

► ► 16 : POLYNÔMES

1►

* Définir un polynôme à coefficients dans \mathbb{K} équivaut à définir une suite (a_i) presque nulle d'éléments de \mathbb{K} (c'est-à-dire qu'il existe un naturel n tel que $a_i = 0$ pour $i \geq n$).

En ce sens, X n'est pas une variable, mais la suite $(0, 1, 0, 0, \dots)$. Alors $X^2 = (0, 0, 1, 0, 0, \dots)$, etc.

Ainsi, peu importe le nom de l'indéterminée (sauf à généraliser par exemple à l'ensemble $\mathbb{K}[X, Y]$ des polynômes en X et Y).

* On note aussi : $P = \sum_{i=0}^{+\infty} a_i X^i$, en précisant que la suite (a_i) est presque nulle.

* L'écriture "développée" d'un polynôme est unique : deux polynômes de $\mathbb{K}[X]$ sont égaux si, et seulement si, ils ont mêmes coefficients.

En particulier, le polynôme $P = \sum_{i=0}^{+\infty} a_i X^i$ est nul si, et seulement si, tous les a_i sont nuls.

2►

* Il faudrait vérifier toutes les propriétés, ce qui est plus long que difficile.

Par exemple, et avec un peu d'avance, $\mathbb{K}[X] = \text{Vect}(1, X, X^2, \dots)$ traduit exactement qu'un polynôme est une combinaison linéaire de $1, X, X^2$, etc., c'est-à-dire une somme finie de puissances de X multipliées par des éléments de \mathbb{K} .

Par exemple, pour montrer la distributivité à droite, on choisit P, Q et R des polynômes, et on écrit

$P = \sum_{i=0}^{+\infty} a_i X^i$ et $Q = \sum_{i=0}^{+\infty} b_i X^i$, les suites (a_i) et (b_i) étant presque nulles.

Alors, pour $\lambda \in \mathbb{K}$: $(P + \lambda Q) \circ R = \sum_{i=0}^{+\infty} (a_i + \lambda b_i) R^i = \sum_{i=0}^{+\infty} a_i R^i + \lambda \sum_{i=0}^{+\infty} b_i R^i = P \circ R + \lambda(Q \circ R)$.

Pour montrer la dernière propriété, il suffit donc d'utiliser le cas particulier $P = X^k$ et $Q = X^l$: pour tout polynôme R , il vient $(X^{k+l}) \circ R = R^{k+l} = R^k \times R^l = (X^k \circ R) \times (X^l \circ R)$. La distributivité à droite permet de conclure.

* Il n'y a pas de distributivité à gauche : par exemple avec $P = X^2, Q = X, R = 1$ et $\lambda = 1$, on obtiendrait $(X + 1)^2 = X^2 + 1 \dots$

* L'application définie de \mathbb{K} dans $\mathbb{K}[X]$ qui à a associe aX^0 est une injection qui permet d'identifier les polynômes de degré nul (ou constants) avec les valeurs constantes qu'ils prennent.

Pratique 1 :

1. $(1 + 2X^2)(2 - X)^3 = (1 + 2X^2)(8 - 12X + 6X^2 - X^3) = 8 - 12X + 22X^2 - 25X^3 + 12X^4 - 2X^5$

2. $X^2 \circ (1 + X) = 1 + 2X + X^2$ et $(1 + X) \circ X^2 = 1 + X^2$

3. $X(1 + X) = X + X^2, X \circ (1 + X) = 1 + X$ et $(1 + X) \circ X = 1 + X$

4. Soit $P = \sum_{i=0}^{+\infty} a_i X^i$ un polynôme pair. Comme $P(-X) = \sum_{i=0}^{+\infty} a_i (-1)^i X^i$, l'égalité $P(X) = P(-X)$ équivaut à $a_i = 0$ pour tout indice i impair.

Donc P est pair si, et seulement si, il s'écrit : $P = \sum_{j=0}^{+\infty} a_{2j} (X^2)^j$, c'est-à-dire $P = Q(X^2)$

avec $Q = \sum_{j=0}^{+\infty} a_{2j} X^j$ (toutes les suites utilisées étant presque nulles).

3►

* *Preuve* : Si un des deux polynômes est nul, les résultats sont simples à vérifier. Sinon, posons $P = \sum_{i=0}^n a_i X^i$ et $Q = \sum_{i=0}^m b_i X^i$, avec $a_n \neq 0$ et $b_m \neq 0$. Quitte à changer les rôles de P et Q , on peut supposer $n \geq m$.

Si $m < n$, alors $P + Q$ est degré n et de coefficient dominant a_n . Si $m = n$ et $a_n + b_n \neq 0$, alors $P + Q$ est également de degré n , sinon, inférieur à n .

$PQ = a_n b_m X^{n+m} + R$ avec R de degré inférieur strictement à $n + m$.

Enfin, grâce à la distributivité à droite, il suffit d'ailleurs de vérifier que $X^n \circ Q = Q^n$ est de degré $n \deg Q$ pour conclure pour la composition. \square

Pratique 2 :

1. On obtient en terme de degrés : $\deg(P^2)$ pair si fini, et $\deg(XQ^2)$ impair si fini, donc il n'y a pas d'autres solutions que $P = Q = 0$.

2. Si un tel polynôme P est de degré n fini, alors $n^2 = n$, donc $n = 0$ ou $n = 1$. Réciproquement, le polynôme nul est solution, ainsi que tout polynôme constant, et si $P = aX + b$ est solution de degré 1, alors : $a(aX + b) + b = aX + b$ donc $a^2 = a$ et $b(a + 1) = b$, donc finalement $P = X$.

