CHAPITRE 6

POLYNÔMES ET FRACTIONS RATIONNELLES

Dans tout ce chapitre on fixe un corps $\mathbb{K}$.

6.1. Propriétés de l'anneau $\mathbb{K}[X]$

On a en vue le théorème qui affirme que tout $P \in \mathbb{R}[X]$ unitaire de degré ≥ 1 s'écrit de façon unique $P = P_1 \cdots P_n$, où chaque P_i est un polynôme unitaire soit de degré 1, soit de degré 2 sans racine réelle, et que cette écriture est unique (à la numérotation près des P_i). Pour formuler commodément ce résultat, il est utile d'introduire la notion de polynôme *irréductible*. Introduisons plus généralement la notion d'élément irréductible dans un anneau commutatif A. (Le lecteur pressé pourra aller directement à la définition 6.5.)

***Définition 6.1* (Éléments inversibles, associés, irréductibles).** — Soit A un anneau commutatif.

(i) Un élément $a \in A$ est dit *inversible* s'il existe $b \in A$ tel que $ab = 1$. Dans ce cas, b est unique et est appelé l'inverse de b et noté a^{-1} ou $1/a$. Bien sûr, l'inverse de b est a.

(ii) On dit que deux éléments $a, b \in A$ sont *associés* s'il existe un élément inversible u tel que $b = ua$ (et donc $a = u^{-1}b$).

(iii) Un élément non nul $p \in A$ est dit *irréductible* s'il est *non inversible* et si ses seuls diviseurs sont les éléments qui lui sont associés et les éléments inversibles, c.-à-d., si toute égalité $p = ab$ entraîne que a est inversible (et donc que $b = a^{-1}p$ est associé à p) ou bien que b est inversible (et donc que $a = b^{-1}p$ est associé à p).

Exemple 6.2. — Dans l'anneau $A = \mathbb{Z}$, les seuls éléments inversibles sont 1 et -1, donc deux entiers a, b sont associés si et seulement si $b = \pm a$. Les éléments irréductibles sont les nombres premiers > 0, i.e. $2, 3, 5, 7, 11, \ldots$ et leurs opposés. Noter que, par définition, les éléments inversibles ± 1 ne sont pas des éléments irréductibles !

Définition 6.3. — Soit $P \in \mathbb{K}[X]$ un polynôme non nul ; écrivons $P = a_d X^d + \cdots + a_1 X + a_0$. Alors a_d s'appelle le *coefficient dominant* de P et l'on dit que P est *unitaire* si $a_d = 1$.

Remarquons aussi que si Q est un polynôme non nul de degré f et de coefficient dominant b_f, alors le produit PQ est de degré $d + f$ et de coefficient dominant $a_d b_f$.

Remarque 6.4. — Dans $\mathbb{K}[X]$, soit P un élément inversible : il existe donc $Q \in \mathbb{K}[X]$ tel que $PQ = 1$. Alors $0 = \deg(1) = \deg(P) + \deg(Q)$, donc P est une constante $a \in \mathbb{K}^*$ (et $Q = a^{-1}$). Réciproquement, tout $a \in \mathbb{K}^*$ est inversible, d'inverse $a^{-1} \in \mathbb{K}$. Donc on obtient que :

$$\boxed{\text{les éléments inversibles de } \mathbb{K}[X] \text{ sont les constantes } a \in \mathbb{K}^*}$$

et donc deux polynômes $P, Q \in \mathbb{K}[X]$ sont associés si et seulement si $Q = aP$ pour un certain $a \in \mathbb{K}^*$. (En particulier, si P, Q sont associés et *unitaires*, alors $P = Q$.)

Par conséquent, la définition générale 6.1 donne ce qui suit (qu'on peut prendre, si l'on veut, comme définition d'un polynôme irréductible) :

(Q) ***Définition 6.5***. — Un polynôme $P \in \mathbb{K}[X]$ est *irréductible* s'il est de degré ≥ 1 et s'il vérifie la propriété suivante : si $P = QR$, avec $Q, R \in \mathbb{K}[X]$, il existe une constante $a \in \mathbb{K}^*$ telle que $a = Q$ (et donc $R = a^{-1}P$) ou bien $a = R$ (et donc $Q = a^{-1}P$).

Remarque 6.6. — Tout polynôme P de degré 1 est irréductible. En effet, si $P = QR$ alors $1 = \deg(P) = \deg(Q) + \deg(R)$ donc l'un de Q ou R est une constante non nulle a (et l'autre égale $a^{-1}P$).

