Chapitre 5

Anneaux euclidiens, principaux, factoriels

Version corrigée du 19 novembre 2004

5.1 Anneaux principaux et anneaux euclidiens

Définition 5.1.1 *Soit A un anneau commutatif. On dit qu'il est principal s'il est intègre et si tout idéal de A est engendré par un élément.*

Des exemples importants d'anneaux principaux sont fournis par les anneaux euclidiens, introduits ci-dessous.

Définition 5.1.2 *Soit A un anneau commutatif intègre. On dit que A est euclidien s'il existe une application $v : A \to \mathbb{N}$ vérifiant la propriété suivante : pour tout $a, b \in A \setminus \{0\}$, il existe $q, r \in A$ tels que*

$$a = bq + r, \quad \text{et } r = 0 \text{ ou bien } v(r) < v(b).$$

Proposition 5.1.1 *Tout anneau euclidien A est principal.*

Démonstration. Soit I un idéal non nul de A. Alors l'ensemble des $v(P)$, pour $P \in I \setminus \{0\}$ est un sous-ensemble non vide de $\mathbb{N}$ donc admet un plus petit élément d. Soit $P_0 \in I$ tel que $v(P_0) = d$ et soit $P \in I$ arbitraire. Comme A est euclidien, il existe $Q, R \in A$ tels que

$$P = P_0 Q + R,$$

et $R = 0$ ou bien $v(R) < v(P_0) = d$. Or $R = P - P_0Q$ appartient à I, donc la seconde possibilité est exclue par minimalité de d. Donc $R = 0$ et $P = P_0Q$. Ceci montre que I est engendré par P_0. La proposition est démontrée. □

Exemples 5.1.1 1) L'anneau $\mathbb{Z}$, muni de la division euclidienne usuelle, est euclidien : l'application $v : \mathbb{Z} \to \mathbb{N}$ est la valeur absolue. D'après la démonstration précédente, tout idéal $I \neq 0$ de $\mathbb{Z}$ est égal à (n), où n est le plus petit élément > 0 de I.

2) Soit k un corps. On suppose connue du lecteur la division euclidienne dans $k[X]$ (on va voir une légère généralisation plus bas). Par conséquent, $k[X]$ est un anneau principal.

5.2 Propriétés de l'anneau $A[X]$

Lemme 5.2.1 *Supposons A intègre. Alors, pour tout $P, Q \in A[X] \setminus \{0\}$,*

$$\deg(PQ) = \deg P + \deg Q.$$

En particulier, $A[X]$ est intègre et ses éléments inversibles sont les éléments inversibles de A.

Démonstration. Soient $P, Q \in A[X] \setminus \{0\}$, de termes dominants aX^d et bX^f, respectivement, où $d = \deg P$ et $f = \deg Q$. Comme A est intègre, $ab \neq 0$ et donc PQ est de degré $d + f$. En particulier, $PQ \neq 0$.

De plus, si P est inversible, d'inverse Q, l'égalité $PQ = 1$ entraîne $\deg P = \deg Q = 0$, et donc P et Q sont des éléments inversibles de A. Le lemme est démontré. □

Proposition 5.2.2 *Soit A un anneau commutatif et $P \in A[X] \setminus \{0\}$, de coefficient dominant α inversible. Pour tout $F \in A[X]$, il existe $Q, R \in A[X]$ tels que*

$$F = PQ + R, \quad \text{et } R = 0 \text{ ou bien } \deg R < \deg P.$$

De plus, Q et R sont uniques si A est intègre.

Démonstration. Montrons l'existence par récurrence sur $\deg F$. C'est clair si $\deg F < d := \deg P$ (ici, on convient que $\deg 0 = -\infty$). Soit $n \geq d$. Supposons le résultat établi pour les degrés $< n$ et soit F de degré n et de coefficient dominant a. Alors

$$F - a\alpha^{-1}X^{n-d}P$$

est de degré $< n$, donc par hypothèse de récurrence il existe $Q, R \in A[X]$ tels que

$$F - a\alpha^{-1}X^{n-d}P = PQ + R,$$

avec $R = 0$ ou bien $\deg R < \deg P$. Alors $F = P(Q + a\alpha^{-1}X^{n-d}) + R$, ce qui prouve le résultat d'existence.

