, \alpha_3) = L$.

Étudions ces deux extensions successivement.

Tout d'abord $F = K(s_1, s_2, s_3) = K(\alpha_1, \alpha_2, \alpha_3)^{\mathcal{S}_3}$ contient les éléments qui sont invariants par permutation quelconque des racines $\alpha_1, \alpha_2, \alpha_3$, ce sont les éléments qui s'expriment en termes des fonctions symétriques élémentaires s_1, s_2, s_3. Un exemple de tel élément est $\Delta = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2$. On note pour la suite qu'on a $\Delta = -4s_2^3 + 27s_3^2$.

La première extension $K(\alpha_1,\alpha_2,\alpha_3)^{\mathcal{A}_3}/K(\alpha_1,\alpha_2,\alpha_3)^{\mathcal{S}_3} = F$ est triviale si $\mathrm{Gal}(L/F)$ est inclus dans $\mathcal{A}_3$. Sinon elle est de degré 2. On sait par la proposition 3.39 que dans ce cas, elle admet un générateur δ tel que $\delta^2 \in K(\alpha_1,\alpha_2,\alpha_3)^{\mathcal{S}_3} = F$. On cherche un tel générateur qui soit donné par des formules simples en termes de s_1, s_2, s_3. On prend $\delta = (\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1) = \sqrt{\Delta}$. En effet, une transposition entre deux racines a pour effet de changer le signe de δ, de sorte que δ est invariant sous l'action de $\mathcal{A}_3$, mais pas de $\mathcal{S}_3$. Évidemment, $\delta^2 = \Delta$ est invariant sous tout $\mathcal{S}_3$, donc est bien dans F. Et grace à l'expression qu'on avait pour Δ, on déduit $\delta = \sqrt{-4s_2^3+27s_3^2}$. Pour résumer on a $K(\alpha_1,\alpha_2,\alpha_3)^{\mathcal{A}_3} = F(\delta)$.

Reste à comprendre l'extension $L = K(\alpha_1,\alpha_2,\alpha_3)/K(\alpha_1,\alpha_2,\alpha_3)^{\mathcal{A}_3} = F(\delta)$, de groupe de Galois $\mathcal{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$. Comme on a rajouté j à K, on sait qu'elle est engendré par un élément x tel que $x^3 \in F(\delta)$. Mieux : la preuve de la proposition 3.39 suggère de chercher un tel élément sous la forme $t+\mathrm{j}g(t)+\mathrm{j}^2g^{(2)}(t)$, pour $t \in L$. Si on prend pour t les éléments les plus simples de $L\backslash F(\delta)$, à savoir $\alpha_1,\alpha_2,\alpha_3$, on est amené à considérer l'élément $u = \alpha_1+\mathrm{j}\alpha_2+\mathrm{j}^2\alpha_3$. Posons symétriquement $v = \alpha_1+\mathrm{j}^2\alpha_2+\mathrm{j}\alpha_3$. Alors comme la multiplication par j de u ou v revient à permuter cycliquement les racines, on voit que u^3 et v^3 sont invariants par le groupe $\mathcal{A}_3$. Ainsi on a bien $u,v \in L$ et $u^3,v^3 \in F(\delta)$.

Reste à trouver une expression pour u et v, on en déduira une expression pour les racines en inversant un système inversible (car on a la troisième équation $\alpha_1+\alpha_2+\alpha_3 = 0$). Pour cela, on va d'abord déterminer u^3 et v^3 qui sont plus simples, puisque dans $F(\delta)$. Comme la transposition $(\alpha_2\alpha_3)$ échange u et v, on voit que $\mathcal{S}_3$ ne préserve pas u^3 ni v^3, mais préserve leur somme u^3+v^3 et leur produit u^3v^3, de sorte qu'on a $u^3+v^3, u^3v^3 \in K(\alpha_1,\alpha_2,\alpha_3)^{\mathcal{S}_3} = F$. Autrement dit u^3+v^3 et u^3v^3 sont des polynomes symétriques qu'il suffit de déterminer. Passant sur le calcul (voir Gozart, p191), on trouve $u^3+v^3 = 27s_3$ et $u^3v^3 = -27s_2^3$. Ainsi u^3, v^3 sont les deux racines du polynome $T^2-27s_3T-27s_2^3$. Le discriminant de ce polynome est -27Δ. On trouve[16] alors $u^3 = \frac{27s_3+\mathrm{i}3\sqrt{3}\delta}{2}$ et $v^3 = \frac{27s_3-\mathrm{i}3\sqrt{3}\delta}{2}$, et finalement

$$u = \sqrt[3]{\frac{27s_3+\mathrm{i}3\sqrt{3}\delta}{2}} \quad \text{et} \quad v = \sqrt[3]{\frac{27s_3-\mathrm{i}3\sqrt{3}\delta}{2}}.$$

Ainsi on a trouvé un élément u (en fait deux avec v) qui vérifie $L = K(\delta)(u)$ et $u^3 \in K(\delta)$.

Ne reste plus qu'à écrire $\alpha_1,\alpha_2,\alpha_3$ en fonction de δ et u (et v), ce qu'on sait être possible. Il suffit d'inverser le système

$$\begin{aligned} \alpha_1+\alpha_2+\alpha_3 &= 0 \\ \alpha_1+\mathrm{j}\alpha_2+\mathrm{j}^2\alpha_3 &= u \\ \alpha_1+\mathrm{j}^2\alpha_2+\mathrm{j}\alpha_3 &= v, \end{aligned}$$

[16] Il faut déterminer qui est u^3 et qui est v^3: il suffit de considérer u^3-v^3 dont on calcule que c'est $\mathrm{i}3\sqrt{3}\delta$.

ce qui donne

$$\begin{aligned}
\alpha_1 &= \frac{u+v}{3} = \frac{1}{3}\left(\sqrt[3]{\frac{27s_3 + \mathrm{i}3\sqrt{3}\delta}{2}} + \sqrt[3]{\frac{27s_3 - \mathrm{i}3\sqrt{3}\delta}{2}}\right)\\
\alpha_2 &= \frac{\mathrm{j}^2 u + \mathrm{j}v}{3} = \frac{1}{3}\left(\mathrm{j}^2\sqrt[3]{\frac{27s_3 + \mathrm{i}3\sqrt{3}\delta}{2}} + \mathrm{j}\sqrt[3]{\frac{27s_3 - \mathrm{i}3\sqrt{3}\delta}{2}}\right)\\
\alpha_2 &= \frac{\mathrm{j}^2 u + \mathrm{j}v}{3} = \frac{1}{3}\left(\mathrm{j}\sqrt[3]{\frac{27s_3 + \mathrm{i}3\sqrt{3}\delta}{2}} + \mathrm{j}^2\sqrt[3]{\frac{27s_3 - \mathrm{i}3\sqrt{3}\delta}{2}}\right),
\end{aligned}$$

qu'on peut réécrire avec juste s_2 et s_3 en utilisant l'expression de δ.