4 Anneaux factoriels, principaux, euclidiens, théorème chinois, modules de torsion sur un anneau principal

Version du 23 octobre 2005

16 Anneaux factoriels

16.1 Éléments irréductibles et éléments associés

Soit A un anneau commutatif **intègre**.

Définition 16.1.1 *1) Un élément $p \in A$ est dit* **irréductible** *s'il est non nul, non inversible, et vérifie la propriété suivante : si $p = ab$, avec $a, b \in A$, alors a ou b est inversible.*

2) On dit que deux éléments non nuls $a, a' \in A$ sont **associés** *s'il existe un élément inversible $u \in A^\times$ tel que $a' = ua$.*

3) On peut donc reformuler la définition 1) en disant que p est irréductible ssi ses seuls diviseurs sont les éléments qui lui sont associés, et les inversibles.

Définition 16.1.2 *Un idéal I de A est* **principal** *s'il est engendré par un seul élément, c.-à-d., si $I = (a)$, pour un certain $a \in A$. Un tel a n'est pas unique en général ; en effet, on a le lemme suivant.*

Lemme 16.1.3 *Soient $a, b \in A \setminus \{0\}$. Alors a et b sont associés $\Leftrightarrow$ ils engendrent le même idéal.*

Démonstration. $\Rightarrow$ est clair. Réciproquement, si $(a) = (b)$, il existe $\alpha, \beta \in A$ tels que $b = \alpha a$ et $a = \beta b$. Alors, $b = \alpha\beta a$ et comme A est intègre il vient $\alpha\beta = 1$. Donc α et β sont inversibles. Ceci prouve le lemme. □

Définition 16.1.4 *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 16.1.5 *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.

16.2 Anneaux factoriels, lemmes d'Euclide et Gauss

Définition 16.2.1 *Soit A un anneau commutatif. On dit que A est* **factoriel** *s'il est* **intègre** *et vérifie les deux conditions suivantes :* **existence** *(E) et* **unicité** *(U) de la* **décomposition en facteurs irréductibles**, *c.-à-d.,*

(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 (Proposition 2.6.4). Mais il y a aussi des exemples d'anneaux factoriels qui ne sont pas noethériens, c.-à-d., la décomposition en facteurs irréductibles peut exister sans que A soit nécessairement noethérien.

Proposition 16.2.2 *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 $i = 1, \ldots, n$. On peut supposer $m \leq n$.

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

$$a = \alpha p_1 \cdots p_n, \qquad d = \delta p'_1 \cdots p'_r,$$
$$b = \beta q_1 \cdots q_s, \qquad c = \gamma q'_1 \cdots q'_t,$$

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

$$(**) \qquad up_1 \cdots p_n \cdot p'_1 \cdots p'_r = q_1 \cdots q_s \cdot q'_1 \cdots q'_t,$$

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 $n - 1$.

Comme a et b sont sans facteur commun, p_1 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 $p_1 = vq'_1$, avec v inversible. Alors, comme A est intègre, on déduit de $(**)$ l'égalité

$$uvp_2 \cdots p_n \cdot p'_1 \cdots p'_r = q_1 \cdots q_s \cdot q'_2 \cdots q'_t,$$

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 16.2.3 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 16.2.4 *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.*

Remarque 16.2.5 Le Lemme de Gauss est **équivalent** à l'assertion $(*)$ ci-dessous :

> $(*)$ Si a et b sont sans facteur commun et divisent x, alors ab divise x.

En effet, soient $a, b \in A$ sans facteur commun. Supposons que A vérifie le Lemme de Gauss et que a, b divisent x. Alors x égale bc et est divisible par a. Comme a et b sont premiers entre eux, a divise c, donc $c = ad$ et $x = bad$ est divisible par ab.

Réciproquement, supposons $(*)$ vérifiée et $x = bc$ divisible par a. Alors x est divisible par ab, d'où $x = abd$, et comme A est intègre il vient $c = ad$, donc a divise c.

Corollaire 16.2.6 *Supposons A factoriel, soient $a_1, \ldots, a_n \in A$, deux à deux sans facteur commun, et soit b un multiple commun aux a_i. Alors b est divisible par $a_1 \cdots a_n$.*

Démonstration. On procède par récurrence sur n. Si $n = 2$, c'est la propriété $(*)$. Supposons $n \geq 3$ et le résultat établi pour $n - 1$. Par hypothèse de récurrence, il existe $c \in A$ tel que

$$b = a_2 \cdots a_n c.$$

Alors, par application répétée du Lemme de Gauss, on obtient que a_1 divise c. Ceci prouve le corollaire. □

16.3 PPCM et PGCD dans un anneau factoriel

Remarque 16.3.1 Soit A un anneau commutatif et soient $a_1, \ldots, a_n \in A$. L'ensemble des multiples communs aux a_i est égal à l'idéal

$$(a_1) \cap \cdots \cap (a_n).$$

D'autre part, un élément d de A divise tous les a_i si, et seulement si, (d) contient l'idéal $(a_1, \ldots, a_n)$ engendré par les a_i.

