CHAPITRE II

Facteurs irréductibles

II.1. Racines

Valeurs.

Définition II.1.1. Soient $f = a_0 + a_1x + \ldots + a_nx^n$ un polynôme à coefficients dans un corps K et α un élément de K. On appelle *valeur de f en α*, on note $f(\alpha)$ l'élément de K défini par

$$f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n.$$

Remarque II.1.2. Le plus souvent K est pour nous le corps des réels ou des complexes. Comme les réels sont des complexes particuliers, on peut aussi calculer la valeur d'un polynôme réel en un complexe. Ainsi, pour $f = x^2 + 1$, on a $f(i) = 0$.

Remplaçant *la chose* x par un nombre α, "les règles de calcul sont en tout point les mêmes" :

Proposition II.1.3. *Soient f et g deux polynômes. Alors, pour tout α on a*

- $(f + g)(\alpha) = f(\alpha) + g(\alpha)$,
- $(fg)(\alpha) = f(\alpha)g(\alpha)$.

Corollaire II.1.4. *Soient f un polynôme à coefficients dans K et α un élément de K. Alors le reste de la division euclidienne de f par $(x - \alpha)$ est $f(\alpha)$.*

Démonstration. Le diviseur $(x - \alpha)$ étant de degré 1, le reste est une constante a. Écrivant $f = (x - \alpha)q + a$, on a $f(\alpha) = (\alpha - \alpha)q(\alpha) + a$, soit $f(\alpha) = a$. □

Racines.

Définition II.1.5. On dit que α est une *racine* ou un *zéro* de f si $f(\alpha) = 0$.

Remarque II.1.6. Nous avons noté [Remarque II.1.2] qu'un polynôme réel peut toujours être considéré comme un polynôme complexe particulier. Ainsi le polynôme $f = x^2 + 1$ n'a pas de racine réelle, mais il a deux racines complexes, i et $-i$.

Lemme II.1.7. *Soit $f = gh$ un produit de deux polynômes. Alors α est une racine de f si et seulement si c'est une racine de g ou de h.*

Démonstration. On a $f(\alpha) = g(\alpha)h(\alpha)$ et le produit $g(\alpha)h(\alpha)$ est nul si et seulement si (au moins) un des facteurs est nul. □

Comme le reste de la division de f par $(x-\alpha)$ est $f(\alpha)$ [Corollaire II.1.4], on tire

PROPOSITION II.1.8. *Soit f. Alors α est une racine de f si et seulement si $(x - \alpha)$ divise f.*

COROLLAIRE II.1.9. *Un polynôme f de degré n à coefficients dans un corps K a au plus n racines distinctes dans K.*

Démonstration. On raisonne par récurrence sur n. Si $f = ax + b$ est de degré $n = 1$, il a exactement une racine : $\alpha = -(b/a)$. Soit maintenant f de degré n. Si f n'a aucune racine, le résultat est vérifié. Si f admet une racine α, on peut écrire $f = (x - \alpha)q$ où q est de degré $n - 1$. Si $\beta \neq \alpha$ est une autre racine, comme ce n'est pas une racine de $(x - \alpha)$ c'est une racine de q [Lemme II.1.7]. Par hypothèse de récurrence, q admet au plus $n - 1$ racines donc f en admet au plus n (celles de q et α). □

II.2. Polynôme irréductible

Lorsqu'on décompose un polynôme f en un produit de facteurs, soit $f = gh$, il peut s'agir d'une *fausse* décomposition du type $f = a(a^{-1}f)$, où le premier facteur est une constante, le second est associé à f (une telle décomposition est en effet toujours possible). En revanche, il peut s'agir d'une *vraie* décomposition si chaque facteur est de degré strictement inférieur à celui de f (et non constant).

DÉFINITION II.2.1. On dit qu'un polynôme f *non constant* à coefficients dans un corps K est *irréductible* (sur K) s'il ne peut se décomposer en produit de facteurs de degré strictement inférieur à celui de f (à coefficients dans K).

Notons bien qu'on écarte les constantes. Lorsqu'on décompose un polynôme de degré 1, l'un des facteurs est nécessairement une constante :

PROPOSITION II.2.2. *Les polynômes de degré 1 sont irréductibles.*

Les polynômes de degré 1 ont toujours une (et une seule) racine. En revanche on va établir que les polynômes irréductibles de degré supérieur n'ont pas de racine (condition nécessaire mais non suffisante).