6.1.1. Conséquences du fait que $\mathbb{C}$ est algébriquement clos. — On rappelle que le corps $\mathbb{C}$ est *algébriquement clos*, i.e. tout polynôme $P \in \mathbb{C}[X]$ de degré $d \geq 1$ admet au moins une racine a dans $\mathbb{C}$, d'où $P = (X - a)Q$ pour un certain $Q \in \mathbb{C}[X]$ de degré $d - 1$. Si P est irréductible et unitaire, il en résulte que $P = X - a$. On a donc le :

(Q) ***Théorème 6.7***. — **(Décomposition en facteurs irréductibles dans $\mathbb{C}[X]$)**

(i) *Les polynômes irréductibles dans $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.*

(ii) *Tout $P \in \mathbb{C}[X]$ de degré $d \geq 1$ s'écrit* $\boxed{P = a(X - \lambda_1)^{m_1} \cdots (X - \lambda_r)^{m_r},}$ *où a est le coefficient dominant de P, $\lambda_1, \ldots, \lambda_r$ sont ses racines, deux à deux distinctes, et chaque m_i est la multiplicité de la racine λ_i.*

(iii) *De plus, cette écriture est unique, à la numérotation près des λ_i.*

Démonstration. — On a déjà vu (i). Prouvons (ii) par récurrence sur d. C'est clair si $d = 1$, donc on peut supposer $d \geq 1$ et le résultat établi pour $d-1$. Soit P de degré d, il possède au moins une racine t_1 dans $\mathbb{C}$ donc $P = (X - t_1)Q$ pour un certain $Q \in \mathbb{C}[X]$ de degré $d - 1$. Par hypothèse de récurrence, $Q = a(X - t_2) \cdots (X - t_d)$ et donc $P = a(X - t_1)(X - t_2) \cdots (X - t_d)$ et a est le coefficient dominant de P. En regroupant les t_i qui sont égaux, on obtient l'écriture voulue. Ceci prouve (ii).

Prouvons (iii). Supposons qu'on ait une autre écriture $P = b(X - \mu_1)^{n_1} \cdots (X - \mu_s)^{n_s}$. Alors b est le coefficient dominant de P donc $b = a$. D'autre part, comme λ_1 est une racine de P, c'est l'un des μ_j et quitte à renuméroter les μ_j on peut supposer que $\lambda_1 = \mu_1$. Alors l'exposant n_1 est la multiplicité de λ_1 comme racine de P, donc $n_1 = m_1$. On a alors $(X - \lambda_2)^{m_2} \cdots (X - \lambda_r)^{m_r} = (X - \mu_2)^{n_2} \cdots (X - \mu_s)^{n_s}$ et l'on peut répéter le même argument : λ_2 est une racine du polynôme de droite, donc quitte à renuméroter les μ_j on peut supposer que $\lambda_2 = \mu_2$, et alors $m_2 = n_2$. De proche en proche, en obtient que $r = s$ et que, quitte à renuméroter les μ_j, on a $\lambda_i = \mu_i$ et $m_i = n_i$ pour $i = 1, \ldots, r$. □

(Q) ***Corollaire 6.8***. — **(Décomposition en facteurs irréductibles dans $\mathbb{R}[X]$)**

(i) *Les polynômes irréductibles dans $\mathbb{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 qui n'ont pas de racines réelles, i.e. dont le discriminant est < 0.*

(ii) *Tout $P \in \mathbb{R}[X]$ de degré $d \geq 1$ et de coefficient dominant u s'écrit*

$$(\star) \qquad P = u(X - t_1)^{m_1} \cdots (X - t_r)^{m_r} P_1^{n_1} \cdots P_s^{n_s}$$

où $t_1, \ldots, t_r$ sont les racines réelles, deux à deux distinctes, de P, chacune étant de multiplicité m_i, et $P_1, \ldots, P_s$ sont des polynômes, deux à deux distincts, de degré 2 sans racines réelles.

(iii) *De plus, cette écriture est unique, à la numérotation près des t_i et des P_j.*

Démonstration. — Remarquons d'abord que tout polynôme $D \in \mathbb{R}[X]$ de degré 2 sans racines réelles est irréductible. En effet, si $D = QR$ alors $2 = \deg(D) = \deg(Q) + \deg(R)$ et comme D n'a pas de racines réelles alors ni P ni Q ne peuvent être de degré 1, donc l'un d'eux est de degré 0 (i.e. une constante non nulle) et l'autre est associé à D.

Soit maintenant $P \in \mathbb{R}[X]$ de degré $d \geq 1$, de coefficient dominant u. Montrons que P est divisible dans $\mathbb{R}[X]$ par un polynôme du type indiqué en (i). Soit α une racine dans $\mathbb{C}$ de P. Si

