May 19, 2010

LE THÉORÈME DE GAUSS

Soient A un anneau factoriel, $K = \operatorname{Frac} A$ son corps des fractions et $A_0 = A \setminus \{0\}$. On choisit un ensemble $\mathcal{R}$ de représentants des irréductibles de A.

Definition 0.1. Soit $P(X) = a_n X^n + \ldots + a_1 X + a_0 \in K[X]$ non nul. Pour $p \in \mathcal{R}$ on pose $v_p(P) = \operatorname{Min}(v_p(a_i)\,;\, a_i \neq 0,\, 0 \leq i \leq n) \in \mathbb{Z}$, et *le contenu de* P est

$$c(P) \sim \prod_{p \in \mathcal{R}} p^{v_p(P)} \quad \in K^\times / A^\times.$$

Example 0.2. Si $P(X) \in A[X]$ est unitaire (i.e. $a_n = 1$) alors $c(P) \sim 1$.

Pour $P(X), Q(X) \in K[X] \setminus \{0\}$ posons $P \sim Q$ s'il existe $u \in A^\times$ tel que $P(X) = uQ(X)$. (Attention, ce n'est pas la relation d'équivalence habituelle sur $K[X] \setminus \{0\}$.)
L'application $c : K[X] \setminus \{0\} \to K^\times / A^\times$ vérifie les propriétés suivantes :

(1) $P(X) \in A[X] \setminus \{0\} \Leftrightarrow c(P) \in A_0/A^\times$; en particulier $c(P) \sim 1 \Rightarrow P(X) \in A[X]$.
(2) $\forall\, a \in K^\times$, $c(aP) \sim ac(P)$.
(3) $P \sim Q \Rightarrow c(P) \sim c(Q)$.
(4) Pour tout $P(X) \in K[X] \setminus \{0\}$ il existe $P_0(X)$ tel que $P \sim c(P)P_0$ et $c(P_0) \sim 1$.

La dernière propriété découle de (2),(3), et du fait que A est factoriel. Noter que par (1) on a $P_0(X) \in A[X]$ et que $\deg P = \deg P_0$.

Lemma 0.3 (Gauss)**.** *Soient $P(X), Q(X) \in K[X] \setminus \{0\}$. On a $c(PQ) \sim c(P)c(Q)$.*

Proof. Supposons d'abord $c(P) \sim c(Q) \sim 1$; alors $P(X), Q(X) \in A[X]$ par la propriété (1). Soit $p \in A$ irréductible. On considère le morphisme de projection $A \to A/(p) = \bar{A}$, $a \mapsto a + (p) = \bar{a}$, qui induit le morphisme $A[X] \to \bar{A}[X]$, $P(X) \mapsto P(X) + pA[X] = \bar{P}(X)$. Alors $c(P) \sim c(Q) \sim 1$ implique $\bar{P}(X) \neq 0$ et $\bar{Q}(X) \neq 0$ dans $\bar{A}[X]$. Comme A est factoriel et que p est irréductible, l'idéal (p) est premier, c'est-à-dire $\bar{A}$ est intègre. Donc $\bar{A}[X]$ est intègre. En particulier $\bar{P} \neq 0$ et $\bar{Q} \neq 0$ implique $\bar{P}\bar{Q} = \bar{P}\bar{Q} \neq 0$, ce qui équivaut à $v_p(PQ) = 0$. Ceci étant valable pour tout $p \in \mathcal{R}$ on obtient $c(PQ) \sim 1$.
En général on a $P \sim c(P)P_0$ et $Q \sim c(Q)Q_0$ avec $c(P_0) \sim c(Q_0) \sim 1$ par la propriété (4), d'où $c(PQ) = c(c(P)c(Q)P_0Q_0) \sim c(P)c(Q)c(P_0Q_0) \sim c(P)c(Q)$ par la propriété (2) et ce qui précède. □

Ce résultat est la clé technique des preuves des deux propositions suivantes.

Proposition 0.4. *Soient A un anneau factoriel et K son corps des fractions. Les éléments irréductibles de $A[X]$ sont :*

(1) *les éléments irréductibles de A,*
(2) *les éléments $P(X) \in A[X]$ tels que*
  (i) *$P(X)$ est irréductible dans $K[X]$,*
  (ii) *$c(P) \sim 1$.*

Remark 0.5. Noter que (i) implique $\deg P \geq 1$. En particulier, soit $P(X) \in A[X] \setminus A$ tel que $c(P) \sim 1$; alors

$$P(X) \text{ irréductible dans } A[X] \quad \Leftrightarrow \quad P(X) \text{ irréductible dans } K[X].$$