PROPOSITION II.2.3. *Soit f un polynôme de degré $n \geq 2$.*

(1) *Si f est irréductible alors f n'a pas de racine.*
(2) *Si $n = 2$ ou 3 et si f n'a pas de racine alors f est irréductible.*

Démonstration. 1) Si f a une racine α, il résulte de la proposition II.1.8 qu'on a la *vraie* décomposition $f = (x - \alpha)g$, où le premier facteur est de degré 1 et le second de degré $n - 1$.

2) Si $n = 2$ ou 3 et si $f = gh$, où g et h sont non constants et de degré strictement inférieur à n, alors l'un de ces facteurs est nécessairement de degré 1. Celui-ci a donc une racine, laquelle est aussi une racine de f [Lemme II.1.7]. □

Remarques II.2.4. 1) En fait, un polynôme réel de degré 3 a toujours une racine (il prend toutes valeurs de $-\infty$ à $+\infty$ — ou l'inverse — et *passe* donc par la valeur 0). Sur les complexes, nous verrons même plus bas que tout polynôme non constant admet une racine (théorème de d'Alembert).
2) Sur le corps $\mathbb{Q}$ des nombres rationnels, on peut montrer qu'il existe des polynômes irréductibles de tout degré n (donc sans racines pour $n \geq 2$).
3) Il faut bien préciser sur quel corps on se place. Par exemple le polynôme $f = x^2 + 1$, est irréductible sur $\mathbb{R}$, mais sur $\mathbb{C}$ il admet la décomposition $f = (x + i)(x - i)$.
4) L'exemple ci-dessous montre qu'à partir du degré 4 un polynôme peut n'avoir aucune racine et cependant ne pas être irréductible.

Exemple II.2.5. Le polynôme $f = x^4 + 2x^2 + 1$ n'a pas de racine réelle. En effet, il prend en tout $\alpha \in \mathbb{R}$ une valeur strictement positive. En revanche, il admet la décomposition $f = (x^2 + 1)(x^2 + 1)$.

Terminons par une remarque simple mais utile. Si $f = gh$ admet une vraie décomposition, multipliant par une constante $a \neq 0$, on obtient la vraie décomposition $af = (ag)h$. On a donc le résultat suivant.

Proposition II.2.6. *Tout polynôme associé à un polynôme irréductible et lui-même irréductible.*

Nombres premiers. La notion de polynôme irréductible correspond à celle de *nombre premier.* On dit qu'un entier $n \geq 2$ est premier s'il n'est pas produit de facteurs strictement plus petits. Ainsi $6 = 2 \times 3$, n'est pas premier, mais $2, 3, 5, 7, 11, \ldots$ le sont. Nous verrons que tout polynôme (non constant) admet un diviseur irréductible. Cela correspond au fait bien connu que tout entier naturel $n \geq 2$ admet un diviseur premier.

Pour trouver tous les nombres premiers jusqu'à n, le grec Eratosthène (qui fut le premier à calculer la circonférence de la Terre, au IV$^{\text{ème}}$ siècle avant Jésus-Christ) a proposé la méthode suivante, dite *du crible.* On dresse la liste des entiers jusqu'à n parmi lesquels 2 est le plus petit nombre premier. Les multiples de 2 (sauf 2 lui-même) ne sont pas premiers, on barre tous ces multiples. Le premier entier non barré est 3, il est premier (il n'est divisible par aucun nombre premier plus petit). On barre tous les multiples de 3 (sauf 3). L'entier suivant non barré est 5. On barre tous les multiples de 5. Ainsi de suite. Finalement, les entiers qui ne sont pas barrés sont premiers.

En fait, pour examiner si un entier est premier, il suffit de tester s'il est divisible par un nombre (premier) inférieur à sa racine carrée. En effet si $n = ab$ alors $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$. Ainsi, pour établir le crible sur les 24 premiers entiers, il suffit de barrer les multiples de 2 et 3.

	2	3	$\cancel{4}$	5	$\cancel{6}$	7	$\cancel{8}$
$\cancel{9}$	$\cancel{10}$	11	$\cancel{12}$	13	$\cancel{14}$	$\cancel{15}$	$\cancel{16}$
17	$\cancel{18}$	19	$\cancel{20}$	$\cancel{21}$	$\cancel{22}$	23	$\cancel{24}$

Les Éléments d'Euclide, rédigés au III$^{\text{ème}}$ siècle avant Jésus-Christ, contiennent plusieurs résultats sur les nombres premiers (par exemple que tout entier admet un facteur premier). On y trouve aussi le joli théorème suivant.