3. Pour un polynôme P d'inverse Q , il vient $PQ = 1$ donc P est une constante, nécessairement non nulle, ce qui convient.


4►

C'est-à-dire : $\mathbb{K}_n[X] = \text{Vect}(1, X, \dots, X^n)$. Cette notation est tolérée, mais mauvaise, car \mathbb{K}_n ne désigne pas un corps...

5►

* Faites bien à ce niveau la différence entre polynôme et fonction polynomiale!

* L'application $\varphi : \mathbb{K}[X] \rightarrow \mathbb{K}^{\mathbb{K}}$ qui à P associe \widehat{P} est un morphisme d'algèbre : $\widehat{P + \lambda Q} = \widehat{P} + \lambda \widehat{Q}$, $\widehat{PQ} = \widehat{P} \widehat{Q}$, $\widehat{0}$ est la fonction nulle, la fonction polynomiale associée à un polynôme constante α est la fonction constante $x \mapsto \alpha$, et également $\widehat{P \circ Q} = \widehat{P} \circ \widehat{Q}$.

 Cette application n'est pas forcément bijective : si on choisit $\mathbb{Z}/2\mathbb{Z}$ pour corps de départ, X et X^2 ont même image par φ .

* De même, l'application e_α de $\mathbb{K}[X]$ dans \mathbb{K} , qui à P associe $\widehat{P}(\alpha)$ où α est un élément de \mathbb{K} , est également un morphisme d'algèbre. On l'appelle "évaluation en α ".

Pratique 3 :

3 étant premier, par le petit théorème de Fermat, on obtient la fonction nulle.

6►

* *Preuve* : a) Unicité : supposons $A = BQ_1 + R_1 = BQ_2 + R_2$ avec les conditions de degrés.

Alors : $B(Q_2 - Q_1) = R_1 - R_2$. Si $Q_1 \neq Q_2$, alors $\deg(R_1 - R_2) \geq \deg B$, impossible.

Donc $Q_1 = Q_2$ et $R_1 = R_2$.

b) Existence : par récurrence sur $n = \deg A$ (si $A = 0$, on a $A = B.0 + 0$).

Si $n = 0$, A est une constante non nulle, et $A = B.0 + A$ si $\deg A < \deg B$, et $A = B.(A/B) + 0$ si B est une constante non nulle.

Supposons maintenant $n \geq 1$ et supposons le résultat établi pour les degrés inférieurs strictement à n .

Si $\deg B > \deg A$, alors $A = B.0 + A$.

Sinon, en notant a_n le coefficient dominant de A et b_p celui de B (avec $p < n$), alors $C = A - \frac{a_n X^{n-p}}{b_p} B$ est de degré strictement inférieur à celui de A .

Par hypothèse de récurrence, il existe donc Q_1 et R_1 , avec $\deg R_1 < \deg B$, tels que $C = BQ_1 + R_1$, d'où $A = B.(Q_1 + \frac{a_n X^{n-p}}{b_p}) + R_1$ qui a bien l'écriture recherchée. On conclut par le principe de récurrence. \square

* Voyez que dans la preuve de l'existence, on "commence" la division euclidienne "classique" telle qu'on l'a déjà posée. Le degré joue ici le même rôle que la valeur absolue pour la division euclidienne dans \mathbb{Z} .

Pratique 4 :

$$\begin{array}{r}
 X^5 \qquad -2X^2 \qquad +1 \quad | \quad X^2 + 1 \\
 -X^5 \qquad -X^3 \qquad \qquad \qquad | \quad X^3 - X - 2 \\
 \hline
 1. \qquad -X^3 \quad -2X^2 \qquad +1 \quad | \\
 \qquad X^3 \qquad +X \qquad \qquad \qquad | \\
 \qquad \qquad -2X^2 \quad +X \quad +1 \\
 \qquad \qquad \qquad X \quad +3
 \end{array}$$

ou $X^5 - 2X^2 + 1 = (X^2 + 1)(X^3 - X - 2) + X + 3$, quotient $X^2 + 1$, reste $X + 3$.

2. Comme déjà expliqué : $X^3 - 3X^2 + 5X - 6 = (X - 2)(X^2 + \dots)$ puis on corrige le terme $-2X^2$ qui apparaît : $\dots = (X - 2)(X^2 - X \dots)$ et enfin : $\dots = (X - 2)(X^2 - X + 3)$ et on vérifie avec le terme constant $-6 = (-2) \times 3$.

3. On pose grâce au théorème : $X^{2024} + X^2 + 1 = (X - 1)(X - 2)Q + aX + b$. Il faut trouver a et b , on choisit des valeurs particulières pour les fonctions polynômes associées, et qui éliminent Q . Pour $X = 1$ il vient $a + b = 3$, et pour $X = 2$, $2a + b = 2^{2024} + 5$, ce qui donne $a = 2^{2024} + 2$ par soustraction, puis b .

De même : $X^{2024} + X^2 + 1 = (X - 1)^2 S + cX + d$. Ici il faut utiliser 1 seulement, mais on peut le faire deux fois en évaluant les dérivées des fonctions polynomiales.

Il vient : $c + d = 3$ et $2026 = c$, donc $d = -2023$.

7►

* *Preuve de c)* : Par hypothèse, il existe Q tel que $A = BQ$ et S tel que $B = AS$, d'où $A = ASQ$. Ainsi le degré de SQ , donc de S et de Q , est nul, d'où le résultat (A étant non nul). \square

* Vérifier que la relation "être associé" est une relation d'équivalence.