Définition et proposition 16.3.2 *Soit A factoriel et soient $a_1, \ldots, a_n \in A \setminus \{0\}$.*

1) *L'idéal $I := (a_1) \cap \cdots \cap (a_n)$ est principal. Soit M un générateur de cet idéal (M est unique à multiplication par un inversible près, c.-à-d., tout autre générateur de I est associé à M) ; alors M est un multiple commun aux a_i, qui divise tout multiple commun des a_i. On dit que M est un* **PPCM** *(plus petit commun multiple) des a_i. Par abus de notation, on écrira $M = \mathrm{ppcm}(a_1, \ldots, a_n)$.*

2) *L'ensemble des idéaux principaux contenant $(a_1, \ldots, a_n)$ possède un unique élément minimal J. Tout générateur d de J est un diviseur commun aux a_i, et si f est un autre diviseur commun aux a_i, alors (f) contient $J = (d)$ et donc f divise d. Donc, d est un diviseur commun aux a_i, qui est divisible par tout diviseur commun des a_i. Par conséquent, tout élément associé à d est un* **PGCD** *(plus grand commun diviseur) des a_i. Par abus de notation, on écrira $d = \mathrm{pgcd}(a_1, \ldots, a_n)$.*

De façon plus concrète, en décomposant chaque a_i en produits d'irréductibles, on peut écrire :

$$(\dagger) \qquad \left\{ \begin{array}{ccc} a_1 & = & u_1\, p_1^{c_{11}} \cdots p_r^{c_{1r}}, \\ \vdots & & \vdots \\ a_n & = & u_n\, p_1^{c_{n1}} \cdots p_r^{c_{nr}}, \end{array} \right.$$

où $p_1, \ldots, p_r \in A$ sont des éléments irréductibles deux à deux non associés, $u_1, \ldots, u_n \in A$ sont inversibles, et $c_{ij} \in \mathbb{N}$. Pour $j = 1, \ldots, r$, posons

$$M_j = \max\{c_{1j}, \ldots, c_{nj}\}, \quad m_j = \min\{c_{1j}, \ldots, c_{nj}\},$$

et soient

$$M = p_1^{M_1} \cdots p_r^{M_r}, \qquad d = p_1^{m_1} \cdots p_r^{m_r}.$$

Alors M est un générateur de I, donc un PPCM des a_i. D'autre part, tout diviseur commun aux a_i divise d, et donc d est un PGCD des a_i.

Démonstration. Soit $b \in A$ un multiple commun aux a_i. Dans la décomposition (†), fixons un indice $j \in \{1, \ldots, r\}$. Alors, b est divisible par $p_j^{c_{ij}}$, pour $i = 1, \ldots, n$, donc aussi par M_j. Comme les $p_j^{M_j}$ sont deux à deux sont diviseurs communs, il résulte du corollaire 16.2.6 que b est divisible par

$$M := p_1^{M_1} \cdots p_r^{M_r}.$$

Ceci montre que M engendre l'idéal $(a_1) \cap \cdots \cap (a_n)$ et est donc un PPCM des a_i.

D'autre part, comme $a_i = u_i\, p_1^{c_{i1}} \cdots p_r^{c_{ir}}$, il résulte de l'unicité de la décomposition en facteurs irréductibles que tout diviseur de a_i est de la forme

$$a_i' = v_i\, p_1^{c_{i1}'} \cdots p_r^{c_{ir}'},$$

où v_i est inversible et $c_{ij}' \leq c_{ij}$ pour $j = 1, \ldots, r$. Donc, si f est un diviseur commun aux a_i, alors

$$f = v\, p_1^{c_1'} \cdots p_r^{c_r'},$$

où v est inversible et où, pour chaque $j = 1, \ldots, r$, c_j' est inférieur à c_{ij}, pour $i = 1, \ldots, n$, donc à m_j. Par conséquent, f divise

$$d = p_1^{m_1} \cdots p_r^{m_r}.$$

Ceci montre que d est un PGCD des a_i. La proposition est démontrée. □

Définition 16.3.3 *On dit que $a_1, \ldots, a_n \in A$ sont* **premiers entre eux** *s'ils n'ont pas de diviseur commun non inversible. Ceci équivaut à dire que leur PGCD est* 1.

Corollaire 16.3.4 (Unicité de l'écriture des fractions)

Soit A factoriel et soit K son corps des fractions.

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) *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 a et b, l'idéal (dp) contiendrait x et y et serait strictement contenu dans (d), contrairement à la définition de (d). Ceci prouve 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 facteur commun. 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. □

16.4 Le théorème de transfert de Gauss

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

Théorème 16.4.1 (Théorème de transfert de Gauss)
Si A est factoriel, $A[X]$ l'est aussi.

Corollaire 16.4.2 *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. Commençons par le lemme suivant. Soient A un anneau, I un idéal de A et $IA[X]$ 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 16.4.3 *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 première assertion. La deuxième en résulte, d'après la proposition 8.1.2. □

Désormais, on suppose que A est **factoriel**, et l'on note K son corps des fractions.

Définition 16.4.4 (Contenu d'un polynôme) *Soit $P \in A[X] \setminus \{0\}$. On note $c(P)$ et l'on appelle* **contenu** *de P un pgcd de ses coefficients. (Ainsi, le contenu est défini à un inversible près). On dit que P est* **primitif** *si $c(P)$ est inversible, c.-à-d., si les coefficients de P sont sans facteur commun.*

Remarque 16.4.5 Soit $a \in A \setminus \{0\}$. On voit facilement que $c(aP) = ac(P)$.

Lemme 16.4.6 (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 16.4.3, 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 16.4.7 (Polynômes irréductibles de $A[X]$)

Soit A factoriel et soit K son corps des fractions. Les éléments irréductibles de $A[X]$ sont les éléments irréductibles de A, et les polynômes primitifs $P \in A[X]$ qui sont irréductibles dans $K[X]$.

Démonstration. Montrons d'abord que les éléments indiqués sont irréductibles dans $A[X]$. Si p est un élément irréductible de A, et si $p = QR$, avec $Q, R \in A[X]$, 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 $A[X]$.

Soit maintenant $P \in A[X]$, primitif, et irréductible dans $K[X]$. Supposons $P = QR$, avec $Q, R \in A[X]$. 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 $A[X]$.