Proof. Montrons d'abord que ces éléments sont irréductibles dans $A[X]$.
(1) Soit $p \in A$ irréductible dans A ; alors $p = P(X)Q(X)$ avec $P, Q \in A[X]$ implique $\deg P + \deg Q = 0$, d'où $\deg P = \deg Q = 0$, i.e. $P(X) = a$ et $Q(X) = b$ avec $a, b \in A$. Alors $p = ab$ implique $a \in A^\times$ ou $b \in A^\times$ puisque p est irréductible dans A, c'est-à-dire $P \in A[X]^\times = A^\times$ ou $Q \in A[X]^\times$. Donc p est irréductible dans $A[X]$.
(2) Soit $P(X) \in A[X]$ vérifiant (i) et (ii) ; alors $P(X) = Q(X)R(X)$ avec $Q, R \in A[X]$ implique $Q(X) \in K[X]^\times = K^\times$ ou $R(X) \in K^\times$ par (i), disons $R(X) = a \in A_0 = A \cap K^\times$. Alors $P(X) = aQ(X)$, d'où $c(P) \sim ac(Q) \sim 1$ par (ii), ce qui équivaut à $a \in A^\times$, ou bien encore à $R(X) \in A[X]^\times$. Donc $P(X)$ est irréductible dans $A[X]$.

Montrons ensuite que tout élément irréductible $P(X)$ de $A[X]$ est dans la liste.
(1) Si $\deg P = 0$, i.e. si $P(X) = a \in A_0$, alors a irréductible dans $A[X]$ implique a irréductible dans A, puisque $A[X]^\times = A^\times$.
(2) Si $\deg P \geq 1$, alors $P(X)$ irréductible dans $A[X]$ et $P \sim c(P)P_0$ avec $c(P_0) \sim 1$ implique $c(P) \sim 1$ (puisque $\deg P_0 \geq 1$). Soient $Q(X), R(X) \in K[X]$ tels que $P(X) = Q(X)R(X)$. Par le lemme précédent on a $c(QR) \sim c(R)c(Q) \sim 1$. Puis $Q \sim c(Q)Q_0$ et $R \sim c(R)R_0$ donne $P \sim Q_0R_0$ avec $c(Q_0) \sim c(R_0) \sim 1$, d'où $P(X) = uQ_0(X)R_0(X)$ avec $u \in A^\times$ et $Q_0, R_0 \in A[X]$. Comme P est irréductible dans $A[X]$, on obtient $Q_0 \in A[X]^\times = A^\times$ ou $R_0 \in A^\times$, ce qui équivaut à $Q \in K^\times$ ou $R \in K^\times$, i.e. P irréductible dans $K[X]$. □

Proposition 0.6 (Théorème de Gauss)**.** *Si A est factoriel alors $A[X]$ est factoriel.*

Proof. Noter que tout se passe à unité près, i.e. aux éléments de $A[X]^\times = A^\times$ près. Soit $P(X) \in A[X]$ non nul.
Existence. On a $P \sim c(P)P_0$ avec $c(P) \in A_0/A^\times$ et $c(P_0) \sim 1$. Comme A est factoriel, par la proposition précédente il suffit de montrer l'existence pour $P(X) \in A[X]$ tel que $c(P) \sim 1$. Comme $K[X]$ est factoriel, on a $P(X) = \prod_{1 \leq j \leq r} P_j(X)$ avec $P_j(X)$ irréductible dans $K[X]$ pour tout $1 \leq j \leq r$. Le lemme montre que $c(P) \sim \prod_{1 \leq j \leq r} c(P_j) \sim 1$, d'où $P \sim \prod_{1 \leq j \leq r} c(P_j) \prod_{1 \leq j \leq r} P_{j,0} \sim \prod_{1 \leq j \leq r} P_{j,0}$. Les $P_{j,0}(X) \in A[X]$ sont irréductibles dans $K[X]$ et tels que $c(P_{j,0}) \sim 1$, donc ils sont irréductibles dans $A[X]$ par la proposition précédente.
Unicité. Soient $a, b \in A$, $P_0(X), Q_0(X) \in A[X]$ tous non nuls tels que $c(P_0) \sim c(Q_0) \sim 1$. Alors $aP_0 \sim bQ_0$ implique $a \sim b$, donc a et b ont la même factorisation à unité près dans A, puisque A est factoriel. Il suffit donc de montrer l'unicité pour les polynômes de contenu 1. Soit $P(X) \in A[X]$ tel que $c(P) \sim 1$ et $P \sim \prod_{1 \leq j \leq r} P_j \sim \prod_{1 \leq k \leq s} Q_k$ avec les P_j, Q_k irréductibles dans $A[X]$. Le lemme montre que, quitte à extraire les contenus, on peut supposer $c(P_j) \sim c(Q_k) \sim 1$ pour tous j, k. Comme $K[X]$ est factoriel, on a $r = s$ et $Q_j = a_j P_j$ (à permutation des facteurs près). On en déduit $c(Q_j) \sim a_j c(P_j)$, d'où $a_j \sim 1$, ce qui donne $Q_j \sim P_j$. □

Corollary 0.7. *Soit $n \geq 1$ entier. Si A est factoriel alors $A[X_1, \ldots, X_n]$ est factoriel.*

Proof. Induction sur n, en utilisant $A[X_1, \ldots, X_n] \simeq (A[X_1, \ldots, X_{n-1}])[X_n]$. □

Pour rendre ces résultats effectifs on a besoin de critères pratiques d'irréductibilité, ce qui est l'objet du paragraphe suivant.