* Par exemple, pour tout naturel non nul n , $X - 1$ divise $X^n - 1$ puisque :

$X^n - 1 = (X - 1)(X^{n-1} + X^{n-2} + \dots + X + 1)$. Et le résultat est vrai aussi pour $n = 0$.

8►

* *Preuve* : L'algorithme d'Euclide étendu montre l'existence d'un couple de Bezout (U, V) tel que $AU + BV = \Delta$ où Δ est un diviseur commun à A et à B de degré maximal puisque tout diviseur commun à A et à B divise donc Δ . En particulier, deux PGCD de A et B ont même degré que Δ et le divisent, donc ils sont tous trois associés. \square

* On a retrouvé dans ce théorème et sa preuve tous les raisonnements vus relativement à la division euclidienne dans \mathbb{Z} .

* Les PGCD de 0 et de A sont les associés de A .

* Comme c'était déjà le cas dans \mathbb{Z} , un couple de Bezout n'est pas unique !

* Comme dans \mathbb{Z} , on montre à partir des intersections les définissant l'associativité et la commutativité de \wedge .

Pratique 5 :

1. $X^4 + X^3 + X^2 + 2 = (X^2 - 1)(X^2 + X + 2) + X + 4$ (1), puis $X^2 - 1 = (X + 4)(X - 4) + 15$ (2) donc $A \wedge B = 1$ (pgcd unitaire).

On remonte depuis (2) : $15 = B - (X + 4)(X - 4)$, puis avec (1) : $15 = B - (A - B(X^2 + X + 2))(X - 4)$, donc $15 = B(1 + (X - 4)(X^2 + X + 2)) - (X - 4)A$.

Ainsi, $U = \frac{4 - X}{15}$ et $V = \frac{X^3 - 3X^2 - 2X - 7}{15}$ donnent $AU + BV = 1$.

2. $X^4 - X = X(X^3 - 1) = X(X - 1)(X^2 + X + 1)$, donc $A \wedge B = B$, et $0.A + 1.B = B$ donne une relation de Bezout.

9►

Même preuve que dans \mathbb{Z} , sans unicité des polynômes U et V puisqu'il suffit de leur ajouter des multiples opposés de A et B respectivement : $A(U + PB) + B(V - PA) = 1$

10►

Ici aussi, même preuve que dans \mathbb{Z} .

11►

Et encore ici, même preuve que dans \mathbb{Z} . On a d'ailleurs les propriétés semblables, comme par exemple : $\text{PPCM}(AC, BC) = C \cdot \text{PPCM}(A, B)$.

12►

* Noter que P' est bien un polynôme !

Si $P = \sum_{i=0}^n a_i X^i$ est de degré $n \geq 1$, alors $P' = \sum_{i=1}^n i a_i X^{i-1} = \sum_{i=0}^{n-1} (i+1) a_{i+1} X^i$ est de degré $n-1$.

Si P est constant, $P' = 0$, et c'est même une équivalence !

* On peut itérer les dérivations : si $P = \sum_{i=0}^{+\infty} a_i X^i$, alors pour n naturel, $P^{(n)} = \sum_{i=n}^{+\infty} \frac{i!}{(i-n)!} a_i X^{i-n}$, la suite (a_i) étant presque nulle.

Ainsi, $P^{(k)} = 0$ pour $k > \deg P$, donc la dérivation D est une opération nilpotente sur $\mathbb{K}_n[X]$ (puisque $D^{n+1} = 0$ sur cet ensemble).

* Contrairement à ce qui est construit sur l'ensemble des fonctions, la dérivation sur $\mathbb{K}[X]$ est définie sans utilisation de limite.

13►

Preuve : La linéarité de la dérivation se démontre par calcul élémentaire.

Pour la dérivée d'un produit, il suffit donc, par linéarité, de considérer le cas $P = X^k$ et $Q = X^l$: $(X^{k+l})' = (k+l)X^{k+l-1} = kX^{k-1}X^l + lX^kX^{l-1}$.

On démontre alors la formule de Leibniz par récurrence sur l'ordre de dérivation, c'est la même preuve que celle vue pour la formule de Leibniz concernant les fonctions.

De même, par distributivité à droite et linéarité de la dérivation, on démontre la formule de dérivation d'une composée avec le cas particulier $P = X^k$: $(Q^k)' = kQ^{k-1}Q'$ se montre par récurrence simple sur k à partir de la dérivation d'un produit, et c'est bien $(kX^{k-1} \circ Q)Q'$. \square

Pratique 6 :

1. $(X - a)^k$ est de degré k , donc sa dérivée n -ième est nulle si $n > k$. Sinon, par récurrence simple : $((X - a)^k)^{(n)} = k(k-1)\dots(k-n+1)(X - a)^{k-n} = \frac{k!}{(k-n)!}(X - a)^{k-n}$
2. Par la formule de Leibniz si pratique lorsqu'un des deux polynômes d'un produit est de petit degré : $(X^2 P)^{(n)} = X^2 P^{(n)} + 2nX P^{(n-1)} + n(n-1)P^{(n-2)}$ si $n \geq 2$. Les cas $n = 0$ et $n = 1$ sont simples.
3. Comme $P^{(n)} = \sum_{i=n}^k \frac{i!}{(i-n)!} a_i X^{i-n}$ avec somme nulle si $n > k$, il vient : $P^{(n)}(0) = 0$ si $k > n$ et $P^{(n)}(0) = n! a_n$

14►

- * Remarquer qu'on a donc $\text{Vect}(1, X, \dots, X^n) = \text{Vect}(1, (X - a), \dots, (X - a)^n)$.
- * Par définition de la forme développée d'un polynôme, on voit qu'il suffit de montrer cette formule de Taylor pour les monômes X^k . C'est donc une conséquence simple de la formule du binôme :

$$X^k = (a + (X - a))^k = \sum_{i=0}^k \binom{k}{i} a^{k-i} (X - a)^i = \sum_{i=0}^k \frac{k!}{(k-i)!} \cdot a^{k-i} \cdot \frac{1}{i!} \cdot (X - a)^i = \sum_{i=0}^k (\widehat{X^k}^{(i)}(a)) \cdot \frac{1}{i!} \cdot (X - a)^i$$

La linéarité de la dérivation permet de conclure.