Réciproquement, supposons que $P \in A[X]$ 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 ad 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. □

Nous pouvons maintenant démontrer le théorème de transfert de Gauss. On suppose A factoriel.

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 16.4.7, 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 16.2.2, 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, où $Q, R \in A[X]$.

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

$$b\,c(Q) = ac(PS) = a,$$

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.

17 Anneaux principaux et anneaux euclidiens

17.1 Les anneaux euclidiens sont principaux

Définition 17.1.1 *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 17.1.2 *Soit A un anneau commutatif. On dit que A est* **euclidien** *s'il est* **intègre** *et s'il existe une application $\rho : A \to \mathbb{N}$ vérifiant la propriété suivante : pour tout $a, b \in A \setminus \{0\}$, il existe $q, r \in A$ tels que*

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

Proposition 17.1.3 *Tout anneau euclidien A est principal. Plus précisément, soit I un idéal non nul de A et soit $a \in I$ tel que $\rho(a)$ soit minimal. Alors $I = (a)$.*

Démonstration. Soit I un idéal non nul de A. Alors l'ensemble des $\rho(P)$, 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 $\rho(P_0) = d$ et soit $P \in I$ arbitraire. Comme A est euclidien, il existe $Q, R \in A$ tels que

$$P = P_0Q + R,$$

et $R = 0$ ou bien $\rho(R) < \rho(P_0) = d$. 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 17.1.4 1) L'anneau $\mathbb{Z}$, muni de la division euclidienne usuelle, est euclidien (l'application $\rho : \mathbb{Z} \to \mathbb{N}$ étant la valeur absolue).

2) Soit k un corps. D'après le théorème 8.1.4, $k[X]$ est euclidien, pour l'application $\rho = \deg$.

17.2 Les anneaux principaux sont factoriels

Lemme 17.2.1 *Soient A un anneau intègre et p un élément non nul de A. Si l'idéal (p) est 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. □

Lemme 17.2.2 (Théorème de Bezout)
Soit A un anneau principal et soient $x, y \in A$ sans facteur commun. Il existe $a, b \in A$ tels que

$$(*) \qquad 1 = ax + by.$$

Démonstration. Soit $I = Ax + Ay$. Comme A est principal, I est engendré par un élément d, de la forme $d = ax + by$. D'autre part, comme (d) contient x et y, alors d est un diviseur commun à x et y. L'hypothèse entraîne que d est inversible, d'où $Ax + Ay = A$. Le lemme en découle. □

Corollaire 17.2.3 *Soit A principal et soit $p \in A$ irréductible. Alors (p) est maximal, donc premier.*

Démonstration. Soit $a \in A$ non divisible par p. Alors p et a sont sans facteur commun donc, d'après le lemme (théorème) de Bezout, il existe $u, v \in A$ tels que $up + vb = 1$. Donc $(p) + Aa = A$, pour tout $a \notin (p)$. Ceci montre que (p) est maximal. □

Théorème 17.2.4 *Soit A un anneau principal. Alors A est noethérien et factoriel. De plus, tout idéal premier non nul de A est enegendré par un élément irréductible et 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 la proposition 2.6.4.

Soit p un élément irréductible de A. D'après le corollaire précédent, l'idéal (p) est maximal, donc a fortiori premier. D'après la proposition 16.2.2, ceci montre que A est factoriel.

Enfin, soit (a) un idéal premier non nul de A. D'après le lemme 17.2.1, a est irréductible, et l'on vient de voir que dans ce cas (a) est un idéal maximal. La proposition est démontrée. □

18 Idéaux étrangers et théorème chinois

18.1 Idéaux étrangers

Soit A un anneau commutatif.

Définition 18.1.1 (Produits d'idéaux de A)

1) Soient $I_1, \dots, I_m$ des idéaux de A, non nécessairement distincts. On note $I_1 \cdots I_m$ l'idéal engendré par les produits $x_1 \cdots x_m$, où $x_j \in I_j$ pour $j = 1, \dots, m$. C'est l'ensemble des sommes finies de tels produits.

2) On observe que si chaque I_j est principal, c.-à-d., $I_j = (a_j)$, alors $I_1 \cdots I_m$ est l'idéal engendré par $a_1 \cdots a_m$.

3) Si $I_1, \dots, I_m$ sont tous égaux à I, on obtient l'idéal I^m, formé des sommes finies arbitraires de produits de m éléments de I :

$$I^m := \left\{ \sum x_1 \cdots x_m \mid x_i \in I \right\}.$$

Remarque 18.1.2 1) On prendra garde que, en général, I^m est stictement plus grand que l'idéal engendré par les puissances m-ièmes d'éléments de I. Par exemple, si $A = k[X, Y]$ et si I est l'idéal engendré par X et Y, alors I^2 est engendré par X^2, XY et Y^2, et XY n'est pas un carré.

2) On a toujours $I_1 \cdots I_m \subseteq I_1 \cap \cdots \cap I_m$, et l'inclusion est en général stricte (prendre, par exemple, $I_j = (a)$, pour tout j).

Soient $I_1, \dots, I_n$ des idéaux de A. On note $I_1 + \cdots + I_n$ l'idéal formé des sommes $x_1 + \cdots + x_n$, où $x_j \in I_j$ pour $j = 1, \dots, n$.