Théorème II.2.7. *Il existe une infinité de nombres premiers.*

Démonstration. Il suffit de montrer que, pour tout entier n, il existe un nombre premier supérieur à n. On pose $N = n! + 1$. On note que N n'est divisible par aucun entier $k, 2 \leq k \leq n$, en effet le reste de la division par k est 1. Mais N admet au moins un facteur premier p qui est donc tel que $p > n$. $\square$

II.3. Unique décomposition

On dit qu'on décompose un polynôme f en *produit de facteurs irréductibles* lorsqu'on écrit

$$f = p_1 p_2 \dots p_n,$$

où les polynômes p_i sont irréductibles. Noter que les facteurs peuvent être répétés (les p_i ne sont pas supposés distincts) et qu'il peut n'y en avoir qu'un seul (si $n = 1$).

Lemme II.3.1. *Tout polynôme non constant se décompose en produit de facteurs irréductibles.*

Démonstration. Soit f un polynôme non constant. S'il est irréductible, il admet une décomposition avec un seul facteur. En particulier le résultat est donc vrai pour les polynômes de degré 1. On raisonne par récurrence sur le degré de f. Considérant le cas où f n'est pas irréductible, on peut écrire $f = gh$, où g et h sont non constants et de degré inférieur à celui de f. Par hypothèse de récurrence, g et h sont produits de facteurs irréductibles et f est le produit de tous ces facteurs (ceux de g et ceux de h). $\square$

On s'intéresse maintenant à l'unicité de cette décomposition. En fait on peut toujours changer l'ordre des facteurs. On peut aussi multiplier un facteur par une constante non nulle et un autre par l'inverse de cette constante. Par exemple $x(x+1) = (2x+2)\left(\frac{1}{2}x\right)$. Cela revient à remplacer certains facteurs par des polynômes associés. On montrera que la décomposition est unique à l'ordre près et à associés près.

Lemme de Gauss.

LEMME II.3.2 (Lemme de Gauss). *Si un polynôme f divise un produit gh et est étranger avec g, alors il divise h.*

Démonstration. Comme f et g sont étrangers, on a une relation de Bézout $1 = pf + qg$ [Corollaire I.5.6]. Multipliant cette relation par h, on tire

$$h = pfh + qgh = (ph)f + q(gh).$$

Donc h est une combinaison de deux multiples de f (f lui-même, et gh que f divise par hypothèse). Ainsi, f divise h. □

LEMME II.3.3. *Soient p un polynôme irréductible et g un polynôme. Alors ou bien p divise g ou bien p et g sont étrangers.*

Démonstration. Si p ne divise pas g, alors g est non nul et le reste de la division de g par p est de degré strictement inférieur à celui de p. A fortiori, l'algorithme d'Euclide conduit à un Pgcd de degré encore inférieur. Comme le Pgcd divise p, il n'a donc d'autre choix que d'être une constante. □

PROPOSITION II.3.4. *Si un polynôme irréductible divise un produit de polynômes, alors il divise l'un des facteurs.*

Démonstration. Supposons qu'un polynôme irréductible p divise le produit $g_1g_2 \dots g_n$ de n polynômes. Si p divise g_n, il divise bien l'un des facteurs. Sinon p est premier avec g_n. D'après le lemme de Gauss, p divise alors le produit $g_1g_2 \dots g_{n-1}$. Par récurrence sur le nombre de facteurs, on conclut que p divise l'un des g_i, pour $i \leq n-1$. □

Unicité.

THÉORÈME II.3.5. *Tout polynôme f à coefficients dans un corps K peut se décomposer en un produit*

$$f = ap_1p_2 \dots p_n$$

où a et une constante et les n polynômes p_i ($n \geq 0$) sont irréductibles et unitaires. En outre, si f est non nul, cette décomposition est unique à l'ordre près des facteurs.