$\alpha \in \mathbb{R}$ alors P est divisible par $X - \alpha$. On peut donc supposer que $\alpha = a + ib$ avec $a, b \in \mathbb{R}$ et $b \neq 0$. Écrivons $P = a_d X^d + \cdots + a_1 X + a_0$ avec les a_i dans $\mathbb{R}$; comme $P(\alpha) = 0$ on a aussi :

$$0 = \overline{P(\alpha)} = \sum_{k=0}^{d} \overline{a_k}\, \overline{\alpha}^k = \sum_{k=0}^{d} a_k\, \overline{\alpha}^k = P(\overline{\alpha}),$$

où l'avant-dernière égalité découle du fait que $a_k \in \mathbb{R}$. Donc $\overline{\alpha}$ est racine de P et donc P est divisible dans $\mathbb{C}[X]$ par le polynôme $D = (X - \alpha)(X - \overline{\alpha}) = X^2 - 2aX + a^2 + b^2$, qui appartient à $\mathbb{R}[X]$ et est sans racines réelles. Faisons dans $\mathbb{R}[X]$ la division euclidienne de P par D : on a $P = DQ + R$ avec $Q, R \in \mathbb{R}[X]$ et $\deg(R) < \deg(D)$. Or dans $\mathbb{C}[X]$, D divise P donc aussi $P - DQ = R$, donc pour une raison de degré on a $R = 0$, donc D divise P dans $\mathbb{R}[X]$.

Ce qui précède montre déjà que si P est irréductible, alors $P = u(X - \alpha)$ ou $P = uD$, ce qui prouve (i). De plus, ceci montre que (ii) est vrai si P est de degré 1. On peut donc supposer $d \geq 2$ et le résultat établi pour $d - 1$. Or, d'après ce qui précède, on a $P = AQ$ avec A irréductible unitaire de degré 1 ou 2, et $\deg(Q) = d - \deg(A) < d$. Donc par hypothèse de récurrence, Q est une constante $\neq 0$ ou bien s'écrit comme en (ii) et donc P s'écrit aussi comme en (ii). Ceci prouve (ii).

(iii) Enfin, l'unicité résulte de l'unicité de l'écriture dans le cas complexe. En effet, si l'on note z_j et $\overline{z_j}$ les racines de P_j pour $j = 1, \ldots, s$, alors l'écriture $(\star)$ équivaut à dire que les racines de P dans $\mathbb{C}$ sont les t_i, de multiplicité m_i, et les z_j et $\overline{z_j}$, chacun de multiplicité n_j. Comme ces racines et leur multiplicités sont uniquement déterminées, il en est de même des P_j et de leur multiplicités. □

Remarque 6.9. — On a utilisé le théorème (admis) que $\mathbb{C}$ est algébriquement clos pour démontrer le théorème sur la décomposition en facteurs irréductibles dans $\mathbb{K}[X]$ lorsque $\mathbb{K} = \mathbb{C}$ ou $\mathbb{R}$. Dans le paragraphe suivant on va démontrer ce théorème pour tout corps $\mathbb{K}$ par une autre méthode, qui donne d'autres résultats importants.

6.1.2. $\mathbb{K}[X]$ est principal, théorème de Bézout, lemme de Gauss. —

Définitions 6.10. — Soit A un anneau commutatif.

(i) Un *idéal* de A est un sous-ensemble I de A qui vérifie les deux propriétés suivantes :

(a) I est un sous-groupe du groupe abélien $(A, +)$, i.e. $0 \in I$ et pour tout $x, y \in I$ on a $x + y \in I$ et $-x \in I$.

(b) I est stable par multiplication par A, c.-à-d., pour tout $x \in I$ et $a \in A$, on a $ax \in I$

(ii) Soient $x_1, \ldots, x_n \in A$, on note $\boxed{(x_1, \ldots, x_n)}$ l'ensemble des sommes $a_1 x_1 + \cdots + a_n x_n$, où $a_1, \ldots, a_n \in A$. On voit facilement que les propriétés (a) et (b) ci-dessus sont vérifiées, donc $(x_1, \ldots, x_n)$ est un idéal de A. On l'appelle l'idéal *engendré par* $x_1, \ldots, x_n$.

(iii) On dit qu'un idéal I est *principal* s'il peut s'écrire $I = (x)$ pour un certain x. Par exemple, l'idéal nul (0) est principal, ainsi que l'idéal (1) = A.

(iv) Enfin, on dit que *l'anneau A est principal* si tout idéal de A est principal.

(Q) ***Théorème 6.11***. — *$\mathbb{K}[X]$ est principal. Plus précisément, pour tout idéal $I \neq 0$ de $\mathbb{K}[X]$, il existe un unique polynôme unitaire P tel que $I = (P)$.*

Démonstration. — L'idéal (0) est principal, donc on peut supposer $I \neq 0$. Alors l'ensemble :

$$\{\deg(P) \mid P \in I - \{0\}\}$$

est un sous-ensemble non vide de $\mathbb{N}$, donc admet un plus petit élément d. Soit alors $P \in I$ tel que $\deg(P) = d$. Quitte à multiplier P par un scalaire $a \in \mathbb{K}^*$, on peut supposer que P est unitaire. Comme I est un idéal, on a $(P) \subset I$. Montrons l'inclusion réciproque.

Soit $Q \in I$; faisant la division euclidienne de Q par P, on obtient $Q = DP + R$, avec $\deg(R) < \deg(P) = d$ (ceci inclut le cas $R = 0$, car par convention $\deg(0) = -\infty$). Comme I est un idéal, alors $R = Q - DP$ appartient à I donc comme $\deg(R) < d$ on a nécessairement $R = 0$, d'où $Q = DP$. Ceci montre que $I \subset (P)$, d'où l'égalité $I = (P)$. Ceci prouve déjà que $\mathbb{K}[X]$ est principal.