Définition 18.1.3 *Soient $I_1, \dots, I_n$ des idéaux de A.*

1) On dit que $I_1, \dots, I_n$ sont **étrangers** *(on dit aussi "premiers entre eux") si l'on a $I_1 + \cdots + I_n = A$.*

2) On dit que $I_1, \dots, I_n$ sont **étrangers deux à deux** *si I_r et I_s sont étrangers, pour tout $r \neq s$.*

Remarque 18.1.4 On prendra garde à ne pas confondre ces deux notions. Si $n \geq 3$, la deuxième condition est beaucoup plus forte que la première ! Pour éviter les confusions, on dira parfois dans le premier cas que $I_1, \ldots, I_n$ sont étrangers "dans leur ensemble"

Lemme 18.1.5 *On suppose que I est étranger à $J_1, \ldots, J_m$ (on ne suppose pas les J_i nécessairement distincts). Alors I est étranger à $J_1 \cdots J_m$.*

Démonstration. Par hypothèse, il existe, pour $i = 1, \ldots, m$, des éléments $x_i \in I$ et $y_i \in J_i$ tels que $x_i + y_i = 1$. Alors

$$1 = \prod_{i=1}^{m} (x_i + y_i),$$

et en développant ce produit on obtient le terme $y_1 \cdots y_m$ qui appartient à $J_1 \cdots J_m$, et une somme de termes qui contiennent au moins un x_i donc appartiennent à I. Ceci prouve le lemme. □

Corollaire 18.1.6 *Supposons $I_1, \ldots, I_n$ étrangers deux à deux, et soient $m_1, \ldots, m_n$ des entiers ≥ 1.*

1) *On a $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$.*

2) *$I_1^{m_1}, \ldots, I_n^{m_n}$ sont étrangers deux à deux.*

3) *Posons $J_k = \prod_{j \neq k} I_j^{m_j}$, pour $k = 1, \ldots, n$. Alors, $J_1, \ldots, J_n$ sont étrangers "dans leur ensemble", c.-à-d., on a $J_1 + \cdots + J_n = A$.*

Démonstration. Dans 1), il suffit de montrer l'inclusion $\supseteq$, puisque l'autre est évidente. On va prouver les assertions 1) et 2) par récurrence sur n. Supposons d'abord $n = 2$.

Par hypothèse, il existe $x_1 \in I_1$ et $x_2 \in I_2$ tels que $x_1 + x_2 = 1$. Alors, pour tout $a \in I_1 \cap I_2$, l'on a :

$$a = a \cdot 1 = ax_1 + ax_2 \in I_1 I_2,$$

d'où $I_1 I_2 = I_1 \cap I_2$. D'autre part, d'après le lemme précédent, I_1 est étranger à $I_2^{m_2}$, puis $I_2^{m_2}$ est étranger à $I_1^{m_1}$, ce qui prouve 2) dans le cas $n = 2$.

Supposons $n \geq 3$ et les deux assertions établies pour $n-1$. Par hypothèse de récurrence, $I_2 \cap \cdots \cap I_n = I_2 \cdots I_n$, et, d'après le lemme, cet idéal est étranger à I_1. On a donc

$$I_1 \cap \cdots \cap I_n = I_1 \cap (I_2 \cdots I_n) = I_1 \cdot I_2 \cdots I_n,$$

ce qui prouve 1). D'autre part, par hypothèse de récurrence, $I_2^{m_2}, \ldots, I_n^{m_n}$ sont étrangers deux à deux. De plus, d'après le cas $n = 2$, chaque $I_k^{m_k}$ est étranger avec $I_1^{m_1}$. L'assertion 2) est démontrée.

Démontrons l'assertion 3). D'abord, $I_1^{m_1}$,..., $I_r^{m_r}$ sont étrangers deux à deux, d'après l'assertion 2). Donc, sans perte de généralité, on peut se limiter au cas où $m_k = 1$ pour tout k.

Pour chaque k, I_k et J_k sont étrangers, d'après le lemme 18.1.5, donc il existe $x_k \in I_k$ et $y_k \in J_k$ tels que $1 = x_k + y_k$. On obtient donc

$$1 = \prod_{k=1}^{n} (x_k + y_k).$$

Développons le produit : les termes qui contiennent un y_k appartiennent à J_k et donc à $J_1 + \cdots + J_r$; le seul autre terme est $x_1 \cdots x_r$, qui appartient à J_k pour tout k. Ceci montre que $1 \in J_1 + \cdots + J_r$, ce qui termine la preuve du corollaire. □

Remarque 18.1.7 a) On voit facilement que si un idéal premier P contient un produit d'idéaux $J_1 \cdots J_r$, alors il contient l'un des J_k.

b) En utilisant a) et le corollaire 11.2.8 (existence d'idéaux maximaux), on peut démontrer le point 2) du corollaire de façon plus conceptuelle. Supposons en effet qu'il existe $r \neq s$ tels que $I_r^{m_r}$ et $I_s^{m_s}$ ne soient pas étrangers. Alors $I_r^{m_r} + I_s^{m_s}$ est un idéal propre, donc est contenu dans un idéal maximal $\mathfrak{m}$. Comme $\mathfrak{m}$ est premier et contient $I_r^{m_r}$ et $I_s^{m_s}$, il contient I_r et I_s, ce qui contredit l'hypothèse $I_r + I_s = A$.

