MATHÉMATIQUES GÉNÉRALES 1
Polynômes

1 Généralités, degré, opérations avec les polynômes

Dans la suite $\mathbb{K}$ sera un corps commutatif ($\mathbb{R}, \mathbb{C}$ ou, parfois, $\mathbb{Q}$).

Définition 1. (Formelle) On appelle *polynôme à une indéterminée avec coefficients dans* $\mathbb{K}$ toute suite $a_0, a_1, \ldots, a_n, \ldots$ d'éléments de $\mathbb{K}$ presque tous nuls. Les a_i sont appelés *coefficients* du polynôme. L'ensemble de tous les polynômes à une indéterminée avec coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$.

Soit $a_0, a_1, \ldots, a_n, \ldots$ un polynôme à une indéterminée avec coefficients dans $\mathbb{K}$. Par définition, l'ensemble $\{i \in \mathbb{N} \mid a_i \neq 0\}$ est fini et donc, s'il est non vide, il admet un maximum.

Définition 2. On appelle *degré du polynôme* $a_0, a_1, \ldots, a_n, \ldots$ l'entier naturel $\max\{i \in \mathbb{N} \mid a_i \neq 0\}$ lorsque $\{i \in \mathbb{N} \mid a_i \neq 0\} \neq \emptyset$. Si $\{i \in \mathbb{N} \mid a_i \neq 0\} = \emptyset$ on pose par convention le degré de la suite identiquement nulle égal à $-\infty$.

On peut munir $\mathbb{K}[X]$ de trois opérations :

1. *Une somme (ponctuelle)* : si $a_0, a_1, \ldots, a_n, \ldots$ et $b_0, b_1, \ldots, b_n, \ldots$ sont deux polynômes leur somme est le polynôme $c_0, c_1, \ldots, c_n, \ldots$, où $c_i = a_i + b_i$ pour tout $i \in \mathbb{N}$; on remarque facilement que les éléments de $c_0, c_1, \ldots, c_n, \ldots$ sont presque tous nuls. En effet, on voit même que le degré du polynôme somme est au plus le maximum des degrés de polynômes $a_0, a_1, \ldots, a_n, \ldots$ et $b_0, b_1, \ldots, b_n, \ldots$.
2. *Un produit externe* : si $a_0, a_1, \ldots, a_n, \ldots$ et $\lambda \in \mathbb{K}$ le polynôme produit de $a_0, a_1, \ldots, a_n, \ldots$ par le scalaire λ est le polynôme $c_0, c_1, \ldots, c_n, \ldots$, où $c_i = \lambda a_i$ pour tout $i \in \mathbb{N}$. On remarque que si $\lambda \neq 0$, $\{i \in \mathbb{N} \mid a_i \neq 0\} = \{i \in \mathbb{N} \mid c_i \neq 0\}$ et les deux polynômes ont le même degré.
3. *Un produit interne (de Cauchy)* : si $a_0, a_1, \ldots, a_n, \ldots$ et $b_0, b_1, \ldots, b_n, \ldots$ sont deux polynômes leur produit est le polynôme $c_0, c_1, \ldots, c_n, \ldots$, où $c_i = \sum_{k=0}^{i} a_k b_{i-k}$ pour tout $i \in \mathbb{N}$. On peut vérifier que le degré du polynôme produit est la somme des degrés des deux facteurs.

Un calcul élémentaire montre que le résultat de la multiplication d'un polynôme $a_0, a_1, \ldots, a_n, \ldots$ par le scalaire λ coïncide avec sa multiplication par le polynôme Λ défini par $\Lambda_0 = \lambda$ et $\Lambda_i = 0$ pour tout $i \in \mathbb{N}^*$. On note par $1 \in \mathbb{K}[X]$ le polynôme $1, 0, \ldots, 0, \ldots$: la multiplication d'un polynôme par 1 redonne le polynôme de départ.
On note X le polynôme $0, 1, 0, \ldots, 0, \ldots$. Une récurrence immédiate montre que X^n est le polynôme ayant comme seul coefficient non nul celui d'indice n qui vaut 1.
On note ensuite $0 \in \mathbb{K}[X]$ le polynôme dont tous les coefficients sont nuls.