De plus, si Q est aussi un générateur de I, alors il existe $F \in \mathbb{K}[X]$ tel que $P = FQ = FDP$, d'où $FD = 1$, donc F est une constante $a \in \mathbb{K}^*$. Donc les générateurs de I sont les polynômes aP associés à P, et parmi eux P est l'unique polynôme unitaire. Le théorème est démontré. □

Définition 6.12. — Soient $P_1, \dots, P_n \in \mathbb{K}[X]$ non tous nuls. On dit que $P_1, \dots, P_n$ sont « *premiers entre eux* » ou « *sans diviseurs communs* » s'ils n'ont pas de diviseurs communs autres que les éléments inversibles, c.-à-d., si la propriété suivante est vérifiée : si un polynôme $D \in \mathbb{K}[X]$ divise chacun des P_i, alors D est une constante $a \in \mathbb{K}^*$.

Corollaire 6.13 **(Théorème de Bézout)**. — *Si $P_1, \dots, P_n \in \mathbb{K}[X]$ sont premiers entre eux, il existe $A_1, \dots, A_n \in \mathbb{K}[X]$ tels que $A_1P_1 + \cdots + A_nP_n = 1$.*

Démonstration. — L'idéal $I = (P_1, \dots, P_n)$ est non nul, donc $I = (D)$ pour un certain polynôme unitaire D. Comme $P_i \in I$ on a $P = DQ_i$ pour un certain Q_i, donc D est un diviseur commun des P_i. D'après l'hypothèse, D est donc une constante, d'où $D = 1$. Mais comme $D \in I = (P_1, \dots, P_n)$, il existe des polynômes $A_1, \dots, A_n$ tels que $A_1P_1 + \cdots + A_nP_n = D = 1$. □

Corollaire 6.14 **(Lemme de Gauss)**. — *Soient $P, A, B \in \mathbb{K}[X]$. Si P divise le produit AB et est premier avec A alors il divise B.*

Démonstration. — Par hypothèse, il existe $Q \in \mathbb{K}[X]$ tel que $AB = QP$. D'autre part, comme P et A sont premiers entre eux, il existe $U, V \in \mathbb{K}[X]$ tels que $UP + VA = 1$. Alors on a

$$B = B(UP + VA) = BUP + VAB = BUP + VQP = (BU + VQ)P$$

ce qui montre que P divise B. □

Corollaire 6.15. — *Soit $P \in \mathbb{K}[X]$ un polynôme* irréductible. *S'il divise un produit $P_1 \cdots P_n$ alors il divise l'un des P_i.*

Démonstration. — On procède par récurrence sur n. C'est ok si $n = 1$ donc on peut supposer $n \geq 2$ et le résultat démontré pour $n - 1$ facteurs. Si P divise P_1, c'est gagné, donc on peut supposer que P ne divise pas P_1. Mais alors P et P_1 sont premiers entre eux : en effet, comme P est irréductible, ses seuls diviseurs autres que les constantes $a \in \mathbb{K}^*$ sont les polynômes associés aP, or ceux-ci ne divisent pas P_1 car sinon P diviserait P_1, contrairement à l'hypothèse faite. Donc, d'après le lemme de Gauss, P divise le produit $P_2 \cdots P_n$ et donc, d'après l'hypothèse de récurrence, il divise l'un des P_i. Ceci prouve le corollaire. □

Théorème 6.16. — *Soit $P \in \mathbb{K}[X]$ de degré $d \geq 1$ et de coefficient dominant u*

(i) *P s'écrit* $\boxed{(\star)\ P = uP_1^{m_1} \cdots P_r^{m_r}}$ *où les P_i sont des polynômes irréductibles unitaires, deux à deux distincts, et les m_i sont des entiers ≥ 1.*

(ii) *Cette écriture est unique, à la numérotation près des P_i.*

Démonstration. — (i) Prouvons l'existence en procédant par récurrence sur $d = \deg(P)$. C'est ok si $d = 1$ donc on peut supposer $d \geq 2$ et (i) démontré pour tout polynôme de degré $< d$. Si P est irréductible c'est gagné, donc on peut supposer que $P = QR$ avec Q, R tous deux de degré > 0 et donc, puisque $\deg(Q) + \deg(R) = d$, tous deux de degré $< d$. Alors, par hypothèse de récurrence, $Q = aD_1 \cdots D_q$ et $R = bD'_1 \cdots D'_r$, où $a, b \in \mathbb{K}^*$ et les D_i et D'_j sont irréductibles et unitaires, mais pas nécessairement distincts. Donc

$$P = abD_1 \cdots D_qD'_1 \cdots D'_r$$

d'où nécessairement $ab = u$, et en regroupant les D_i et D'_j qui sont égaux on obtient une écriture comme voulue.

