Agrégation : Anneaux, corps et polynômes

Cyril Demarche

21 décembre 2023

1 Algèbres de polynômes

1.1 Généralités

Définition 1.1. Soient A un anneau commutatif et I un ensemble fini non vide.

On définit l'anneau $A[(X_i)_{i\in I}]$ comme étant l'ensemble $A^{(\mathbf{N}^I)}$ des suites indicées par $\mathbf{N}^I$, à valeurs dans A, à support fini, muni des lois suivantes, pour tous $(a_{\underline{n}})_{\underline{n}\in\mathbf{N}^I}$ et $(b_{\underline{n}})_{\underline{n}\in\mathbf{N}^I}$ dans $A^{(\mathbf{N}^I)}$:

1. $(a_{\underline{n}}) + (b_{\underline{n}}) := (a_{\underline{n}} + b_{\underline{n}})$.
2. $(c_{\underline{n}}) := (a_{\underline{n}}) \cdot (b_{\underline{n}})$ est défini par

$$c_{\underline{n}} := \sum_{\underline{m}+\underline{k}=\underline{n}} a_{\underline{m}} \cdot b_{\underline{k}} \,.$$

Par construction, on dispose d'un morphisme d'anneaux injectif : $A \to A[(X_i)_{i\in I}]$ défini par $a \mapsto (a\delta_{\underline{n},\underline{0}})_{\underline{n}\in\mathbf{N}^I}$, qui muni $A[(X_i)_{i\in I}]$ d'une structure naturelle de A-algèbre. Les éléments de A (vus dans $A[(X_i)_{i\in I}]$) sont appelés les polynômes constants.

Pour tout $i \in I$, on note $\underline{i} := (\delta_{i,j})_{j\in I}$.

Pour simplifier les notations, il est commode de noter, pour tout $i \in I$, $X_i := (a_{\underline{n}}) \in A^{(\mathbf{N}^I)}$ défini par $a_{\underline{n}} = \delta_{\underline{n},\underline{i}}$, puis on introduit, pour tout $\underline{n} \in \mathbf{N}^I$, le monôme $X^{\underline{n}} := \prod_{i\in I} X_i^{n_i}$.

Alors par définition tout élément de $A[(X_i)_{i\in I}]$ s'écrit de façon unique sous la forme $\sum_{\underline{n}\in\mathbf{N}^I} a_{\underline{n}} X^{\underline{n}}$ avec $a_{\underline{n}} \in A$ pour tout $\underline{n} \in \mathbf{N}^I$, nul presque partout. Avec cette notation, les lois d'anneau deviennent naturelles :

$$\sum_{\underline{n}\in\mathbf{N}^I} a_{\underline{n}} X^{\underline{n}} + \sum_{\underline{n}\in\mathbf{N}^I} b_{\underline{n}} X^{\underline{n}} = \sum_{\underline{n}\in\mathbf{N}^I} (a_{\underline{n}} + b_{\underline{n}}) X^{\underline{n}} \,,$$

$$\left(\sum_{\underline{n}\in\mathbf{N}^I} a_{\underline{n}} X^{\underline{n}}\right) \cdot \left(\sum_{\underline{n}\in\mathbf{N}^I} b_{\underline{n}} X^{\underline{n}}\right) = \sum_{\underline{n}\in\mathbf{N}^I} \left(\sum_{\underline{m}+\underline{k}=\underline{n}} a_{\underline{m}} \cdot b_{\underline{k}}\right) X^{\underline{n}} \,.$$

Remarque 1.2. Les définitions précédentes se généralisent sans difficulté à un ensemble I infini (en remplaçant I par (I) dans la définition).

En particulier, quand $|I| = 1$, on obtient l'algèbre $A[X]$, dont les éléments sont exactement les suites à support fini à valeurs dans A, notés $\sum_{k=0}^{d} a_k X^k$ (où d est un entier naturel), avec les lois d'anneau classiques.

Définition 1.3. Soit $P = \sum_{\underline{m} \in \mathbf{N}^n} a_{\underline{m}} X^{\underline{m}}$. Pour toute A-algèbre commutative B et tout $\underline{b} := (b_1, \dots, b_n) \in B^n$, on définit l'évaluation de P en $\underline{b}$ par

$$P(b_1, \dots, b_n) := \sum_{\underline{m} \in \mathbf{N}^n} a_{\underline{m}} b_1^{m_1} \dots b_n^{m_n} .$$

En particulier, on dispose d'une application (morphisme de A-algèbres) "évaluation en $\underline{b}$" $\mathrm{ev}_{\underline{b}} : A[X] \to B$ et d'une application "fonction polynômiale associée à P" $\widetilde{P} : B^n \to B$.

La proposition suivante est la propriété universelle des algèbres de polynômes :

Proposition 1.4. *Soit B une A-algèbre commutative et $n \geq 1$.*

La donnée d'un morphisme de A-algèbres $A[X_1, \dots, X_n] \to B$ est équivalente à celle de n éléments de B : pour tous $(b_1, \dots, b_n) \in B$, il existe un unique morphisme de A-algèbres $\varphi : A[X_1, \dots, X_n] \to B$ tel que $\varphi(X_i) = b_i$ (i.e. $\varphi = \mathrm{ev}_{\underline{b}}$).

Démonstration. □

Le résultat suivant est clair :

Proposition 1.5. *On dispose d'un isomorphisme canonique de A-algèbres*

$$A[X_1, \dots, X_{n-1}][X_n] \xrightarrow{\sim} A[X_1, \dots, X_n] .$$

Définissons maintenant le degré d'un polynôme :

Définition 1.6. Le degré (total) d'un monôme $X^{\underline{m}} = X_1^{m_1} \dots X_n^{m_n}$ est $m_1 + \dots + m_n$.

Soit $P \in A[X_1, \dots, X_n]$ non nul. Le degré (total) de P est celui de son monôme de degré maximal.

Par convention, on décide souvent que le degré du polynôme nul est $-\infty$.

Pour un polynôme de $A[X]$, on en déduit la notion de coefficient dominant, qui est le coefficient d'indice égal au degré du polynôme.

Remarque 1.7. On dispose d'autres notions de degré pour les polynômes à $n \geq 2$ indéterminées. Par exemple, pour tout $1 \leq k \leq n$, l'isomorphisme $A[X_1, \dots, X_{k-1}, X_{k+1}, \dots, X_n][X_k] = A[X_1, \dots, X_n]$ permet de définir le degré partiel par rapport à X_k.

On peut aussi définir le multidegré d'un monôme $X^{\underline{m}}$ comme étant égal à $\underline{m} \in \mathbf{N}^n$, et définir le multidegré d'un polynôme comme le max (pour l'ordre lexicographique) des multidegrés des monômes apparaissant dans ce polynôme.

Proposition 1.8. *Soit A un anneau commutatif unitaire.*

Alors A est intègre si et seulement si $A[X]$ est intègre si et seulement si $A[X_1, \dots, X_n]$ est intègre.

Démonstration. L'inclusion $A \to A[X] \to A[X_1, \dots, X_n]$ prouve le sens réciproque. Pour le sens direct, il suffit de raisonner sur les coefficients dominants de deux polynômes non nuls et de faire leur produit. □

Corollaire 1.9. *Soient $P, Q \in A[X_1, \dots, X_n]$.*

- $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$, *avec égalité si* $\deg(P) \neq \deg(Q)$.
- $\deg(PQ) \leq \deg(P) + \deg(Q)$, *avec égalité si A est intègre.*

Une notion important est celle de polynôme homogène :

Définition 1.10. Soit $P \in A[X_1, \dots, X_n]$.

On dit que P est homogène de degré d si tous les monômes non nuls de P ont degré d.

Remarquons que par convention, le polynôme nul est homogène de tout degré.

Exemple 1.11. Si K est un corps, l'ensemble des polynômes de $K[X_1, \dots, X_n]$ homogènes de degré d est un sous-espace vectoriel de $K[X_1, \dots, X_n]$ de dimension $\binom{n+d-1}{d}$.

En effet, une base est donnée par les monômes $X_1^{m_1} \dots X_n^{m_n}$ avec $m_1 + \dots + m_n = d$. Le nombre de tels n-uplets $(m_1, \dots, m_n)$ dans $\mathbf{N}^n$ est $\binom{n+d-1}{d}$ (on peut le montrer avec des barres et des étoiles, ou alors en reliant ce nombre au nombre de suites croissantes de d nombres dans $\{1, \dots, n\}$, qui coïncide avec le nombre de suites strictement croissantes (donc de sous-ensembles) de d nombres dans $\{1, \dots, n + d - 1\}$.

Lemme 1.12. *Le polynôme $P(X_1, \dots, X_n)$ est homogène de degré d si et seulement $P(TX_1, \dots, TX_n) = T^d P(X_1, \dots, X_n)$ dans $A[X_1, \dots, X_n, T]$.*

Proposition 1.13. *Tout polynôme $P \in A[X_1, \dots, X_n]$ s'écrit de manière unique sous la forme $P = \sum_{d \geq 0} P_d$, avec $P_d \in A[X_1, \dots, X_n]$ homogène de degré d.*

On dispose de notions de dérivées formelles pour les polynômes, définies comme suit :

Définition 1.14. Soit $P = \sum_{\underline{k} \in \mathbf{N}^n} a_{\underline{k}} X^{\underline{k}} \in A[X_1, \dots, X_n]$. Pour tout $1 \leq i \leq n$, on peut noter $P = \sum_{k=0^{d_i}} P_k(X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n) X_i^k$ et on définit

$$\frac{\partial P}{\partial X_i} := \sum_{k=1^{d_i}} k P_k(X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n) X_i^{k-1} .$$

En particulier, si $P = \sum_{k=0}^{d} a_k X^k$, on a $P' := \sum_{k=1}^{d} k a_k X^{k-1}$.

On dispose de la formule de Taylor bien connue :

Proposition 1.15. *Soit A un anneau intègre, $a \in A$. Soit $P \in A[X]$ un polynôme de degré n. On suppose que $n! \neq 0$ dans A (i.e. la caractéristique de A est nulle ou $> n$).*

Alors $k!$ divise $P^{(k)}(a)$ pour tout $2 \leq k \leq n$, et on a l'égalité dans $A[X]$

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} (X - a)^k .$$

Démonstration. On considère le polynôme $F(X) := P(X + a)$, qui est de degré n, et vérifie $F^{(k)}(X) = P^{(k)}(X + a)$. Quitte à remplacer P par F, il suffit de montrer le résultat pour $a = 0$.

On écrit alors $P = \sum_{k=0}^{n} a_k X^k$.

Il est alors clair que $P^{(k)}(0) = k! a_k$, ce qui assure le résultat. $\square$

Remarque 1.16. On dispose également d'une version en n variables de la formule de Taylor.

1.2 Séries formelles

On peut définir une variante de l'algèbre des polynômes : il s'agit de l'algèbre des séries formelles.

Définition 1.17. Soit A un anneau commutatif et I un ensemble fini non vide.

On définit l'anneau $A[[(X_i)_{i\in I}]]$ comme étant l'ensemble $A^{\mathbf{N}^I}$ des suites indicées par $\mathbf{N}^I$, à valeurs dans A, muni des lois suivantes, pour tous $(a_{\underline{n}})_{\underline{n}\in\mathbf{N}^I}$ et $(b_{\underline{n}})_{\underline{n}\in\mathbf{N}^I}$ dans $A^{\mathbf{N}^I}$:

1. $(a_{\underline{n}}) + (b_{\underline{n}}) := (a_{\underline{n}} + b_{\underline{n}})$.
2. $(c_{\underline{n}}) := (a_{\underline{n}}) \cdot (b_{\underline{n}})$ est défini par

$$c_{\underline{n}} := \sum_{\underline{m}+\underline{k}=\underline{n}} a_{\underline{m}} \cdot b_{\underline{k}} \,.$$

Avec les notations précédentes, tout élément de $A[[(X_i)_{i\in I}]]$ s'écrit de façon unique sous la forme $\sum_{\underline{n}\in\mathbf{N}^I} a_{\underline{n}} X^{\underline{n}}$ avec $a_{\underline{n}} \in A$ pour tout $\underline{n} \in \mathbf{N}^I$. Avec cette notation, les lois d'anneau deviennent naturelles :

$$\sum_{\underline{n}\in\mathbf{N}^I} a_{\underline{n}} X^{\underline{n}} + \sum_{\underline{n}\in\mathbf{N}^I} b_{\underline{n}} X^{\underline{n}} = \sum_{\underline{n}\in\mathbf{N}^I} (a_{\underline{n}} + b_{\underline{n}}) X^{\underline{n}} \,,$$

$$\left(\sum_{\underline{n}\in\mathbf{N}^I} a_{\underline{n}} X^{\underline{n}}\right) \cdot \left(\sum_{\underline{n}\in\mathbf{N}^I} b_{\underline{n}} X^{\underline{n}}\right) = \sum_{\underline{n}\in\mathbf{N}^I} \left(\sum_{\underline{m}+\underline{k}=\underline{n}} a_{\underline{m}} \cdot b_{\underline{k}}\right) X^{\underline{n}} \,.$$

En particulier, quand $|I| = 1$, on obtient l'algèbre $A[[X]]$, dont les éléments sont exactement les suites à valeurs dans A, notés $\sum_{k\geq 0} a_k X^k$, avec les lois d'anneau classiques.