18.2 Théorème chinois des restes

Définition 18.2.1 (Produits d'anneaux) *Soit $(A_i)_{i \in I}$ une famille d'anneaux. Le groupe abélien $\prod_{i \in I} A_i$ est muni d'une structure d'anneau, où la multiplication est définie coordonnée par coordonnée :*

$$(a_i)_{i \in I} \cdot (b_i)_{i \in I} = (a_i b_i)_{i \in I}$$

L'élément neutre, noté 1, est la famille $(a_i)_{i \in I}$ telle que $a_i = 1$ pour tout $i \in I$. Si I est fini, disons $I = \{1, \ldots, n\}$, cet anneau se note

$$A_1 \times \cdots \times A_n \quad \textit{ou} \quad A_1 \oplus \cdots \oplus A_n.$$

Théorème 18.2.2 (Théorème chinois des restes)

On suppose $I_1, \ldots, I_n$ étrangers deux à deux. Alors le morphisme naturel $\psi : A \to A/I_1 \oplus \cdots \oplus A/I_n$ induit un isomorphisme

$$A/(I_1 \cap \cdots \cap I_n) \xrightarrow{\sim} \bigoplus_{r=1}^{n} A/I_r.$$

Démonstration. Il est clair que $\ker \psi = \bigcap_{r=1}^{n} I_r$. On va établir l'isomorphisme annoncé par récurrence sur n. Commençons par remarquer que, pour démontrer la surjectivité de ψ, il suffit de trouver $\varepsilon_1, \cdots, \varepsilon_n \in A$ tels que $\psi(\varepsilon_r) = (0, \ldots, 0, 1, 0, \ldots, 0)$ (où 1 est à la r-ième place), car alors un élément arbitraire

$$(\overline{a_1}, \ldots, \overline{a_n})$$

sera l'image de $a_1\varepsilon_1 + \cdots + a_n\varepsilon_n$.

Supposons $n = 2$. Par hypothèse, il existe $x_1 \in I_1$ et $x_2 \in I_2$ tels que $x_1 + x_2 = 1$. Alors $1 - x_1 = x_2$ appartient à $1 + I_1$ et à I_2 et donc on peut prendre $\varepsilon_1 = 1 - x_1$, et de même $\varepsilon_2 = 1 - x_2$. Ceci prouve le théorème dans le cas $n = 2$.

Supposons $n \geq 3$ et le théorème établi pour $n - 1$. D'après le lemme 18.1.5 et le corollaire 18.1.6, $I_2 \cap \cdots \cap I_n$ égale $I_2 \cdots I_n$ et est étranger à I_1. Donc, d'après le cas $n = 2$, la projection

$$A \longrightarrow A/I_1 \bigoplus A/(I_2 \cap \cdots \cap I_n)$$

induit un isomorphisme

$$A/(I_1 \cap \cdots \cap I_n) \xrightarrow{\sim} A/I_1 \bigoplus A/(I_2 \cap \cdots \cap I_n). \tag{1}$$

De plus, par hypothèse de récurrence, la projection $A \to \bigoplus_{r=2}^{n} A/I_r$ induit un isomorphisme

$$A/(I_2 \cap \cdots \cap I_n) \xrightarrow{\sim} \bigoplus_{r=2}^{n} A/I_r. \tag{2}$$

En composant les isomorphismes (1) et (2), on obtient l'isomorphisme annoncé. Ceci prouve le théorème. □

19 Modules de torsion sur un anneau principal

19.1 Annulateurs et modules de torsion

Définition 19.1.1 *Soient M un A-module et $m \in M$. On pose*

$$\mathrm{Ann}(m) = \{a \in A \mid am = 0\}, \text{ et } \mathrm{Ann}(M) = \{a \in A \mid \forall x \in M,\ ax = 0\}.$$

Ce sont des idéaux de A. De plus, si $(x_i)_{i\in I}$ est un système de générateurs de M (fini ou infini), on voit facilement que

$$\mathrm{Ann}(M) = \bigcap_{x\in M} \mathrm{Ann}(x) = \bigcap_{i\in I} \mathrm{Ann}(x_i).$$

Définition 19.1.2 *On dit que M est un A-module* **de torsion** *si $\mathrm{Ann}(m) \neq (0)$, pour tout $m \in M$.*

Définition 19.1.3 *On dit que M est un A-module* **monogène** *(ou* **cyclique***) s'il peut être engendré par un seul générateur x. Ceci équivaut à dire que $M \cong A/I$, où $I = \mathrm{Ann}(x)$.*

Lemme 19.1.4 *Supposons A* **intègre** *et soit M un A-module* **de torsion** *et* **de type fini**. *Alors $\mathrm{Ann}(M) \neq (0)$.*

Démonstration. Soit $x_1, \ldots, x_n$ un système fini de générateurs de M. Comme M est de torsion, $I_k := \mathrm{Ann}(x_k)$ est non nul, pour tout k. Alors $\mathrm{Ann}(M) = I_1 \cap \cdots \cap I_n$ est non nul, car il contient $I_1 \cdots I_n$, qui est $\neq (0)$ puisque A est intègre. □

Exercice 19.1.1 Le $\mathbb{Z}$-module quotient $\mathbb{Q}/\mathbb{Z}$ est de torsion mais pas de type fini, et l'on a $\mathrm{Ann}(\mathbb{Q}/\mathbb{Z}) = 0$.

Définition 19.1.5 *Soit M un A-module. On note*

$$M_{tors} = \{m \in M \mid \exists a \in A \setminus \{0\} \text{ tel que } am = 0\}$$

l'ensemble des éléments de torsion de M.

Lemme 19.1.6 *On suppose A* **intègre**. *Alors M_{tors} est un sous-module de M, appelé le* **sous-module de torsion**, *et le module quotient M/M_{tors} est sans torsion.*

Démonstration. Soient $m, m' \in M_{\mathrm{tors}}$ et $b \in A \setminus \{0\}$. Par hypothèse, il existe $a, a' \in A \setminus \{0\}$ tels que $am = 0 = a'm'$. Comme A est intègre, $aa' \neq 0$ et $ba \neq 0$ et donc les égalités $0 = (aa')(m - m')$ et $(ba)m = 0$ montrent que $m - m'$ et bm appartiennent à M_{tors}. Ceci prouve la première assertion.