(ii) Prouvons l'unicité en procédant par récurrence sur le nombre de facteurs $N = m_1 + \cdots + m_r$ dans le terme de droite de $(\star)$. C'est ok si $N = 1$ donc on peut supposer $N \geq 2$ et l'unicité démontrée pour tout produit de $N-1$ facteurs. Supposons que $P = uP_1^{m_1} \cdots P_r^{m_r} = vQ_1^{n_1} \cdots Q_r^{n_s}$, avec $u, v \in \mathbb{K}^*$ et les P_i et Q_j irréductibles et unitaires. Alors v est le coefficient dominant de P donc égale u. D'autre part, d'après le corollaire 6.15, P_1 divise l'un des Q_j et, quitte à renuméroter

les Q_j on peut supposer que P_1 divise Q_1. Comme P_1 et Q_1 sont tous deux irréductibles et unitaires, il en résulte que $P_1 = Q_1$. Alors, en simplifiant par $uP_1 = vQ_1$ on obtient l'égalité :

$$P_1^{m_1-1} \cdots P_r^{m_r} = P_1^{n_1-1} Q_2^{n_2} \cdots Q_s^{n_s}$$

et par hypothèse de récurrence, on en déduit que, quitte à renuméroter les Q_j pour $j \geq 2$, on a $s = r$ et $Q_i = P_i$ et $n_i = m_i$ pour $i = 1, \ldots, r$. Le théorème est démontré. □

6.2. Le corps $\mathbb{K}(X)$ des fractions rationnelles

Définition 6.17. — (i) On définit l'ensemble $\mathbb{K}(X)$ des fractions rationnelles sur $\mathbb{K}$ à partir des polynômes de la même façon que l'on a défini $\mathbb{Q}$ à partir de $\mathbb{Z}$: une fraction rationnelle est un quotient $\dfrac{P}{Q}$, où $P, Q \in \mathbb{K}[X]$ et $Q \neq 0$, et deux telles expressions $\dfrac{P}{Q}$ et $\dfrac{A}{B}$ sont *égales* si et seulement si $PB = AQ$. [(1)]

(ii) La somme de deux fractions $F = \dfrac{P}{Q}$ et $G = \dfrac{R}{S}$ est définie en mettant les deux fractions au même dénominateur :

$$F + G = \frac{P}{Q} + \frac{R}{S} = \frac{PS}{QS} + \frac{QR}{QS} = \frac{PS + QR}{QS}.$$

Ceci ne dépend pas des écritures $F = P/Q$ et $G = R/S$ choisies, car si $F = A/B$ et $G = C/D$ alors $PB = QA$ et $RD = SC$ et comme :

$$\frac{A}{B} + \frac{C}{D} = \frac{AD + BC}{BD} \qquad \text{et} \qquad (AD + BC)QS = PBDS + RDBQ = (PS + QR)BD$$

on a bien $\dfrac{P}{Q} + \dfrac{R}{S} = \dfrac{A}{B} + \dfrac{C}{D}$.

(iii) Le produit FG est défini par $FG = \dfrac{PR}{QS}$; à nouveau ceci ne dépend pas des écritures $F = P/Q$ et $G = R/S$ choisies, car si $F = A/B$ et $G = C/D$ alors $\dfrac{A}{B}\dfrac{C}{D} = \dfrac{AC}{BD}$ égale $\dfrac{PR}{QS}$ puisque $ACQS = PBRD$.

(iv) On vérifie sans difficulté que l'addition et la multiplication ainsi définies font de $\mathbb{K}(X)$ un anneau commutatif. C'est même un *corps* car toute fraction $F = \dfrac{P}{Q}$ non nulle (i.e. telle que $P \neq 0$) possède pour inverse la fraction $\dfrac{Q}{P}$. On dira donc que $\mathbb{K}(X)$ est le *corps des fractions rationnelles* sur $\mathbb{K}$.

(Q) ***Proposition 6.18*** **(Fractions irréductibles)**. — *Soit $F \in \mathbb{K}(X) - \{0\}$.*

(i) *F peut s'écrire sous la forme d'une* fraction irréductible $\dfrac{P}{Q}$, *avec $P, Q \in \mathbb{K}[X]$* premiers entre eux. *Une telle écriture est unique à un scalaire près ; plus précisément, si $\dfrac{R}{S}$ est une autre écriture de F, il existe $D \in \mathbb{K}[X]$ tel que $S = DQ$ et $R = DP$. En particulier, si la fraction $\dfrac{R}{S}$ est aussi irréductible, il existe $a \in \mathbb{K}^*$ tel que $S = aQ$ et $R = aP$.*

(ii) *Par conséquent, l'écriture sous forme irréductible $F = \dfrac{P}{Q}$ est unique si l'on impose à Q d'être unitaire.*

(iii) *On pose* $\deg(F) = \deg(P) - \deg(Q)$ *; ceci ne dépend pas de l'écriture choisie, car pour toute écriture $F = R/S$ on a* $\deg(R) - \deg(S) = \deg(P) - \deg(Q)$.

