

Polynômes

Table des matières

1	Le \mathbb{K}-espace vectoriel des polynômes sur \mathbb{K}	1
1.1	Définition des polynômes à coefficients dans \mathbb{K}	1
1.2	Degré et coefficient dominant d'un polynôme	2
1.3	L'espace vectoriel $\mathbb{K}[X]$	2
1.4	Bases canoniques de $\mathbb{K}_n[X]$ et $\mathbb{K}[X]$	2
1.5	Génération de $\mathbb{K}_n[X]$ et de $\mathbb{K}[X]$	2
2	L'anneau des polynômes sur \mathbb{K}	3
2.1	Produit de polynômes	3
2.2	Notations	3
3	La division euclidienne	3
4	Fonctions polynômes	4
4.1	Définition des fonctions polynômes	4
4.2	Algorithme de HORNER	4
4.3	Racines d'un polynôme	4
4.4	Interpolation de Lagrange	4
4.5	Extension de la définition	5
5	Dérivation des polynômes	5
5.1	Définition	5
5.2	Formule de LEIBNIZ	5
5.3	Formule de Taylor pour les polynômes	5
5.4	Polynômes dérivés et ordre de multiplicité des racines	5
6	Arithmétique des polynômes	6
6.1	Décomposition en produit de facteurs irréductibles	6
6.2	Un peu de vocabulaire	6
6.3	Polynômes irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$	6

\mathbb{K} est l'un des corps \mathbb{Q} , \mathbb{R} ou \mathbb{C} . $\mathbb{K}^{\mathbb{N}}$ est le \mathbb{K} -e.v. des suites d'éléments de \mathbb{K} .

1 Le \mathbb{K} -espace vectoriel des polynômes sur \mathbb{K}

1.1 Définition des polynômes à coefficients dans \mathbb{K}

Définition : un *polynôme* à coefficients dans \mathbb{K} est une suite $A = (a_n)_{n \in \mathbb{N}}$ d'éléments de \mathbb{K} , nulle à partir d'un certain rang. En d'autres termes: il existe un rang n_0 tel que $a_n = 0$ pour tout $n \geq n_0$.

Nous notons $\mathbb{K}[X]$ l'ensemble des polynômes sur \mathbb{K} .

Le *polynôme nul* est la suite dont tous les termes sont nuls; ce polynôme sera noté $\mathbf{0}$.

Pour $n \in \mathbb{N}$, nous noterons e_n le polynôme défini par $(e_n)_k = \delta_{n,k}$. Le polynôme e_0 sera aussi noté $\mathbf{1}$.

1.2 Degré et coefficient dominant d'un polynôme

Définition : soit $A = (a_n)_{n \in \mathbb{N}}$ un polynôme non nul ; le *degré* de A est le plus grand indice n tel que $a_n \neq 0$; il est noté $\deg(P)$; conventionnellement, $\deg(\mathbf{0}) = -\infty$. L'ensemble des polynômes de degré n au plus est noté $\mathbb{K}_n[X]$.

Nous avons $\mathbb{K}_n[X] \subset \mathbb{K}_{n+1}[X]$ pour tout $n \in \mathbb{N}$; ces inclusions sont toutes strictes, car e_{n+1} appartient à $\mathbb{K}_{n+1}[X]$ mais pas à $\mathbb{K}_n[X]$. Nous avons également $\bigcup_{n \in \mathbb{N}} \mathbb{K}_n[X] = \mathbb{K}[X]$.

Le *coefficient dominant* de $A \neq \mathbf{0}$ est a_d , où $d = \deg(A)$. Nous dirons que A est *unitaire* lorsque ce coefficient vaut 1.

1.3 L'espace vectoriel $\mathbb{K}[X]$

Proposition : soient $A = (a_n)_{n \in \mathbb{N}}$ et $B = (b_n)_{n \in \mathbb{N}}$ deux polynômes, et $\lambda \in \mathbb{K}$. Alors $A + B$ et λA sont encore des polynômes.

Preuve : il existe un rang n_0 à partir duquel a_n et b_n sont nuls ; donc $a_n + b_n$ et λa_n sont nuls à partir de ce rang, et par suite $A + B$ et λA sont des suites à termes nuls APCR.