1.3 Polynômes symétriques

On dispose d'une action naturelle du groupe $\mathfrak{S}_n$ sur la A-algèbre $A[X_1, \dots, X_n]$ définie par : pour tout $\sigma \in \mathfrak{S}_n$, pour tout $P \in A[X_1, \dots, X_n]$, $\sigma\cdot P := P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$.

Définition 1.18. Soit $P \in A[X_1, \dots, X_n]$. On dit que P est symétrique (resp. antisymétrique) si pour tout $\sigma \in \mathfrak{S}_n$, $\sigma \cdot P = P$ (resp. $\sigma \cdot P = \varepsilon(\sigma)P$).

Exemples 1.19.

1. Les polynômes $\sum_{i=1}^n X_i$ et $\prod_{i=1}^n X_i$ sont symétriques.
2. Le polynôme de Vandermonde $\Delta := \prod_{1\leq i<j\leq n}(X_i - X_j)$ est antisymétrique, Δ^2 est symétrique.

Les exemples fondamenteaux de polynômes symétriques sont les suivants :

Définition 1.20. Pour tout $1 \leq k \leq n$, on définit le k-ième polynôme symétrique élémentaire

$$e_k(X_1, \dots, X_n) := \sum_{1\leq i_1<\dots i_k\leq n} X_{i_1} \dots X_{i_k} \in \mathbf{Z}[X_1, \dots, X_n] \,.$$

Lemme 1.21. *Pour tout $1 \leq k \leq n$, le polynôme $e_k(X_1, \dots, X_n)$ est symétrique.*

Le théorème de structure suivant décrit complètement la sous-algèbre des polynômes symétriques :

Théorème 1.22. *Soit A un anneau commutatif. Pour tout polynôme symétrique $P \in A[X_1, \dots, X_n]$, il existe un unique polynôme $Q \in A[X_1, \dots, X_n]$ tel que*

$$P = Q(e_1, \dots, e_n)\,.$$

En particulier, la sous-algèbre des polynômes symétriques est isomorphe à la A-algèbre $A[e_1, \dots, e_n]$, elle-même isomorphe à une A-algèbre de polynômes $A[Y_1, \dots, Y_n]$.

Remarque 1.23. Le théorème n'est pas seulement un théorème d'existence, il vient avec un algorithme explicite permettant de calculer le polynôme Q à partir de P (voir la preuve ci-dessous).

Démonstration. On munit l'ensemble des monômes non nuls de $A[X_1, \dots, X_n]$ (ou l'ensemble $\mathbf{N}^n$ des multidegrés) de l'ordre lexicographique suivant :

$$X_1^{k_1} \dots X_n^{k_n} < X_1^{k_1'} \dots X_n^{k_n'}$$

si et seulement s'il existe $1 \leq i \leq n-1$ tel que $k_j = k_j'$ por tout $j \leq i$ et $k_{i+1} < k_{i+1}'$.

— Preuve de l'existence par récurrence sur (le multidegré d') un monôme dominant de P : soit P un polynôme symétrique non nul. Il existe dans P un monôme dominant (maximal pour l'ordre lexicographique introduit ci-dessus), disons $aX_1^{k_1} \dots X_n^{k_n}$. Puisque P est symétrique, on a $k_1 \geq k_2 \geq \dots \geq k_n$. On considère alors $R := P - ae_1^{k_1-k_2} e_2^{k_2-k_3} \dots e_{n-1}^{k_{n-1}-k_n} e_n^{k_n}$. Puisque le monôme dominant de
$$e_1^{k_1-k_2} e_2^{k_2-k_3} \dots e_{n-1}^{k_{n-1}-k_n} e_n^{k_n}$$
est $X_1^{k_1} \dots X_n^{k_n}$, on voit que le coefficient dominant de R est strictement inférieur à $X_1^{k_1} \dots X_n^{k_n}$.
Par hypothèse de récurrence, il existe $\widetilde{Q} \in A[X_1, \dots, X_n]$ tel que le polynôme symétrique R s'écrive $R = \widetilde{Q}(e_1, \dots, e_n)$. Finalement, $P = Q(e_1, \dots, e_n)$ avec $Q = aX_1^{k_1-k_2} X_2^{k_2-k_3} \dots X_{n-1}^{k_{n-1}-k_n} X_n^{k_n} + \widetilde{Q}(X_1, \dots, X_n)$.

— Preuve de l'unicité : soit $Q \in A[X_1, \dots, X_n]$ tel que $Q(e_1, \dots, e_n) = 0$. Soit $X_1^{k_1} \dots X_n^{k_n}$ un monôme apparaissant dans Q. Le monôme dominant de $Q(e_1, \dots, e_n)$ est alors $X_1^{\sum_{i \geq 1} k_i} X_2^{\sum_{i \geq 2} k_i} \dots X_n^{k_n}$. Donc il est clair que deux monômes distincts dans Q ont des monômes dominants distincts quand on les évalue en $(e_1, \dots, e_n)$. Puisque les $X_1^{k_1} \dots X_n^{k_n}$ forment une famille libre dans $A[X_1, \dots, X_n]$, cela assure que $Q = 0$. D'où l'unicité recherchée.

□

Exemple 1.24. Écrire $X^3 + Y^3 + Z^3$ comme polynôme en les fonctions symétriques élémentaires.

Il existe aussi un résultat pour les polynômes antisymétriques :

Proposition 1.25. *Soit A intègre de caractéristique différente de 2, $P \in A[X_1, \dots, X_n]$. Alors P est antisymétrique si et seulement s'il existe un polynôme symétrique S tel que $P = \Delta S$.*

Démonstration. On considère l'anneau intègre $B := A[X_1, \ldots, X_{n-1}]$ et on voit $P \in B[X_n]$. Puisque pour tout $1 \leq i \leq n-1$, $P(X_1, \ldots, X_{n-1}, X_i) = -P(X_1, \ldots, X_{n-1}, X_i)$ (en utilisant l'action de la transposition $(i\, n)$), on en déduit $2P(X_1, \ldots, X_{n-1}, X_i) = 0$, donc $P(X_1, \ldots, X_{n-1}, X_i) = 0$ car A n'est pas de caractéristique 2. Donc pour tout $1 \leq i \leq n-1$, X_i est racine de P vu comme un polynôme de $B[X_n]$, donc $\prod_{i=1}^{n-1}(X_n - X_i)$ divise P dans $A[X_1, \ldots, X_n]$, i.e. $P = \prod_{i=1}^{n-1}(X_n - X_i)Q$. On voit désormais $Q \in A[X_1, \ldots, X_{n-2}, X_n][X_{n-1}]$. Pour tout $1 \leq i \leq n-2$, $0 = P(X_1, \ldots, X_{n-2}, X_i, X_n) = (X_n - X_i)\prod_{j=1}^{n-2}(X_n - X_j)Q(X_1, \ldots, X_{n-2}, X_i, X_n)$. Donc $Q(X_1, \ldots, X_{n-2}, X_i, X_n) = 0$, donc X_i est racine de Q dans $A[X_1, \ldots, X_{n-2}, X_n][X_{n-1}]$, donc $\prod_{i=1}^{n-2}(X_{n-1} - X_i)$ divise Q. Donc $\prod_{i=1}^{n-2}(X_{n-1} - X_i)\prod_{i=1}^{n-1}(X_n - X_i)$ divise P dans $A[X_1, \ldots, X_n]$. Par récurrence, on en déduit que Δ divise P, donc $P = \Delta S$ avec $S \in A[X_1, \ldots, X_n]$.

Enfin, comme P et Δ sont antisymétriques et $A[X_1, \ldots, X_n]$ est intègre, il est clair que S est symétrique. □

Quelques applications :

Définition 1.26. (Sommes de Newton) Pour tout $k \geq 1$, on pose $p_k(X_1, \ldots, X_n) := \sum_{i=1}^{n} X_i^k \in \mathbf{Z}[X_1, \ldots, X_n]$.

Il est clair que ces polynômes sont des polynômes symétriques.

Proposition 1.27. *Pour tout $k \leq n$, on a*

$$ke_k(X_1, \ldots, X_n) = \sum_{i=1}^{k}(-1)^{i-1}e_{k-i}(X_1, \ldots, X_n)p_i(X_1, \ldots, X_n)\,,$$

et pour tout $k > n$,

$$\sum_{i=k-n}^{k}(-1)^i e_{k-i}(X_1, \ldots, X_n)p_i(X_1, \ldots, X_n) = 0\,.$$

Démonstration. On peut considérer le polynôme $\prod_{i=1}^{n}(T - X_i)$ dans $\mathbf{Z}[X_1, \ldots, X_n, T]$ et le développer. Une récurrence simple sur n assure que

$$\prod_{i=1}^{n}(T - X_i) = \sum_{k=0}^{n}(-1)^{n-k}e_{n-k}(X_1, \ldots, X_n)T^k\,.$$

Pour tout $1 \leq i \leq n$, on évalue cette égalité en $T = X_i$, on en déduit :

$$0 = \sum_{k=0}^{n}(-1)^{n-k}e_{n-k}(X_1, \ldots, X_n)X_i^k\,,$$

puis en sommant sur i, on obtient

$$0 = \sum_{k=0}^{n}(-1)^{n-k}e_{n-k}(X_1, \ldots, X_n)p_k(X_1, \ldots, X_n)\,.$$

En isolant le terme correspondant à $k = 0$, on obtient

$$ne_n(X_1, \ldots, X_n) = \sum_{k=1}^{n}(-1)^{k-1}e_{n-k}(X_1, \ldots, X_n)p_k(X_1, \ldots, X_n)\,,$$

ce qui est l'une des formules souhaitées. Si maintenant on se donner un entier $d > n$, on peut exprimer $e_k(X_1, \dots, X_n)$ en calculant $e_k(X_1, \dots, X_d)$ avec les formules précédentes, puis en posant $X_i = 0$ pour tout $n+1 \leq i \leq n$, ce qui donne :

$$\begin{array}{rl} 0 = & \sum_{k=0}^{d}(-1)^{d-k}e_{d-k}(X_1, \dots, X_n, 0, \dots, 0)p_k(X_1, \dots, X_n, 0, \dots, 0) \\ = & \sum_{k=d-n}^{d}(-1)^{d-k}e_{d-k}(X_1, \dots, X_n)p_k(X_1, \dots, X_n) \end{array},$$

ce qui donne bien la seconde formule souhaitée.

Pour obtenir la première formule en général, dans le cas où $k < n$, il suffit de la déduire du cas $k = n$ en remarquant que le monôme d'indice $(i_1, \dots, i_k)$ dans $e_k(X_1, \dots, X_n)$ s'obtient en spécialisant $X_j = 0$ pour tout $j \notin \{i_1, \dots, i_k\}$, et qu'on obtient alors le monôme $e_k(X_{i_1}, \dots, X_{i_k})$. Si on spécialise de même le membre de droite de l'égalité souhaitée, on obtient

$$\sum_{i=1}^{k}(-1)^{i-1}e_{k-i}(X_{i_1}, \dots, X_{i_k})p_i(X_{i_1}, \dots, X_{i_k}) .$$

Or par le premier cas, on a bien

$$ke_k(X_{i_1}, \dots, X_{i_k}) = \sum_{i=1}^{k}(-1)^{i-1}e_{k-i}(X_{i_1}, \dots, X_{i_k})p_i(X_{i_1}, \dots, X_{i_k}) .$$

Cela assure que le monôme d'indice $(i_1, \dots, i_k)$ dans le membre de gauche est égal au monôme de même indice dans le membre de droite. Puisque les deux membres de l'égalité souhaitée sont clairement homogènes de degré k, cela assure la première formule dans le cas général. □

Une conséquence possible (utile par exemple dans la preuve du théorème de Burnside sur les sous-groupes d'exposant fini dans $\mathrm{GL}_n(\mathbf{C})$:

Corollaire 1.28. *Soit K un corps de caractéristique nulle (ou de caractéristique $> n$), soit $A \in M_n(K)$.*

Alors A est nilpotente si et seulement si pour tout $1 \leq k \leq n$, $\mathrm{tr}\,(A^k) = 0$.

Démonstration. Un sens est évident : si A est nilpotente, la trace de ses puissances est nulle. Montrons la réciproque : on suppose que pour tout $1 \leq k \leq n$, $\mathrm{tr}\,(A^k) = 0$. Notons $\lambda_1, \dots, \lambda_n$ les valeurs propres de A dans un corps de décomposition de son polynôme caractéristique.

Alors par hypothèse, pour tout $1 \leq k \leq n$, $\lambda_1^k + \dots + \lambda_n^k = 0$, i.e. $p_k(\lambda_1, \dots, \lambda_n) = 0$. Alors la proposition précédente assure que pour tout $1 \leq k \leq n$, $ke_k(\lambda_1, \dots, \lambda_n) = 0$. Comme K est de caractéristique $> n$, cela implique que $e_k(\lambda_1, \dots, \lambda_n) = 0$ pour tout $1 \leq k \leq n$. Donc le polynôme caractéristique de A s'écrit (voir la preuve précédente ou la proposition **??**) :

$$\prod_{k=1}^{n}(X - \lambda_k) = X^n + \sum_{k=0}^{n-1}(-1)^{n-k}e_{n-k}(\lambda_1, \dots, \lambda_n)X^k = X^n ,$$

ce qui assure que $A^n = 0$ par Cayley-Hamilton. □

Remarque 1.29. On peut également démontrer ce corollaire à l'aide d'un déterminant de Vandermonde.