---

(1) De façon précise, on peut donc dire que l'ensemble des fractions rationnelles est l'ensemble des *classes d'équivalence* de couples $(P, Q) \in \mathbb{K}[X] \times \big(\mathbb{K}[X] - \{0\}\big)$, où deux couples (P, Q) et (A, B) sont équivalents si et seulement si $PB = AQ$.

Démonstration. — Soit $I = \{B \in \mathbb{K}[X] \mid BF \in \mathbb{K}[X]\}$. On voit facilement que I est un idéal de $\mathbb{K}[X]$, non nul donc engendré par un unique polynôme unitaire Q. Posons $P = QF \in \mathbb{K}[X]$. Si F s'écrit R/S, alors $S \in I$ et donc il existe $D \in \mathbb{K}[X]$ tel que $S = DQ$ et alors $R = SF = DQF = DP$. En particulier, si la fraction R/S est irréductible, i.e. si R et S sont premiers entre eux, alors D est une constante $a \in \mathbb{K}^*$. Ceci prouve (i). Alors (ii) en découle aussitôt, ainsi que (iii), car si $R = DP$ et $S = DQ$ alors $\deg(R) = \deg(P) + \deg(D)$ et $\deg(S) = \deg(Q) + \deg(D)$ d'où $\deg(R) - \deg(S) = \deg(P) - \deg(Q)$. □

Définition 6.19. — Un *élément simple* de $\mathbb{K}(X)$ est une fraction rationnelle de la forme $\dfrac{R}{Q^n}$ où $Q \in \mathbb{K}[X]$ est irréductible, $\deg(R) < \deg(Q)$ et $n \in \mathbb{N}^*$.

(Q) ***Théorème 6.20* (Décomposition en éléments simples)**. — *Soit $F \in \mathbb{K}(X) - \{0\}$.*

(i) *F s'écrit de façon unique comme somme d'un polynôme et d'éléments simples.*

(ii) *Plus précisément, écrivons $F = \dfrac{P}{Q}$ avec P, Q premiers entre eux. Soit $Q = Q_1^{m_1} \cdots Q_r^{m_r}$ la décomposition de Q en facteurs irréductibles. Pour tout $i = 1, \ldots, r$ et tout $j \in \{0, \ldots, m_i - 1\}$, il existe un unique polynôme $R_{i,j}$ de degré $< \deg(Q_i)$ tel que :*

$$(\star) \quad \frac{P}{Q} = E + \frac{R_{1,0}}{Q_1^{m_1}} + \frac{R_{1,1}}{Q_1^{m_1-1}} + \cdots + \frac{R_{1,m_1-1}}{Q_1} + \frac{R_{2,0}}{Q_2^{m_2}} + \frac{R_{2,1}}{Q_2^{m_2-1}} + \cdots + \frac{R_{2,m_2-1}}{Q_2} + \cdots + \frac{R_{r,0}}{Q_r^{m_r}} + \frac{R_{r,1}}{Q_r^{m_r-1}} + \cdots + \frac{R_{r,m_r-1}}{Q_r}$$

où E est un polynôme. De plus, E est le quotient de la division euclidienne de P par Q.

Démonstration. — Prouvons d'abord l'existence de la décomposition $(\star)$. Les polynômes $Q_1^{m_1}$ et $B_1 = Q_2^{m_2} \cdots Q_r^{m_r}$ sont premiers entre eux, donc d'après le théorème de Bézout il existe $U, V \in \mathbb{K}[X]$ tels que $UB_1 + VQ_1^{m_1} = 1$. Donc :

$$\frac{P}{Q} = \frac{P}{Q}(UB_1 + VQ_1^{m_1}) = \frac{P_1}{Q_1^{m_1}} + \frac{S_1}{B_1}$$

où l'on a posé $P_1 = PU$ et $S_1 = PV$. Puis, écrivant $B_1 = Q_2^{m_2} B_2$ on obtient de la même façon que $\dfrac{S_1}{B_1}$ se décompose en une somme $\dfrac{P_2}{Q_2^{m_2}} + \dfrac{S_2}{B_2}$. En répétant ce processus, on arrive à une écriture :

$$(1) \qquad \frac{P}{Q} = \frac{P_1}{Q_1^{m_1}} + \frac{P_2}{Q_2^{m_2}} + \cdots + \frac{P_r}{Q_r^{m_r}}.$$