En utilisant les opérations sur les polynômes on voit que tout polynôme $a_0, a_1, \ldots, a_n, \ldots$ peut s'écrire de façon unique comme $\sum_{i\in\mathbb{N}} a_i X^i$, où $a_i X^i$ dénote la multiplication du scalaire a_i par le polynôme X^i et on pose par convention $X^0 = 1$. On retrouve ainsi l'écriture habituelle. On observera que, par définition même, deux polynômes coïncident si et seulement s'ils ont les mêmes coefficients.
Avec cette notation, on peut résumer les propriétés sur le degré comme suit :

Proposition 1. *Soient $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. On a*
- $\deg(P+Q) \leqslant \max(\deg P, \deg Q)$ *avec inégalité si et seulement si* $\deg P = \deg Q$ *et les* coefficients dominants *(i.e. d'indice maximal) de P et Q sont opposés.*
- $\deg(PQ) = \deg P + \deg Q$*, où par convention $-\infty + n = -\infty$.*
- $\deg(\lambda P) = \deg P$ *si $\lambda \neq 0$ et $= -\infty$ sinon.*

La propriété suivante découle immédiatement de la Proposition qu'on vient de voir.

Proposition 2. *Soient $P, Q \in \mathbb{K}[X]$. On a $PQ = 0$ si et seulement si $P = 0$ ou $Q = 0$.*

Les propriétés suivantes découlent des propriétés analogues pour $\mathbb{K}$.

Remarque 1. La somme de polynômes
- est *associative* : $(P+Q)+R = P+(Q+R)$ pour tous $P, Q, R \in \mathbb{K}[X]$;
- est *commutative* $P+Q = Q+P$ pour tous $P, Q \in \mathbb{K}[X]$;
- a un *élément neutre* $P+0 = 0+P = P$ pour tout $P \in \mathbb{K}[X]$;
- tout polynôme P a un *opposé* $-P = (-1)P$, à savoir le polynôme dont les coefficients sont les opposés des coefficients de P : $P+(-P) = (-P)+P = 0$.

On dit alors que $(\mathbb{K}[X], +)$ est un *groupe abélien*.
Le produit externe satisfait
- $\lambda(P+Q) = \lambda P + \lambda Q$ pour tout $\lambda \in \mathbb{K}$ et tous $P, Q \in \mathbb{K}[X]$;
- $(\lambda+\mu)P = \lambda P + \mu P$ pour tous $\lambda, \mu \in \mathbb{K}$ et tout $P \in \mathbb{K}[X]$;
- $(\lambda\mu)P = \lambda(\mu P)$ pour tous $\lambda, \mu \in \mathbb{K}$ et tout $P \in \mathbb{K}[X]$;
- $1P = P$ pour tout $P \in \mathbb{K}[X]$ (ici $1 \in \mathbb{K}$).

On dit alors que $\mathbb{K}[X]$ muni de la somme et du produit externe est un $\mathbb{K}$-*espace vectoriel*.
Le produit interne
- est *associatif* : $(PQ)R = P(QR)$ pour tous $P, Q, R \in \mathbb{K}[X]$;
- est *commutatif* $PQ = QP$ pour tous $P, Q \in \mathbb{K}[X]$;
- a un *élément neutre* $P1 = 1P = P$ pour tout $P \in \mathbb{K}[X]$;
- est *distributif par rapport à la somme* : $P(Q+R) = PQ + PR$.

On dit alors que $\mathbb{K}[X]$ muni de la somme et du produit interne est un *anneau abélien unitaire*. ($\mathbb{K}[X]$ avec seulement le produit interne est un *monoïde abélien* alors qu'avec toutes ces opérations il est une $\mathbb{K}$-*algèbre associative, commutative et unitaire*).

Remarque 2. Il y a une inclusion naturelle de $\mathbb{K}$ dans $\mathbb{K}[X]$ définie par $a \mapsto a1 = a$. Cette inclusion préserve la structure de corps commutatif de $\mathbb{K}$.

Définition 3. Soit A un ensemble muni d'une loi de composition interne $\cdot$ admettant un élément neutre $e \in A$. Soit $y \in A$. On dit que y est *inversible* dans A par rapport à $\cdot$ s'il existe $z \in A$ tel que $y \cdot z = z \cdot y = e$.

Proposition 3. *Les éléments inversibles de $\mathbb{K}[X]$ (par rapport au produit interne) sont précisément ceux de $\mathbb{K}^*$.*

Démonstration. Il suffit de considérer le degré. □

Définition 4. On note $\mathbb{K}[X]_{\leqslant n}$ l'ensemble des polynômes de $\mathbb{K}[X]$ de degré $\leqslant n$.

La proposition vue sur le degré montre que la somme de deux polynômes de $\mathbb{K}[X]_{\leqslant n}$ est encore un polynôme de $\mathbb{K}[X]_{\leqslant n}$. De même, la multiplication d'un polynôme de $\mathbb{K}[X]_{\leqslant n}$ par un scalaire est encore un polynôme de $\mathbb{K}[X]_{\leqslant n}$.