Remarque : $\mathbb{K}[X]$ n'est pas vide, c'est donc un s.e.v. de $\mathbb{K}^{\mathbb{N}}$. Pour tout $n \in \mathbb{N}$, $\mathbb{K}_n[X]$ est un s.e.v. strict de $\mathbb{K}[X]$.

Proposition : soient A et B deux polynômes ; alors $\deg(A + B) \leq \max(\deg(A), \deg(B))$; si $\deg(A) \neq \deg(B)$ alors $\deg(A + B) = \max(\deg(A), \deg(B))$.

Preuve : notons $n = \deg(A)$ et $p = \deg(B)$; alors $k > \max(n, p)$ implique $a_k = b_k = 0$, donc la suite $A + B$ est à termes nuls à partir du rang $\max(n, p)$, autrement dit le degré de $A + B$ est majoré par $\max(n, p)$. Si $n < p$, alors $a_p = 0$ et $b_p \neq 0$, donc $A + B$ est un polynôme de degré p exactement.

Remarquons que, si $\lambda \neq 0$, alors $\deg(\lambda A) = \deg(A)$.

1.4 Bases canoniques de $\mathbb{K}_n[X]$ et $\mathbb{K}[X]$

Proposition : la famille $(e_k)_{0 \leq k \leq n}$ est une base de $\mathbb{K}_n[X]$.

Preuve : il est clair que cette famille est libre ; elle est génératrice, car le polynôme $A = (a_n)_{n \in \mathbb{N}}$, de degré d au plus, s'écrit $A = \sum_{0 \leq k \leq d} a_k e_k$.

Proposition : la famille $(e_n)_{n \in \mathbb{N}}$ est une base de $\mathbb{K}[X]$, au sens suivant : tout polynôme $A = (a_n)_{n \in \mathbb{N}}$ de degré d au plus s'écrit d'une façon et d'une seule $A = \sum_{0 \leq k \leq d} a_k e_k$.

1.5 Génération de $\mathbb{K}_n[X]$ et de $\mathbb{K}[X]$

Définition : une famille $(P_k)_{0 \leq k \leq n}$ de polynômes est à *degrés échelonnés* si $\deg(P_k) = k$ pour tout $k \in \llbracket 0, n \rrbracket$.

Théorème : toute famille $(P_k)_{0 \leq k \leq n}$ de polynômes à degrés échelonnés est une base de $\mathbb{K}_n[X]$.

Preuve : soit $(\lambda_k)_{0 \leq k \leq n}$ une famille de scalaires vérifiant $\sum_{0 \leq k \leq n} \lambda_k P_k = \mathbf{0}$. Supposons ces scalaires non tous

nuls, et notons d le plus grand indice $k \in \llbracket 0, n \rrbracket$ tel que $\lambda_k \neq 0$. Alors $\sum_{0 \leq k \leq d} \lambda_k P_k = \mathbf{0}$, ce que nous écrivons

$\sum_{0 \leq k < d} \lambda_k P_k = -\lambda_d P_d$. Le membre de gauche est de degré au plus $n - 1$, tandis que le membre de droite est de degré n : d'où la contradiction.

Théorème : toute famille $(P_n)_{n \in \mathbb{N}}$ de polynômes vérifiant $\deg(P_n) = n$ pour tout $n \in \mathbb{N}$ est une base de $\mathbb{K}[X]$.

Preuve : soit Q de degré $n \geq 0$; alors $Q \in \mathbb{K}_n[X]$, donc Q est engendré d'une et une seule façon par la famille libre $(P_k)_{0 \leq k \leq n}$.

2 L'anneau des polynômes sur \mathbb{K}

2.1 Produit de polynômes

Définition : soient $A = (a_n)_{n \in \mathbb{N}}$ et $B = (b_n)_{n \in \mathbb{N}}$ deux polynômes ; le produit $A \times B$ est la suite T de terme général $t_n = \sum_{0 \leq k \leq n} a_k b_{n-k}$.

Proposition : $A \times B$ est un polynôme, de degré $\deg(A) + \deg(B)$.