De plus, montrons l'unicité lorsque A est intègre. Soient Q_1 et R_1 vérifiant les mêmes conditions, alors

$$P(Q - Q - 1) = R - R_1.$$

Si $Q - Q_1$ était $\neq 0$ alors, comme A est intègre, $P(Q - Q_1)$ serait de degré $\geq \deg P$. Or, $R - R_1$ est nul ou de degré $< \deg P$. Il en résulte que $Q = Q_1$ et $R = R_1$. La proposition est démontrée. □

Corollaire 5.2.3 *Si k est un corps, alors $k[X]$ est euclidien, pour l'application $v = \deg$. Par conséquent, $k[X]$ est principal. Plus précisément, tout idéal $I \neq 0$ de $k[X]$ est engendré par l'unique polynôme unitaire de degré minimal contenu dans I.*

Démonstration. D'une part, $k[X]$ est intègre, d'après le lemme 5.2.1. D'autre part, $k[X]$ est euclidien, pour $v = \deg$, d'après la proposition 5.2.2. Plus précisément, soit I un idéal non nul et P un polynôme unitaire de I de degré d minimal. D'après la démonstration de la proposition 5.1.1, P engendre I. D'autre part, si Q est un polynôme unitaire de même degré, alors $P - Q$ appartient à I et est de degré $< d$, donc est nul. Ceci prouve le corollaire. □

5.3 Anneaux factoriels

5.3.1 Anneaux factoriels, lemmes d'Euclide et Gauss

Dans la suite de ce chapitre, A désigne un anneau commutatif intègre. La définition et proposition qui suivent auraient pu être incluses dans le paragraphe §4.5.

Définition 5.3.1 *Soient $a, b \in A$. On dit que a et b sont "premiers entre eux" ou sans facteur commun, si tout diviseur commun à a et b est un élément inversible. Ceci équivaut à dire que A est le seul idéal principal contenant a et b.*

Lemme 5.3.1 *Soit $p \in A$ irréductible et $a \in A \setminus \{0\}$. Si $a \notin (p)$ alors a et p sont sans facteur commun.*

Démonstration. Soit b un élément non inversible divisant a et p. Alors, b est associé à p et il en résulte que p divise a. Ceci prouve le lemme. □

Notation On écrira $a \mid b$ (resp., $a \nmid b$) pour signifier que a divise (resp., ne divise pas) b.

Définition 5.3.2 *Soit A un anneau commutatif intègre. On dit que A est (un anneau) factoriel s'il vérifie les deux conditions suivantes : existence (E) et unicité (U) de la décomposition en facteurs irréductibles.*

(E) Tout $a \in A \setminus \{0\}$, non inversible, s'écrit

$$a = p_1 \cdots p_r,$$

où $r \geq 1$ et les p_i sont des éléments irréductibles de A ;

(U) La décomposition précédente est unique, au sens suivant : si l'on a deux décompositions

$$a = p_1 \cdots p_r = q_1 \cdots q_s,$$

où les p_i et les q_j sont irréductibles, alors $s = r$ et il existe une permutation $\sigma \in S_r$ telle que p_i et $q_{\sigma(i)}$ soient associés, pour tout $i = 1, \ldots, r$. C.-à-d., de façon plus concise, la décomposition est unique à l'ordre des termes et aux inversibles près.

On rappelle que (E) est satisfaite si A est noethérien (Théorème 4.5.3).

Proposition 5.3.2 *Soit A un anneau commutatif intègre vérifiant* (E)*. Les propriétés suivantes sont équivalentes.*

1) *A vérifie* (U).

2) *Pour tout élément irréductible $p \in A$, l'idéal (p) est premier.*

3) *A vérifie le Lemme d'Euclide, c.-à-d., si $p \in A$ est irréductible et divise un produit $ab \neq 0$, il divise a ou b.*

4) *A vérifie le Lemme de Gauss, c.-à-d., pour tout $a, b, c \in A \setminus \{0\}$, si a divise bc et si a, b sont sans facteur commun, alors a divise c.*

Démonstration. Il est clair que 2) et 3) sont équivalents. L'implication 4) $\Rightarrow$ 3) est facile. En effet, soit p irréductible divisant un produit $ab \neq 0$. Si $p \nmid a$ alors, d'après le lemme précédent, a et p sont sans facteur commun, et l'hypothèse 4) donne alors que p divise b.

Montrons que 2) $\Rightarrow$ (U). Plus précisément, montrons que si l'on a une égalité

$$(*) \qquad p_1 \cdots p_m = u q_1 \cdots q_n,$$

où u est inversible et les p_i et q_j sont irréductibles, alors $m = n$ et il existe une permutation $\sigma \in S_n$ telle que p_i et $q_{\sigma(i)}$ soient associés, pour $i = 1, \ldots, n$. Si $m = 0$, le terme de gauche vaut 1 et ceci entraîne $n = 0$, car sinon q_1 serait inversible, ce qui n'est pas le cas pour un élément irréductible. Supposons $m > 0$ et le résultat établi pour $m - 1$.