Prouvons la seconde. Soient $m \in M$ et $b \in A \setminus \{0\}$ tels que $b\pi(m) = 0$, où π désigne la projection $M \to M/M_{\mathrm{tors}}$. Alors $bm \in M_{\mathrm{tors}}$, donc il existe $a \in A \setminus \{0\}$ tel que $abm = 0$. Comme $ab \neq 0$ (puisque A est intègre), ceci implique $m \in M_{\mathrm{tors}}$, d'où $\pi(m) = 0$. Le lemme est démontré. □

19.2 Décomposition primaire des modules de torsion sur un anneau principal

Soit A un anneau principal.

Définition 19.2.1 *On note $\mathcal{P}$ l'ensemble des idéaux (p), où p est irréductible ; ce sont les idéaux maximaux de A. En particulier, les éléments de $\mathcal{P}$ sont deux à deux étrangers.*

Remarque 19.2.2 $\mathcal{P}$ est en bijection avec l'ensemble des classes d'équivalence d'éléments irréductibles de A, pour la relation $p \sim p'$ si p et p' sont associés.

Lemme 19.2.3 *Tout idéal propre $I \neq (0)$ s'écrit de façon unique comme un produit $\mathfrak{p}_1 \cdots \mathfrak{p}_n$ d'éléments de $\mathcal{P}$.*

Démonstration. Soit a un générateur de I et $a = p_1 \cdots p_n$ sa décomposition en facteurs irréductibles. Posant $\mathfrak{p}_i = (p_i)$, on obtient

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n = (p_1) \cdots (p_n) = (a).$$

Ceci prouve l'existence. D'autre part, supposons

$$(*) \qquad (a) = \mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

avec $\mathfrak{q}_i \in \mathcal{P}$. Alors $\mathfrak{q}_i = (q_i)$, avec q_i irréductible, et $(*)$ entraîne :

$$a = u\, q_1 \cdots q_s, \qquad \text{avec } u \text{ inversible.}$$

L'unicité de la décomposition en facteurs irréductibles entraîne que $s = n$ et que, quitte à renuméroter, q_i et p_i sont associés, c.-à-d., $(q_i) = (p_i)$, pour $i = 1, \ldots, n$. Ceci prouve l'unicité. □

Définition et proposition 19.2.4 1) *Soient M un A-module et $p \in A$ un élément irréductible. On pose*

$$M(p) := \{m \in M \mid \exists n \geq 1 \text{ tel que } p^n m = 0\}.$$

C'est un sous-module de M_{tors}, appelé la **composante p-primaire**.

2) *On dit que M est p-primaire s'il est égal à $M(p)$.*

3) *Soit $\mathfrak{p} = (p)$. On désignera aussi $M(p)$ par $M(\mathfrak{p})$ et l'on dira que c'est la composante $\mathfrak{p}$-primaire de M.*

Démonstration. Il est clair que $M(p) \subseteq M_{\text{tors}}$, et la seule chose à vérifier est que $M(p)$ soit un sous-module. Soient $a \in A$ et $x, x' \in M(p)$. Il existe $n, n' \in \mathbb{N}^*$ tels que $p^n x = 0 = p^{n'} x'$. Alors, $x + ax'$ est annulé par p^s, où $s = \max\{n, n'\}$. □

Lemme 19.2.5 *Soit M un A-module p-primaire.*

1) *Pour tout $x \in M \setminus \{0\}$, on a $\mathrm{Ann}(x) = (p^n)$, pour un certain $n \geq 1$.*

2) *Si M est de type fini, alors $\mathrm{Ann}(M) = (p^n)$, pour un certain $n \geq 1$.*

Démonstration. Posons $\mathrm{Ann}(x) = (a)$; c'est un idéal propre, puisque $x \neq 0$. D'autre part, par hypothèse, il existe $t \geq 1$ tel que $p^t x = 0$. Donc $p^t \in (a)$ et donc a divise p^t. Comme p est irréductible, on obtient que a est associé à un certain p^n, avec $n \leq t$. Ceci prouve la première assertion.

Supposons de plus que M soit engendré par des éléments $x_1, \ldots, x_r$. Posons $\mathrm{Ann}(x_i) = (p^{n_i})$, pour tout i. Alors

$$\mathrm{Ann}(M) = \bigcap_{i=1}^{r} \mathrm{Ann}(x_i) = (p^n),$$

où $n = \max(n_1, \ldots, n_r)$. Ceci prouve le lemme. □

Lemme 19.2.6 *Soit M un A-module. La somme des sous-modules $M_{\mathfrak{p}}$, pour $\mathfrak{p} \in \mathcal{P}$, est une somme directe.*

Démonstration. Soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \mathcal{P}$, deux à deux distincts. Supposons qu'on ait une égalité

$$x_1 = x_2 + \cdots + x_r,$$

où $x_k \in M_{\mathfrak{p}_k}$ pour tout k. Il existe des entiers $n_1, \ldots, n_r \geq 1$ tels que

$$\mathfrak{p}_k^{n_k} x_k = 0, \qquad \forall k = 1, \ldots, r.$$

Alors $x_1 = x_2 + \cdots + x_r$ est annulé par $I_1^{n_1}$ et par $I_2^{n_2} \cdots I_r^{n_r}$. Or, ces deux idéaux sont étrangers, d'après le corollaire 18.1.6. Ceci entraîne $x_1 = 0$, et le lemme en découle. □

Théorème 19.2.7 (Décomposition primaire des modules de torsion sur un anneau principal)

Soit A principal et soit M un A-module **de torsion**. *Alors*

1) $$M = \bigoplus_{\mathfrak{p} \in \mathcal{P}} M(\mathfrak{p}).$$

2) *Supposons de plus M de type fini et soit* $\mathrm{Ann}(M) = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$ *la décomposition de son annulateur en produits d'idéaux maximaux. Alors,*

$$M = \bigoplus_{i=1}^{r} M(\mathfrak{p}_i),$$

et l'on a $\mathrm{Ann}\, M(\mathfrak{p}_i) = \mathfrak{p}_i^{n_i}$*, pour* $i = 1, \ldots, r$.