Définition 5. Soient $P(X) = \sum_{i=0}^{n} a_i X^i$ et $Q(X) = \sum_{j=0}^{m} b_j X^j$ deux polynômes de $\mathbb{K}[X]$. On peut définir la *composition* $P \circ Q \in \mathbb{K}[X]$ de P et Q de la façon suivante :

$$P \circ Q(X) = P(Q(X)) = \sum_{i=0}^{n} a_i Q^i(X).$$

Attention ! La composition de polynômes est associative (i.e. $(P \circ Q) \circ R = P \circ (Q \circ R)$) mais pas commutative, à savoir $P \circ Q \neq Q \circ P$ en général.

Exemple 1. Soient $P(X) = X + 1$ et $Q(X) = X^2$. On a alors $P \circ Q(X) = X^2 + 1 \neq Q \circ P(X) = X^2 + 2X + 1$.

2 Division euclidienne, Bézout, PGCD, ppcm

Théorème 1. (Division euclidienne) *Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Il existe deux polynômes $Q, R \in \mathbb{K}[X]$ uniques, avec $\deg R < \deg B$, tels que $A = BQ + R$.*

Définition 6. On appelle R le *reste de la division euclidienne* de A par B. On dit aussi que B *divise* A s'il existe Q tel que $A = BQ$. On remarquera que si B n'est pas nul, B divise A si et seulement si le reste de la division euclidienne de A par B vaut 0.

Démonstration. Unicité : Supposons que $A = BQ + R$ et $A = BQ' + R'$. On en tire $B(Q - Q') = R' - R$. Or $\deg(R' - R) \leqslant \max(\deg R', \deg R) < \deg B$, d'où $Q - Q' = 0$ et par conséquent $R' - R = 0$.
Existence : Supposons d'abord $\deg A < \deg B$. Dans ce cas il suffit de prendre $Q = 0$ et $R = A$. On peut alors supposer $\deg A \geqslant \deg B$. On va raisonner par récurrence sur $n = \deg A - \deg B = m - d$. Soient $A = \sum_{i=0}^{m} a_i X^i$ et $B = \sum_{j=0}^{d} b_j X^j$. Si $n = 0$ on pose $Q = a_m/b_d$ et $R = A - BQ$. Sinon on considère $P_1 = a_m X^n / b_d$ et on pose $A_1 = A - BP_1$. On constate que $\deg A_1 < \deg A$. On applique l'hypothèse de récurrence au couple A_1, B et on obtient deux polynômes Q_1, R_1. On alors $A_1 = BQ_1 + R_1$, d'où on tire $A = B(Q_1 + P_1) + R_1$, ce qui permet d'obtenir $Q = Q_1 + P_1$ et $R = R_1$. □

On aura remarqué que la preuve du théorème donne en effet un algorithme pour calculer Q et R.

Exemple 2. On prend $A = X^7 + 5X^5 - 2X^4 + X^3 - 4X^2 - 4$ et $B = X^3 - 1$. On pose $P_1 = X^4$, d'où $A_1 = A - BP_1 = 5X^5 - X^4 + X^3 - 4X^2 - 4$. On pose $P_2 = 5X^2$ d'où $A_2 = A_1 - BP_2 = -X^4 + X^3 + X^2 - 4$. On pose $P_3 = -X$ d'où $A_3 = A_2 - BP_3 = X^3 + X^2 - X - 4$. Enfin $P_4 = 1$ d'où $A_4 = A_3 - BP_4 = X^2 - X - 3$. Comme $\deg A_4 < \deg B$ la procédure est terminée ; on en déduit que $A = BP_1 + A_1 = BP_1 + BP_2 + A_2 = ... = BP_1 + BP_2 + BP_3 + BP_4 + A_4 = B(P_1 + P_2 + P_3 + P_4) + A_4$: le quotient de la division

est donc $P_1+P_2+P_3+P_4 = X^4+5X^2-X+1$ et le reste est $A_4 = X^2-X-3$. On peut vérifier que effectivement $A = (X^3-1)(X^4+5X^2-X+1)+X^2-X-3$. L'ensemble de ce calcul peut s'effectuer en présentant les choses comme suit :

$$\begin{array}{rrrrrrr|l}
X^7 & +5X^5 & -2X^4 & +X^3 & -4X^2 & & -4 & X^3-1 \\
\cline{8-8}
X^7 & & -X^4 & & & & & X^4+5X^2-X+1 \\
\cline{1-7}
 & 5X^5 & -X^4 & +X^3 & -4X^2 & & -4 & \\
 & 5X^5 & & & -5X^2 & & & \\
\cline{2-7}
 & & -X^4 & +X^3 & +X^2 & & -4 & \\
 & & -X^4 & & & +X & & \\
\cline{3-7}
 & & & X^3 & +X^2 & -X & -4 & \\
 & & & X^3 & & & -1 & \\
\cline{4-7}
 & & & & X^2 & -X & -3 &
\end{array}$$

Remarque 3. Les affirmations suivantes sont évidentes. Soient A, B deux polynômes de $\mathbb{K}[X]$.
Si $A = 0$ alors tout $B \in \mathbb{K}[X]$ divise A.
Si $B = 0$ et B divise A alors $A = 0$.
Si B est un polynôme constant non nul alors B divise tout $A \in \mathbb{K}[X]$.
Si B divise A alors $A = 0$ ou $\deg B \leqslant \deg A$.