Il résulte de $(*)$ que l'on a

$$\overline{q}_1 \cdots \overline{q}_n = 0$$

dans l'anneau $A/(p_1)$; comme ce dernier est intègre, par hypothèse, on obtient que p_1 divise l'un des q_i, donc lui est associé (puisque q_i est irréductible). Donc, quitte à changer la numérotation des q_j, on peut supposer que $p_1 = v q_1$, avec v inversible. Alors, comme A est intègre, on déduit de $(*)$ l'égalité

$$p_2 \cdots p_m = uv q_2 \cdots q_n,$$

et le résultat cherché découle alors de l'hypothèse de récurrence. Ceci prouve que 2) $\Rightarrow$ (U).

Montrons maintenant que 1) $\Rightarrow$ 4). Supposons A factoriel et soient $a, b, c, d \in A \setminus \{0\}$ tels que $ad = bc$, avec a et b sans facteur commun. Montrons que a divise c. On a des égalités

$$\begin{aligned} a &= \alpha p_1 \cdots p_n, & d &= \delta p'_1 \cdots p'_r, \\ b &= \beta q_1 \cdots q_s, & c &= \gamma q'_1 \cdots q'_t, \end{aligned}$$

avec $\alpha, \beta, \gamma, \delta$ inversibles, $n, r, s, t \geq 0$, et les p_i, p'_j, q_k et q'_ℓ irréductibles. On a donc une égalité

$$(**) \qquad u p_1 \cdots p_n \cdot p'_1 \cdots p'_r = q_1 \cdots q_s \cdot q'_1 \cdots q'_t,$$

avec u inversible. Montrons, par récurrence sur n, que ceci entraîne que $a \mid c$. Si $n = 0$, alors a est inversible et l'assertion est claire. Supposons $n \geq 1$ et le résultat établi pour $n - 1$.

Soit $i \in \{1, \ldots, n\}$. Comme a et b sont sans facteur commun, p_i ne peut être conjugué à l'un des q_j ; l'hypothèse (U) entraîne donc que p_1 est associé à un q'_k. Quitte à renuméroter les q'_k, on peut supposer que $p_1 = v q'_1$, avec v inversible. Alors, comme A est intègre, on déduit de $(**)$ l'égalité

$$uv p_2 \cdots p_n \cdot p'_1 \cdots p'_r = q_1 \cdots q_s \cdot q'_2 \cdots q'_t,$$

et le résultat cherché découle alors de l'hypothèse de récurrence. Ceci prouve que si A vérifie (E) et (U), il vérifie 4). Ceci achève la démonstration de la proposition. □

Remarque a) En procédant comme ci-dessus, on peut démontrer directement l'implication : A factoriel $\Rightarrow$ 3).

b) Ce qu'on appelle Lemme d'Euclide, resp. de Gauss, est l'assertion que si A est factoriel, il vérifie la condition 3), resp. 4). Pour mémoire, énonçons ci-dessous ces deux lemmes sous leur forme usuelle.

Proposition 5.3.3 *Supposons A factoriel et soient $a, b, c \in A \setminus \{0\}$ tels que a divise bc.*

(Lemme d'Euclide) *Si a est irréductible, il divise b ou c.*

(Lemme de Gauss) *Si a est sans facteur commun avec b, il divise c.*

5.3.2 Les anneaux principaux sont factoriels

Lemme 5.3.4 *Soient A un anneau intègre et p un élément non nul de A tel que l'idéal (p) soit premier. Alors p est irréductible.*

Démonstration. Soient $a, b \in A$ tels que $p = ab$. Comme (p) est premier, ceci entraîne, disons, que $a \in (p)$, d'où $a = p\alpha$, avec $\alpha \in A$. Alors $p = p\alpha b$, et comme A est intègre il vient $\alpha b = 1$. Donc b est inversible. Ceci montre que p est irréductible. □

Proposition 5.3.5 *Soit A un anneau principal. Alors A est noethérien et factoriel. De plus, tout idéal premier non nul de A est maximal.*

Démonstration. Par hypothèse, A est intègre. Comme tout idéal de A est engendré par un élément, A est noethérien. En particulier, il vérifie la condition (E), d'après le théorème 4.5.3.