Si on veut faire le calcul complet, soit $P = \sum_{k=0}^n b_k X^k$ un polynôme de degré n , alors :

$$P = \sum_{k=0}^n b_k \sum_{i=0}^k \frac{k!}{(k-i)!} \cdot a^{k-i} \cdot \frac{1}{i!} \cdot (X - a)^i = \sum_{i=0}^n \frac{1}{i!} \cdot (X - a)^i \left(\sum_{k=i}^n b_k \frac{k!}{(k-i)!} \cdot a^{k-i} \right) = \sum_{i=0}^n \frac{\widehat{P}^{(i)}(a)}{i!} (X - a)^i$$

- * Ainsi, la connaissance des valeurs en a des fonctions polynomiales associées aux dérivées de P suffit à la connaissance de P , et en particulier des coefficients de P dans la nouvelle base.

Pratique 7 :

1. $P(1) = 3$, $P'(1) = 5$, $P''(1) = 8$ et le coefficient dominant de P est 1, donc

$$P = 3 + 5(X - 1) + 4(X - 1)^2 + (X - 1)^3$$

2. Plutôt que d'utiliser la base "canonique" $(1, X, X^2)$ de $\mathbb{R}_2[X]$, utilisons l'expression du reste dans la base $(1, X - 1, (X - 1)^2)$: $P = X^5 + 1 = (X - 1)^3 \cdot Q + a + b(X - 1) + c(X - 1)^2$, où l'évaluation en 1 de P donne $a = 2$, de P' donne $5 = b$ et de P'' donne $20 = 2c$.
Le reste cherché est donc : $2 + 5(X - 1) + 10(X - 1)^2$

15►

- * *Preuve* : La division euclidienne de P par $X - a$ donne un reste constant r : $P = (X - a)Q + r$. En évaluant en a , il vient $\widehat{P}(a) = 0 = r$, donc $(X - a)$ divise P .
La réciproque est évidente. □
- * Plus généralement, si a est racine de P et que P divise le polynôme S , alors a est racine de S .
- * a est un **nombre algébrique** (sous-entendu sur \mathbb{Q}) s'il existe un polynôme Q à coefficients dans \mathbb{Q} dont a est racine.
Par exemple, 1 est algébrique car racine de $X - 1$, $\sqrt{2}$ est algébrique car racine de $X^2 - 2$.
On peut montrer que π et e ne sont pas algébriques, on dit que ce sont des **nombres transcendants**.
- * Le polynôme nul admet une infinité de racines, et c'est le seul ! (comme on le verra plus loin)

Pratique 8 :

Simple calcul puisque $2^3 - 3 \times 4 + 4 = 0$. Puis : $X^3 - 3X^2 + 4 = (X - 2)(X^2 - X - 2)$

16►

Dans la Pratique 6, on peut continuer, du fait que $X^2 - X - 2$ s'annule pour $X = 2$, et il vient : $X^3 - 3X^2 + 4 = (X - 2)^2(X + 1)$. On dit que 2 est racine double du polynôme P de départ, et on observe que $\widehat{P}(2) = 0$ et $\widehat{P}'(2) = 0$.

17►

* On parle alors de racine simple, double, triple, de multiplicité 4, etc.

* Autrement dit, a est racine de P d'ordre de multiplicité n si P s'écrit : $P = (X - a)^n Q$ avec $\widehat{Q}(a) \neq 0$, ou de manière équivalente, Q n'est pas divisible par $X - a$, ou encore $(X - a)^n$ divise P mais pas $(X - a)^{n+1}$.

* Si a est racine de P d'ordre de multiplicité n et que P divise Q , alors a est racine de Q d'ordre de multiplicité supérieure à n .

18►

* Preuve par récurrence simple sur k , le cas $k = 1$ découlant directement de la définition.

* Rappel : \mathbb{C} est algébriquement clos, un polynôme de $\mathbb{C}[X]$ de degré $n \geq 0$ admet exactement n racines complexes en comptant leurs ordres de multiplicité...

* Dans le cas du théorème avec la condition $\deg P = \sum_{i=1}^k m_i$, le polynôme P est dit scindé sur \mathbb{K} .

* Suivant la situation, on a intérêt à écrire un polynôme P scindé sur \mathbb{K} sous la forme :

$$P = \lambda \prod_{\alpha \text{ racine de } P} (X - \alpha)^{m(\alpha)}$$

où $m(\alpha)$ est l'ordre de multiplicité de α comme racine de P et λ est le coefficient dominant de P , et dans ce cas les racines intervenant sont distinctes deux à deux, ou alors

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

où n est le degré de P , et les racines intervenant sont répétées suivant leur multiplicité.

* Un polynôme de degré n qui admet au moins $n + 1$ racines en comptant les ordres de multiplicité est le polynôme nul.