Définition 7. (PGCD) Soient A, B deux polynômes de $\mathbb{K}[X]$. On appelle *PGCD* de A et B tout polynôme $P \in \mathbb{K}[X]$ satisfaisant ces deux conditions :

1. P divise A et B ;
2. si $D \in \mathbb{K}[X]$ est un diviseur commun de A et B alors D divise P.

Remarque 4. Bien sûr $\mathrm{PGCD}(A,B) = \mathrm{PGCD}(B,A)$. De plus on a $\mathrm{PGCD}(CA,CB) = C\mathrm{PGCD}(B,A)$. En effet, si P est un polynôme qui divise A et B, CP est un polynôme qui divise CA et CB ce qui montre que $C\mathrm{PGCD}(B,A)$ divise $\mathrm{PGCD}(CA,CB)$. Par ailleurs, C divise CA et CB et donc il divise aussi $\mathrm{PGCD}(CA,CB)$ ce qui montre que $\mathrm{PGCD}(CA,CB)$ divise $C\mathrm{PGCD}(B,A)$.

Proposition 4. *$PGCD(A,B) = 0$ si et seulement si $A = B = 0$.*
Si $PGCD(A,B) \neq 0$, alors il est unique à multiplication par une constante non nulle près. Il existe donc un unique $PGCD(A,B)$ unitaire (de coefficient dominant égal à 1) ou nul.

Démonstration. $\mathrm{PGCD}(A,B) = 0$ si et seulement si tout polynôme divise A et B. Dans ce cas, on unicité du $PGCD$.
Supposons que $P \neq 0$ et $\tilde{P}$ satisfont tous les deux les conditions de la définition. Puisque P est un diviseur de A et B on doit avoir $\tilde{P} = \tilde{Q}P$ et, de même $P = Q\tilde{P}$. Il en suit que $P = Q\tilde{Q}P$ et donc $\tilde{Q}Q = 1$, car $P \neq 0$. □

Il suffit maintenant de montrer l'existence du PGCD. Si $A = B = 0$ alors on prend $\mathrm{PGCD}(A,B) = 0$. Si $A = 0$ mais $B \neq 0$ on prend $\mathrm{PGCD}(A,B) = B$. On va donc considérer le cas $A, B \neq 0$. Avant de continuer, remarquons aussi que si $\deg A = 0$ et $B \neq 0$ alors $\mathrm{PGCD}(A,B) = 1$.

Proposition 5. (Algorithme d'Euclide) *Si $A, B \in \mathbb{K}[X]$ ne sont pas tous les deux nuls, leur PGCD existe et peut être calculé grâce à* l'algorithme d'Euclide.

Démonstration. Sans perte de généralité on peut supposer que $B \neq 0$. On fait la division euclidienne de A par B : $A = BQ + R$. On remarque alors que un polynôme divise A et B si et seulement s'il divise B et R. On en déduit que $\mathrm{PGCD}(A, B) = \mathrm{PGCD}(B, R)$. Puisque la suite des degrés des restes est strictement décroissante, on obtiendra, en un nombre fini de divisions, un reste nul. Le PGCD cherché est le dernier diviseur (qui est aussi le dernier reste non nul). □

Exemple 3. Calculons le PGCD de $A = X^7 + 5X^5 - 2X^4 + X^3 - 4X^2 - 4$ et $B = X^3 - 1$. On a $\mathrm{PGCD}(A, B) = \mathrm{PGCD}(X^3 - 1, X^2 - X - 3)$. On fait un autre division euclidienne $X^3 - 1 = (X^2 - X - 3)(X + 1) + (4X + 2)$ et encore une $X^2 - X - 3 = (4X + 2)(\frac{1}{4}X - \frac{3}{8}) + \frac{9}{4}$. On déduit que $\mathrm{PGCD}(A, B) = 1$.

Définition 8. On dit que deux polynômes A et B sont *premiers entre-eux* si $\mathrm{PGCD}(A, B) = 1$.

En remontant, l'algorithme d'Euclide montre aussi l'existence de deux polynômes U et V tels que $\deg V < \deg A$, $\deg U < \deg B$ et $AU + BV = \mathrm{PGCD}(A, B)$.