Soit p un élément irréductible de A. D'après la proposition 4.5.2, l'idéal (p) est maximal parmi les idéaux principaux de A. Comme A est principal, ceci entraîne que (p) est maximal, donc a fortiori premier. D'après la proposition 5.3.2, ceci montre que A est factoriel.

Enfin, soit (a) un idéal premier non nul de A. D'après le lemme précédent, a est irréductible, et l'on vient de voir que dans ce cas (a) est un idéal maximal. La proposition est démontrée. □

5.4 Valuations, PGCD et PPCM

5.4.1 Valuations

Soit A un anneau intègre.

Définition 5.4.1 *Une application $v : A \to \mathbb{N} \cup \{+\infty\}$ est une valuation si elle vérifie : 1) $v(a) = +\infty \Leftrightarrow a = 0$,*
2) $v(ab) = v(a) + v(b)$, pour tout $a, b \in A \setminus \{0\}$,
3) $v(a + b) \geq \min(v(a), v(b))$, pour tout $a, b \in A \setminus \{0\}$.

Notons $\mathcal{I}$ l'ensemble des idéaux principaux de A, autres que (0) et A, et notons $\mathcal{P}$ l'ensemble des éléments maximaux de $\mathcal{I}$. (Attention ! On s'écarte de la notation introduite au §4.5). D'après la proposition 4.5.2, $\mathcal{P}$ est l'ensemble des idéaux (p), où p est irréductible. La notion de factorialité peut se formuler, de façon équivalente, en termes des éléments de $\mathcal{I}$ et $\mathcal{P}$. On laisse au lecteur la vérification (facile) de la proposition suivante.

Proposition 5.4.1 *A est factoriel ssi les conditions suivantes sont vérifiées.*

(E′) *Tout $(a) \in \mathcal{I}$ égale un produit $(p_1)^{n_1} \cdots (p_r)^{n_r}$, où $r \geq 1$, $n_1, \ldots, n_r \geq 1$, et les p_i sont irréductibles et deux à deux non associés.*

(U′) *Cette décomposition est unique, à renumérotation des (p_i) près.*

Supposons A factoriel et soit $a \in A \setminus \{0\}$. D'après la proposition précédente, il existe des entiers $v_{\mathfrak{p}}(a)$, pour $\mathfrak{p} \in \mathcal{P}$, nuls sauf un nombre fini d'entre eux, tels que

$$(a) = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{v_{\mathfrak{p}}(a)}.$$

Par convention, $\mathfrak{p}^0 = (1)$ pour tout $\mathfrak{p}$, et le produit ci-dessus ne porte que sur les $\mathfrak{p}$ tels que $v_{\mathfrak{p}}(a) \geq 1$. Si a est inversible, on a $v_{\mathfrak{p}}(a) = 0$ pour tout $\mathfrak{p} \in \mathcal{P}$ et le terme de droite égale (1). On pose aussi $v_{\mathfrak{p}}(0) = +\infty$, pour tout $\mathfrak{p} \in \mathcal{P}$.

Soit $\mathfrak{p} \in \mathcal{P}$ et soit p un générateur de $\mathfrak{p}$; c'est un élément irréductible.

Lemme 5.4.2 1) *Pour tout $a \in A \setminus \{0\}$, on a*

$$v_{\mathfrak{p}}(a) = \max\{n \geq 0 \mid a \in \mathfrak{p}^n\} = \max\{n \geq 0 \mid p^n \text{ divise } a\}.$$

2) *$v_{\mathfrak{p}}$ est une valuation.*

Démonstration. 1) La seconde égalité découle du fait que $\mathfrak{p}^n = (p^n)$. Montrons la 1ère égalité. Considérons une décomposition

$$a = p_1 \cdots p_t, \tag{1}$$

où les p_i sont irréductibles. Dans cette décomposition, regroupons les p_i qui sont associés ; on obtient ainsi une écriture

$$a = up^n q_2^{n_2} \cdots q_r^{n_r}, \tag{2}$$

où : u est inversible, $p = q_1$ est l'élément irréductible qu'on s'était fixé, n désigne le nombre de p_i dans (1) qui sont associés à p (éventuellement, $n = 0$), et les éléments p et $q_2, \ldots, q_r$ sont deux à deux non associés.

Alors $(a) = (p)^n (q_2)^{n_2} \cdots (q_r)^{n_r}$ et donc $v_\mathfrak{p}(a) = n$, d'après la définition de $v_\mathfrak{p}$. D'autre part, n est le plus grand entier ≥ 0 tel que p^n divise a. En effet, si on avait $a = p^{n+1}b$, on obtiendrait (puisque A est intègre), l'égalité $pb = uq_2^{n_2} \cdots q_r^{n_r}$, et donc, d'après l'unicité de la décomposition en éléments irréductibles, p serait associé à l'un des q_i, $i \geq 2$, ce qui n'est pas le cas. Ceci prouve la 1ère égalité de l'assertion 1).