Pratique 9 :

$$X^n - 1 = \prod_{k=0}^{n-1} (X - e^{2ik\pi/n}) = (X - 1)(1 + X + X^2 + \dots + X^{n-1}) \text{ donc}$$

$$1 + X + X^2 + \dots + X^{n-1} = \prod_{k=1}^{n-1} (X - e^{2ik\pi/n})$$

19►

* Preuve : $P \mapsto \widehat{P}$ est en particulier un morphisme de groupe, on montre l'injectivité en calculant son noyau. Si $\widehat{P} = 0$, c'est que P admet une infinité de racines puisque \mathbb{K} est infini, donc $P = 0$. \square

* Ce résultat est donc faux si le corps de base est fini. Par exemple, dans $\mathbb{Z}/3\mathbb{Z}[X]$, le polynôme $X(X-1)(X-2)$ et le polynôme nul ont même fonction polynôme associée : la fonction nulle.

20►

Preuve : $1 \iff 2$ est déjà vu.

$2 \implies 3$: Supposons $P = (X-\alpha)^m Q$ avec $Q(\alpha) \neq 0$, alors $P(\alpha) = 0$ et $P' = (X-\alpha)^{m-1}(mQ + (X-\alpha)Q')$ admet bien α pour racine de multiplicité $m-1$ puisque $mQ(\alpha) \neq 0$.

$3 \implies 2$: La division euclidienne de P par $(X-\alpha)^m$ s'écrit : $P = (X-\alpha)^m Q + R$. Il vient : $P' = (X-\alpha)^{m-1}(mQ + (X-\alpha)Q') + R'$ avec R' divisible par $(X-\alpha)^{m-1}$, donc $R' = 0$ puisque $\deg R \leq m-1$. Comme R est donc constant et de valeur nulle en α , $R = 0$. Ainsi $(X-\alpha)^m$ divise P , mais pas $(X-\alpha)^{m+1}$ sans quoi, d'après la partie directe, α serait racine de P' d'ordre m .

$2 \implies 4$: s'obtient en itérant la propriété 3 (ou par récurrence simple sur m).

$4 \implies 1$: Utiliser la formule de Taylor en α pour P , les termes jusqu'à $(X-\alpha)^m$ non inclus étant nuls. Clairement $(X-\alpha)^m$ divise P mais pas $(X-\alpha)^{m+1}$. \square

Pratique 10 :

Notons $P = X^4 - 2X^3 + 2X^2 - 2X + 1$, on a $P(1) = 0$ et $P' = 4X^3 - 6X^2 + 4X - 2$ donc $P'(1) = 0$, $P'' = 12X^2 - 12X + 4$ donc $P''(1) = 4$. Ainsi 1 est racine de P d'ordre de multiplicité 2, $(X-1)^2$ divise P mais pas $(X-1)^3$.

21►

* Preuve admise.

* Tout polynôme de degré $n \geq 1$ à coefficients complexes peut donc s'écrire sous les formes :

$$P = \lambda \prod_{i=1}^n (X - \alpha_i) \text{ où les } \alpha_i \text{ sont les racines complexes de } P \text{ répétées suivant leurs ordres de multiplicité,}$$

$$P = \lambda \prod_{\alpha \text{ racine de } P} (X - \alpha)^{m(\alpha)} \text{ où } \alpha \text{ (d'ordre de multiplicité } m(\alpha)) \text{ décrit l'ensemble des racines de } P,$$

et où λ est le coefficient dominant de P .

* Ce théorème ne fonctionne pas dans $\mathbb{R}[X]$: $X^2 + 1$ sans racine réelle ne s'y factorise pas.

Pratique 11 :

$X^2 + 1$ divise $X^n + X$ si, et seulement si, i et $-i$ sont racines de $X^n + X$, c'est-à-dire : $i^n + i = 0$ et $(-1)^n i^n - i = 0$, ce qui équivaut à n congru à 3 modulo 4.

22►

* *Preuve* : on cherche dans $(X-x_1)(X-x_2)\dots(X-x_n)$ le coefficient de X^k . Pour cela, dans chaque facteur il faut choisir X ou $-x_i$, mais en tout il faut faire k fois le choix de X , donc $n-k$ fois celui d'un x_i , et ce avec toutes les combinaisons possibles, on obtient donc : $(-1)^{n-k} \sigma_{n-k}$ égal au coefficient a_k/a_n dans P/a_n . Ce qui donne les formules. \square

* Ces formules généralisent celles pour un polynôme de degré 2, que l'on écrit aussi $a_2(X^2 - SX + P)$, avec $S = \sigma_1$ (somme des deux racines complexes) et $P = \sigma_2$ (produit des deux racines complexes).

* Quand on recherche les racines d'un polynôme donné, s'il en manque une (si on en connaît $\deg P - 1$ non nécessairement distinctes deux à deux), on obtient la dernière par σ_1 par exemple.

Pratique 12 :

1. $\sigma_1 = 1$, $\sigma_2 = 3/2$ et $\sigma_4 = 5/2$.

2. a , b et c sont les racines de $P = X^3 - X^2 + X - 1$ car ici $\sigma_1 = 1$, $\sigma_1^2 - 2\sigma_2 = -1$ donc $\sigma_2 = 1$ et $\sigma_3 = 1$.
1 est racine évidente de $P = (X - 1)(X^2 + 1)$, donc $\{a; b; c\} = \{1; i; -i\}$.


23►

À l'inverse, on sait exprimer les racines d'un polynôme de degré 2 à l'aide de formules faisant intervenir les coefficients du polynôme et la fonction racine carrée. Différents mathématiciens (Tartaglia, Cardan, Ferrari, Bombelli) ont au XVI^e siècle établi des formules semblables (à base de radicaux) pour le cas de polynômes de degré 3 ou 4. Enfin, Abel (1802-1829 !) et Galois (1811-1832 !) ont montré qu'il n'existe pas de telles formules pour les polynômes de degré ≥ 5 .