On peut aussi utiliser ce théorème pour définir le discriminant d'un polynôme :

Proposition 1.30. *Soit K un corps (ou un anneau intègre) et $P = \sum_{i=0}^{n} a_i X^i \in K[X]$ de degré n. Soit L un corps contenant L tel que P soit scindé dans L de racines $\alpha_1, \ldots, \alpha_n \in L$.*

Alors $\mathrm{disc}(P) := a_{2n-2} \prod_{i<j}(\alpha_j - \alpha_i)^2$ est dans K, et il existe $\Delta \in \mathbf{Z}[X_1, \ldots, X_n]$ indépendant de P tel que $\mathrm{disc}(P) = \Delta(a_0, \ldots, a_n)$.

Proposition 1.31. *Soit A un anneau intègre et $P \in A[X]$.*

Alors P est à racines simples (dans un corps de décomposition) si et seulement si $\mathrm{disc}(P) \neq 0$ si et seulement si $(P, P') = 1$.

Exemples 1.32.
— Si $P = aX^2 + bX + c$ est de degré 2, alors $\mathrm{disc}(P) = b^2 - 4ac$.
— Si $P = X^3 + pX + q$ est de degré 3, alors $\mathrm{disc}(P) = -4p^3 - 27q^2$.

Théorème 1.33. *Soit $P \in \mathbf{R}[X]$ de degré n.*
— *Si $\mathrm{disc}(P) = 0$, alors P a une racine multiple dans $\mathbf{C}$.*
— *Si $\mathrm{disc}(P) > 0$, alors le nombre de racines réelles de P est congru à n modulo 4.*
— *Si $\mathrm{disc}(P) < 0$, alors le nombre de racines réelles de P est congru à $n-2$ modulo 4.*

1.4 Racines d'un polynôme ; relations coefficients-racines

Définition 1.34. Soit K un corps et $P \in K[X]$.

Un élément $\alpha \in K$ est dit racine de P si $P(\alpha) = 0$. On rappelle que cela équivaut à $X - \alpha$ divise P dans $K[X]$. La multiplicité de α comme racine de P est le plus grand entier $n \geq 1$ tel que $(X - \alpha)^n$ divise P.

Lemme 1.35. *Soit A un anneau intègre, $P \in A[X]$ un polynôme non constant de degré n. Soient $\alpha_1, \ldots, \alpha_k$ des racines distinctes de P dans A, de multiplicité respective $m_1, \ldots, m_k$. Alors $m_1 + \cdots + m_k \leq n$.*

Proposition 1.36. *Soit K un corps de caractéristique nulle. Soit $P \in K[X]$ et $\alpha \in K$. Alors α est racine de P de multiplicité m si et seulement si*
— *pour tout $0 \leq k \leq m-1$, $P^{(k)}(\alpha) = 0$.*
— *$P^{(m)}(\alpha) \neq 0$.*

Remarque 1.37. Le résultat est faux si la caractéristique p est inférieure ou égale à m. Seul le sens direct reste vrai. Par exemple, en caractéristique $p > 0$, le polynôme X^p admet 0 comme racine de multiplicité p, mais toutes ses dérivées évaluées en 0 sont nulles, y compris la dérivée p-ième car $p = 0$ dans K.

Proposition 1.38. *Soit K un corps, $P \in K[X]$ un polynôme unitaire de degré n, et $\alpha_1, \ldots, \alpha_n$ les racines de P.*

Alors $P = X^n + \sum_{k=0}^{n-1} (-1)^{n-k} e_{n-k}(\alpha_1, \ldots, \alpha_n) X^k$.

Démonstration. Il suffit de développer, et on peut utiliser une récurrence sur n. □

On le reformule souvent en disant que si $\alpha_1, \ldots, \alpha_n \in K$ sont toutes les racines d'un polynôme $P = \sum_{k=0}^{n} a_k X^k$ de degré n, alors pour tout k, $e_k(\alpha_1, \ldots, \alpha_n) = (-1)^k \frac{a_{n-k}}{a_n}$.

Quelques applications :

Définition 1.39. Un corps K est dit algébriquement clos si tout polynôme $P \in K[X]$ non constant est scindé, si et seulement si tout polynôme $P \in K[X]$ non constant a une racine dans K.

Théorème 1.40 (d'Alembert-Gauss)**.** *Le corps* $\mathbf{C}$ *est algébriquement clos.*

Démonstration. Soit $P \in \mathbf{C}[X]$ un polynôme non constant, de degré n. On cherche à montrer que P admet une racine dans $\mathbf{C}$.

On définit $Q := P\overline{P}$. Alors par construction $Q \in \mathbf{R}[X]$ car $\bar{Q} = Q$ et $\deg(Q) = 2n$.

Si Q admet une racine dans $\mathbf{C}$, alors P admet une racine dans $\mathbf{C}$. Il suffit donc de montrer que tout polynôme non constant de $\mathbf{R}[X]$ a une racine complexe. Soit $P \in \mathbf{R}[X]$ un polynôme non constant de degré n. Quitte à diviser par son coefficient dominant, on peut supposer P unitaire.

On peut écrire $n = 2^k m$ avec $k \geq 0$ et m impair. On raisonne par récurrence sur k.

- Si $k = 0$, alors P est un polynôme réel unitaire de degré impair, $\lim_{-\infty} P = -\infty$ et $\lim_{+\infty} P = +\infty$. Puisque la fonction associée à P est continue, le théorème des valeurs intermédiaires assure que P a une racine réelle.
- Suposons maintenant $k \geq 1$ et le théorème démontré pour tous les polynômes de degré $2^i m'$ avec m' impair et $i < k$. Il existe une extension finie K de $\mathbf{R}$ dans laquelle P est scindé (par exemple, un corps de décomposition de P sur $\mathbf{R}$). On note $x_1, \dots, x_n$ ses racines. Pour tout $\lambda \in \mathbf{R}$ et tout $1 \leq i < j \leq n$, on définit $y_{i,j}(\lambda) := x_i + x_j + \lambda x_i x_j \in K$. On construit alors le polynôme $P_\lambda := \prod_{1 \leq i < j \leq n} (X - y_{i,j}(\lambda)) \in K[X]$. Pour tout $i < j$, $x_{i,j}(\lambda)$ est une fonction symétrique de x_i et x_j, et plus généralement, le polynôme $P_\lambda(X_1, \dots, X_n, X) := \prod_{1 \leq i < j \leq n} (X - (X_i + X_j + \lambda X_i X_j))$ est symétrique en $(X_1, \dots, X_n)$, i.e. dans $\mathbf{R}[X][X_1, \dots, X_n]$. Donc par le théorème de structure des polynômes symétriques, il existe un polynôme $Q_\lambda(X_1, \dots, X_n, X) \in \mathbf{R}[X_1, \dots, X_n, X]$ tel que
$$P_\lambda(X_1, \dots, X_n, X) = Q_\lambda(e_1(X_1, \dots, X_n), \dots, e_n(X_1, \dots, X_n), X)\,.$$
En particulier, en évaluant en les x_i, on obtient que $P_\lambda(X) = Q_\lambda(e_1(x_1, \dots, x_n), \dots, e_n(x_1, \dots, x_n), X$
Or pour tout i, $e_i(x_1, \dots, x_n)$ est au signe près un coefficient de P (voir la proposition 1.38), donc $e_i(x_1, \dots, x_n) \in \mathbf{R}$, donc $P_\lambda(X) \in \mathbf{R}[X]$ (car Q_λ est à coefficients réels). Or le degré de P_λ vaut $\frac{n(n-1)}{2} = 2^{k-1} m(n-1)$, avec $m(n-1)$ impair. Par conséquent, on peut appliquer l'hypothèse de récurrence à P_λ : il existe une racine $z_\lambda \in \mathbf{C}$ de P_λ.

□

Théorème 1.41 (Kronecker)**.** *Soit* $P \in \mathbf{Z}[X]$ *un polynôme unitaire dont toutes les racines dans* $\mathbf{C}$ *sont de module* ≤ 1*. Alors les racines de* P *sont soit nulles, soit des racines de l'unité.*

De façon équivalente, un entier algébrique dont tous les conjugués sont de module ≤ 1 est soit nul, soit une racine de l'unité.

Démonstration. □

2 Anneaux factoriels

2.1 Généralités ; lien avec les anneaux principaux

La notion d'anneau factoriel généralise les notions d'anneau euclidien et d'anneau principal étudiées dans la première partie de ce cours.

Définition 2.1. Soit A un anneau commutatif intègre. On dit que A est factoriel si les deux conditions suivantes son vérifiées :

(E) Pour tout $a \in A \setminus \{0\}$, si a n'est pas inversible, il existe des éléments irréductibles $p_1, \dots, p_r \in A$ tels que $a = p_1 \dots p_r$.

(U) Pour tous $p_1, \dots, p_r, q_1, \dots, q_s \in A$ irréductibles, si $p_1 \dots p_r = q_1 \dots q_s$, alors $r = s$ et il existe une permutation $\sigma \in \mathfrak{S}_r$ telle que pour tout $1 \leq i \leq r$, $p_{\sigma(i)}$ et q_i sont associés.

Autrement dit, la première condition exprime l'existence d'une décomposition en produit d'éléments irréductibles, et la seconde son unicité aux inversibles près.

Exemples 2.2. Les anneaux $\mathbf{Z}$ et $K[X]$ sont factoriels.

Remarque 2.3. L'existence (E) d'une décomposition en irréductible est vérifiée dans tout anneau noethérien, i.e. tel que tout idéal soit engendré par un nombre fini d'éléments. C'est donc vrai dans une grande généralité. La condition contraignante (et très utile) est l'unicité (U) de la décomposition.

Proposition 2.4. *Soit A un anneau commutatif intègre, telle que (E) soit vérifiée. Alors les assertions suivantes sont équivalentes :*

1. *A est factoriel (i.e. A vérifie (U)).*
2. *Tout élément irréductible de A est premier.*
3. *A vérifie le lemme d'Euclide.*
4. *A vérifie le lemme de Gauss.*

Démonstration.

— Remarquons d'abord que dans tout anneau intègre, le lemme de Gauss implique le lemme d'Euclide. Supposons en effet le premier, et soit $p \in A$ irréductible, et $a, b \in A$ tels que p divise ab. Si p ne divise pas a, alors p est premier avec a (en effet, tout diviseur d de p est soit inversible, soit associé à p, et comme p ne divise pas a, tout diviseur d commun à a et p est inversible). Donc par le lemme de Gauss, p divise b, ce qui démontre le lemme d'Euclide.

— On suppose désormais que A vérifie (E). On suppose le lemme d'Euclide (i.e. la propriété 3). Montrons le lemme de Gauss. Soient $a, b, c \in A$ tels que a divise bc et a et b sont premiers entre eux. Si a est inversible, on a bien que a divise c. Sinon, par la propriété (E), il existe des décompositions en irréductibles $a = p_1 \dots p_r$, $c = q_1 \dots q_s$. Comme a est premier avec b, p_r ne divise pas b, donc par Euclide, p_r divise c, donc l'un des q_i. Donc p_r et q_i sont associés. Par récurrence sur r, on en déduit que $r \leq s$ et a divise c, d'où le lemme de Gauss.

— Les propriétés 2 et 3 sont clairement équivalentes (en général).

— Il reste à montrer que 1 et 3 sont équivalents. Supposons que A est factoriel. Soient p irréductible et $a, b \in A$ tels que p divise ab. Il existe $c \in A$ tel que $ab = pc$. En écrivant les décompositions en irréductibles de a, b et c, la propriété (U) assure que p divise a ou b, d'où le lemme d'Euclide.

Réciproquement, supposons le lemme d'Euclide. Soient $p_1 \dots p_r = l_1 \dots l_s$ deux décompositions en irréductibles. Par le lemme d'Euclide, p_r divise l'un des l_i, donc p_r et l'un des l_i sont associés. Après division par p_r, on obtient deux décompositions égales de tailles strictement inférieures. Une récurrence sur r permet de conclure à la véracité de (U).

□

L'exemple suivant est fondamental :

Théorème 2.5. *Tout anneau principal est factoriel.*

Démonstration. cf plus haut. □

Exemples 2.6.

1. l'anneau intègre $\mathbf{Z}[i\sqrt{5}]$ n'est pas factoriel (il vérifie (E) et pas (U)). Par exemple, on peut utiliser les décompositions $2 \cdot 3 = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$.
2. l'anneau intègre $K[X,Y]/(Y^2 - X^3)$ est intègre, mais n'est pas factoriel (il vérifie (E) et pas (U)).
3. $K[X,Y]$ et $\mathbf{Z}[X]$ sont factoriels (preuve plus loin) non principaux.
4. L'anneau des fonctions entières (holomorphes sur $\mathbf{C}$) est intègre et ne vérifie par la propriété (E) (par exemple, la fonction sin ne se décompose pas comme un produit de fonctions holomorphes irréductibles). De même, l'anneau $\bigcup_{n \geq 1} K[X^{\frac{1}{2^n}}]$ est intègre et ne vérifie pas (E) (par exemple, l'élément X ne se décompose en produit fini d'irréductibles).

2.2 Pgcd, ppcm

On a déjà défini précédemment la notion de pgcd et de ppcm dans un anneau commutatif quelconque.