2) Il est clair que $v_\mathfrak{p}(a) = +\infty$ ssi $a = 0$. Soient $a, b \in A \setminus \{0\}$. L'égalité $v_\mathfrak{p}(ab) = v_\mathfrak{p}(a) + v_\mathfrak{p}(b)$ résulte immédiatement du point 1). Montrons que

$$v_\mathfrak{p}(a + b) \geq \min(v_\mathfrak{p}(a), v_\mathfrak{p}(b)).$$

On peut écrire $a = p^m \alpha$ et $b = p^n \beta$, où $m = v_\mathfrak{p}(a)$ et $n = v_\mathfrak{p}(b)$. Supposons, par exemple, $m \leq n$. Alors

$$a + b = p^m(\alpha + p^{n-m}\beta),$$

et donc $v_\mathfrak{p}(a + b) \geq m$. Ceci termine la preuve du lemme. □

Pour tout élément irréductible $p \in A$, on écrira souvent v_p au lieu de $v_{(p)}$.

Proposition 5.4.3 *Soient $a, b \in A \setminus \{0\}$. Alors $a \mid b \Leftrightarrow v_\mathfrak{p}(a) \leq v_\mathfrak{p}(b)$, pour tout $\mathfrak{p} \in \mathcal{P}$.*

Démonstration. Si $b = ac$ alors

$$v_\mathfrak{p}(b) = v_\mathfrak{p}(a) + v_\mathfrak{p}(c) \geq v_\mathfrak{p}(a),$$

pour tout $\mathfrak{p} \in \mathcal{P}$. Ceci prouve l'implication $\Rightarrow$.

Montrons l'implication $\Leftarrow$. Soient $(p_1), \ldots, (p_r)$ les éléments de $\mathcal{P}$ qui interviennent dans la décomposition de (a) ou (b). On peut donc écrire

$$a = up_1^{m_1} \cdots p_r^{m_r}, \qquad b = vp_1^{n_1} \cdots p_r^{n_r},$$

avec u, v inversibles et les m_i et $n_i \geq 0$. Alors $v_{p_i}(a) = m_i$ et $v_{p_i}(b) = n_i$, pour $i = 1, \ldots, r$. L'implication $\Leftarrow$ en découle. □

5.4.2 PPCM et PGCD

Proposition 5.4.4 *Soit A factoriel et soient $a, b \in A \setminus \{0\}$.*

1) *L'idéal $(a) \cap (b)$ est principal. Tout générateur de cet idéal divise tout multiple commun à a et b, et est appelé un PPCM de a et b. Par abus de notation, on désignera par* $\mathrm{ppcm}(a, b)$ *l'un de ces générateurs.*

2) *L'ensemble des idéaux principaux contenant a et b possède un unique élément minimal. Tout générateur de cet idéal est multiple de tout diviseur commun à a et b, et est appelé un PGCD de a et b. Par abus de notation, on désignera par* $\mathrm{pgcd}(a, b)$ *l'un de ces générateurs.*

3) *Soit d, resp. m, un PGCD, resp. PPCM, de a et b. Alors dm est associé à ab. En particulier, a et b sont sans facteur commun $\Leftrightarrow$ ab est un PPCM de a et b.*

Démonstration. Soit $c \in A \setminus \{0\}$. Alors c appartient à $(a) \cap (b)$ ssi a et b divisent c, et ceci équivaut à

$$v_{\mathfrak{p}}(c) \geq \max(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(b)), \quad \forall \mathfrak{p} \in \mathcal{P}.$$

De même, (c) contient a et b ssi c divise a et b, et ceci équivaut à

$$v_{\mathfrak{p}}(c) \leq \min(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(b)), \quad \forall \mathfrak{p} \in \mathcal{P}.$$

Soient $(p_1), \ldots, (p_r)$ les éléments de $\mathcal{P}$ qui interviennent dans la décomposition de (a) ou (b) et, pour chaque i, soient $m_i = v_{p_i}(a)$ et $n_i = v_{p_i}(b)$. Il résulte de ce qui précède que :

1) $(a) \cap (b)$ est principal, engendré par $m := \prod_{i=1}^{n} p_i^{\max(m_i, n_i)}$. Cet élément est donc un ppcm de a et b.