Démonstration. Existence. Si $f = a$ est constant, la décomposition se fait alors sans facteurs irréductibles ($n = 0$). Sinon on sait qu'on peut écrire

$$f = q_1q_2 \dots q_n$$

où les q_i sont irréductibles [Lemme II.3.1]. Si le coefficient directeur de q_i est a_i, on a $q_i = a_ip_i$ où p_i est unitaire. Comme p_i est associé à q_i, il est irréductible [Proposition II.2.6]. Prenant pour a le produit des a_i, on obtient la décomposition voulue.
Unicité. Si f est nul, la constante a est nulle. Le produit de cette constante par n'importe quel polynôme est donc nul et dans ce cas, mais dans ce cas seulement la décomposition n'est évidemment pas unique. Sinon, on montre

que la décomposition est unique par récurrence sur le degré. Tout d'abord, la constante a est le coefficient directeur du produit $ap_1p_2\dots p_r$ (puisque les p_i sont unitaires), elle est donc uniquement déterminée. En particulier, la décomposition est donc unique pour les polynômes de degré 0. Pour un polynôme de degré $n > 0$, considérons alors deux décompositions

$$f = ap_1p_2\dots p_r = bq_1q_2\dots q_s.$$

Comme on vient de le dire, $a = b$ et, simplifiant par cette constante, on a

$$p_1p_2\dots p_r = q_1q_2\dots q_s.$$

Mais alors p_1 divise l'un des q_j [Corollaire II.3.4]. Quitte à réarranger les facteurs, on peut supposer que p_1 divise q_1. Comme q_1 est irréductible, il ne peut s'agir que d'une *fausse* factorisation, de la forme $q_1 = up_1$, où u est une constante. Mais comme p_1 et q_1 sont unitaires, alors $p_1 = q_1$. Simplifiant par p_1 on tire

$$p_2\dots p_r = q_2\dots q_s,$$

deux décompositions d'un même polynôme g de degré inférieur à celui de f. Par hypothèse de récurrence, ces décompositions sont les mêmes (à l'ordre près des facteurs). □

II.4. Théorème de d'Alembert

Donnons sans démonstration le théorème de d'Alembert (démontré par Gauss) annoncé plus haut [Remarque II.2.4 (1)].

THÉORÈME II.4.1. *Tout polynôme non constant admet* (*au moins*) *une racine complexe.*

Il en résulte que les seuls polynômes irréductibles sur les complexes sont les polynômes de degré 1 (les polynômes de degré $n > 1$ ne peuvent être irréductibles lorsqu'ils ont une racine [Proposition II.2.3]).

COROLLAIRE II.4.2. *Sur les complexes, tout polynôme f se décompose* (*de manière unique*) *en produit de la forme*

$$f = a(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n).$$

Polynômes réels irréductibles. Les polynômes de degré 1 sont toujours irréductibles ainsi que les polynômes de degré 2 qui n'ont pas de racine [Proposition II.2.3]. Sur les réels, ces derniers sont les polynômes de la forme $f = ax^2 + bx + c$ dont le *discriminant* $\Delta = b^2 - 4ac$ est strictement négatif. En s'appuyant sur le théorème de d'Alembert on montre qu'il n'y en a pas d'autre :

COROLLAIRE II.4.3. *Sur les réels, les polynômes irréductibles sont*

- *les polynômes de degré 1* (*dits* de première espèce,)
- *les polynômes de degré 2 de discriminant* $\Delta < 0$, (*dits* de deuxième espèce,)

Il suffit d'établir que les polynômes de degré $n \geq 3$ ne sont jamais irréductibles. On commence par un lemme.

LEMME II.4.4. *Si un polynôme réel admet une racine complexe, il admet alors aussi la racine complexe conjuguée.*

Démonstration. Soit $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Supposons que $f(\alpha) = 0$, pour $\alpha \in \mathbb{C}$. Prenant le conjugué de $f(\alpha)$, on obtient

$$\overline{f(\alpha)} = a_n \overline{\alpha}^n + a_{n-1}\overline{\alpha}^{n-1} + \ldots + a_1\overline{\alpha} + a_0 = 0.$$

En effet, le conjugué d'une somme (resp. d'un produit) est la somme (resp. le produit) des conjugués et on ne change pas les coefficients (réels) en prenant leur conjugué. Donc $\overline{\alpha}$ est une racine de f. □

On peut maintenant montrer qu'un polynôme f de degré $n \geq 3$ n'est pas irréductible sur les réels. On sait que f admet une racine complexe α [Théorème II.4.1] et on considère deux cas :
1) $\underline{\alpha \text{ est réel}}$. Dans ce cas $(x - \alpha)$ est un diviseur de f sur $\mathbb{R}$, et f n'est pas irréductible.
2) $\underline{\alpha \text{ n'est pas réel}}$. Dans ce cas $(x - \alpha)$ divise f sur $\mathbb{C}$. A priori on peut simplement conclure que f n'est pas irréductible sur $\mathbb{C}$. Mais d'après le lemme, f admet aussi la racine $\overline{\alpha}$ et donc $(x - \overline{\alpha})$ est un autre facteur de f. Dans l'unique décomposition de f on a ces deux facteurs et on peut écrire

$$f = (x - \alpha)(x - \overline{\alpha})q = \big(x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}\big)q.$$