24►

* Cette notion de polynôme irréductible est très proche de celle de nombre premier dans \mathbb{N} : ce sont les "incassables" en "plus petits", au sens de la relation d'ordre pour les naturels, au sens du degré pour les polynômes.

* Pour montrer qu'un polynôme P est irréductible, on suppose qu'il s'écrit $P = QR$ avec Q et R polynômes, et on montre que Q ou R est constant.

*  Cette notion d'irréductibilité est fortement liée au corps de base : $X^2 + 1$ est irréductible sur \mathbb{R} , mais se décompose en $(X + i)(X - i)$ sur \mathbb{C} , de même $X^2 - 2$ est irréductible sur \mathbb{Q} mais se décompose en $(X - \sqrt{2})(X + \sqrt{2})$ sur \mathbb{R} ou sur \mathbb{C} .

* Un polynôme de degré 1 est toujours irréductible.

25►

* C'est le théorème pour les polynômes correspondant au théorème de factorisation première pour les naturels.

* *Preuve* : par récurrence sur le degré n du polynôme considéré P .

Si $n = 1$, P est irréductible et s'écrit de manière unique $\lambda(X - a)$ avec λ son coefficient dominant et $X - a$ unitaire irréductible. L'existence et l'unicité (par celle du coefficient dominant) sont claires.

Soit $n \geq 2$ le degré d'un polynôme P . Si P est irréductible, alors $P = \lambda.(P/\lambda)$ avec λ le coefficient dominant de P et P/λ irréductible unitaire. Sinon, $P = QR$ avec Q et R de degrés strictement inférieurs à n , et par hypothèse de récurrence, on obtient en décomposant Q et R la forme voulue pour P . D'où l'existence.

Si maintenant $P = \lambda_1 \prod_i Q_i = \lambda_2 \prod_i R_i$ avec λ_1 et λ_2 deux scalaires, Q_i et R_i irréductibles unitaires, alors $\lambda_1 = \lambda_2$ par unicité du coefficient dominant de P . Après simplification des facteurs identiques, supposons qu'il reste un polynôme Q_j à gauche de l'égalité et des facteurs R_k à droite. Q_j divise le produit de droite et est premier avec chacun des R_k (sinon on aurait pu simplifier davantage), donc d'après le théorème de Gauss il divise le dernier des R_k , ce qui est impossible. Les deux décompositions sont donc identiques à l'ordre près des facteurs. On conclut alors par le principe de récurrence. \square

* Une factorisation irréductible est en général difficile à obtenir car liée à la détermination des racines. Sans quoi, elle permet le calcul aisé des pgcd et ppcm, comme dans le cadre des naturels.

Pratique 13 :

1. $X^2 + 1$ sur \mathbb{R} et $(X + i)(X - i)$ sur \mathbb{C} pour $X^2 + 1$.

$(X - 2)(X^2 + 2X + 4)$ sur \mathbb{R} et $(X - 2)(X - 2j)(X - 2j^2)$ sur \mathbb{C} pour $X^3 - 8$.

2. $X^3 - 4X^2 + 5X - 2 = (X - 2)(X^2 - 2X + 1) = (X - 2)(X - 1)^2$ et

$X^4 - 4X^3 + 3X^2 + 4X - 4 = (X - 1)(X^3 - 3X^2 + 4) = (X - 1)(X + 1)(X^2 - 4X + 4) = (X - 1)(X + 1)(X - 2)^2$,
de pgcd $(X - 1)(X - 2)$ et de ppcm $(X - 1)^2(X + 1)(X - 2)^2$.

26►

C'est la conséquence directe du théorème de D'Alembert-Gauss !

27►

Preuve : En notant de manière générale \bar{P} le polynôme déduit de P en remplaçant les coefficients de P par leurs conjugués, on a $P = \bar{P}$ pour un polynôme réel, et $\bar{P}(\bar{\alpha}) = \overline{P(\alpha)} = 0$ si α est racine complexe de P . Donc $\bar{\alpha}$ est aussi racine de P si P est réel et s'annule en α .

Plus précisément, si $P = (X - \alpha)^k Q$ avec $Q(\alpha) \neq 0$, alors $P = \bar{P} = (X - \bar{\alpha})^k \bar{Q}$ avec $\bar{Q}(\bar{\alpha}) = \overline{Q(\alpha)} \neq 0$, donc l'ordre de multiplicité de $\bar{\alpha}$ comme racine de P est égal à celui de α . \square

28►

* *Preuve* : la preuve est claire dans le cas d'un polynôme de degré 1 ou de degré 2 à discriminant négatif strictement, sans racine réelle donc sans factorisation possible sur \mathbb{R} .

Soit P un polynôme réel de degré ≥ 3 . Si P admet une racine réelle a , il n'est pas irréductible puisque divisible par $(X - a)$. Sinon, il admet une racine complexe α ainsi que $\bar{\alpha}$ d'après la proposition précédente. Le reste de la division euclidienne de P par $X^2 - 2\operatorname{Re}(\alpha)X + |\alpha|^2$ est de degré 1 au plus et s'annule en α et $\bar{\alpha}$, donc ce reste est nul, et P est divisible par $X^2 - 2\operatorname{Re}(\alpha)X + |\alpha|^2$ donc non irréductible. \square

* On obtient la factorisation irréductible d'un polynôme réel à partir de sa factorisation sur \mathbb{C} : on conserve les facteurs liés aux racines réelles, et on regroupe deux à deux ceux liés aux racines complexes non réelles conjuguées.