Proposition 2.7. *Soit A un anneau euclidien. Soient $a = up_1^{\alpha_1} \dots p_r^{\alpha_r}$ et $b = vp_1^{\beta_1} \dots p_r^{\beta_r}$ deux éléments de A avec leur décomposition en produit de puissances d'irréductibles deux-à-deux non associés ($\alpha_i; \beta_i \geq 0$).*

Alors a et b admettent des pgcd et des ppcm, que l'on peut calculer ainsi :

$$\mathrm{pgcd}(a,b) = p_1^{\min(\alpha_1,\beta_1)} \dots p_r^{\min(\alpha_r,\beta_r)}$$

et

$$\mathrm{ppcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} \dots p_r^{\max(\alpha_r,\beta_r)}.$$

Remarque 2.8. Cette proposition fournit un algorithme théorique pour calculer pgcd et ppcm, nécessitant de calculer les décompositions de a et b en produits d'irréductibles. Cet algorithme est très inefficace dans un anneau euclidien, où l'algorithme d'Euclide est nettement plus rapide.

2.3 Contenu d'un polynôme et applications

Définition 2.9. Soit A un anneau factoriel, et $P = \sum_{i=0}^{n} a_i X^i \in A[X]$. On définit le contenu de P, et on note $C(P)$, la quantité suivante :

$$C(P) := \mathrm{pgcd}(a_0, \dots, a_n)\,.$$

On dit que P est primitif si $C(P) = 1$.

On voit par exemple que pour tout $a \in A$, et tout $P \in A[X]$, on a $C(aP) = aC(P)$.

Lemme 2.10 (contenus de Gauss)**.** *Soit $P, Q \in A[X]$. Alors $C(PQ) = C(P)C(Q)$.*

Démonstration. Supposons d'abord que $C(P) = C(Q) = 1$.

Soit p un élément irréductible de A. Par définition, les images $\bar{P}$ et $\bar{Q}$ de P et Q dans $A[X]/(p) \cong (A/(p))[X]$ sont non nulles. Or $A/(p)$ est intègre (car (p) est premier), donc $(A/(p))[X]$ est intègre, donc $\bar{P}\bar{Q} \neq 0$, donc $\overline{PQ} \neq 0$ dans $A/(p)[X]$. Cela assure que p ne divise pas $C(PQ)$.

Cela prouve que $C(PQ) = 1$ (car il n'admet aucun diviseur irréductible).

Revenons au cas général. Il existe des polynômes primitifs $P_1, Q_1 \in A[X]$ tels que $P = C(P)P_1$ et $Q = C(Q)Q_1$. Donc par le premier point, on sait que $C(P_1Q_1) = 1$. On en déduit que

$$C(PQ) = C(C(P)P_1C(Q)Q_1) = C(P)C(Q)C(P_1Q_1) = C(P)C(Q)\,,$$

ce qui conclut la preuve. $\square$

Ce lemme permet de décrire les éléments irréductibles de l'anneau $A[X]$, et de faire le lien avec les irréductibles de $K[X]$.

Corollaire 2.11. *Soit A un anneau factoriel de corps des fractions égal à K.*

Les éléments irréductibles de $A[X]$ sont exactement

— *les irréductibles de A (vus comme polynômes constants).*

— *les polynômes primitifs de $A[X]$ qui sont irréductibles dans $K[X]$.*

Démonstration. Puisque A est intègre, pour tout $p \in A$, p est irréductible dans A si et seulement si p est irréductible dans $A[X]$ (le degré d'un produit est la somme des degrés).

Soit $P \in A[X]$ non constant. Si P n'est pas primitif, alors il existe $Q \in A[X]$ tel que $P = C(P)Q$, avec $C(P), Q \notin A[X]^\times = A^\times$, donc P n'est pas irréductible. Supposons que P est primitif. Si P est irréductible dans $K[X]$, et $P = QR$ dans $A[X]$, alors Q ou R est inversible dans $K[X]$, donc constant. Donc Q ou R est dans A. Comme P est primitif, Q ou R est inversible dans A, ce qui assure que P est irréductible. Réciproquement, supposons P irréductible dans $A[X]$. Soient $Q, R \in K[X]$ tels que $P = QR$. Il existe $q, r \in A \setminus \{O\}$ tels que $qQ, rR \in A[X]$. Alors $qrP = (qQ)(rR)$. Donc le lemme des contenus assure que $qr = C(qQ)C(rR)$. Donc $P = \frac{qQ}{C(qQ)} \frac{rR}{C(rR)}$ dans $A[X]$. Puisque P est irréductible dans $A[X]$, l'un des deux polynômes $\frac{qQ}{C(qQ)}$ ou $\frac{rR}{C(rR)}$ est constant, donc Q ou R est constant. Cela assure que P est irréductible dans $K[X]$. $\square$

2.4 Théorème de transfert

Le résultat suivant est une autre application du lemme des contenus de Gauss :

Théorème 2.12 (Gauss)**.** *Soit A un anneau factoriel. Alors $A[X]$ est factoriel.*

Démonstration. L'anneau $A[X]$ est bien intègre.

Prouvons d'abord la propriété d'existence (E). Soit $P \in A[X]$ non nul, non inversible. On a deux cas :

— si $\deg(P) = 0$, alors $P \in A$ non nul et non inversible. Comme A est factoriel, P est produit d'irréductibles de A, donc de $A[X]$ par le corollaire.

— si $\deg(P) > 0$. Alors il existe $P_1 \in A[X]$ primitif tel que $P = C(P)P_1$. Comme $K[X]$ est factoriel, il existe $Q_1, \dots, Q_r \in K[X]$ irréductibles tels que $P_1 = Q_1 \dots Q_r$. Pour tout i, il existe $q_i \in A \setminus \{0\}$ tel que $q_i Q_i \in A[X]$. Alors $(q_1 \dots q_r)P_1 = (q_1Q_1) \dots (q_rQ_r)$ dans $A[X]$. Par le lemme des contenus, $q_1 \dots q_r = C(q_1Q_1) \dots C(q_rQ_r)$, donc $P_1 = \frac{q_1Q_1}{C(q_1Q_1)} \cdots \frac{q_rQ_r}{C(q_rQ_r)}$ dans $A[X]$. En outre, pour tout i, $\frac{q_iQ_i}{C(q_iQ_i)}$ est irréductible dans $K[X]$ (car associé à Q_i) et primitif, donc $\frac{q_iQ_i}{C(q_iQ_i)}$ est irréductible dans $A[X]$ par le corollaire. En décomposant également $C(P)$ en produit d'irréductibles dans A, on obtient que P est produit d'irréductibles dans $A[X]$. D'où la propriété (E).

Montons maintenant l'unicité (U). Soient $p_1, \dots, p_r, q_1, \dots, q_s \in A$ irréductibles, $P_1, \dots, P_R, Q_1, \dots, Q_S \in A[X]$ primitifs et irréductibles dans $K[X]$. Supposons que $p_1 \dots p_r P_1 \dots P_R = q_1 \dots q_s Q_1 \dots Q_S$. Par le lemme des contenus, on a $p_1 \dots p_r = q_1 \dots q_s$ dans A, donc comme A vérifie (U), on a $r = s$ et quitte à permuter les q_i, on a p_i et q_i sont associés (dans A) pour tout i. Donc $P_1 \dots P_R = uQ_1 \dots Q_S$ pour un certain $u \in A^\times$. Comme $K[X]$ vérifie (U) et les P_i, Q_j sont irréductibles dans $K[X]$, on en déduit que $R = S$ et à permutation près, pour tout i, $Q_i = \lambda_i P_i$ pour certains $\lambda_i \in K^\times$. Aurtement dit, il existe $a_i, b_i \in A$ non nuls tels que $b_iQ_i = a_iP_i$. Or P_i et Q_i sont primitifs, donc en calculant les contenus, a_i et b_i sont associés dans A, donc P_i et Q_i sont associés dans $A[X]$. Cela termine la preuve de (U).

Donc $A[X]$ est bien factoriel. □

Une récurrence simple démontre le corollaire suivant :

Corollaire 2.13. *Si A est factoriel, $A[X_1, \dots, X_n]$ est factoriel. Par exemple, $K[X_1, \dots, X_n]$ est factoriel, non principal si $n \geq 2$.*

2.5 Critères d'irréductibilité

Dans cette partie, on rappelle et établit certains critères d'irréductibilité de polynômes en une variable sur un corps ou sur un anneau factoriel.

Le premier énoncé est évident, nous en verrons une généralisation dans le chapitre sur les extensions de corps.

Proposition 2.14. *Soit K un corps et $P \in K[X]$ un polynôme non constant de degré 2 ou 3.*

Alors P est irréductible si et seulement si P n'admet pas de racine dans K.

Démonstration. Si P est réductible, il existe $Q, R \in K[X]$ non constants tels que $P = QR$. Alors les hypothèses assure que Q ou R est de degré 1, donc il a une racine, donc P a une racine. La réciproque est évidente. □

Une méthode importante pour montrer l'irréductiblité de certains polynômes sur un anneau est la méthode de réduction modulo un idéal.

Proposition 2.15. *Soit A un anneau intègre, et I un idéal de A. Soit $P \in A[X]$ et $\bar{P}$ son image dans $(A/I)[X]$. On suppose que le coefficient dominant de P est inversible dans A.*

Si $\bar{P}$ est irréductible dans $(A/I)[X]$, alors P est irréductible dans $A[X]$.

Démonstration. Soient $Q, R \in A[X]$ tels que $P = QR$. Alors $\bar{P} = \bar{Q}\bar{R}$ dans $(A/I)[X]$. Comme $\bar{P}$ est irréductible, on peut supposer que $\bar{Q}$ est un polynôme constant inversible, i.e. $\bar{Q} \in (A/I)^\times$. Par hypothèse sur le coefficient dominant de P, Q est un polynôme constant, et il est inversible dans A. Cela assure que P est irréductible dans $A[X]$. $\square$

Exemples 2.16.
1. le polynôme $X^3 + 5X^2 - 7X + 3$ est irréductible dans $\mathbf{Q}[X]$ (réduire modulo 2).
2. le polynôme $X^5 + X^2 + X + 2$ est irréductible dans $\mathbf{Q}[X]$ (réduire modulo 2 et 3).
3. le polynôme $X^4 + 1$ est irréductible dans $\mathbf{Q}[X]$, mais réductible dans $\mathbf{F}_p[X]$ pour tout nombre premier p.

Le critère suivant est extrêmement utile.

Théorème 2.17 (Critère d'irréductibilité d'Eisenstein)**.** *Soit A un anneau factoriel de corps des fractions K. Soit $P = \sum_{i=0}^n a_i X^i \in A[X]$ $p \in A$ un élément irréductible. On suppose que $p | a_i$ pour tout $0 \leq i \leq n-1$, $p \not| a_n$ et $p^2 \not| a_0$.*

Alors P est irréductible dans $K[X]$.

Si de plus $C(P) = 1$, alors P est irréductible dans $A[X]$.

Démonstration. Soit $P = QR$ avec $Q, R \in \mathbf{A}[X]$. En réduisant modulo p, on obtient $\bar{P} = \bar{Q}\bar{R}$ dans $(A/P)[X]$. Or par hypothèse $\bar{P} = \overline{a_n} X^n$, avec $\overline{a_n} \neq 0$ dans A/p. Comme A/p est intègre, on en déduit que $\bar{Q}$ et $\bar{R}$ sont des monômes, i.e. il existe $m, k \in \mathbf{N}$ tels que $\bar{Q} = \overline{q_m} X^m$, $\bar{R} = \overline{r_k} X^k$, $q_m r_k = a_n$ et $m + k = n$. Or $p^2 \not| a_0$, donc $p \not| q_0$ ou $p \not| r_0$. Par conséquent, on a $m = 0$ ou $k = 0$, i.e. P ou R est constant dans $A[X]$.

Finalement, P n'admet pas de décomposition QR avec Q et R non constants dans $A[X]$. Par le lemme des contenus, cela assure que P est irréductible dans $K[X]$.

Le second point de l'énoncé découle également du lemme des contenus. $\square$

Voici quelques applications de ce critère :

Exemples 2.18.
1. Pour tout p premier et tout $n \geq 1$, le polynôme $X^n - p$ est irréductible dans $\mathbf{Q}[X]$. En particulier, il existe des polynômes irréductibles de tout degré sur $\mathbf{Q}$.
2. Si p est un nombre premier, et $n \geq 1$, le polynôme cyclotomique ϕ_{p^n} est irréductible dans $\mathbf{Q}[X]$ (cf plus bas). Il suffit d'appliquer Eisenstein à $\phi_{p^n}(X+1)$.

3 Extensions de corps

3.1 Généralités

La notation suivante sera utile dans la suite :

Définition 3.1. Soit $A \to B$ un morphisme injectif d'anneaux commutatifs unitaires (i.e. B est une A-algèbre). Pour toute partie $P \subset B$, on note $A[P]$ le sous-A-algèbre de B engendrée par A et P. Concrètement,

$$A[P] := \{Q(x_1, \ldots, x_n), n \in \mathbf{N}, Q \in A[X_1, \ldots, X_n], x_i \in P, \} .$$

En particulier, si $b_1, \ldots, b_n \in B$, on a ainsi défini la sous-algèbre $A[b_1, \ldots, b_n]$ comme l'image du morphisme d'évaluation $\mathrm{ev}_{\underline{b}} : A[X_1, \ldots, X_n] \to B$ défini par $\mathrm{ev}_{\underline{b}}(Q) := Q(b_1, \ldots, b_n)$.