Preuve : notons p et q les degrés respectifs de A et B . Soit $n > p + q$: $t_n = \sum_{0 \leq k \leq n} a_k b_{n-k}$; si $k > p$, alors $a_k = 0$; si $k \leq p$, alors $n - k > p + q - k \geq q$ et donc $b_{n-k} = 0$. Dans tous les cas, $a_k b_{n-k}$ est nul. Donc le degré de $A \times B$ est au plus $p + q$. Observons que $t_{p+q} = \sum_{0 \leq k \leq p+q} a_k b_{p+q-k}$ se réduit à $a_p b_q$, lequel est non nul ; donc

$\deg(A \times B) = p + q$, et le coefficient dominant de $A \times B$ est égal au produit des coefficients dominants de A et B .

Proposition : $e_p \times e_q = e_{p+q}$.

Preuve : ceci découle de la définition de la famille (e_n) et du calcul effectué dans la précédente preuve.

Proposition : le produit des polynômes est une loi associative.

Preuve : soient $A = (a_n)_{n \in \mathbb{N}}$, $B = (b_n)_{n \in \mathbb{N}}$ et $C = (c_n)_{n \in \mathbb{N}}$ trois polynômes. Alors

$$\begin{aligned} ((A \times B) \times C)_n &= \sum_{0 \leq i \leq n} (A \times B)_i c_{n-i} = \sum_{0 \leq i \leq n} \sum_{0 \leq j \leq i} a_j b_{i-j} c_{n-i} = \sum_{0 \leq j \leq i \leq n} a_j b_{i-j} c_{n-i} \\ &= \sum_{0 \leq j \leq n} a_j \sum_{j \leq i \leq n} b_{i-j} c_{n-i} = \sum_{0 \leq j \leq n} a_j (B \times C)_{n-j} = (A \times (B \times C))_n \end{aligned}$$

Théorème : $(\mathbb{K}[X], +, \times)$ est un anneau commutatif et intègre.

Preuve : $\mathbb{K}[X]$ n'est pas vide ; la loi est associative, elle est clairement commutative et distributive sur l'addition. Le neutre est $\mathbf{1}$. L'intégrité est une conséquence de la formule donnant le degré du produit de deux polynômes.

Remarque : les éléments inversibles de l'anneau $\mathbb{K}[X]$ sont les polynômes constants non nuls.

2.2 Notations

Notons $\mathbf{1} = (\delta_{n,0})_{n \in \mathbb{N}}$ et $X = (\delta_{n,1})_{n \in \mathbb{N}}$

Proposition le polynôme X^n est défini par $(X^n)_j = \delta_{n,j}$.

Preuve : par récurrence : $X^0 = \mathbf{1} = e_0$; si $X^n = e_n$, alors $X^{n+1} = X^n \times X = e_n \times e_1 = e_{n+1}$.

Théorème : la fonction $\lambda \in \mathbb{K} \mapsto \lambda \mathbf{1} \in \mathbb{K}[X]$ est un morphisme injectif de \mathbb{K} dans $\mathbb{K}[X]$, pour la structure de \mathbb{K} -e.v. et pour la structure d'anneau.

Nous identifions désormais $\lambda \in \mathbb{K}$ et $\lambda \mathbf{1}$. Les images des éléments de \mathbb{K} par ce morphisme sont appelées *polynômes constants*. En particulier, nous identifions 1 et $\mathbf{1}$.

Le polynôme $A = (a_n)_{n \in \mathbb{N}}$ sera désormais noté $A = \sum_{0 \leq k \leq d} a_k X^k$, où $d \geq \deg(A)$.

3 La division euclidienne

Théorème : soient A et B deux polynômes, avec $B \neq 0$. Notons n le degré de B . Il existe un et un seul couple (Q, R) de polynômes vérifiant $A = BQ + R$ avec $Q \in \mathbb{K}[X]$ et $R \in \mathbb{K}_{n-1}[X]$.

Nous dirons que Q est le *quotient* et R le *reste* dans la *division euclidienne*.

Existence : si $\deg(A) < n$, alors $Q = 0$ et $R = A$ conviennent. Supposons l'existence de Q et R établie pour tout polynôme A de degré $p \geq n - 1$, et soit A de degré $p + 1$. Notons $A = \sum_{0 \leq k \leq p+1} a_k X^k$ et $B = \sum_{0 \leq k \leq n} b_k X^k$.