* Pour conclure, si $P \in \mathbb{C}[X]$:
$$P = \lambda \cdot \prod_{\alpha \text{ racine de } P} (X - \alpha)^{m(\alpha)},$$

et si $P \in \mathbb{R}[X]$:

$$P = \lambda \cdot \prod_{\alpha \text{ racine réelle de } P} (X - \alpha)^{m(\alpha)} \cdot \prod_{\beta \text{ racine à partie imaginaire } > 0 \text{ de } P} (X^2 - 2\operatorname{Re}(\beta)X + |\beta|^2)^{m(\beta)}$$

où λ est le coefficient dominant de P .

Pratique 14 :

$X^3 + 1 = (X + 1)(X^2 - X + 1)$ s'obtient directement en voyant que -1 est racine évidente, ou depuis la factorisation sur \mathbb{C} : $(X + 1)(X + j)(X + \bar{j})$ en regroupant les facteurs relatifs à j et \bar{j} .

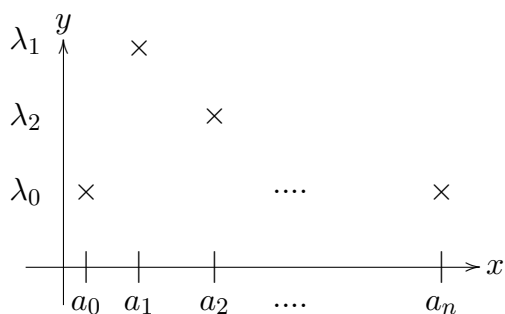
Sur \mathbb{C} : $X^4 + 1 = (X - e^{i\pi/4})(X + e^{i\pi/4})(X - ie^{i\pi/4})(X + ie^{i\pi/4})$, et en regroupant les racines conjuguées (la première et la quatrième, la deuxième et la troisième), on obtient :

$$X^4 + 1 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$$

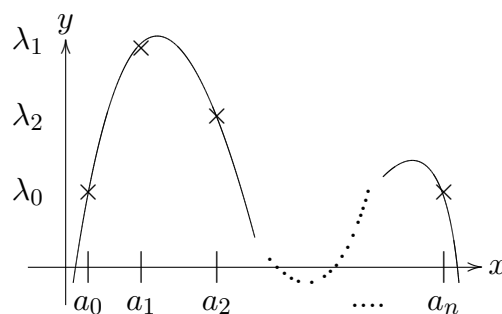
29►

* Rappel pour le symbole de Kronecker : $\delta_{i,j} = 1$ si $i = j$, 0 sinon.

* Le problème est le suivant.



On cherche à faire passer une courbe polynomiale par un nuage de points



Cela revient à résoudre le système linéaire à $n + 1$ équations $P_L(a_i) = \lambda_i$, $i \in \llbracket 0, n \rrbracket$ et d'inconnues les coefficients du polynôme P_L .

Pour cela, on utilise le principe de superposition des solutions, en résolvant les systèmes successifs de seconds membres nuls sauf à la ligne i où figure 1, pour $i = 1$ à $n + 1$.

Autrement dit, on résout successivement chaque problème de Lagrange associé au nuage de points $(a_0, 0), (a_1, 0), \dots, (a_i, 1), \dots, (a_n, 0)$, de solution particulière L_i que l'on cherche de degré n (pour avoir $n + 1$ inconnues et autant d'équations).

L_i s'annule donc en chaque point a_j sauf en a_i où il vaut 1, donc L_i est multiple de $\prod_{j \in \llbracket 0, n \rrbracket, j \neq i} (X - a_j)$, le coefficient multiplicatif étant donné par la valeur en a_i , ce qui donne la formule annoncée.

Il suffit alors de multiplier L_i par λ_i pour obtenir un polynôme solution au problème de Lagrange associé au nuage de points $(a_0, 0), (a_1, 0), \dots, (a_i, \lambda_i), \dots, (a_n, 0)$, et enfin de sommer toutes ces solutions pour donner une solution au problème de départ : $P_L = \sum_{i=0}^n \lambda_i L_i$.

Notez que pour trouver l'ensemble des solutions au problème de Lagrange de départ donc au système précisé, il suffit d'y ajouter la solution générale du système homogène, c'est-à-dire l'ensemble des polynômes s'annulant en chaque a_i , c'est-à-dire les multiples de $(X - a_0)(X - a_1)(X - a_2) \dots (X - a_n)$.

Enfin, le polynôme $\sum_{i=0}^n L_i$ est de degré au plus n et prend $n + 1$ fois la valeur 1 (aux points a_i) donc est égal à 1.

Pratique 15 :

$$P_L = 1 \times \frac{(X-1)(X-2)}{(-1)(-2)} + 2 \times \frac{X(X-2)}{1 \cdot (-1)} - 1 \times \frac{X(X-1)}{2 \cdot 1}.$$

Les autres solutions s'écrivent $P_L + Q \cdot X(X-1)(X-2)$ avec Q polynôme quelconque.

30►

On voit facilement que la relation proposée définit une relation d'équivalence entre les couples (A, B) de $\mathbb{K}[X]^2$, les classes d'équivalences étant les fractions rationnelles, chaque écriture (A, B) d'une classe en étant un représentant.

En particulier, la classe de $(A, 1)$ est notée A , et $\mathbb{K}[X]$ est ainsi plongé dans l'ensemble des fractions rationnelles $\mathbb{K}(X)$.

Dans $\mathbb{K}(X)$, les fractions $\frac{1}{X}$ et $\frac{X+1}{X(X+1)}$ par exemple sont les mêmes.

31►

Il faut tout d'abord vérifier que ces lois sont indépendantes des représentants choisis.