On dit par exemple qu'une A-algèbre B est de type fini s'il existe $n \geq 1$ et $x_1, \ldots, x_n \in B$ tels que $B = A[x_1, \ldots, x_n]$.

On rappelle qu'un corps est un anneau commutatif (non nul) unitaire tel que tout élément non nul est inversible. On dispose de notions évidentes de sous-corps et de morphisme de corps.

On rappelle qu'un corps K admet exactement deux idéaux, à savoir $\{0\}$ et K. Réciproquement, tout anneau commutatif unitaire admettant exactement deux idéaux est un corps.

On rappelle également la construction suivante :

Définition 3.2. Soit A anneau commutatif intègre. On définit $K := \{(a, b) \in K \times K^\times\} / \sim$, où $\sim$ est la relation d'équivalence définie par $(a, b) \sim (a', b')$ si et seulement si $ab' = a'b$.

Alors K, muni des deux opérations suivantes :
— $(a, b) + (a', b') := (ab' + a'b, bb')$
— $(a, b) \cdot (a', b') := (aa', bb')$

est un corps, appelé corps des fractions de A et noté $\mathrm{Frac}(A)$. L'application naturelle $A \to K$ définie par $a \mapsto (a, 1)$ est un morphisme injectif d'anneaux.

En outre, K est le plus petit corps contenant A, au sens de la propriété universelle évidente. Par exemple, $\mathrm{Frac}(\mathbf{Z}) = \mathbf{Q}$ et $\mathrm{Frac}(K[X]) = K(X)$. Le corps des fractions de l'anneau des fonctions holomorphes sur $\mathbf{C}$ est le corps des fonctions méromorphes sur $\mathbf{C}$.

Lemme 3.3. *Soient K un corps et A un anneau unitaire.*
Tout morphisme d'anneaux $\varphi : K \to A$ est injectif.

Démonstration. Le noyau $\ker(\varphi)$ est un idéal de K, il est donc égal à $\{0\}$ ou à A. Comme $\varphi(1) = 1$, le morphisme φ n'est pas nul, donc $\ker(\varphi) = \{0\}$, donc φ est injectif. □

On rappelle la définition de la caractéristique d'un anneau :

Définition 3.4. Soit A un anneau commutatif unitaire. On dispose d'un morphisme d'anneaux naturel $\mathbf{Z} \to A$ défini par $n \mapsto n1$, où $n1 := 1 + \cdots + 1$ (n fois) si $n \geq 0$, et $n1 = 1 + \cdots + 1$ ($-n$ fois) si $n < 0$.

Alors le noyau de ce morphisme est un idéal de $\mathbf{Z}$, de la forme $n\mathbf{Z}$ pour un unique $n \in \mathbf{N}$. Cet entier n est appelé la caractéristique de l'anneau A.

Proposition 3.5. *Soit K un corps (ou plus généralement un anneau intègre).*
Alors la caractéristique de K est soit nulle, soit un nombre premier.

Proposition 3.6. *Soit K un corps de caractéristique $p \geq 0$.*
— *si $p = 0$, alors le sous-corps de K engendré par 1 est canoniquement isomorphe à $\mathbf{Q}$.*

— *si $p > 0$, alors le sous-corps de K engendré par 1 est canoniquement isomorphe à $\mathbf{Z}/p\mathbf{Z}$.*

Ce sous-corps est appelé sous-corps premier de K.

En caractéristique positive, un corps est naturellement muni d'un morphisme supplémentaire, reposant sur le lemme suivant :

Lemme 3.7. *Soit p un nombre premier et $1 \leq k \leq p$.*
Alors p divise $\binom{p}{k}$.

Définition 3.8. Soit K un corps de caractéristique positive.
Alors l'application $K \to K$ définie par $x \mapsto x^p$ est un morphisme de corps, appelé morphisme de Frobenius de K. En particulier, $(x+y)^p = x^p + y^p$ pour tous $x, y \in K$.

Intéressons-nous maintenant à la notion d'extension de corps.

Définition 3.9. Une extension de corps est la donnée de deux corps K et L et d'un morphisme de corps (injectif) $i : K \to L$. On la note L/K.

Remarque 3.10. En identifiant K à l'image du morphisme i, on peut voir K comme un sous-corps de L. La plupart du temps, on n'explicitera pas le morphisme i, et on verra K comme un sous-corps de L.

Exemples 3.11.
1. K est une extension de K (l'extension triviale).
2. $\mathbf{C}/\mathbf{R}$ est une extension de corps, comme $\mathbf{C}/\mathbf{Q}$, $\mathbf{R}/\mathbf{Q}$, $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ ou $\mathbf{Q}(i)/\mathbf{Q}$.
3. Si p est un nombre premier et $n \geq 1$, $\mathbf{F}_{p^n}/\mathbf{F}_p$ est une extension de corps (cf plus loin).
4. Si K est un corps, $K(X)/K$ est une extension de corps.

On dispose aussi d'une notion évidente de sous-extension.

Définition 3.12. Soit L/K une extension de corps. Si $P \subset L$ est une partie, on note $K(P)$ la plus petite sous-extension de L/K contenant P, i.e. le sous-corps de L engendré par K et P.
Si $P = \{x_1, \ldots, x_n\}$, on définit ainsi le sous-corps $K(x_1, \ldots, x_n)$ de L comme le sous-corps de L engendré par K et les x_i.

Plus concrètement,

$$K(x_1, \ldots, x_n) = \left\{ \frac{P(x_1, \ldots, x_n)}{Q(x_1, \ldots, x_n)}, P, Q \in K[X_1, \ldots, X_n], Q(x_1, \ldots, x_n) \neq 0 \right\} .$$

Définition 3.13. Une extension L/K est dite de type fini s'il existe $x_1, \ldots, x_n \in L$ tels que $L = K(x_1, \ldots, x_n)$. On dit que l'extension est monogène si l'on peut trouver $\alpha \in L$ tel que $L = K(\alpha)$.

La proposition suivante est évidente, mais très utile :

Proposition 3.14. *Si L/K est une extension de corps, la loi de composition externe $K \times L \to L$ donnée par $\lambda \cdot x := i(\lambda)x$ munit K d'une structure de K-espace vectoriel (et même de K-algèbre).*

Définition 3.15. Si L/K est une extension de corps, on appelle degré de L sur K et on note $[L : K]$ la dimension de L comme K-espace vectoriel. On dit que l'extension est finie si cette dimension est finie. Une extension finie est en particulier de type fini.

Exemples 3.16.

1. $[K : K] = 1$.
2. $[\mathbf{C} : \mathbf{R}] = 2$ car une $\mathbf{R}$-base de $\mathbf{C}$ est donnée par $(1, i)$. $\mathbf{C}/\mathbf{Q}$ et $\mathbf{R}/\mathbf{Q}$ sont de degré infini et ne sont pas de type fini (le vérifier), alors que $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ ou $\mathbf{Q}(i)/\mathbf{Q}$ sont de degré 2.
3. Si p est un nombre premier et $n \geq 1$, $[\mathbf{F}_{p^n} : \mathbf{F}_p] = n$.
4. Si K est un corps, $K(X)/K$ est une extension infinie, mais de type fini (et même monogène).

Un résultat fondamental sur les extensions finies est le suivant :

Théorème 3.17 (de la base téléscopique)**.** *Soit M/K une extension de corps, et L/K une sous-extension (on voit cela comme deux sous-corps de L, i.e. $K \subset L \subset M$). On suppose que M/K et L/M sont des extensions finies.*

Alors L/K est une extension finie, et

$$[L : K] = [L : M][M : K]\,.$$

Plus précisément, si $(m_1, \ldots, m_n)$ est une K-base de M et $(l_1, \ldots, l_k)$ est une M-base de L, alors $(m_i l_j)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq k}}$ est une K-base de L.

Démonstration. Soit $x \in M$. Par hypothèse, il existe $\lambda_1, \ldots, \lambda_n \in L$ tels que $x = \sum_{i=1}^n \lambda_i m_i$. Pour tout $1 \leq i \leq n$, $\lambda_i \in L$, donc il existe $\mu_{i,1}, \ldots, \mu_{i,k} \in K$ tels que $\lambda_i = \sum_{j=1}^k \mu_{i,j} l_j$. Alors finalement $x = \sum_{i=1}^n \sum_{j=1}^k \mu_{i,j} m_i l_j$. Donc la famille est bien génératrice.

Soient $\mu_{i,j} \in K$ tels que $\sum_{i=1}^n \sum_{j=1}^k \mu_{i,j} m_i l_j = 0$. En écrivant $\sum_{i=1}^n \left(\sum_{j=1}^k \mu_{i,j} l_j \right) m_i = 0$, puisque (m_i) est libre sur L, on en déduit que pour tout $1 \leq i \leq n$, $\sum_{j=1}^k \mu_{i,j} l_j = 0$. Or (l_j) est libre sur K, donc pour tout $1 \leq j \leq k$, $\mu_{i,j} = 0$. Donc la famille est libre. $\square$

3.2 Éléments algébriques et transcendants

Les notions d'extensions de corps et de polynômes en une indéterminée sont très liées. Dans cette direction, nous introduisons les définitions suivantes :

Définition 3.18. Soit L/K une extension de corps. Un élément $\alpha \in L$ est dit algébrique sur K s'il existe $P \in K[X]$ non nul tel que $P(\alpha) = 0$. Dans le cas contraire, α est dit transcendant sur K.

Définition 3.19. L'extension L/K est dite algébrique si tout élément de L est algébrique sur K.

Exemples 3.20.

1. Dans l'extension $\mathbf{C}/\mathbf{R}$, l'élément i est algébrique, et $\mathbf{C}/\mathbf{R}$ est algébrique.
2. Dans l'extension $\mathbf{C}/\mathbf{Q}$, les racines de l'unité $e^{\frac{2ik\pi}{n}}$ sont algébriques.
3. Dans l'extension $\mathbf{R}/\mathbf{Q}$, les nombres π et e sont transcendants (difficile !). Plus facile (cf plus loin), le nombre de Liouville $\sum_{n \geq 1} 10^{-n!}$ est transcendant. Donc $\mathbf{R}/\mathbf{Q}$ n'est pas algébrique.

4. Dans l'extension $K(X)/K$, l'élément X est transcendant sur K. Donc cette extension n'est pas algébrique.

Proposition 3.21. *Soit $(a_n) \in \mathbf{Z}^{\mathbf{N}}$ une suite d'entiers, bornée, non stationnaire à* 0. *Soit $b \geq 2$ entier.*

Alors $\theta := \sum_{n=0}^{+\infty} \frac{a_n}{b^{n!}}$ est transcendant.

Remarque 3.22. Puisque l'ensemble des suites bornées d'entiers relatifs à support infini est non dénombrable (l'ensemble $\{1, 2\}^{\mathbf{N}}$ est déjà non dénombrable), cela permet de construire une famille explicite non dénombrable de nombres transcendants. Ces nombres sont appelés les nombres de Liouville.

Le plus "simple" de ces nombres est sans doute

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{1}{10^{n!}} = \quad & 0,11000100000000000000000100000000000000000000000000000000000000000000000000000000\\ & 00000000000000000000000000000000000000000000100000000000000000000000000000000\dots\end{aligned}$$

Démonstration. On commence par montrer le lemme suivant, qui affirme que les nombres algébriques sont mal approximables par des nombres rationnels :

Lemme 3.23. *Soit $\alpha \in \mathbf{R}$ tel qu'il existe une constante $K > 0$ et une suite de rationnels $(\frac{p_n}{q_n})_{n \in \mathbf{N}}$ deux-à-deux distincts tels que $|\alpha - \frac{p_n}{q_n}| \leq \frac{K}{q_n^n}$.*

Alors α est transcendant (sur $\mathbf{Q}$).

Démonstration. On raisonne par l'absurde : supposons α algébrique (sur $\mathbf{Q}$). Alors il existe un polynôme $P(X) = a_d X^d + \cdots + a_0 \in \mathbf{Z}[X]$ tel que $P(\alpha) = 0$. Puisque P n'a qu'un nombre fini de racines, il existe $\epsilon > 0$ tel que P ne s'annule pas sur $[\alpha - \epsilon; \alpha + \epsilon] \setminus \{\alpha\}$. Donc si $\frac{p}{q} \neq \alpha \in \mathbf{Q} \cap [\alpha - \epsilon; \alpha + \epsilon]$, $P(\frac{p}{q}) \neq 0$, donc

$$|P(\frac{p}{q})| = \left| \frac{a_d p^d + a_{d-1} p^{d-1} q + \cdots + a_0 q^d}{q^d} \right| \neq 0\,.$$

Or le numérateur de cette fraction est un entier non nul, donc

$$|P(\frac{p}{q})| \geq \frac{1}{q^d}\,.$$

En outre, le théorème des accroissements finis assure qu'il existe $M \in \mathbf{R}$ tel que pour $\frac{p}{q} \in \mathbf{Q} \cap [\alpha - \epsilon; \alpha + \epsilon]$,

$$|P(\frac{p}{q})| = |P(\frac{p}{q}) - P(\alpha)| \leq M |\alpha - \frac{p}{q}|\,.$$

Donc finalement pour $\frac{p}{q} \neq \alpha \in \mathbf{Q} \cap [\alpha - \epsilon; \alpha + \epsilon]$, $\frac{1}{Mq^d} \leq |\alpha - \frac{p}{q}|$. Or la suite $(\frac{p_n}{q_n})$ converge vers α, donc pour tout n assez grand, on a

$$\frac{1}{M q_n^d} \leq |\alpha - \frac{p_n}{q_n}| \leq \frac{K}{q_n^n}\,.$$

Ceci est contradictoire puisque (q_n) tend vers l'infini. Donc on en déduit que α n'est pas algébrique, donc α est transcendant. □

Notons $A := \max\{|a_n|, n \in \mathbf{N}\}$. Soit $N \in \mathbf{N}$ tel que $a_N \neq 0$. Posons $p_N := \sum_{n=0}^N a_n b^{N!-n!}$ et $q_N := b^{N!}$. Alors $\theta - \frac{p_N}{q_N} = \sum_{j=1}^\infty \frac{a_{N+j}}{b^{(N+j)!}}$. Or pour tout $j \geq 2$, on a $(N+j)! - (N+1)! \geq j$, donc

$$\left|\sum_{j=1}^\infty \frac{a_{N+j}}{b^{(N+j)!}}\right| \leq \frac{A}{b^{(N+1)!}} \sum_{j \geq 0} \frac{1}{b^j} \leq \frac{Ab}{(b-1)b^{(N+1)!}} .$$

Donc

$$\left|\theta - \frac{p_N}{q_N}\right| \leq \frac{Ab}{(b-1)b^{(N+1)!}} = \frac{Ab}{(b-1)q_N^{N+1}} \leq \frac{Ab}{(b-1)q_N^N} .$$

On conclut alors avec le lemme précédent que θ est transcendant. □

La définition suivante est analogue à celle du polynôme minimal d'un endomorphisme :

Définition 3.24. Soit L/K une extension de corps, et $\alpha \in L$.