Définissons $A_1 = A - \frac{a_{p+1}}{b_n} X^{p+1-n} B$; alors $\deg(A_1) \leq p$; l'hypothèse de récurrence assure l'existence de Q_1 et R_1 vérifiant $A_1 = BQ_1 + R_1$ et $\deg(R_1) < n$. Du coup :

$$A = \frac{a_{p+1}}{b_n} X^{p+1-n} B + BQ_1 + R_1 = B \left(\frac{a_{p+1}}{b_n} X^{p+1-n} + Q_1 \right) + R_1$$

Donc $Q = \frac{a_{p+1}}{b_n} X^{p+1-n} + Q_1$ et R_1 sont le quotient et le reste dans la division euclidienne de A par B . Ceci établit l'existence pour A de degré $p + 1$.

Unicité: supposons que $A = BQ + R = BQ_1 + R_1$, avec R et R_1 tous deux de degré inférieur à n . Alors $R - R_1 = B(Q_1 - Q)$; si $Q \neq Q_1$, alors $B(Q_1 - Q)$ est de degré au moins n , tandis que $R - R_1$ est de degré au plus $n - 1$, ce qui est impossible. Donc $Q = Q_1$ et par suite $R = R_1$.

4 Fonctions polynômes

4.1 Définition des fonctions polynômes

Définition: soit $P \in \mathbb{K}[X]$, avec $P = \sum_{k=0}^n a_k X^k$. Nous notons $\tilde{P} : x \in \mathbb{K} \mapsto \sum_{k=0}^n a_k x^k$. \tilde{P} est la *fonction polynôme* associée à P .

Proposition: $P \mapsto \tilde{P}$ est un morphisme injectif de $\mathbb{K}[X]$ dans l'ensemble $\mathcal{F}(\mathbb{K}, \mathbb{K})$ des fonctions de \mathbb{K} dans \mathbb{K} , pour la structure de \mathbb{K} -e.v. et pour la structure d'anneau.

4.2 Algorithme de Horner

L'algorithme suivant permet d'évaluer $\tilde{P}(x)$ en effectuant n multiplications et autant d'additions.

Soit $P = \sum_{k=0}^n a_k X^k$. Définissons la suite $(V_k)_{0 \leq k \leq n}$ de scalaires comme suit: $V_0 = a_n$ et $V_k = xV_{k+1} + a_{n-k}$ pour $k \in \llbracket 1, n \rrbracket$. Alors $V_n = \tilde{P}(x)$.

4.3 Racines d'un polynôme

Définition: nous dirons que $a \in \mathbb{K}$ est *racine* de $P \in \mathbb{K}[X]$ si $\tilde{P}(a) = 0$.

Proposition: $a \in \mathbb{K}$ est *racine* de $P \in \mathbb{K}[X]$ si $X - a$ divise P .

Preuve: effectuons la division euclidienne de P par $X - a$: il vient $P = (X - a)Q + R$, avec $\deg(R) < 1$; donc R est un polynôme constant. En évaluant les deux membres en a , il vient $R = P(a)$.

Le résultat suivant est essentiel.

Théorème: si P , de degré n au plus, possède au moins $n + 1$ racines, alors $P = \mathbf{0}$.

Preuve: supposons qu'il existe un entier n et un polynôme $P \neq \mathbf{0}$ de degré n au plus, qui possède au moins $n + 1$ racines. Nous pouvons supposer n minimal pour cette propriété; donc $n \geq 1$, puisqu'un polynôme constant, non nul, n'a pas de racines. Soit α une racine de P , alors $P = (X - \alpha)Q$, avec Q de degré $n - 1$ et possédant au moins n racines, ce qui est contradictoire.

4.4 Interpolation de Lagrange

Théorème: soient $(x_k)_{0 \leq k \leq n}$ et $(y_k)_{0 \leq k \leq n}$ deux familles d'éléments de \mathbb{K} , les x_k étant deux à deux distincts. Il existe un et seul polynôme $P \in \mathbb{K}_n[X]$ tel que $P(x_k) = y_k$ pour tout $k \in \llbracket 0, n \rrbracket$.

P est le *polynôme d'interpolation* de LAGRANGE relatif aux points $M_k(x_k, y_k)$.

Preuve: notons $\Phi : P \in \mathbb{K}_n[X] \mapsto (P(x_k))_{0 \leq k \leq n}$. Φ est clairement linéaire. Elle est injective: si $P \in \ker(\Phi)$, alors P , de degré n au plus, possède au moins $n + 1$ racines, donc $P = \mathbf{0}$. Les \mathbb{K} -e.v. $\mathbb{K}_n[X]$ et \mathbb{K}^{n+1} ont même dimension, donc Φ est bijectif.