2) Tout idéal principal contenant a et b contient l'idéal engendré par

$$d := \prod_{i=1}^{n} p_i^{\min(m_i, n_i)}.$$

Cet élément est donc un pgcd de a et b.

3) De plus, l'on a $dm = \prod_{i=1}^{n} p_i^{m_i + n_i}$, et cet élément est associé au produit ab. Enfin, a et b sont sans facteur commun ssi $(d) = (1)$, ce qui équivaut à $(m) = (ab)$. la proposition est démontrée. □

Remarque 5.4.1 Les définitions précédentes s'étendent au cas de N éléments $a_1, \ldots, a_N$ de $A \setminus \{0\}$: un pgcd des a_i est un élément d de A tel que

$$v_{\mathfrak{p}}(d) = \min(v_{\mathfrak{p}}(a_1), \ldots, v_{\mathfrak{p}}(a_N)), \qquad \forall \mathfrak{p} \in \mathcal{P};$$

tout idéal principal contenant les a_i contient l'idéal (d). On dit que les a_i sont sans facteur commun si $(d) = (1)$.

De même, un ppcm des a_i est un élément m de A tel que

$$v_{\mathfrak{p}}(m) = \max(v_{\mathfrak{p}}(a_1), \ldots, v_{\mathfrak{p}}(a_N)), \qquad \forall \mathfrak{p} \in \mathcal{P};$$

c'est un générateur de l'idéal $(a_1) \cap \cdots \cap (a_N)$.

Corollaire 5.4.5 (Unicité de l'écriture des fractions) *Soit A factoriel.*

1) *Soient $x, y \in A \setminus \{0\}$ et soit d un* pgcd *de x et y. Alors x/d et y/d sont sans facteur commun.*

2) *Soit K le corps des fractions de A. Tout élément $f \neq 0$ de K s'écrit de façon unique, aux inversibles près, $f = a/b$, avec $a, b \in A \setminus \{0\}$ sans facteur commun.*

Démonstration. 1) Écrivons $x = da$ et $y = db$. Si p était un élément non inversible divisant x et y, l'idéal (dp) contiendrait x et y et serait strictement contenu dans (d), contrairement à la définition de (d). Ceci prouve le point 1).

2) Soit $f \in K \setminus \{0\}$. Par définition de K, il existe $x, y \in A \setminus \{0\}$ tels que $f = x/y$. Soit d un pgcd de x et y ; posons $x = da$ et $y = db$. Alors a, b sont sans facteur commun, et $f = da/db = a/b$. Ceci prouve l'existence.

Montrons l'unicité, aux inversibles près. Supposons que $f = c/d$, avec c et d sans facteurs communs. Alors, on a l'égalité

$$ad = bc.$$

Comme a, b (resp. c, d) sans sont facteur commun, il résulte du Lemme de Gauss que $a \mid c$ et $b \mid d$ (resp. $d \mid b$ et $c \mid a$). Par conséquent, a et c sont associés, de même que b et d. Ceci prouve le corollaire. □

5.4.3 Le théorème de Bezout

Proposition 5.4.6 (Théorème de Bezout)

Soit A un anneau principal, soient $x_1, \ldots, x_n \in A \setminus \{0\}$ et soit d un pgcd *des x_i. Il existe des éléments $a_1, \ldots, a_n$ tels que*

$$(*) \qquad d = a_1 x_1 + \cdots + a_n x_n.$$

En particulier, les x_i sont sans facteur commun ssi l'idéal qu'ils engendrent est égal à A.

Démonstration. Soit I l'idéal engendré par les éléments $x_1, \ldots, x_n$. Comme A est principal, I est engendré par un élément d, nécessairement de la forme $(*)$ ci-dessus. D'autre part, il est clair que d est un pgcd des x_i. La proposition en découle. □

5.5 Le théorème de transfert de Gauss

5.5.1 Énoncé du théorème

Le but de cette section est de démontrer le théorème suivant.

Théorème 5.5.1 (Théorème de transfert de Gauss)
Si A est factoriel, $A[X]$ l'est aussi.

Corollaire 5.5.2 *Si A est factoriel, $A[X_1, \ldots, X_n]$ l'est aussi.*

Démonstration. Le corollaire découle du théorème par récurrence sur n, vu l'isomorphisme $A[X_1, \ldots, X_n] \cong (A[X_1, \ldots, X_{n-1}])[X_n]$. □

Pour la démonstration du théorème, on aura besoin de notions et résultats préliminaires. Démontrons d'abord la proposition suivante. Soit K le corps des fractions de A.