On dispose d'un morphisme de K-algèbres $\mathrm{ev}_\alpha : K[X] \to L$ défini par $P \mapsto P(\alpha)$.

L'ensemble des polynômes de $K[X]$ annulant α est un idéal de $K[X]$, égal au noyau de ev_α. On appelle polynôme minimal de α le générateur unitaire de cet idéal, noté π_α.

En particulier, α est transcendant si et seulement si ev_α est injectif.

Si α est transcendant, on a un isomorphisme de K-algèbres $K[X] \xrightarrow{\sim} K[\alpha]$, et si α est algébrique, on a un isomorphisme $K[X]/(\pi_\alpha) \xrightarrow{\sim} K[\alpha]$.

La proposition suivante est fausse dans le contexte des endomorphismes, car l'anneau des endomorphismes n'est pas intègre en général.

Proposition 3.25. *Soit $\alpha \in L$ un élément algébrique sur K.*

Alors le polynôme minimal de α est irréductible dans $K[X]$.

Démonstration. Soient $P, Q \in K[X]$ tels que $\pi_\alpha = PQ$. Alors en évaluant en α, on obtient $0 = P(\alpha)Q(\alpha)$. Donc $P(\alpha) = 0$ ou $Q(\alpha) = 0$. Par minimalité de π_α, on en déduit que π_α divise P ou Q, donc P ou Q est inversible, donc π_α est irréductible. □

Exemples 3.26.
1. Le polynôme minimal de i sur $\mathbf{Q}$ (ou sur $\mathbf{R}$) est $X^2 + 1$.
2. Si $\alpha \in K$, son polynôme minimal sur K est $X - \alpha$.
3. Dans l'extension $\mathbf{C}/\mathbf{Q}$, les racines de l'unité $e^{\frac{2i\pi}{n}}$ ont pour polynôme minimal $\phi_n \in \mathbf{Q}[X]$ (cf plus loin).

Proposition 3.27.
1. *Soit $\alpha \in L$. Alors α est algébrique sur K si et seulement si $K[\alpha]$ est de dimension finie sur K si et seulement si $K(\alpha)/K$ est finie si et seulement si $K[\alpha] = K(\alpha)$.*
2. *Une extension finie est algébrique.*
3. *Une extension algébrique et de type fini est finie.*

Démonstration.
1. Tout d'abord, si $\alpha = 0$, toutes ces assertions sont clairement vraies. Supposons désormais $\alpha \neq 0$. Si α est algébrique, alors il existe $n \geq 1$ tel que $\alpha^n \in \mathrm{Vect}_K(1, \alpha, \ldots, \alpha^{n-1})$. Une récurrence simple assure alors que $K[\alpha] = \mathrm{Vect}_K(1, \alpha, \ldots, \alpha^{n-1})$, donc $K[\alpha]$ est un K-espace vectoriel de dimension

finie. Si $P \in K[X]$ est un polynôme non nul annulant α, alors cela fournit une relation de la forme

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0\,,$$

avec $a_i \in K$. Si $a_0 = 0$, alors en divisant par une puissance assez grande de α, on peut supposer que $a_0 \neq 0$. On en déduit que $\alpha^{-1} = \frac{-1}{a_0}\left(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1\right)$, donc $\alpha^{-1} \in K[\alpha]$. Plus généralement, si $Q \in K[X]$ vérifie $Q(\alpha) \neq 0$, alors Q n'est pas multiple de π_α. Comme π_α est irréductible, cela implique que π_α et Q sont premiers entre eux, donc il existe $U, V \in K[X]$ tels que $U\pi_\alpha + VQ = 1$. En évaluant en α, on obtient $V(\alpha)Q(\alpha) = 1$, donc $Q(\alpha)$ est inversible dans $K[\alpha]$ d'inverse $V(\alpha)$. Cela assure que $K[\alpha] = K(\alpha)$.

Supposons maintenant $K[\alpha] = K(\alpha)$. Alors $\alpha^{-1} \in K[\alpha]$, donc il existe $P \in K[X]$ tel que $\alpha^{-1} = P(\alpha)$. Alors $XP - 1 \in K[X]$ annule α, donc α est algébrique.

Supposons maintenant $K[\alpha]/K$ finie de degré n. Alors $(1, \alpha, \ldots, \alpha^n)$ est liée dans le K-espace vectoriel $K[\alpha]$, ce qui assure que α est algébrique.

2. C'est une conséquence du premier point.
3. idem.

□

Corollaire 3.28. *Soit L/K une extension de corps.*

L'ensemble des éléments de L algébriques sur K est un sous-corps de L.

Démonstration. Notons L^{alg} cet ensemble.

Pour tous $x, y \in L^{\mathrm{alg}}$ avec $y \neq 0$, $K(x)$ est de dimension finie sur K et $K(x)(y)$ est de dimension finie sur $K(x)$ (car y est algébrique sur $K(x)$, car il l'est sur K). Alors $K(x, y) = K(x)(y)$ est une extension finie de K. Or $x - y, xy^{-1} \in K(x, y)$, donc $K(x-y)$ et $K(xy^{-1})$ sont des extensions finies de K, ce qui assure $x-y$ et $xy^{-1} \in L^{\mathrm{alg}}$. Puisque L^{alg} contient K, cela suffit à prouver que L^{alg}/K est une sous-extension de L/K. □

En revanche, cet énoncé ne donne pas de méthode simple pour trouver un polynôme annulateur de $\alpha + \beta$ ou $\alpha\beta$ à partir de polynômes annulateurs de α et de β. Pour cela, on pourra utiliser le résultant (qui n'est pas officiellement au programme) ou raisonner à la main sur certains exemples.

Définition 3.29. On dit qu'une extension L/K est une clôture algébrique de K si L/K est algébrique et L est algébriquement clos.

C'est un théorème hors programme qui affirme que tout corps admet une clôture algébrique. Nous n'en avons pas besoin à l'agrégation. Néanmoins, on dispose d'une alternative pour construire certaines clôtures algébriques particulières :

Proposition 3.30. *Soit K un corps et L/K une extension telle que L soit algébriquement clos.*

Alors l'ensemble des éléments de L algébriques sur K est une clôture algébrique de K.

Démonstration. Par le corollaire précédent, l'ensemble L^{alg} ainsi défini est un sous-corps de L, et par définition, L^{alg} est une extension algébrique de K. Montrons que L^{alg} est algébriquement clos : soit $P \in L^{\mathrm{alg}}[X]$ non constant. Le polynôme P a un nombre fini de coefficients non nuls, qui sont des élément $\alpha_0, \dots, \alpha_n$ algébriques sur K par définition. Donc $M := K(\alpha_0, \dots, \alpha_n)$ est une extension finie de K. Comme L est algébriquement clos, le polynôme P admet une racine $\zeta \in L$. Puisque ζ est algébrique sur M, l'extension $M(\zeta)/M$ est finie, donc l'extension $K(\alpha_0, \dots, \alpha_n, \zeta)/K$ est finie, donc $K(\zeta)/K$ est finie, donc ζ est un élément de L algébrique sur K, donc $\zeta \in L^{\mathrm{alg}}$. Cela assure que L^{alg} est algébriquement clos. □

Exemple 3.31. Si K est un sous-corps de $\mathbf{C}$, l'ensemble $\overline{K}$ des nombres complexes algébriques sur K est un clôture algébrique de K. Par exemple, l'ensemble $\overline{\mathbf{Q}}$ des nombres algébriques est une clôture algébrique de $\mathbf{Q}$.

3.3 Corps de rupture, corps de décomposition

L'objectif de cette section est, partant d'un polynôme $P \in K[X]$, de construire des extensions L de K, les plus petites possibles, telles que P ait une racine (ou toutes ses racines) dans L.

Définition 3.32. Soit $P \in K[X]$ un polynôme irréductible. Un corps de rupture de K est une paire (L, α), où L/K est une extension de K, $\alpha \in L$ vérifie $P(\alpha) = 0$ et $L = K(\alpha)$.

Proposition 3.33. *Tout polynôme irréductible $P \in K[X]$ admet un corps de rupture. En outre, ce corps est de degré $\deg(P)$ sur K et si (L, α) et (L', α') sont des corps de rupture de $P \in K[X]$, alors il existe un unique isomorphisme d'extensions de K : $\varphi : L \to L'$ tel que $\varphi(\alpha) = \alpha'$.*

Démonstration. On pose $L := K[X]/(P)$ et $\alpha := \bar{X} \in L$. Alors L est un corps contenant K, puisque P est irréductible. En outre, $L = K(\alpha)$ par construction. Donc (L, α) est bien un corps de rupture de P sur K.

Pour l'unicité, si (L', α') est un tel corps de rupture, on considère l'application naturelle $\mathrm{ev}_{\alpha'} : K[X] \to L'$ définie par $Q \mapsto Q(\alpha')$. Alors par définition $(P) \subset \ker(\mathrm{ev}_{\alpha'})$, et il y a égalité car P est irréductible (P est donc le polynôme minimal de α' sur K). Donc $\mathrm{ev}_{\alpha'}$ induit un morphisme injectif $L = K[X]/(P) \to L'$ envoyant α sur α'. Comme $L' = K(\alpha')$, on voit que ce morphisme est un isomorphisme. En outre, un K-morphisme $L \to L'$ est complètement déterminé par l'image de α puisque $L = K(\alpha)$, ce qui assure l'unicté de l'isomorphisme $(L, \alpha) \to (L', \alpha')$. □

Exemples 3.34.

1. $\mathbf{C} := \mathbf{R}[X]/(X^2 + 1)$ est un corps de rupture de $X^2 + 1$ sur $\mathbf{R}$.
2. Soit p un nombre premier, et $P \in \mathbf{F}_p[X]$ un polynôme irréductible de degré n. Alors $\mathbf{F}_p[X]/(P)$ est un corps fini de cardinal p^n.
3. Si n est une puissance d'un nombre premier (ou même n un entier quelconque, cf plus loin), et $\zeta_n \in \mathbf{C}$ une racine primitive de l'unité, alors on a un isomorphisme canonique $\mathbf{Q}[X]/(\phi_n) \xrightarrow{\sim} \mathbf{Q}(\zeta_n)$ (car ϕ_n est irréductible sur $\mathbf{Q}$).

En itérant la construction du corps de rupture, on peut construire une extension contenant toutes les racines d'un polynôme donné :

Définition 3.35. Soit $P \in K[X]$ un polynôme de degré n.

Un corps de décomposition de P sur K est une extension L/K telle qu'il existe $x_1, \dots, x_n \in L$ vérifiant que P est scindé sur L de racines $x_1, \dots, x_n$ et $L = K(x_1, \dots, x_n)$.

Proposition 3.36. *Tout polynôme de $K[X]$ admet un corps de décomposition. Il est unique à isomorphisme (non unique) près.*

Démonstration.

— Existence : on raisonne par récurrence sur le degré n de P. Si $n = 1$, le résultat est clair avec $L = K$. Soit $P \in K[X]$ de degré $n \geq 2$. Il existe $Q \in K[X]$ un facteur irréductible de P. On note (L_1, α_1) un corps de rupture de Q sur K. Alors il existe $P_1 \in K_1[X]$ tel que $P = (X - \alpha_1)P_1$. Alors $\deg(P_1) = n - 1$, donc par hypothèse de récurrence , P_1 admet un corps de décomposition L sur K_1 : il existe $\alpha_2, \dots, \alpha_n \in L$ racines de P_1 telles que $L = K_1(\alpha_2, \dots, \alpha_n)$. Puisque $K_1 = K(\alpha_1)$, on voit que $L = K(\alpha_1, \dots, \alpha_n)$ et P est bien scindé sur L de racines les α_i, ce qui assure que L est un corps de décomposition de P sur K.