Théorème 2. (Bézout) *Soient $A, B \in \mathbb{K}[X]$ deux polynômes non nuls.*
Il existe deux polynômes U et V tels que $\deg U < \deg B$, $\deg V < \deg A$ et $AU + BV = PGCD(A, B)$.
A et B sont premiers entre-eux si et seulement s'il existe U et V tels que $AV + BU = 1$.

Définition 9. On appelle *polynômes de Bézout pour A et B* les polynômes dont l'existence est assurée par le théorème précédent.

Démonstration. Quitte à échanger A avec B on peut supposer que $\deg A \geqslant \deg B$. Par l'algorithme d'Euclide on a $A - Q_0B = R_1$, $B - Q_1R_1 = R_2$, $R_1 - Q_2R_2 = R_3$,..., $R_{n-2} - Q_{n-1}R_{n-1} = R_n$, $R_{n-1} - Q_nR_n = 0$, où R_n est donc le PGCD de A et B et $\deg B > \deg R_1 > \cdots > \deg R_n$. En remplaçant l'expression pour R_i dans l'égalité suivante, de proche en proche, on voit qu'on peut expliciter R_{i+1} comme $AV_i + BU_i$. Il reste à vérifier la condition sur les degrés. Pour cela on pose $V_0 = 1$ et $U_0 = -Q_0$, $V_1 = -Q_1$, $U_1 = 1 - Q_1Q_0 = 1 - Q_1U_0$. Les formules suivantes se vérifient facilement par récurrence : $V_{i+1} = V_{i-1} - Q_{i+1}V_i$ et $U_{i+1} = U_{i-1} - Q_{i+1}U_i$. En tenant compte du fait que $\deg R_i = \deg R_{i+1} + \deg Q_{i+1}$ on a que $\deg Q_{i+1} > 0$, ce qui montre que la suite $\deg U_i$ est croissante et $\deg U_{i+1} = \deg Q_{i+1} + \deg U_i = -\deg R_{i+1} + \deg R_i + \deg U_i$. Il en suit $\deg U + \deg R_n = \deg U_n + \deg R_n = \deg U_0 + \deg B = \deg A$ et donc $\deg U < \deg A$. Le fait d'avoir $AV = R - BU$ implique $\deg V < \deg A$ en tenant compte du fait que $\deg R \leqslant \deg B$.
Reciproquement, si $AV + BU = 1$, alors tout polynôme qui divise A et B doit diviser 1 et puisque 1 divise tout polynôme il est, par définition, le PGCD de A et B. □

Exemple 4. Pour les polynômes de l'exemple précédent on a

$$A\frac{2X^2 - X + 5}{18} + B\frac{2X^6 - X^5 - X^4 - 7X^3 - 58X^2 + 11X - 2}{18}.$$

Théorème 3. (Gauss) *Soient A, B et C trois polynômes tels que A divise le produit BC et A et B sont premiers entre eux. Alors A divise C.*

Démonstration. Le théorème de Bézout dit qu'il existe U et V tels que $AU + BV = 1$. En multipliant par C on obtient $A(UC) + (BC)V = C$. Puisque A divise le terme de gauche, il doit diviser C. □

Corollaire 1. *Soient A, B et D trois polynômes tels que A et B sont premiers entre eux et divisent D. Alors, AB divise D.*

Démonstration. On écrit $D = CB$ et on applique le théorème de Gauss. □

Définition 10. Soient A et B deux polynômes. On appelle $\text{ppcm}(A, B)$ un polynôme divisible par A et B et qui divise tout multiple commun de A et B.

Si l'un parmi A ou B est nul, alors on doit avoir $\text{ppcm}(A, B) = 0$ (car 0 est le seul multiple de 0). Si A et B sont premiers entre eux, le corollaire qu'on vient de voir dit que $\text{ppcm}(A, B) = AB$. Dans le cas où A ou B sont non nuls mais arbitraires on a la relation $AB = \text{ppcm}(A, B)\text{PGCD}(A, B)$. Celle-ci découle du fait que $\text{ppcm}(CA, CB) = C\text{ppcm}(A, B)$ et qu'en divisant deux polynômes par leur PGCD on obtient deux polynômes premiers entre eux. Comme pour le PGCD, le ppcm est unique à multiplication par un nombre non-nul près.

3 Polynômes irréductibles, critères d'irréductibilité

Définition 11. Soit P un polynôme de $\mathbb{K}[X]$ de degré positif (à savoir non nul et non inversible). On dit qu'il est *irréductible sur* $\mathbb{K}$ si pour tous B et $C \in \mathbb{K}[X]$ tels que $P = BC$, B ou C a pour degré 0 (à savoir est inversible).