Nous pouvons expliciter le polynôme P : notant $L_k = \frac{\prod_{j \neq k} (X - x_j)}{\prod_{j \neq k} (x_k - x_j)}$, nous avons clairement $\tilde{L}_k(x_j) = \delta_{j,k}$

donc $\sum_{k=0}^n y_k L_k$ convient.

4.5 Extension de la définition

Théorème : soit $(A, +, \bullet, \times)$ possédant à la fois la structure de \mathbb{K} -e.v. et la structure d'anneau. Soit $\alpha \in A$, distinct de 0_A . Il existe un et un seul morphisme Φ de $\mathbb{K}[X]$ dans A vérifiant $\Phi(X) = \alpha$. Ce morphisme est défini comme suit : si $P = \sum_{k=0}^n a_k X^k$, alors $\Phi(P) = \sum_{k=0}^n a_k \alpha^k$.

Exemple 1 : si E est un \mathbb{K} -e.v. alors $\mathcal{L}(E)$ est à la fois un \mathbb{K} -e.v. et un anneau. Pour tout élément f de $\mathcal{L}(E)$, définissons $P(f) = \Phi(P)$ selon l'homomorphisme précédent. Ceci revient à définir par récurrence $f^0 = Id_E$, et $f^{n+1} = f \circ f^n$ pour tout naturel n , et à poser $P(f) = \sum_{k=0}^n a_k f^k$. $P(f)$ est un *polynôme d'endomorphisme*.

Exemple 2 : $\mathbb{K}[X]$ possède les deux structures requises. Pour $Q \in \mathbb{K}[X]$ fixé, $P \mapsto P(Q)$ est un endomorphisme de $\mathbb{K}[X]$. Notons $P(Q) = P \circ Q$, par analogie avec la composition des fonctions. Si $Q = \lambda$ est constant, $P \circ Q = P(\lambda)$ l'est aussi. Si $Q = X$, alors $P \circ X = P$, ce qui justifie la notation $P(X)$ souvent utilisée (mais pas vraiment utile). Si $Q = X - a$ avec $a \in \mathbb{K}$, alors $P \circ Q = P(X - a)$ et $P \mapsto P(X - a)$ est un automorphisme de $\mathbb{K}[X]$ et de $\mathbb{K}_n[X]$.

5 Dérivation des polynômes

5.1 Définition

Définition : soit $P = \sum_{0 \leq k \leq n} a_k X^k$. Le *polynôme dérivé* de P est $P' = \sum_{1 \leq k \leq n} k a_k X^{k-1}$. Nous notons $D : P \in \mathbb{K}[X] \mapsto P'$; D est l'*opérateur de dérivation* dans $\mathbb{K}[X]$.

Proposition : D est un endomorphisme surjectif de $\mathbb{K}[X]$. Son noyau est $\mathbb{K}_0[X]$. Si $\deg(P) \geq 1$, alors $\deg(P') = \deg(P) - 1$.

Notons D^k le k -ième itéré de l'endomorphisme D . Les polynômes dérivés successifs de P sont les $P^{(k)} = D^k(P)$.

Proposition : $D^k(X^n) = \frac{n!}{(n-k)!} X^{n-k}$ pour $k \in \llbracket 0, n \rrbracket$; en particulier $D^n(X^n) = n!$, et $D^k(X^n) = \mathbf{0}$ pour $k > n$.

Proposition : $(PQ)' = PQ' + P'Q$. Si $\mathbb{K} = \mathbb{R}$, alors $\widetilde{P}' = (\widetilde{P})'$.

5.2 Formule de Leibniz

Proposition : soient P et Q deux polynômes. $D^k(PQ) = \sum_{0 \leq k \leq n} \binom{n}{k} D^k(P) D^n - k(Q)$.

Preuve : par récurrence sur n .

5.3 Formule de Taylor pour les polynômes

Théorème : soit $P \in \mathbb{K}_n[X]$; nous avons :

$$\begin{aligned} P(X) &= \sum_{k=0}^n \frac{P^{(k)}(a)}{k!} (X - a)^k \\ P(X + a) &= \sum_{k=0}^n \frac{a^k}{k!} P^{(k)}(X) = \sum_{k=0}^n \frac{P^{(k)}(a)}{k!} X^k \end{aligned}$$

Preuve : par linéarité, il suffit de vérifier les formules pour $P = X^n$.