— (À revoir) Unicité : soit $i : K \to K'$ un isomorphisme de corps, et soient L (resp. L') un corps de décomposition de P (resp. $i(P)$) sur K (resp. sur K'). On montre par récurrence sur $n = [L : K]$ qu'il existe un isomorphisme de corps $\varphi : L \to L'$ qui soit compatible à i. Pour $n = 1$, c'est évident, puisque $L = K$ et P est scindé sur K, donc $i(P)$ est scindé sur K', donc $L' = K'$, et $\varphi = i$ convient. Supposons maintenant $n > 1$. Il existe $\alpha_1 \in L$ racine de P. $K(\alpha_1)$ est contenu dans L, et c'est un corps de rupture d'un facteur irréductible Q de P sur K. Alors $i(P)$ admet $i(Q)$ comme facteur irréductible sur K', et $i(Q)$ est scindé sur L', donc L' contient $K'(\alpha_1')$, où α_1' est une racine de $i(Q)$ dans L'. Or $K(\alpha_1)$ est isomorphe à $K[X]/(Q)$ et $K'(\alpha_1')$ à $K'[X]/(i(Q))$, donc i induit un isomorphisme de corps $K[X]/(Q) \to K'[X]/(i(Q))$, donc un isomorphisme de corps $i' : K(\alpha_1) \to K'(\alpha_1')$ compatible avec i. Or L (resp. L') est un corps de rupture de $\frac{P}{X-\alpha_1}$ (resp. de $i'(\frac{P}{X-\alpha_1}) = \frac{i(P)}{X-\alpha_1'}$) sur $K(\alpha_1)$ (resp. sur $K'(\alpha_1')$). Donc par hypothèse de récurrence, il existe un isomorphisme $\varphi : L \to L'$ compatible avec i', donc compatible avec i.

$\square$

Exemples 3.37.

1. Pour un polynôme irréductible de degré 2, tout corps de rupture est un corps de décomposition.
2. Considérons $P = X^3 - 2 \in \mathbf{Q}[X]$. Ce polynôme est irréductible, et $\mathbf{Q}(\sqrt[3]{2})$ est un corps de rupture de P sur $\mathbf{Q}$, mais pas un corps de décomposition. Un corps de décomposition de P sur K est donné par $\mathbf{Q}(j, \sqrt[3]{2})$, où $j := e^{\frac{2i\pi}{3}}$. Le premier est de degré 3 sur $\mathbf{Q}$, le second de degré 6.

Proposition 3.38. *Soit $P \in K[X]$ un polynôme de degré n.*

Alors le degré d'un corps de décomposition de P sur K divise $n!$.

Démonstration. En raisonnant par récurrence sur le degré de P, et en utilisant des corps de rupture successifs, on montre facilement que le degré d'un corps de décomposition est $\leq n!$. $\square$

3.4 Corps finis

Dans cette section, on construit et on classifie tous les corps finis.

On rappelle que pour tout $n \geq 1$, $\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si n est premier. Dans la suite, on notera $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$.

Lemme 3.39. *Soit K un corps fini.*

Alors K est une extension finie de $\mathbf{F}_p$ pour un certain nombre premier p, et il existe $n \geq 1$ tel que $|K| = p^n$.

Démonstration. Puisque K est fini, la caractéristique de K est un nombre premier p. Le sous-corps premier de K est donc égal à $\mathbf{F}_p$. Puisque K est fini, c'est une extension finie de $\mathbf{F}_p$, donc comme $\mathbf{F}_p$-espace vectoriel, K est isomorphe à $\mathbf{F}_p^n$, avec $n = [K : \mathbf{F}_p]$. Donc $|K| = p^n$. □

Théorème 3.40. *Soit p un nombre premier, $n \geq 1$ et $q := p^n$.*

Alors il existe un corps de cardinal q, et il est unique à isomorphisme près.

On notera $\mathbf{F}_q$ "le" corps de cardinal q.

Démonstration.
— On commence par l'existence. Notons K un corps de décomposition de $P := X^q - X$ sur $\mathbf{F}_p$, et considérons l'ensemble E des racines de P dans K. Puisque $P' = -1$ dans $\mathbf{F}_p[X]$, le polynôme P est scindé à racines simples dans K. Donc E est de cardinal q. Montrons que E est un sous-corps de K : $0 \in E$, et pour tout $x, y \in E$, on a $(x-y)^q = x^q - y^q$ puisque l'élévation à la puissance q est la composée n fois du morphisme de Frobenius avec lui-même. Donc $(x-y)^q = x^q - y^q = x - y$, donc $x - y \in E$. De même, $(xy^{-1})^q = x^q(y^q)^{-1} = xy^{-1}$, donc $xy^{-1} \in E$. Donc E est un sous-corps de K contenant toutes les racines de P. Donc $E = K$, donc K est un corps de cardinal q.
— Montrons l'unicité : soit K un corps de cardinal q. Puisque $K^\times$ est un groupe de cardinal $q-1$, le théorème de Lagrange assure que pour tout $x \in K^\times$, $x^{q-1} = 1$, donc $x^q = x$. Cette égalité étant aussi vérifiée par 0, on a donc que pour tout $x \in K$, $x^q - x = 0$. Donc tout élément de K est racine du polynôme $X^q - X$, qui est de degré $q = |K|$. Donc K est un corps de décomposition de $X^q - X$ sur $\mathbf{F}_p$. On conclut par unicité du corps de décomposition à isomorphisme près.

□

Proposition 3.41. *Soient K, K' deux corps finis de cardinaux respectifs p^n et ℓ^m, avec p et ℓ premiers.*

Alors K' est une extension de K (i.e. il existe un morphisme de corps $K \to K'$) si et seulement si $p = \ell$ et n divise m.

Démonstration. Supposons d'abord que $p = \ell$ et $n|m$. Considérons alors l'ensemble L des $x \in K'$ tels que $x^{p^n} = x$. Puisque $n|m$, on voit que $p^n - 1|p^m - 1$, donc $L \setminus \{0\}$ est un sous-groupe de cardinal $p^n - 1$ du groupe cyclique $K'^\times$. On en déduit que L est un sous-corps de K' de cardinal p^n. Par un unicité dans le théorème précédent, L est isomorphe à K, donc K' est une extension de K.

Supposons maintenant que K' soit une extension de K. Puisque K s'identifie à un sous-corps de K', ces deux corps ont la même caractéristique, donc $p = \ell$. En outre, K' est un K-espace vectoriel de dimension finie d, ce qui assure que $|K'| = |K|^d$, donc $m = nd$, donc n divise m. □

Le théorème principal n'explique pas comment construire explicitement les corps finis, la notion de corps de décomposition n'étant pas très utilisable en pratique. On lui préférera celle de corps de rupture pour consttruire concrètement les corps finis. On rappelle d'abord la définition suivante :

Définition 3.42. On définit la fonction de Möbius $\mu : \mathbf{N}^* \to \{-1, 0, 1\}$ par $\mu(1) = 1$, $\mu(p_1 \dots p_r) = (-1)^r$ si $p_1, \dots, p_r$ sont des nombres premiers distincts, et $\mu(n) = 0$ si n a un facteur carré.

Théorème 3.43. *Soit K un corps fini de cardinal q.*

Alors pour tout $n \geq 1$, il existe un polynôme irréductible de degré n dans $K[X]$.

Plus précisément, si $I(n, q)$ désigne le nombre de polynômes irréductibles unitaires sur K, on a

$$I(n, q) = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \geq 1 \,.$$

Démonstration. Notons $\mathcal{I}(n, q)$ l'ensemble des polynômes irréductibles unitaires sur K.

Montrons d'abord que

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{I}(d,q)} P \,,$$

Les deux membres de l'égalité étant unitaires, il suffit de montrer que dans un corps de décomposition de $X^{q^n} - X$, les deux polynômes sont scindés, à racines simples, avec les mêmes racines. Notons L un corps de décomposition sur K de $X^{q^n} - X$. Comme vérifié plus haut, l'ensemble K' des racines de ce polynôme dans L est un sous-corps de L contenant K, donc $K' = L$, et les racines de $X^{q^n} - X$ sont exactement les éléments de L. En outre, la dérivée de $X^{q^n} - X$ étant égale à 1, ce polynôme est à racines simples, donc $X^{q^n} - X = \prod_{\zeta \in L}(X - \zeta)$ et L est une extension de K de cardinal q^n.

Soit $P \in \mathcal{I}(d, q)$ avec $d|n$. Un corps de rupture M de P sur K est une extension de degré d de K, donc un corps de cardinal q^d. Par unicité des corps finis, on sait que M est un corps de décomposition de $X^{q^d} - X$. Puisque $d|n$, cela assure que M se plonge dans L, donc L contient une racine de P. Donc cette racine est annulée par $X^{q^n} - X$, et P est on polynôme minimal, donc $P | X^{q^n} - X$ dans $K[X]$. Puisque deux polynômes unitaires irréductibles distincts sont non associés, l'unicité de la décomposition en irréductibles dans $K[X]$ assure que $\prod_{d|n} \prod_{P \in \mathcal{I}(d,q)} P$ divise $X^{q^n} - X$ dans $K[X]$.

Réciproquement, si $\zeta \in L$, notons P son polynôme minimal sur K, de degré d. On sait que $P \in \mathcal{I}(d, q)$. En outre, $K \subset K(\zeta) \subset L$, donc la multiplicativité des degrés assure que $d|n$. Donc toute racine de $X^{q^n} - X$ est racine de $\prod_{d|n} \prod_{P \in \mathcal{I}(d,q)} P$, d'où l'égalité

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{I}(d,q)} P \,.$$

En calculant les degrés, on en déduit

$$q^n = \sum_{d|n} dI(d, q) \,.$$

En particulier, on en déduit que $nI(n, q) \leq q^n$ et

$$nI(n, q) = q^n - \sum_{\substack{d|n \\ d \neq n}} dI(d, q) \,.$$

Or d'après ce calcul, pour tout d, $dI(d,q) \leq q^d$, donc on déduit de l'égalité précédente que

$$nI(n,q) \geq q^n - \sum_{k=1}^{\frac{n}{2}} q^k > q^n - q^{\frac{n}{2}+1} \geq 0\,.$$

Pour avoir le résultat exact, il faut utiliser une inversion de Möbius, que nous ne détaillerons pas ici. □

Exemples 3.44.

1. Il existe exactement un polynôme irréductible de degré 2 sur $\mathbf{F}_2$, à savoir X^2+X+1. Il existe deux polynômes irréductibles de degré 3 sur $\mathbf{F}_2$: X^3+X^2+1 et X^3+X+1. Les 3 polynômes irréductibles de degré 4 sur $\mathbf{F}_2$ sont X^4+X+1, X^4+X^3+1, $X^4+X^3+X^2+X+1$.
2. Les 3 polynômes irréductibles unitaires de degré 2 sur $\mathbf{F}_3$ sont X^1+1, X^2+X-1, X^2-X-1. Il y a exactement 7 polynômes irréductibles unitaires de degré 3 sur $\mathbf{F}_3$.

Le théorème permet de construire le corps fini $\mathbf{F}_{p^n}$ comme un corps de rupture d'un polynôme irréductible de degré n dans $\mathbf{F}_p[X]$. On en déduit au passage que tout corps fini est engendré sur $\mathbf{F}_p$ par un unique élément (ce que l'on peut montrer également via le fait que $\mathbf{F}_{p^n}^\times$ est cyclique).

Par exemple, $\mathbf{F}_4 \cong \mathbf{F}_2[X]/(X^2+X+1)$, $\mathbf{F}_8 \cong \mathbf{F}_2[X]/(X^3+X+1) \cong \mathbf{F}_2[X]/(X^3+X^2+1)$.

3.5 Symbole de Legendre et loi de réciprocité quadratique

Dans cette partie, on s'intéresse aux carrés dans les corps finis.

Définition 3.45. Soit K un corps. On note $K^{\times 2}$ le sous-groupe de $K^\times$ formé des carrés.

Proposition 3.46. *Soit K un corps fini de cardinal q.*

- *Si q est pair, alors tout élément de K est un carré (et donc $K^{\times 2} = K^\times$.*
- *Si q est impair, alors $K^{\times 2}$ est un sous-groupe d'indice 2 de $K^\times$.*

Démonstration. On considère l'application $\varphi : K^\times \to K^\times$ définie par $\varphi(x) := x^2$. C'est clairement un morphisme de groupes d'image $K^{\times 2}$. Or $\ker(\varphi) = \{x \in K^\times : x^2 = 1\} = \{\pm 1\}$, car $X^2-1 = (X-1)(X+1)$ et K est intègre.

On distingue désormais les deux cas :

- si q est pair, alors $1 = -1$ dans K, donc φ est injectif, donc bijectif, donc tout élément de K est un carré.
- si q est impair, alors $1 \neq -1$ dans K, donc $|\ker\varphi| = 2$, donc par théorème d'isomorphisme, $|K^{\times 2}| = \frac{|K^\times|}{2} = \frac{q-1}{2}$ et $K^{\times 2}$ est donc bien un sous-groupe d'indice 2 dans $K^\times$.

□

Corollaire 3.47. *Si q est impair, alors $|K^{\times 2}| = \frac{q-1}{2}$ et $|K^2| = \frac{q+1}{2}$.*

Corollaire 3.48. *Soit K un corps fini et $a, b \in K^\times, c \in K$.*

Alors l'équation $ax^2+by^2 = c$ a une solution $(x,y) \in K \times K$. En particulier, tout élément de K est somme de deux carrés dans K.

Démonstration. Si $q = |K|$ est pair, c'est évident. On suppose désormais q impair.

