Théorème de transfert de Gauss (Perrin)

Pierre Lissy

April 29, 2010

Définition 1. *On considère un polynôme $P = \sum a_i X^i$ à coefficients dans A. Par définition le contenu de ce polynôme est un pgcd des coefficients de P, noté $c(P)$. Un polynôme est dit primitif ssi $c(P) = 1$. Le polynôme est clairement multiplicatif sur les scalaires car si $a \in A$, alors les coefficients de aP sont les aa_i et $c(aP) = pgcd(aa_i) = apgcd(a_i) = ac(P)$.*

Lemme 1 (Gauss)**.** $c(PQ) = c(P)c(Q)$

Proof. Il suffit de le faire pour des polynômes P et Q entre eux. En effet, si on pose $p = c(P)$ et $q = c(Q)$, alors les polynômes $P' = P/p$ et $Q' = Q/q$ sont encore à coefficients dans A et sont clairement primitifs. On aura donc que $c(P'Q') = 1$,et donc $C(PQ) = C(pqP'Q') = pq = C(P)C(Q)$.

Considérons donc P et Q primitifs. Supposons $c(PQ) \neq 1$. Alors comme l'anneau A est factoriel, on a existence d'un p irréductible qui divse $c(PQ)$. Or $c(P) = c(Q) = 1$ donc il existe un certain i_0 et un certain j_0 tels que pour $i < i_0$ et $j < j_0$ on a $p|a_i$ et $p|b_j$ mais $p \not| a_{i_0}$, $p \not| b_{j_0}$. Par hypothèse c divise le coefficient numéro $i_0 + j_0$ de PQ, ie $p| \sum_{i+j=i_0+j_0} a_i b_i = a_{i_0}b_{j_0} + \sum_{i+j=i_0+j_0, i<i_0} \text{ ou } _{j<j_0} a_i b_i$, ce qui implique que $p|a_{i_0}b_{i_0}$ et donc vu que p est irréductible et A factoriel on a $p|a_{i_0}$ ou $p|b_{j_0}$ ce qui est supposé être faux par hypothèse. D'où la contradiction. □

Voici comment nous allons procéder pour la démonstration. Comme A est intégre, alors on peut considérer le corps des fractions K de A, et l'anneau $K[X]$ aura la bonen idée d'être lui principal, ce qui nosu simplifiera la vie. Commençons grâce au contenu par déterminer les irréductibles de $A[X]$ en fonction de ceux de $K[X]$.

Corollaire 1. *Les irréductibles de $A[X]$ sont les constantes irréductibles et les polynômes irréductibles dans $K[x]$ primitifs*

Proof. D'abord, ces éléments sont irréductibles. En effet, une constante irréductible est p qui se factorise sous la forme $P(X)Q(X)$ est tel pour une raison de degré que les polynômes P et Q sont de degré 0. Donc $p = ab$ et forcément soit a soit b est inversible dans A donc dans $A^*[X]$ (les inversibles de $A^*[X]$ sont ceux de A. Si l'on considère un polynôme primitif irréductible dans K[X] et qu'on le factorise sous la forme $Q(X)R(X)$ dans $A[X]$ alors au moins un des deux polynômes Q ou R est inversible dans $K[X]$, par exemple $Q = a$ constante. Mais alors comme P est primitif on a $1 = aC(Q)$ donc nécessairement a est un inversible de l'anneau. Ainsi, ona bien que notre élément est irréductible dans $A[X]$.

Ensuite, ce sont les seuls. En effet d'abord si le polynôme est de degré 0 et irréductible c'est clair qu'il doit être égal à un élément irréductible de A. Ensuite, si l'on considère dorénavant P de degré plus grand que 1, alors si P est irréductible il doit être primitif (sinon on factorise P sous la forme $c(P)P'$ et $c(P)$ est une constante non irréductible). Supposons P non irréductible dans $K[X]$ Alors $P = QR$ avec Q et R à coefficients dans K. des polynômes non constants. Posons $Q(X) = \sum a_i/b_i X^i$ et $R(X) = \sum a'_i/b'_i$. Alros en posant a un pgcd des a_i, b un ppcm des b_i, de même a' et b', on écrit $Q = a/bQ'$ avec Q' à coefficients entiers et primitif, de même $R = a'/b'R'$. Quitte à simplifier on peut supposer a et b premiers entre eux, de même pour a' et b'. On obtient alorsl'égalité dans $A[X]$ $bdP = acQ'R'$. En passant aux contenus cela donne $bd = ac$ modulo un inversible de A. Ainsi, $bd/ac \in A*$ et $P = \lambda Q'R'$ avec $\lambda \in A*$. Comme P est irréductible sur A on obtient Q' ou R' inversible donc de degré 0 et dans A^*, ce qui est supposé faux. □

Corollaire 2. *$A[X]$ est factoriel.*

Proof. pour l'existence de la décomposition, on commence par considérer le cas des polynômes primitifs. On décompose notre P en éléments irréductibles dans $K[X]$, $P = f_1^{\alpha_1} f_r^{\alpha_r}$. On écrit comme précedemment $f_i^{\alpha_i} = a_i/b_i f_i'$ avec f_i' a coefficients de A primitif. En passant au contenu, on a $c(\prod b_i P) = c(\prod a_i \prod f_i'^{\alpha_i})$. et donc on écrit P sous la forme $P = u \prod f_i'^{\alpha_i}$. et c'est ce qu'on veut. DAns le cas général, on écrit P sous la forme dP' avec P' primitif qu'on décompose dans $A|X]$ et d qu'on décompose dans A.

Pour l'unicitéé, on montre que P irréductible implique que l'idéal (P) est premier.

1. Si p est une constante irréductible alors par théorème d'isomorphisme des anneaux $A[X]/(p) \simeq A/(p)[X]$ (considérer le morphisme de réduction modulo p).

2. Si P est irréductible de degré supérieur. Alors grâce aà une manipulation sur les contenus similaire à des choses déjà faites, on montre très facilement que $PK[X] = \cap A[X] = PA[X]$. Donc par théorème sur les anneaux on a un morphisme injectif de $A[X]/PA[X]$ dans $K[X]/PK[X]$ et cet anneau eétant intègre, tout sous-anneau l'est aussi.

□