On va maintenant décomposer chaque fraction $\dfrac{P_i}{Q_i^{m_i}}$. Omettons l'indice i et considérons donc une fraction P/Q^m. Faisant la division euclidienne de P par Q, on obtient $P = D_0 Q + R_0$, avec $\deg(R_0) < \deg(Q)$. Puis, faisant la division euclidienne de D_0 par Q, on obtient $D_0 = D_1 Q + R_1$, avec $\deg(R_1) < \deg(Q)$, et donc

$$P = R_0 + R_1 Q + D_1 Q^2.$$

Puis, faisant la division euclidienne de D_1 par Q, on obtient $D_1 = D_2 Q + R_2$, avec $\deg(R_2) < \deg(Q)$, et donc $P = R_0 + R_1 Q + R_2 Q^2 + D_2 Q^3$. En répétant ce processus, on arrive à une écriture :

$$P = R_0 + R_1 Q + R_2 Q^2 + \cdots + R_{m-1} Q^{m-1} + D_{m-1} Q^m \quad \text{avec} \deg(R_i) < \deg(Q),$$

d'où

$$(2) \qquad \frac{P}{Q^m} = \frac{R_0}{Q^m} + \frac{R_1}{Q^{m-1}} + \frac{R_2}{Q^{m-2}} + \cdots + \frac{R_{m-1}}{Q} + D_{m-1}.$$

Appliquons (2) à chaque $P_i/Q_i^{m_i}$, en remplaçant dans le terme de droite R_j/Q^{m-j} par $R_{i,j}/Q_i^{m_i-j}$ et D_{m-1} par D_{i,m_i-1}, et injectons ceci dans (1). On obtient alors la décomposition $(\star)$, avec $E = D_{1,m_1-1} + \cdots + D_{r,m_r-1}$. Ceci prouve l'existence.

Pour prouver l'unicité on a besoin de trois lemmes.

Lemme 6.20.1. — *Les fractions rationnelles de degré* < 0 *forment un* sous-groupe *de* $\mathbb{K}(X)$.

Démonstration. — Par convention, la fraction nulle est de degré $-\infty$, et si F est de degré < 0 il en est de même de $-F$. Il suffit donc de montrer que si F, G sont de degré < 0, il en est de même de $F+G$. Écrivons $F = A/B$ et $G = R/S$, avec $\deg(A) < \deg(B)$ et $\deg(R) < \deg(S)$. Alors $F+G = \dfrac{AS+BR}{BS}$ et $AS+BR$ est de degré $\leq m = \max\big(\deg(AS), \deg(BR)\big)$. Or $\deg(AS) = \deg(A) + \deg(S)$ et $\deg(BR) = \deg(B) + \deg(R)$ sont tous deux $< \deg(B) + \deg(S) = \deg(BS)$. Donc $\deg(F+G) < 0$. Ceci prouve le lemme. □

Corollaire 6.20.2. — *Toute fraction rationnelle* $F = \dfrac{P}{Q}$ *s'écrit de façon unique* $F = E + \dfrac{R}{Q}$, *où* E, R *sont des polynômes et* $\deg(R) < \deg(Q)$. *De plus,* E *est le quotient et* R *le reste de la division euclidienne de* P *par* Q.

Démonstration. — Faisant la division euclidienne $P = EQ+R$, avec $\deg(R) < \deg(Q)$, on obtient l'écriture voulue. Cette écriture est unique, car si $E_1 + \dfrac{R_1}{Q_1}$ en est une autre, on obtient :

$$E - E_1 = \frac{R_1}{Q_1} - \frac{R}{Q}.$$

D'après le lemme précédent, le terme de droite est de degré < 0, tandis que le terme de gauche est un polynôme, donc ces deux termes sont nuls, d'où $E_1 = E$ et $\dfrac{R_1}{Q_1} = \dfrac{R}{Q}$. □

Lemme 6.20.3. — (i) *Soient* $Q_1, \ldots, Q_n \in \mathbb{K}[X]$ *des polynômes irréductibles deux à deux distincts,* $m_1, \ldots, m_n$ *des entiers* ≥ 1, *et* $P_1, \ldots, P_n \in \mathbb{K}[X]$ *des polynômes tels que* $\deg(P_i) < \deg(Q_i^{m_i})$ *pour tout* i. *Si*

$$\frac{P_1}{Q_1^{m_1}} + \cdots + \frac{P_n}{Q_n^{m_n}} = 0$$

alors $P_1 = 0 = \cdots = P_n$.

(ii) *Toute fraction rationnelle* $F = \dfrac{P}{Q}$ *de degré* < 0 *s'écrit de façon unique*

$$\frac{P}{Q} = \frac{P_1}{Q_1^{m_1}} + \cdots + \frac{P_n}{Q_n^{m_n}}$$

où les Q_i *sont des polynômes irréductibles deux à deux distincts et chaque polynôme* P_i *est de degré* $< \deg(Q_i^{m_i})$.

Démonstration. — (i) Montrons que $P_1 = 0$. On a $\dfrac{-P_1}{Q_1^{m_1}} = \dfrac{P_2}{Q_2^{m_2}} + \cdots + \dfrac{P_n}{Q_n^{m_n}}$, notons cette quantité Y, c'est une fraction rationnelle de degré < 0. De plus, d'après les deux écritures de Y on voit que $Q_1^{m_1}Y$ et B_1Y sont des polynômes.