Les sous-ensembles $A := \{ax^2, x \in L\}$ et $B := \{c - by^2, y \in K\}$ de K sont en bijection avec l'ensemble K^2 des carrés dans K, donc $|A| = |B| = \frac{q+1}{2}$. Donc $|A|+|B| = q+1 > q = |K|$. Donc les sous-ensembles A et B ne sont pas disjoints dans K (i.e. $a \cap B \neq \emptyset$), donc il existe $x, y \in K$ tels que $ax^2 = c - by^2$, ce qui conclut la preuve. $\square$

Remarque 3.49. On peut reformuler cet énoncé géométriquement en disant que toute conique sur un corps fini a un point rationnel.

Proposition 3.50. *Soit K un corps fini de cardinal q impair et $a \in K^\times$.*

Alors $a^{\frac{q-1}{2}} = 1$ si et seulement si a est un carré dans K, et $a^{\frac{q-1}{2}} = -1$ sinon.

Démonstration. On peut par exemple écrire la factorisation $X^{q-1} - 1 = (X^{\frac{q-1}{2}} - 1)(X^{\frac{q-1}{2}} + 1)$. Or ce polynôme admet les $q-1$ éléments de $K^\times$ comme racine par le théorème de Lagrange, donc pour tout $a \in K^\times$, $a^{\frac{q-1}{2}} = \pm 1$. S'il existe $b \in K^\times$ tel que $q = b^2$, alors $a^{\frac{q-1}{2}} = b^{q-1} = 1$, donc $X^{\frac{q-1}{2}} - 1$ admet tous les carrés non nuls comme racines. Or il y a $\frac{q-1}{2}$ carrés dans $K^\times$, donc les racines de $X^{\frac{q-1}{2}} - 1$ sont exactement les carrés non nuls, et celles de $X^{\frac{q-1}{2}} + 1$ sont donc les non carrés. $\square$

On définit maintenant :

Définition 3.51. Soit K un corps fini de cardinal q impair. Pour tout $a \in K$, on définit le symbole de Legendre de a par

$$\left(\frac{a}{K}\right) = \begin{cases} 1 \text{ si } a \in K^{\times 2} \\ -1 \text{ si } a \in K^\times \setminus K^{\times 2} \\ 0 \text{ si } a = 0 \end{cases} .$$

Autrement dit, en utilisant la proposition précédente, $\left(\frac{a}{K}\right) = a^{\frac{q-1}{2}}$.

Si $K = \mathbf{Z}/p\mathbf{Z}$, on note $\left(\frac{a}{p}\right) := \left(\frac{a}{K}\right)$.

Proposition 3.52. *L'application $\left(\frac{\cdot}{K}\right) : K^\times \to \{\pm 1\}$ est un morphisme de groupes.*

Démonstration. C'est évident avec la formule $\left(\frac{a}{K}\right) = a^{\frac{q-1}{2}}$. $\square$

Exemple 3.53. Pour tout p premier impair, on a

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} .$$

Le résultat suivant est fondamental en arithmétique :

Théorème 3.54 (Loi de réciprocité quadratique)**.** *Soient p, q deux nombres premiers impairs distincts.*

1. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.
2. $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$

Démonstration. Une preuve a été donnée en cours, à l'aide des sommes de Gauss sur les corps finis. $\square$

4 Compléments sur les polynômes cyclotomiques

Introduisons maintenant les polynômes cyclotomiques $\phi_n(X) := \prod_{\zeta \in \mu_n^*}(X - \zeta)$, où $\mu_n^* \subset \mu_n(\mathbf{C})$ désigne l'ensemble des racines primitives n-ièmes de l'unité dans $\mathbf{C}$. Le théorème de Lagrange et la description des racines n-ièmes de l'unité dans $\mathbf{C}$ assurent que $X^n - 1 = \prod_{d|n} \phi_d(X)$. Puisque les $\phi_d(X)$ sont unitaires, une récurrence simple (déjà vue) assure que :

Proposition 4.1. *Pour tout $n \geq 1$, $\phi_n(X) \in \mathbf{Z}[X]$.*

Une première application est la version faible du théorème de Dirichlet :

Proposition 4.2. *Pour tout $n \geq 1$, il existe une infinité de nombres premiers p de la forme $p = kn + 1$, avec $k \in \mathbf{N}$.*

Ce résultat est un cas très particulier du théorème de la progression arithmétique de Dirichlet, dont la preuve (via l'analyse complexe) est un peu au-delà du programme de l'agrégation.

Démonstration. Soit $n \geq 1$ et $k \geq n + 2$.

L'entier $\phi_n(k!)$ est supérieur ou égal à 2 (en utilisant par exemple la factorisation de ϕ_n), donc il admet un facteur premier p. Puisque 0 n'est pas racine de ϕ_n, p ne divise pas $k!$, donc $p > k$.

Puisque p divise $\phi_n(k!)$, on voit que $\overline{k!}$ est racine de $\overline{\phi_n}$ dans $\mathbf{F}_p$. Or ϕ_n divise $X^n - 1$ dans $\mathbf{Z}$, donc dans $\mathbf{F}_p$, donc $\overline{k!}^n = 1$ dans $\mathbf{F}_p$. Donc l'ordre de $\overline{k!}$ dans $\mathbf{F}_p^\times$ est un diviseur d de n. Si $d < n$, alors $\overline{k!}$ est racine de $X^d - 1$ dans $\mathbf{F}_p$, donc d'un certain ϕ_r avec $r|d$. En utilisant la factorisation de $X^n - 1$ dans $\mathbf{Z}[X]$, on voit donc que $\overline{k!}$ est racine double de $X^n - 1$ dans $\mathbf{F}_p$, ce qui assure que p divise n, ce qui est contradictoire car $p > n$.

Donc finalement $\overline{k!}$ est d'ordre exactement n dans $\mathbf{F}_p^\times$, qui est un groupe d'ordre $p - 1$. Donc Lagrange implique de n divise $p - 1$, donc que p est congru à 1 modulo n.

On a donc construit, pour tout $k \geq n+2$, un nombre premier $p > n$ tel que $p \equiv 1 \ [n]$, ce qui conclut la preuve. □

Une autre application classique :

Théorème 4.3 (Wedderburn)**.** *"Tout corps fini est commutatif". Plus précisément, tout anneau intègre fini (pas commutatif a priori) est un corps (commutatif).*

Démonstration. Soit K un tel anneau intègre fini.

Remarquons d'abord que tout élément x non nul de K est inversible, puisque l'application $K \setminus \{0\} \to K \setminus \{0\}$ définie par $y \mapsto xy$ est injective (car K est intègre), donc bijective par égalité des cardinaux, ce qui assure que x admet un inverse à droite. Par symétrie, x admet un inverse à gauche, et cela assure que x est inversible.

Notons $k := \{t \in K : tx = xt, \ \forall x \in K\}$ le centre de K. Alors k est un corps (commutatif, fini) dont on note $q \geq 2$ le cardinal.

L'application $k \times K \to K$ définie par $(t, x) \mapsto tx$ munit K d'une structure de k-espace vectoriel. Puisque K est fini, K est un k-espace vectoriel de dimension finie. Notons d sa dimension, alors $K \cong k^d$, donc $|K| = |k|^d$.

Considérons alors le groupe $G := K^\times = K \setminus \{0\}$ (non commutatif a priori) et faisons le agir sur lui-même par conjugaison, i.e. $x \cdot y := xyx^{-1}$.

Écrivons l'équation aux classes pour cette action :

$$|K^\times| = |(K^\times)^G| + \sum_{x \in G \backslash K^\times, x \notin K^G} \frac{K^\times}{\mathrm{Stab}_{K^\times}(x)}.$$

Or $K^G = k$ par définition, et pour tout $x \in K \setminus k$, l'ensemble des $y \in K$ tels que $xy = yx$ est un sous-k-espace vectoriel de K, non trivial, donc cet ensemble est de cardinal q^r, avec $1 \leq r < d$. En particulier, pour tout $x \in K \setminus k$, $|\mathrm{Stab}_{K^\times}(x)| = q^r - 1$ pour un tel $1 \leq r < d$. En outre, $q^r - 1$ divise $q^d - 1$, ce qui implique que r divise d. On obtient donc un ensemble fini d'entiers $1 \leq r_1, \dots, r_a < d$ (où a est le nombre d'orbites non réduites à un singleton) tels que r_i divise d pour tout i et l'équation aux classes s'écrive

$$q^d - 1 = q - 1 + \sum_{i=1}^{a} \frac{q^d - 1}{q^{r_i} - 1}. \tag{1}$$

Revenons à l'égalité (1) : puisque dans $\mathbf{Z}[X]$, $\phi_d(X)$ divise $X^d - 1$, et aussi $\frac{X^d-1}{X^{r_i}-1}$, on en déduit que $\phi_d(q)$ divise $q - 1$ dans $\mathbf{Z}$. Or

$$|\phi_d(q)| = \prod_{\zeta \in \mu_d^*} |q - \zeta|,$$

et pour tout $\zeta \neq 1$, $|q - \zeta| > q - 1$ (faire un dessin).

Finalement, si $d > 1$, on voit que $\phi_d(q) > q - 1$, ce qui contredit le fait que $\phi_d(q)$ divise $q - 1$. On en déduit donc que $d = 1$, ce qui signifie que $K = k$, donc K est commutatif. □

Une propriété importante des polynômes cyclotomiques :

Théorème 4.4. *Pour tout $n \geq 1$, ϕ_n est irréductible dans $\mathbf{Q}[X]$ (et dans $\mathbf{Z}[X]$).*

Démonstration. Par le lemme des contenus, comme ϕ_n est unitaire, l'irréductiblité dans $\mathbf{Q}[X]$ et dans $\mathbf{Z}[X]$ est équivalente. On montre la seconde. Soient $f, g \in \mathbf{Z}[X]$ tels que $\phi_n = fg$, avec f irréductible (non constant) dans $\mathbf{Z}[X]$ (et dans $\mathbf{Q}[X]$). Il existe une racine ζ de f dans $\mathbf{C}$. Puisque ζ est racine de ϕ_n, c'est une racine primitive n-ième de l'unité.

Soit p un nombre premier ne divisant pas n. Alors ζ^p est une racine primitive n-ième de l'unité, donc $\phi_n(\zeta^p) = 0$, donc $f(\zeta^p)g(\zeta^p) = 0$. Raisonnons par l'absurde et supposons $f(\zeta^p) \neq 0$. Alors $g(\zeta^p) = 0$, donc $g(X^p) \in \mathbf{Z}[X]$ est un polynôme annulateur de ζ. Or f étant irréductible, c'est le polynôme minimal de ζ sur $\mathbf{Q}$, donc f divise $g(X^p)$ dans $Q[X]$, donc dans $\mathbf{Z}[X]$ (car f est unitaire). Donc il existe $h \in \mathbf{Z}[X]$ tel que $g(X^p) = fh$. On réduit maintenant cette égalité modulo p : dans $\mathbf{F}_p[X]$, on a $\overline{g(X^p)} = \bar{f}\bar{h}$. Puisque $\mathbf{F}_p$ est de caractéristique p, l'élévation à la puissance p est un morphisme d'anneaux, qui est l'identité sur $\mathbf{F}_p$, donc $\overline{g(X^p)} = \bar{g}^p$. On a donc $\bar{g}^p = \bar{f}\bar{h}$. Or $\bar{f}$ admet un facteur irréductible $\bar{q}$ dans $\mathbf{F}_p[X]$. Alors $\bar{q}$ divise $\bar{f}$, donc $\bar{g}^p$, donc $\bar{g}$ par le lemme d'Euclide. Or $\bar{\phi}_n = \bar{f}\bar{g}$, donc $\bar{q}^2$ divise $\bar{\phi}_n$. Enfin, ϕ_n divise $X^n - 1$ dans $\mathbf{Z}$, donc $\bar{q}^2$ divise $X^n - 1$, donc $\bar{q}$ divise la dérivée nX^{n-1} avec $n \neq 0$ dans $\mathbf{F}_p$ (car p ne divise pas n). Donc $\bar{q}$ divise 1, ce qui est contradictoire. Finalement, cela assure que $f(\zeta^p) = 0$. Une récurrence simple permet d'en déduire que pour tout $m \geq 1$ premier avec n, $f(\zeta^m) = 0$. Or toute racine primitive n-ième de l'unité dans $\mathbf{C}$ est de la forme ζ^m avec m premier à n, donc toute racine primitive n-ième de l'unité est racine de f, donc ϕ_n divise f, donc $\phi_n = f$, donc ϕ_n est irréductible. □

Corollaire 4.5. *Soit $\zeta \in \mathbf{C}$ une racine primitive n-ième de l'unité.*
Alors $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \varphi(n)$.

Démonstration. Le théorème assure que ϕ_n est le polynôme minimal de ζ sur $\mathbf{Q}$. □

Avec un peu de travail, on peut en déduire le

Théorème 4.6 (Gauss-Wantzel)**.** *Soit $n \geq 1$. Alors le polygone régulier à n côtés (inscrit dans le cercle unité) est constructible à la règle et au compas si et seulement si $n = 2^r p_1 \dots p_s$, avec $r \geq 1$ et $p_i = 2^{2^{n_i}} + 1$ sont des nombres premiers de Fermat distincts.*

Remarque 4.7. Les seuls nombres de Fermat premiers connus sont 3, 5, 17, 257, 65537.