Proposition 5.5.3 *Soit A intègre et soit $P \in A[X]$ vérifiant l'une des deux conditions suivantes :*

i) P est un élément irréductible de A ;

ii) $\deg P \geq 1$*, les coefficients de P sont sans facteur commun, et P est irréductible en tant qu'élément de $K[X]$.*

Alors P est un élément irréductible de $A[X]$.

Démonstration. Supposons $P = QR$, avec $QR \in A[X]$.

1) Si P est un élément irréductible $p \in A$, alors Q et R sont de degré 0, donc appartiennent à A, et l'irréductibilité de p entraîne que Q ou R est inversible. Ceci prouve que p est irréductible dans $A[X]$.

2) Supposons ii) vérifiée. L'irréductibilité de P comme élément de $K[X]$ entraîne, disons, que $\deg Q = 0$. Donc Q appartient à A, et est un diviseur commun à tous les coefficients de P. Par conséquent, Q est inversible. Ceci prouve que P est un élément irréductible de $A[X]$. La proposition est démontrée. □

On aura besoin plus loin du lemme suivant. Soit I un idéal de A et notons $IA[X]$ l'idéal de $A[X]$ engendré par I. On observe que $IA[X]$ est formé des polynômes dont tous les coefficients appartiennent à I.

Lemme 5.5.4 *On a un isomorphisme de A-algèbres*

$$A[X]/IA[X] \xrightarrow{\sim} (A/I)[X].$$

Par conséquent, si I est un idéal premier de A, alors $IA[X]$ est un idéal premier de $A[X]$.

Démonstration. Soit π la projection $A \to A/I$; ceci fait de A/I une A-algèbre. D'après la propriété universelle de $A[X]$, il existe un unique morphisme de A-algèbres $\phi : A[X] \to (A/I)[X]$ tel que $\phi(X) = X$. Explicitement, pour tout $P = a_0 + \cdots + a_d X^d$, on a

$$\phi(P) = \pi(a_0) + \cdots + \pi(a_d)X^d.$$

Il est clair que ce morphisme est surjectif, et son noyau est l'idéal des polynômes dont tous les coefficients sont dans I, c.-à-d., $IA[X]$. Ceci prouve la 1ère assertion. La 2ème en résulte, d'après le lemme 5.2.1. □

5.5.2 Contenu d'un polynôme

Désormais, on suppose que A est factoriel.

Définition 5.5.1 *Soit $P \in A[X] \setminus \{0\}$. On note $c(P)$ et l'on appelle <u>contenu</u> de P un pgcd de ses coefficients. (Ainsi, le contenu est défini à un inversible près). On dit que P est <u>primitif</u> si $c(P)$ est inversible, c.-à-d., si les coefficients de P sont sans facteur commun.*

Remarque 5.5.1 Soit $a \in A \setminus \{0\}$. On voit facilement que $c(aP) = ac(P)$.

Lemme 5.5.5 (Lemme des contenus de Gauss)
On a $c(PQ) = c(P)c(Q)$, pour tout $P, Q \in A[X] \setminus \{0\}$.

Démonstration. On peut écrire $P = c(P)\widetilde{P}$ et $Q = c(Q)\widetilde{Q}$, où $\widetilde{P}$ et $\widetilde{Q}$ sont primitifs. Alors

$$PQ = c(P)c(Q)\widetilde{P}\widetilde{Q},$$

et donc $c(PQ) = c(P)c(Q)c(\widetilde{P}\widetilde{Q})$, d'après la remarque précédente.

Par conséquent, on peut supposer P et Q primitifs, et il s'agit de montrer que PQ l'est aussi. Supposons que ce ne soit pas le cas, et soit p un élément irréductible divisant $c(PQ)$.

Alors, dans l'anneau $A[X]/pA[X]$, on a $\overline{PQ} = 0$. Mais, d'après le lemme 5.5.4, l'on a

$$A[X]/pA[X] \cong (A/pA)[X],$$

et cet anneau est intègre, car pA est un idéal premier de A puisque A est factoriel. Par conséquent, on a $\overline{P} = 0$ ou $\overline{Q} = 0$, et donc p divise tous les coefficients de P ou de Q, ce qui contredit l'hypothèse que P et Q sont primitifs. Cette contradiction montre que PQ est primitif, et le lemme est démontré. □

Proposition 5.5.6 *Soit $P \in A[X]$. Alors P est irréductibles $\Leftrightarrow$ P vérifie l'une des conditions i) ou ii) de la proposition* 5.5.3.