D'autre part, comme les polynômes $Q_1^{m_1}$ et $B_1 = Q_2^{m_2} \cdots Q_r^{m_r}$ sont premiers entre eux, il existe $U, V \in \mathbb{K}[X]$ tels que $UQ_1^{m_1} + VB_1 = 1$. Alors

$$Y = (UQ_1^{m_1} + VB_1)Y = UQ_1^{m_1}Y + VB_1Y$$

est un polynôme. Comme $\deg(Y) < 0$ il en résulte que $Y = 0$, d'où $P_1 = 0$. On montre de même que $P_i = 0$ pour tout $i = 2, \ldots, n$. Ceci prouve (i).

(ii) Supposons qu'on ait deux telles écritures. Alors, notant Q_i les polynômes irréductibles qui apparaissent dans les deux écritures et R_j et S_k ceux qui n'apparaissent que dans une, on a une égalité :

$$\sum_i \frac{A_i}{Q_i^{m_i}} + \sum_j \frac{C_j}{R_j^{r_j}} = \sum_i \frac{B_i}{Q_i^{n_i}} + \sum_k \frac{D_k}{S_k^{s_k}}$$

avec $A_i/Q_i^{m_i}$, $B_i/Q_i^{n_i}$, $C_j/R_j^{r_j}$ et $D_k/S_k^{s_k}$ de degré < 0 pour tous i, j, k, et les Q_i, R_j et S_k tous distincts. On a donc

$$0 = \sum_i \frac{A_i Q_i^{n_i} - B_i Q_i^{m_i}}{Q_i^{m_i+n_i}} + \sum_j \frac{C_j}{R_j^{r_j}} - \sum_k \frac{D_k}{S_k^{s_k}}$$

et d'après le point (i) ceci entraîne que $C_j = 0 = R_k$ pour tous j, k et que pour tout i on a $A_i Q_i^{n_i} = B_i Q_i^{m_i}$, d'où $\dfrac{A_i}{Q_i^{m_i}} = \dfrac{B_i}{Q_i^{n_i}}$. Ceci prouve (ii). □

Lemme 6.20.4. — *Soient $Q, P \in \mathbb{K}[X]$ et $m \in \mathbb{N}^*$ avec Q irréductible et* $\deg(P) < \deg(Q^m)$. *Alors la fraction $F = P/Q^m$ s'écrit d'au plus une façon sous la forme :*

$$F = \frac{P}{Q^m} = \frac{R_0}{Q^m} + \frac{R_1}{Q^{m-1}} + \frac{R_2}{Q^{m-2}} + \cdots + \frac{R_{m-1}}{Q}$$

avec les R_i dans $\mathbb{K}[X]$, tous de degré $< \deg(Q)$.

Démonstration. — Supposons qu'on ait deux écritures

$$F = \frac{R_0}{Q^m} + \frac{R_1}{Q^{m-1}} + \cdots + \frac{R_{m-1}}{Q} = \frac{S_0}{Q^m} + \frac{S_1}{Q^{m-1}} + \cdots + \frac{S_{m-1}}{Q}.$$

Alors en multipliant par Q^m on obtient l'égalité :

$$S_0 - R_0 = Q\Big[(R_1 - S_1) + Q(R_2 - S_2) + \cdots + Q^{m-2}(R_{m-1} - S_{m-1})\Big].$$

Le terme de droite est multiple de Q, donc de degré $\geq \deg(Q)$, tandis que le terme de gauche est de degré $< \deg(Q)$, donc les deux termes sont nuls, d'où $S_0 = R_0$. Alors, en simplifiant par Q on obtient l'égalité :

$$S_1 - R_1 = Q\Big[(R_2 - S_2) + \cdots + Q^{m-3}(R_{m-1} - S_{m-1})\Big]$$

et le même argument donne que $S_1 = R_1$. De proche en proche, on obtient que $S_i = R_i$ pour tout $i = 1, \ldots, m-1$. Ceci prouve le lemme. □

On peut maintenant démontrer l'unicité de l'écriture ($\star$) dans le théorème 6.20. Pour chaque indice $i \in \{1, \ldots, r\}$, la somme des $R_{i,j}/Q_i^{m_i-j}$ pour $j = 1, \ldots, m_i$ est une fraction $P_i/Q_i^{m_i}$, de degré < 0 d'après le lemme 6.20.1. D'après le corollaire 6.20.2 et le lemme 6.20.3, E est le quotient de la division euclidienne de P par Q et chaque fraction $P_i/Q_i^{m_i}$ est uniquement déterminée. Enfin, pour chaque i l'écriture

$$\frac{P_i}{Q_i^{m_i}} = \frac{R_{i,0}}{Q_i^{m_i}} + \frac{R_{i,1}}{Q_1^{m_i-1}} + \cdots + \frac{R_{i,m_1-1}}{Q_i}$$

est unique, d'après le lemme 6.20.4. Ceci achève la démonstration du théorème 6.20. □