Exemple 5. Tout polynôme de degré 1 est irréductible. Attention ! X^2+1 est irréductible sur $\mathbb{K} = \mathbb{R}$ mais pas sur $\mathbb{K} = \mathbb{C}$ car on peut écrire $X^2 + 1 = (X + i)(X - i)$.

Théorème 4. (Décomposition en facteurs irréductibles) *Soit $A \in \mathbb{K}[X]$ un polynôme non nul. Il existe un unique $a \in \mathbb{K}^*$ et des polynômes irréductibles unitaires $P_1, \ldots, P_k$ de $\mathbb{K}[X]$ tels que $A = aP_1 \ldots P_k$. De plus, la décomposition est unique, c'est-à-dire que les $P_1, \ldots, P_k$ sont uniques à permutation près.*

Démonstration. On choisit a comme le coefficient directeur de A (i.e. celui du terme de plus grand degré). Si A n'est pas divisible par des par des polynômes de degré positif et strictement plus petit que $\deg A$ on a fini. Sinon on écrit A comme produit et on répète ce raisonnement sur chaque facteur. Puisque le degré des facteurs décroît strictement, ce procédé se termine en un nombre fini d'étapes.
Pour l'unicité il suffit de voir que deux polynômes irréductibles sont soit le même à multiplication d'une constante non nulle près, ou sont premiers entre eux. Ceci vient du fait que le PGCD est un diviseur des deux polynômes. Si on choisit les P_i unitaires, ils doivent vraiment coïncider. □

Cette décomposition donne une autre façon pour calculer le PGCD et le ppcm de deux polynômes : on commence par décomposer les deux polynômes en facteurs irréductibles puis on prend tous les facteurs communs (avec la plus petite multiplicité) pour obtenir le PGCD et tous les facteurs possibles (avec ma plus grande multiplicité) pour obtenir le ppcm.

Définition 12. Soit $P \in \mathbb{K}[K]$ un polynôme de degré positif. On dit que P est *premier dans* $\mathbb{K}[K]$ si à chaque fois que P divise un produit de polynômes BC de $\mathbb{K}[K]$ il divise au moins l'un des deux.

Proposition 6. *Un polynôme P de $\mathbb{K}[K]$ est irréductible sur $\mathbb{K}$ si et seulement s'il est premier dans $\mathbb{K}[K]$.*

Démonstration. Supposons P premier. Si on a $P = BC$ alors P divise BC et donc divise soit B soit C. On peut supposer que $B = PQ$. Mais alors $P = PQC$ et donc $\deg C = 0$ et P est irréductible.
Supposons alors P irréductible. En utilisant le théorème précédent on voit que P doit apparaître dans la décomposition de BC. L'unicité assure que les facteurs irréductibles de la décomposition de BC sont l'union des facteurs irréductibles des décompositions de B et C. La conclusion suit. □

Théorème 5. *Les seuls polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*

Ce théorème est une traduction du théorème de d'Alambert-Gauss qu'on verra dans la prochaine section. Une conséquence immédiate est que tout polynôme de $\mathbb{C}[X]$ se factorise en produit de polynômes de degré 1, à savoir de la forme $X - \alpha$.

Théorème 6. *Les seuls polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 avec* discriminant négatif.

Définition 13. Soit $P = aX^2 + bX + c$ un polynôme de degré 2 (en particulier $a \neq 0$). Le *discriminant* de P est le nombre $b^2 - 4ac$.

Remarque 5. La conjugaison complexe induit une application $\phi : \mathbb{C}[X] \longrightarrow \mathbb{C}[X]$ définie par $\sum_i a_i X^i \mapsto \sum_i \bar{a}_i X^i$. Les propriétés suivantes sont faciles à vérifier :
- $\phi(P) = P$ si et seulement si tous les coefficients de P sont dans $\mathbb{R}$;
- $\phi(P + Q) = \phi(P) + \phi(Q)$;
- $\phi(PQ) = \phi(P)\phi(Q)$.

Démonstration. Soit $A \in \mathbb{R}[X]$. On peut supposer A unitaire. Puisque $A \in \mathbb{C}[X]$ on peut décomposer A en produit de polynômes de degré 1 sur $\mathbb{C}$. En utilisant l'application défini dans la remarque et ses propriétés, on voit que ϕ de la décomposition de A doit être encore une décomposition pour A. Il en suit que si $X - \alpha$ est un facteur irréductible de A avec $\alpha \in \mathbb{C} \setminus \mathbb{R}$ alors $X - \bar{\alpha}$ doit être aussi un facteur irréductible de A. Leur produit donne $X^2 + 2\Re(\alpha)X + |\alpha|^2$ qui est bien un polynôme réel. De plus $4\Re(\alpha)^2 - 4|\alpha|^2 = -4\Im(\alpha)^2 < 0$.
Réciproquement si P est un polynôme réel de degré 2 qui peut s'écrire comme produit de deux polynômes réels de degré 1 alors $(\alpha X - \beta)(\gamma X - \delta) = \alpha\gamma X^2 - (\alpha\delta + \beta\gamma)X + \beta\delta$ et son discriminant est $(\alpha\delta + \beta\gamma)^2 - 4\beta\delta\alpha\gamma = (\alpha\delta - \beta\gamma)^2 \geqslant 0$. □

Complément : irréductibilité dans $\mathbb{Q}[X]$.