Démonstration. On a déjà vu l'implication $\Leftarrow$. Réciproquement, supposons que P soit irréductible. Si $P \in A$, il est clair que c'est un élément irréductible de A. On peut donc supposer $\deg P \geq 1$; on a alors

$$P = c(P)\widetilde{P},$$

où $\widetilde{P}$ a même degré que P. En particulier, $\widetilde{P}$ n'est pas inversible et donc $c(P)$ l'est. Ainsi, P est primitif. Reste à montrer que P est irréductible dans $K[X]$. Supposons qu'on ait

$$P = QR$$

avec $Q, R \in K[X] \setminus \{0\}$. Alors on peut écrire $Q = (1/b)Q'$, avec $b \in A \setminus \{0\}$ et $Q' \in A[X]$, puis $Q' = a\widetilde{Q}$, avec $a = c(Q')$ et $\widetilde{Q}$ primitif de même degré que Q. De même, on a

$$R = \frac{c}{d}\widetilde{R},$$

avec $\widetilde{R} \in A[X]$ primitif et de même degré que R. Alors,

$$bdP = ac\widetilde{Q}\widetilde{R}.$$

Prenant les contenus et appliquant le lemme précédent, on obtient que bc et ac sont associés. Il en résulte que

$$P = u\widetilde{Q}\widetilde{R},$$

où u est un élément inversible de A. Comme P est supposé irréductible dans $A[X]$, ceci entraîne que $\widetilde{Q}$ ou $\widetilde{R}$ est un élément inversible de A, et alors Q ou R est un élément non nul de K. Ceci prouve que P est irréductible dans $K[X]$, et la proposition est démontrée. □

5.5.3 Preuve du théorème de transfert de Gauss

Montrons que $A[X]$ vérifie (E). Considérons d'abord un élément primitif $P \in A[X]$, de degré ≥ 1. Vu comme élément de $K[X]$, P s'écrit :

$$P = P_1^{n_1} \cdots P_r^{n_r},$$

où les P_i sont des polynômes irréductibles de $K[X]$ de degré ≥ 1. Pour chaque i, on peut écrire $P_i = (a_i/b_i)\widetilde{P}_i$, avec $a_i, b_i \in A \setminus \{0\}$ et $\widetilde{P}_i \in A[X]$ primitif. De plus, chaque $\widetilde{P}_i$ est, comme P_i, irréductible dans $K[X]$. Donc, d'après la proposition 5.5.3, chaque $\widetilde{P}_i$ est un élément irréductible de $A[X]$. De plus, on a l'égalité

$$(b_1^{n_1} \cdots b_r^{n_r})\, P = (a_1^{n_1} \cdots a_r^{n_r})\, \widetilde{P}_1^{n_1} \cdots \widetilde{P}_r^{n_r}.$$

Prenant les contenus, on voit que $b_1^{n_1} \cdots b_r^{n_r}$ et $a_1^{n_1} \cdots a_r^{n_r}$ sont associés. Par conséquent,

$$P = u\widetilde{P}_1^{n_1} \cdots \widetilde{P}_r^{n_r},$$

avec $u \in A$ inversible, et ceci est une décomposition de P en facteurs irréductibles.

Enfin, soit $P \in A[X] \setminus \{0\}$ arbitraire. On peut écrire $P = c(P)\widetilde{P}$, où $\widetilde{P}$ est primitif. Alors $\widetilde{P}$ admet une décomposition comme ci-dessus, et, d'autre part, $c(P) \in A$ se décompose en produit d'irréductibles. Ceci prouve que $A[X]$ vérifie (E).

Pour montrer que $A[X]$ est factoriel, il reste à montrer, d'après la proposition 5.3.2, que tout élément irréductible engendre un idéal premier. Si p est un élément irréductible de A, ceci résulte du fait que

$$A[X]/pA[X] \cong (A/pA)[X]$$

est intègre. D'autre part, soit $P \in A[X]$ un élément irréductible de degré ≥ 1. Supposons que P divise un produit $QR \neq 0$. Comme P est irréductible dans $K[X]$, qui est factoriel, on peut supposer que P divise Q dans $K[X]$. Il existe donc $a, b \in A \setminus \{0\}$ et $S \in A[X]$ primitif tels que

$$(*) \qquad Q = P\left(\frac{a}{b}S\right),$$

d'où $bQ = aPS$. D'après le lemme des contenus, on obtient que $bc(Q) = a$, d'où $a/b \in A$. Alors $(*)$ montre que P divise Q dans $A[X]$. Ceci prouve que l'idéal (P) de $A[X]$ est premier. Ceci termine la preuve du théorème de transfert de Gauss.