Notant que $\alpha + \overline{\alpha}$ et $\alpha\overline{\alpha}$ sont réels, $g = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}$ est donc un polynôme réel de degré 2. Par ailleurs, q est (l'unique) quotient de la division euclidienne de f par g, ainsi q est réel, de degré $n-2$. Comme f est de degré $n \geq 3$, la décomposition $f = gq$ est donc une vraie décomposition sur $\mathbb{R}$.

II.5. Multiplicité

Racines multiples. Dans l'unique décomposition d'un polynôme en produit de facteurs irréductibles [Théorème II.3.5], les facteurs de la forme $(x - \alpha)$ correspondent aux racines. Il se peut qu'un tel facteur intervienne plusieurs fois :

DÉFINITION II.5.1. Soit f un polynôme à coefficients dans un corps K. On dit que $\alpha \in K$ est une *racine d'ordre k* de f si k est le plus grand entier tel que $(x - \alpha)^k$ divise f. Si $k = 1$, on dit que α est une *racine simple* et, si $k > 1$, que c'est une *racine multiple* (*racine double* si $k = 2$, *triple* si $k = 3$).

On peut préciser le corollaire II.1.9 sur le nombre des racines en prenant en compte les multiplicités :

COROLLAIRE II.5.2. *Soit f un polynôme de degré n admettant les racines $\alpha_1, \ldots, \alpha_r$ respectivement de multiplicité $k_1, \ldots, k_r$. Alors*

$$k_1 + \ldots + k_r \leq n.$$

Sur les complexes, il résulte du théorème de d'Alembert [Théorème II.4.1] que f est produit de facteurs de la forme $(x-\alpha)$. Regroupant les facteurs correspondant à une même racine, on peut écrire

$$f = a(x-\alpha_1)^{k_1}\dots(x-\alpha_r)^{k_r}.$$

Corollaire II.5.3. *Soit f un polynôme complexe de degré n admettant les racines* (*complexes*) $\alpha_1,\dots,\alpha_r$ *respectivement de multiplicités $k_1,\dots,k_r$. Alors*

$$k_1+\dots+k_r = n.$$

Dérivée. Sans référence aux fonctions, on peut définir la dérivée d'un polynôme de manière formelle :

Définition II.5.4. Soit

$$f = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$$

un polynôme à coefficients dans un corps K. On appelle *dérivée* de f, on note f', le polynôme

$$f' = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \dots + a_1.$$

Remarque II.5.5. Si f est un polynôme réel ou complexe de degré n on voit que sa dérivée f' est de degré $n-1$. En particulier $f'=0$ si et seulement si f est une constante.

On a les règles de calcul suivantes :

Proposition II.5.6. *Soient f et g deux polynômes à coefficients dans K et a une constante. Alors*

(i) $(f+g)' = f'+g'$.
(i) $(af)' = af'$.
(iii) $(fg)' = f'g+fg'$.

Démonstration. Les formules pour la dérivée de la somme ou du produit par une constante sont faciles à établir. Pour le produit, on peut considérer que f et g sont sommes de monômes. Appliquant les résultats précédents, on peut se ramener au cas où $f=x^n$ et $g=x^m$. On a alors

$$(fg)' = (x^{n+m})' = (n+m)x^{n+m-1} = nx^{n-1}x^m + mx^{m-1}x^n = f'g+fg'.$$

□

Une récurrence sur n donne le corollaire suivant

Corollaire II.5.7. *Soient f un polynôme à coefficients dans un corps K et n un entier. Alors*

$$(f^n)' = nf^{n-1}f'.$$

En particulier, pour tout $\alpha\in K$, on a $[(x-\alpha)^n]' = n(x-\alpha)^{n-1}$.

Compte tenu de la remarque II.5.5 on peut aussi tirer le résultat suivant de la dérivée de la somme (ou d'une différence) :

Corollaire II.5.8. *Soient f et g deux polynômes réels ou complexes. Alors $f'=g'$ si et seulement si la différence $f-g$ est une constante.*

Formule de Taylor. On peut définir la dérivée seconde (dérivée de la dérivée) et, par itération, les dérivées successives de f :

DÉFINITION II.5.9. Soit f un polynôme à coefficients dans un corps K. Pour tout entier k on appelle *dérivée d'ordre* k de f, on note $f^{(k)}$, la dérivée de $f^{(k-1)}$.