Théorème 7. (Critère d'Eisenstein) *Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Q}[X]$ un polynôme dont tous les coefficients a_i sont des entiers. S'il existe un nombre premier p tel que*
- *pour tout $i \in \{0, \ldots, n-1\}$ p divise a_i*
- *p ne divise pas a_n*
- *p^2 ne divise pas a_0*

alors P est irréductible sur $\mathbb{Q}$.

Démonstration. On a besoin du

Lemme 1. (Gauss) *Soit P un polynôme à coefficients entiers. Si P est le produit de deux polynômes de $\mathbb{Q}[X]$ alors P est aussi le produit de deux polynômes à coefficients entiers.*

Démonstration. On a $P = AB$. On peut alors écrire $A = \frac{c_1}{d_1}A_1$ où d_1 est le ppcm des dénominateurs des coefficients de A, c_1 le PGCD des numérateurs et A est a coefficients entiers. On fait de même avec B : $B = \frac{c_2}{d_2}B_2$. On a alors $P = (\frac{c_1}{d_1}A_1)(\frac{c_2}{d_2}B_2)$ et, quitte à simplifier, on peut supposer que $\frac{c_1c_2}{d_1d_2}$ est une fraction réduite. On a alors une égalité entre polynômes à coefficients entiers : $d_1d_2P = c_1c_2A_1B_2$. Il suffit de montrer que $d_1d_2 = 1$. Sinon, soit p un nombre premier qui divise d_1d_2. Puisque les coefficients de A_1 sont premiers entre eux il existe un plus petit indice i tel que a_i n'est pas divisible par p. De même il existe un plus petit indice j tel que b_j n'est pas divisible par p. Il en suit que le coefficient d'indice $i + j$ de d_1d_2P n'est pas divisible par p (car p ne divise pas c_1c_2) ce qui est absurde. □

Supposons par l'absurde que P s'écrit comme produit de deux polynômes de $\mathbb{Q}[X]$ que, d'après le lemme de Gauss, on peut supposer être à coefficients entiers : $P = \sum_{i=0}^{n} a_iX^i = \sum_{j=0}^{k} b_jX^j \sum_{l=0}^{n-k} c_lX^l$. On a $a_i = \sum_{j+l=i} b_jc_l$. Puisque p divise $a_0 = b_0c_0$ mais pas p^2, p divise un et un seul parmi b_0 et c_0. Sans perte de généralité on peut supposer que p divise b_0. On voit sans peine, par récurrence, que p doit diviser b_j pour tout j puisque $k < n$ et p divise a_j si $j < n$. Il en suit que p divise $a_n = b_kc_{n-k}$, contre l'hypothèse. □

4 Fonctions polynomiales, racines

Étant donné un polynôme $P = \sum_{i=0}^{n} a_iX^i \in \mathbb{K}[X]$ on peut lui associer une fonction polynomiale, notée encore P et définie comme suit :

Définition 14.

$$P : \mathbb{K} \longrightarrow \mathbb{K}$$
$$x \mapsto P(x) = \sum_{i=0}^{n} a_ix^i$$

Remarque 6. Il est facile de voir que la fonction polynomiale associée à la somme de deux polynômes est la somme des fonctions polynomiales associées aux deux polynômes. La propriété analogue est valable pour le produit.

Définition 15. Soit $P \in \mathbb{K}[X]$ un polynôme est $P(x)$ la fonction polynomiale associée. On appelle *racine de P* tout nombre $\alpha \in \mathbb{K}$ tel que $P(\alpha) = 0$.

Proposition 7. *Soit P un polynôme de $\mathbb{K}[X]$. P admet $\alpha \in \mathbb{K}$ comme racine si et seulement si le polynôme $X - \alpha$ divise P.*

Démonstration. On fait la division euclidienne de P par $X - \alpha$. On a $P = Q(X - \alpha) + R$, où $\deg R \leqslant 0$. En considérant les fonctions polynomiales associées aux polynômes à droite et à gauche de l'égalité on voit bien $P(\alpha) = R$. Il en suit que $X - \alpha$ divise P si et seulement si $R = 0$ si et seulement si α est racine de de P. □

Puisque $X - \alpha$ et $X - \beta$ sont premier entre eux si et seulement si $\alpha \neq \beta$ on a :

Corollaire 2. — *Un polynôme de degré n a au plus n racines distinctes.*
— *Soit P est un polynôme de degré $\leqslant n$. S'il existe $n+1$ éléments de $\mathbb{K}$, deux à deux distincts, qui sont racines de P alors P est le polynôme nul.*

Définition 16. Soit P un polynôme et α une racine de P. On appelle *multiplicité de la racine* α le $\max\{r \in \mathbb{N} \mid (X-\alpha)^r$ divise $P\}$. On dit que α est une *racine simple* si sa multiplicité vaut 1 et multiple si sa multiplicité vaut > 1.