5.4 Polynômes dérivés et ordre de multiplicité des racines

Définition : nous dirons que $\alpha \in \mathbb{K}$ est racine de P d'ordre de multiplicité d lorsque P est divisible par $(X - \alpha)^d$ mais pas par $(X - \alpha)^{d+1}$.

Théorème : $\alpha \in \mathbb{K}$ est racine d'ordre d de P ssi $P^{(k)}(\alpha) = 0$ pour $k \in \llbracket 0, d - 1 \rrbracket$ et $P^{(d)}(\alpha) \neq 0$.

Preuve : utiliser la formule de TAYLOR.

6 Arithmétique des polynômes

Définition : soient A et B deux polynômes ; on dira que A est multiple de B (ou que B est diviseur de A , ou que B divise A) s'il existe un polynôme Q tel que $A = B \times Q$. Si $B \neq \mathbf{0}$, ceci revient à dire que le reste dans la division euclidienne de A par B est nul. Sur $\mathbb{K}[X]$, la relation «divise» est réflexive et transitive ; sur l'ensemble des polynômes unitaires, c'est une relation d'ordre partiel. Le plus grand élément est $\mathbf{0}$, et il n'existe pas de plus petit élément.

6.1 Décomposition en produit de facteurs irréductibles

Définition : P est irréductible s'il n'a pour diviseurs que les polynômes constants et les polynômes λP , où $\lambda \neq 0$.

Exemple : un polynôme de degré 1 au plus est irréductible.

Théorème : tout élément $P \neq 0$ de $\mathbb{K}[X]$ se décompose d'une façon et d'une seule (à l'ordre des facteurs près)

sous la forme $P = \lambda \prod_{k=1}^d Q_k^{\alpha_k}$ où $\lambda \in \mathbb{K}$, les Q_k sont irréductibles, unitaires et deux à deux distincts, et les α_k sont des naturels non nuls.

Preuve : pour l'existence, récurrence sur le degré de P . Pour l'unicité, raisonner par l'absurde.

6.2 Un peu de vocabulaire

Nous dirons que $P \in \mathbb{K}[X]$ non constant est *scindé* s'il possède $n = \deg(P)$ racines, distinctes ou confondues, comptées chacune avec son ordre de multiplicité.

Nous dirons que \mathbb{K} est *algébriquement clos* si tout élément non constant de $\mathbb{K}[X]$ est scindé. \mathbb{C} est algébriquement clos (cf. plus bas) ; \mathbb{Q} n'est pas algébriquement clos : observer $X^2 - 2$; \mathbb{R} n'est pas algébriquement clos : observer $X^2 + 1$.

Soit $P \in \mathbb{K}[X]$; résoudre l'équation algébrique $P(X) = 0$, c'est chercher les éléments α de \mathbb{K} qui vérifient $\tilde{P}(\alpha) = 0$.

Soit A un ensemble qui est à la fois un \mathbb{K} -e.v. et un anneau. Un élément α de A est *algébrique* sur \mathbb{K} s'il est solution d'une équation algébrique à coefficients dans \mathbb{K} .

Exemple : $\sqrt{2}$ est algébrique sur \mathbb{Q} ; i est algébrique sur \mathbb{R} . Si E est un \mathbb{K} -e.v. de dimension n , alors, comme $\mathcal{L}(E)$ est de dimension n^2 , tout élément de $\mathcal{L}(E)$ est algébrique sur \mathbb{K} , de degré n^2 au plus. Un projecteur p non banal d'un \mathbb{K} -e.v. est algébrique sur \mathbb{K} , puisque $p^2 = p$.

6.3 Polynômes irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$

Théorème : (d'ALEMBERT-GAUSS, alias «théorème fondamental de l'algèbre») les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1 au plus.

Remarque : ceci revient à dire que \mathbb{C} est algébriquement clos.

Théorème : les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 au plus, et les polynômes de degré 2 de la forme $aX^2 + bX + c$ avec $b^2 - 4ac < 0$.

Théorème : (GALOIS) il n'existe pas d'algorithme permettant de décomposer un élément *quelconque* de $\mathbb{R}[X]$ ou de $\mathbb{C}[X]$ en produit de facteurs irréductibles.

FIN