En particulier, $f^{(0)} = f$, la *dérivée première* $f^{(1)}$ n'est autre que la dérivée f' de f et la *dérivée seconde* $f^{(2)}$ peut aussi se noter f".

REMARQUE II.5.10. Comme le fait de dériver abaisse le degré, il est clair que pour f de degré n et $k > n$, on a $f^{(k)} = 0$.

On établit maintenant la formule dite *formule de Taylor* :

THÉORÈME II.5.11. *Soit f un polynôme (réel ou complexe) de degré n. Pour toute constante a on a alors*

$$f = f(a) + (x-a)f'(a) + \ldots + \frac{(x-a)^n}{n!} f^{(n)}(a).$$

Démonstration. On raisonne par récurrence sur n. Pour f constant, on a de manière triviale $f = f(a)$. On pose

$$g = f(a) + (x-a)f'(a) + \ldots + \frac{(x-a)^n}{n!} f^{(n)}(a).$$

Dérivant g, il résulte des règles de calcul [Proposition II.5.6] et du corollaire II.5.7 (donnant la dérivée de $(x-a)^k$) qu'on a

$$g' = f'(a) + \ldots + \frac{(x-a)^{n-1}}{(n-1)!} f^{(n)}(a).$$

Par hypothèse de récurrence, on voit que g' est l'expression de la formule de Taylor pour la dérivée f' de f (de degré $n-1$). Ainsi $f' = g'$ et donc $f = g + C$, où C est une constante [Corollaire II.5.8]. Comme par ailleurs, $g(a) = f(a)$, alors $C = 0$, soit $f = g$. $\square$

Calculant f en $x = a + h$, donc faisant $x - a = h$, on tire :

COROLLAIRE II.5.12. *Soit f un polynôme de degré n (réel ou complexe). Pour tout a et tout h on a alors*

$$f(a+h) = f(a) + hf'(a) + \ldots + \frac{h^n}{n!} f^{(n)}(a).$$

Dérivées et multiplicité.

THÉORÈME II.5.13. *Soient f un polynôme (réel ou complexe), α un nombre (réel ou complexe) et k un entier. Alors les assertions suivantes sont équivalentes :*

(i) *α est une racine d'ordre k de f.*
(ii) *$f(\alpha) = f^{(1)}(\alpha) = \ldots = f^{(k-1)}(\alpha) = 0$ et $f^{(k)}(\alpha) \neq 0$.*

En particulier,

- α est une racine simple si et seulement si $f(\alpha) = 0$ et $f'(\alpha) \neq 0$,
- α est une racine double si et seulement si $f(\alpha) = f'(\alpha) = 0$ et $f"(\alpha) \neq 0$,

ainsi de suite.

On pourrait dire que α est une racine d'ordre 0 si $f(\alpha) \neq 0$ (α *n'est pas* racine de f).

Démonstration. Montrons d'abord que $(x-\alpha)^k$ divise f si et seulement si $f(\alpha) = f^{(1)}(\alpha) = \ldots = f^{(k-1)}(\alpha) = 0$.
— Supposons que $f(\alpha) = f^{(1)}(\alpha) = \ldots = f^{(k-1)}(\alpha) = 0$. Dans la formule de Taylor [Théorème II.5.11], les k premiers termes sont nuls. On peut donc mettre $(x-\alpha)^k$ en facteur.
— Inversement, supposons que $(x-\alpha)^k$ divise f. Alors $f = (x-\alpha)^k g$. Dérivant cette égalité, on obtient, d'après les règles de calculs [Proposition II.5.6] :

$$f' = k(x-\alpha)^{k-1}g + (x-\alpha)^k g'.$$

Alors $(x-\alpha)^{k-1}$ divise f'. Par le même raisonnement, $(x-\alpha)^{k-2}$ divise $f"$, ainsi de suite, et donc $f(\alpha) = f^{(1)}(\alpha) = \ldots = f^{(k-1)}(\alpha) = 0$.

Le plus grand entier k tel que $f(\alpha) = f^{(1)}(\alpha) = \ldots = f^{(k-1)}(\alpha) = 0$ est donc le plus grand entier k tel que $(x-\alpha)^k$ divise f. $\square$