Théorème 8. (d'Alambert-Gauss) *Tout polynôme de $\mathbb{C}[X]$ de degré $\geqslant 1$ a au moins une racine (dans $\mathbb{C}$).*

Définition 17. On définit une application *la dérivation*

$$\mathbb{K}[X] \longrightarrow \mathbb{K}[X]$$

par

$$P = \sum_{i=0}^{n} a_i X^i \mapsto P' = \sum_{i=1}^{n} i a_i X^{i-1}$$

où P' est le *polynôme dérivé de P*.

L'application qui associe à un polynôme le polynôme dérivé satisfait :
— pour tous $A, B \in \mathbb{K}[X]$ et $\lambda \mathbb{K}$ $(A+B)' = A' + B'$ et $(\lambda A) = \lambda(A')$ (on dit que l'application est *linéaire*)
— pour tous $A, B \in \mathbb{K}[X]$ $(AB)' = (A')B + A(B')$ (*règle de Leibnitz*)

Définition 18. Le polynôme *dérivé kième* de P est le polynôme $P^{(k)}$ obtenu en dérivant P k fois. On peut définir cela par récurrence : $P^{(k)} = (P^{(k-1)})'$.

L'égalité suivante (dite *formule de Leibnitz*) se montre par récurrence en utilisant la règle de Leibnitz :

$$(AB)^{(k)} = \sum_{j=0}^{k} C_k^j A^{(j)} B^{(k-j)}$$

où A et B sont deux polynômes, et on pose par convention $A^{(0)} = A$ et $A^{(1)} = A'$ pour tout polynôme A.

Corollaire 3. *Si un polynôme P admet des racines multiples alors $PGCD(P, P') \neq 1$.*

Attention : la réciproque du corollaire est vraie sur $\mathbb{C}$ mais pas sur $\mathbb{R}$ ou $\mathbb{Q}$.

Proposition 8. (Formule de Taylor) *Soit $P \in \mathbb{K}[X]$ de degré n. On a*

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

Démonstration. On sait qu'on peut écrire $P = \sum_{i=1}^{n} a_i (X-\alpha)^i$. il suffit alors d'identifier les a_i en considérant les dérivées successives de P et en les évaluant en α. □

Corollaire 4. *Soit $\alpha \in \mathbb{K}$ une racine de $P \in \mathbb{K}[X]$. La multiplicité de α est r si et seulement si $P^{(k)}(\alpha) = 0$ pour tout $k < r$ mais $P^{(r)}(\alpha) \neq 0$. En particulier une racine est multiple si et seulement si elle est aussi racine de P'.*

Complément : Racines rationnelles d'un polynôme rationnel

Proposition 9. (Racines d'un polynôme rationnel) *Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Q}[X]$ un polynôme à coefficients dans $\mathbb{Z}$ et soit $\frac{b}{c}$ une racine en forme réduite (i.e. $PGCD(b,c) = 1$). Alors on a que b divise a_0 et c divise a_n.*

Démonstration. Il suffit d'évaluer P en $\frac{b}{c}$ et de multiplier par $c^n \neq 0$. □

Remarque 7. Soit $0 \neq \lambda \in \mathbb{K}$ et soit $P \in \mathbb{K}[X]$. Un élément $\alpha \in \mathbb{K}$ est racine de P si et seulement si elle est racine du polynôme λP. Ceci dit que la proposition précédente permet de déterminer toutes les racines rationnelles d'un polynôme rationnel.

Exemple 6. On considère le polynôme $4X^5 + 5X^4 - 3X^3 - 4X^2 + X - 3$. S'il admet une racine rationnelle elle doit être de la forme $\pm\frac{1}{1}$, $\pm\frac{3}{1}$, $\pm\frac{1}{2}$, $\pm\frac{3}{2}$, $\pm\frac{1}{4}$ ou $\pm\frac{3}{4}$ car, à signe près, les seuls diviseurs de 3 sont 1 et 3 et les seuls diviseurs de 4 sont 1, 2 et 4. En évaluant le polynôme sur ces valeurs on constate qu'il admet une unique racine rationnelle qui est 1.