Démonstration. 1) On a déjà vu que la somme des $M(\mathfrak{p})$ est directe. Montrons qu'elle vaut M. Soit $m \in M$, non nul. Comme M est de torsion, $\mathrm{Ann}(m)$ est non nul, donc égale un produit

$$\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$$

où $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \mathcal{P}$ sont deux à deux distincts. Pour $k = 1, \ldots, r$, posons

$$J_k = \prod_{j \neq k} \mathfrak{p}_j^{n_j}.$$

D'après le corollaire 18.1.6, $J_1, \ldots, J_r$ sont étrangers, donc on peut écrire

$$1 = y_1 + \cdots + y_r,$$

où $y_k \in J_k$. Chaque $y_k m$ est annulé par $\mathfrak{p}_k^{n_k}$, donc appartient à $M(\mathfrak{p}_k)$. De plus, on a

$$m = 1 \cdot m = y_1 m + \cdots + y_r m.$$

Ceci prouve la première assertion.

Supposons de plus que M soit engendré par un nombre fini d'éléments $x_1, \ldots, x_n$. Chaque x_i a des composantes $x_{i,\mathfrak{p}}$ non nulles seulement pour $\mathfrak{p}$ dans un sous-ensemble fini $\mathcal{P}_i$ de $\mathcal{P}$. La réunion de ces sous-ensembles est un sous-ensemble fini $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ de $\mathcal{P}$, et l'on a

$$M = \bigoplus_{i=1}^{r} M(\mathfrak{p}_i).$$

De plus, chaque $M(\mathfrak{p}_i)$, étant un quotient de M, est de type fini, donc $\mathrm{Ann}\, M(p_i) = \mathfrak{p}_i^{n_i}$, pour un certain $n_i \geq 1$, d'après le lemme 19.2.5.

Par conséquent, $\mathrm{Ann}(M) = \bigcap_{i=1}^{r} \mathfrak{p}_i^{n_i}$, et comme les $\mathfrak{p}_i$ sont deux à deux étrangers, on obtient

$$\mathrm{Ann}(M) = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}.$$

Ceci achève la preuve du point 2). Le théorème est démontré. □

Corollaire 19.2.8 (Décomposition des fractions sur un anneau principal ou euclidien)

Soit A principal et soit K son corps des fractions.

1) *Le A-module K/A est de torsion et sa décomposition primaire est la suivante :*

$$K/A = \bigoplus_{(p)\in\mathcal{P}} A[\tfrac{1}{p}]/A,$$

où $A[\frac{1}{p}] = \{\frac{a}{p^n} \mid n \geq 1, a \in A\} = \bigcup_{n\geq 0} \frac{1}{p^n}A$.

2) *Si A est* **euclidien**, *relativement à $\rho : A\setminus\{0\} \to \mathbb{N}$, alors tout $x \in A[\frac{1}{p}]$ s'écrit comme une somme finie*

$$(*) \qquad x = a + \sum_{i=1}^{r} \frac{a_i}{p^i},$$

où $a, a_i \in A$ et $\rho(a_i) < \rho(p)$ si $a_i \neq 0$. De plus, cette écriture est **unique si** *ρ vérifie la condition ci-dessous :*

$$(**) \qquad \rho(a-b) \leq \max\{\rho(a), \rho(b)\} \leq \rho(ab), \qquad \forall a, b \in A \setminus \{0\}.$$

(Si $a = b$, on convient que $\rho(0) = -\infty$).

Démonstration. D'abord, $K/A = \bigoplus_{(p)\in\mathcal{P}}(K/A)(p)$, d'après le théorème précédent. Notons π la projection $K \to K/A$. Pour tout $t \in K$, on a

$$\pi(t) \in (K/A)(p) \Leftrightarrow \exists n \geq 1 \text{ tel que } p^n t = a \in A.$$

L'assertion 1) en découle.

2) On convient que $\rho(0) = -\infty$. Montrons par récurrence sur n que tout $x \in \frac{1}{p^n}A$ s'écrit

$$x = \sum_{i=0}^{n-1} \frac{a_i}{p^{n-i}} + a_n,$$

où $a_0, \ldots, a_n \in A$ et $\rho(a_i) < \rho(p)$ pour $i = 0, \ldots, n-1$. C'est clair si $n = 0$. Supposons $n \geq 1$ et le résultat établi pour $n-1$. Soit $x = a/p^n$, où $a \in A$. Comme (A, ρ) est euclidien, il existe $a', a_0 \in A$ tels que $a = pa' + a_0$ et $\rho(a_0) < \rho(p)$. Alors, d'une part,

$$(1) \qquad \frac{a}{p^n} = \frac{a_0}{p^n} + \frac{a'}{p^{n-1}}.$$

D'autre part, par hypothèse de récurrence, il existe $a_1, \ldots, a_n \in A$ vérifiant $\rho(a_i) < \rho(p)$ et

$$\frac{a'}{p^{n-1}} = \sum_{i=1}^{n-1} \frac{a_i}{p^{n-i}} + a_n. \tag{2}$$

En combinant (1) et (2), on obtient le résultat au cran n. Ceci prouve l'existence.