Par exemple pour l'addition, si $\frac{A}{B} = \frac{A'}{B'}$ et $\frac{C}{D} = \frac{C'}{D'}$, alors $\frac{AD+BC}{BD} = \frac{A'D'+B'C'}{B'D'}$ parce que $(AD+BC)(B'D') = AB'DD'+BCB'D' = BA'DD'+B'C'BD = (A'D'+B'C')BD$ puisque $AB' = A'B$ et $CD' = C'D$.

On admet ici que l'ensemble des propriétés de corps sont bien vérifiées, c'est fastidieux mais sans difficulté.

En particulier, l'opposé de $\frac{A}{B}$ est $\frac{-A}{B}$, son inverse (si $A \neq 0$) est $\frac{B}{A}$.

Ces lois prolongent celles de $\mathbb{K}[X]$ puisque $\frac{A}{1} + \frac{B}{1} = \frac{A+B}{1}$ et $\frac{A}{1} \times \frac{B}{1} = \frac{AB}{1}$.

32►

* Toutes ces notions sont indépendantes des représentants des fractions choisis.

* Par exemple, la fraction complexe $F = \frac{X(X-1)}{(X+1)(X-i)^2}$ est de degré -1 , admet pour racines 0 et 1 de multiplicités 1, et pour pôles -1 et i de multiplicités respectives 1 et 2.

33►

* *Preuve* : La division euclidienne de A par B s'écrit : $A = BE + R$ avec $\deg R < \deg B$, donc $F = E + \frac{R}{B}$ avec les conditions imposées, ce qui montre l'existence.

Si maintenant $F = E_1 + R_1 = E_2 + R_2$ avec E_1 et E_2 polynômes et R_1 et R_2 de degrés strictement négatifs, alors $E_1 - E_2 = R_2 - R_1$ impose $E_1 = E_2$ et $R_1 = R_2$ à cause des conditions de degrés. D'où l'unicité. \square

* Par exemple : $F = \frac{X^2 + 1}{2X^2 + X + 1} = \frac{1}{2} \cdot \frac{2X^2 + 2}{2X^2 + X + 1} = \frac{1}{2} + \frac{-X + 1}{2X^2 + X + 1}$ où on a écrit au numérateur : $2X^2 + 2 = 2X^2 + X + 1 + (-X + 1)$.

34►

* *Preuve* : Soit $F = \frac{A}{B}$ sous forme irréductible, on écrit B sous la forme : $B = \prod_{k=1}^p (X - a_k)^{m_k}$. Les polynômes $V_k = B / (X - a_k)^{m_k}$ sont premiers entre eux dans leur ensemble, il existe donc des polynômes U_k tels que $1 = \sum_{k=1}^p U_k V_k$, ce qui conduit à $F = \frac{A}{B} = \sum_{k=1}^p \frac{AU_k}{(X - a_k)^{m_k}}$. Il suffit alors d'utiliser pour chaque polynôme AU_k la formule de Taylor en a_k pour obtenir la forme réduite voulue de F : d'où l'existence. Supposons qu'il existe maintenant deux décompositions de R où $F = E + R$ avec E partie entière de F et $\deg R < 0$. En supprimant les termes communs, il reste une égalité dans laquelle on trouve par hypothèse un pôle a et deux coefficients distincts relativement à la plus grande puissance de $(X - a)$ intervenant. En isolant ces termes, on obtient $\frac{\alpha}{(X - a)^m}$ égal à une fraction de degré strictement négatif et pour laquelle le pôle a a une multiplicité strictement inférieure à m . En multipliant par $(X - a)^m$ puis en évaluant en $X = a$, il reste $\alpha = 0$, contradiction. On a donc l'unicité de la décomposition en éléments simples sur \mathbb{C} . \square

* Reprenez les techniques de détermination de cette décomposition : c'est le chapitre 8.

35►

Comme vu au chapitre 8, on regroupe depuis la réduction en éléments simples sur \mathbb{C} les termes de type $\frac{\alpha}{(X - a)^k}$ conjugués deux à deux et par divisions euclidiennes successives par $(X^2 - 2\operatorname{Re}(a)X + |a|^2)$ on obtient l'existence. L'unicité se démontre comme au point précédent.

Reprendre également le chapitre 8 pour les techniques d'obtention pratique de cette décomposition.

36►

Preuve : Par hypothèse : $B = (X - a)C$ avec $C(a) \neq 0$. En multipliant F par $(X - a)$ puis en évaluant en a , on obtient : $\frac{A(a)}{C(a)} = \alpha$. Or $C(a) = B'(a)$ puisque $B' = C + (X - a)C'$. \square

Pratique 16 :

1. La partie entière est égale à 1 : $\frac{X^n}{X^n - 1} = \frac{X^n - 1 + 1}{X^n - 1} = 1 + \frac{1}{X^n - 1}$

Les pôles, simples, sont les racines n -ièmes de l'unité, disons $\zeta_k = \exp(\frac{2ik\pi}{n})$ pour $k = 0$ à $n - 1$.

La partie polaire relative à ζ_k est donnée par la proposition précédente : $\frac{1}{n\zeta_k^{n-1}} = \frac{\zeta}{n}$, ce qui donne la réduction demandée.

2. La partie entière de P'/P est nulle. En notant : $P = \lambda \prod_a (X - a)^{m(a)}$ où a décrit l'ensemble des racines

de P , $P' = \lambda \sum_b \left(m(b)(X - b)^{m(b)-1} \prod_{a \neq b} (X - a)^{m(a)} \right)$, donc $\frac{P'}{P} = \sum_b \frac{m(b)}{X - b}$ où b décrit l'ensemble des racines de P , $m(b)$ étant l'ordre de multiplicité de b .