Supposons maintenant que ρ vérifie la condition $(**)$. Pour montrer l'unicité annoncée, il suffit de montrer que si l'on a une égalité

$$a_0 + a_1 p + \cdots + a_n p^n = b_0 + b_1 p + \cdots + b_n p^n, \tag{3}$$

avec $a_0, b_0, \ldots, a_n, b_n \in A$ et $\rho(p) > \rho(a_i), \rho(b_i)$ pour $i = 0, \ldots, n-1$, alors $a_i = b_i$ pour tout i. Procédons par récurrence sur n. C'est clair si $n = 0$. Supposons $n \geq 1$ et l'assertion établie pour $n-1$. Il résulte de (3) que $a_0 - b_0 = p\alpha$, avec $\alpha \in A$. Si on avait $\alpha \neq 0$, on aurait

$$\rho(p) \leq \rho(p\alpha) = \rho(a_0 - b_0) \leq \max\{\rho(a_0), \rho(b_0)\} < \rho(p),$$

une contradiction. Donc $a_0 = b_0$, et (3) entraîne

$$a_1 + \cdots + a_n p^{n-1} = b_1 + \cdots + b_n p^{n-1}.$$

Par hypothèse de récurrence, on conclut que $b_i = a_i$ pour tout i. Le corollaire est démontré. □

Remarque 19.2.9 L'hypothèse $(**)$ sur ρ entraîne l'unicité du quotient et du reste dans la division euclidienne, *cf.* la démonstration ci-dessus, et celle de la proposition 1.2.1.

Corollaire 19.2.10 (Décomposition des fractions rationnelles en éléments simples)

Soient k un corps et $k(X)$ le corps des fractions rationnelles (c.-à-d., le corps des fractions de $k[X]$). Notons $\mathcal{P}$ l'ensemble des polynômes irréductibles unitaires de $k[X]$. Alors, tout élément $F \in k(X)$ s'écrit de façon unique comme une somme finie

$$F = E + \sum_{P \in \mathcal{P}} \sum_{j \geq 1} \frac{a_{P,j}}{P^j},$$

avec E et les $a_{P,j}$ dans $k[X]$, nuls sauf pour un nombre fini d'indices, et $\deg(a_{P,j}) < \deg P$ pour tout P et j. En particulier, si k est algébriquement clos,

$$F = E + \sum_{\lambda \in k} \sum_{j \geq 1} \frac{a_{\lambda,j}}{(X-\lambda)^j},$$

où $E \in k[X]$ et $a_{\lambda,j} \in k$.

Démonstration. Ceci résulte du corollaire précédent, puisque l'application $\deg : k[X] \setminus \{0\} \to \mathbb{N}$ vérifie l'hypothèse $(**)$. □

Remarque 19.2.11 Dans $\mathbb{Q}$, et a fortiori dans $\mathbb{Q}/\mathbb{Z}$, on a l'égalité

$$\frac{1}{2} - \frac{1}{3} = \frac{2}{3} - \frac{1}{2}.$$

Ceci s'explique par le fait que dans $\mathbb{Z}[\frac{1}{2}]/\mathbb{Z}$ et $\mathbb{Z}[\frac{1}{3}]/\mathbb{Z}$ on a les égalités

$$\frac{1}{2} \equiv -\frac{1}{2} \quad \text{et} \quad -\frac{1}{3} \equiv \frac{2}{3}.$$

La valeur absolue $\mathbb{Z} \to \mathbb{N}$ ne vérifie pas la condition $(**)$ car, par exemple $|-1-1| = 2 > \max\{|-1|, |1|\}$. De même, dans la division euclidienne par un entier $n > 0$, la condition $|r| < n$ ne suffit pas à déterminer uniquement le reste ; on a unicité seulement si l'on impose à r de vérifier $0 \leq r < n$.

Table des matières

Bibliographie

[BAlg] N. Bourbaki, Algèbre, Chapitres 4 à 7, Masson, 1981.

[BM] J. Briançon, Ph. Maisonobe, Éléments d'algèbre commutative (niveau M1), Ellipses, 2004.

[De] R. Dedekind, Sur la théorie des nombres entiers algébriques, Gauthier-Villars, 1877 ; traduit en anglais avec une introduction de J. Stillwell dans : Theory of algebraic integers, Cambridge Univ. Press 1996.

[Die] J. Dieudonné, Cours de géométrie algébrique, tome 2, P.U.F., 1974.

[Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes (2 tomes), Cedic Fernand Nathan, 1979, et 2ème édition, Cassini, 2005.

[Elk] R. Elkik, Cours d'algèbre, Ellipses, 2002.

[Esc] J.-P. Escofier, Théorie de Galois, Dunod, 2000.

[Ja1] N. Jacobson, Basic algebra I, W. H. Freeman & Co., 1974.

[Kru] W. Krull, Idealtheorie, Springer Verlag, 1937 (2e édition 1968).

[La] S. Lang, Algebra, Addison-Wesley, 1965. Traduction française de la 3ème édition : Algèbre, Dunod, 2004.

[Pe1] D. Perrin, Cours d'algèbre, E.N.S.J.F. 1981, et 3ème édition, Ellipses, 1996.

[Pe2] D. Perrin, Géométrie algébrique - Une introduction, Inter Éditions/-CNRS Éditions, 1995.

[Sa] P. Samuel, Théorie algébrique des nombres, Hermann, 1967.

[St] J. Stillwell, Chapitre d'introduction dans [De].

[vdW] B. L. van der Waerden, History of algebra from al-Khwarizmi to Emmy Noether, Springer Verlag, 1985.