6.9 Démonstration des résultats de la section 6.3

On présente les démonstration manquantes des résultats de la section 6.3 du chapitre 6, à l'exception de l'existence d'anneaux principaux non euclidiens.

6.9.1 Tout anneau euclidien est principal

Commençons par démontrer que tout anneau euclidien est principal, c'est-à-dire le point 4 du théorème 7. En un sens, il n'y a strictement rien de nouveau par rapport aux démonstrations déjà connues du fait que $\mathbf{Z}$ et $\mathbf{K}[X]$ ($\mathbf{K}$ un corps) sont principaux, démonstrations basées de manière cruciale sur la division euclidienne.

Soit donc A un anneau euclidien, et ν un stathme euclidien sur A. Par définition d'un anneau euclidien, A est intègre.

Soit $\mathcal{I}$ un idéal de A. Il s'agit de montrer qu'il existe $a \in A$ tel que $\mathcal{I} = aA$. Si $\mathcal{I} = \{0\}$, $a = 0$ convient. On suppose à présent $\mathcal{I} \neq \{0\}$. On peut donc considérer le plus petit élément ν_0 de la partie non vide de $\mathbf{N}$ égale à $\nu(\mathcal{I} \setminus \{0\})$, et $a \in \mathcal{I} \setminus \{0\}$ un élément tel que $\nu(a) = \nu_0$. Montrons que $\mathcal{I} = aA$. Comme $a \in \mathcal{I}$, on a l'inclusion $aA \subset \mathcal{I}$. Soit à présent $b \in \mathcal{I}$. Soit $b = aq + r$ une division euclidienne de b par a (rappelons que a est non nul). En particulier on a $r = 0$ ou $\nu(r) < \nu(a) = \nu_0$. Mais par ailleurs on a $r = b - aq$ donc $r \in \mathcal{I}$. Si $r \neq 0$, on a donc $r \in \mathcal{I} \setminus \{0\}$ et $\nu(r) < \nu_0$ contredit la définition de ν_0. Donc $r = 0$ et $b = aq$, et finalement $b \in aA$. Donc $\mathcal{I} \subset aA$, d'où on déduit $\mathcal{I} = aA$

6.9.2 Tout anneau principal vérifie Bézout, Gauss et Euclide

Démontrons à présent le théorème 10.

Soit A un anneau principal. D'après la proposition 3, il suffit de montrer que A vérifie le théorème de Bézout. Soit $a, b \in A$ premiers entre eux. Il s'agit de montrer que $aA + bA = A$ (rappelons que la réciproque est vraie sur n'importe quel anneau intègre). Comme A est principal, il existe $d \in A$ tel que $aA + bA = dA$. En particulier $aA \subset dA$, donc d divise a. De même d divise b. Comme a et b sont premiers entre eux, d est inversible, donc $dA = A$ et $aA + bA = A$.

6.9.3 Tout anneau factoriel vérifie Gauss et Euclide

On démontre le théorème 9.

On va en fait démontrer un résultat en peu plus général.

Théorème 42. *Soit A un anneau intègre. On suppose que tout élément de A non nul et non inversible s'écrit comme un produit d'éléments irréductibles de A. Alors les propriétés suivantes sont équivalentes ,*

1. *A est factoriel ;*
2. *A vérifie le lemme de Gauss ;*
3. *A vérifie le lemme d'Euclide.*

Démonstration. On sait (proposition 3) que (2) implique (3) pour n'importe quel anneau intègre.

Montrons que (1) implique (2). Supposons donc A factoriel et montrons que le lemme de Gauss est vérifié.

Soit $a, b, c \in A$ tels que a divise bc et a et b sont premiers entre eux. Montrons que a divise c. Le résultat est immédiat si a est nul ou inversible. Soit $\pi \in \mathscr{I}(A)$. Montrons que $v_\pi(a) \leqslant v_{\pi(c)}$. Supposons $v_\pi(b) > 0$. Comme a et b sont premiers entre eux, d'après le théorème 19, on a $v_\pi(a) = 0$. En particulier $v_\pi(a) \leqslant v_{\pi(c)}$. Supposons $v_\pi(b) = 0$. Alors $v_\pi(bc) = v_\pi(b) + v_\pi(c) = v_\pi(c)$. Comme a divise bc, d'après le théorème 16, on a $v_\pi(a) \leqslant v_\pi(bc)$. Donc finalement on a $v_\pi(a) \leqslant v_\pi(c)$.

Ainsi pour tout $\pi \in \mathscr{I}(A)$ on a $v_\pi(a) \leqslant v_{\pi(c)}$. Donc, d'après le théorème 16, a divise c.

Il reste à montrer que (3) implique (1). Supposons donc que A vérifie le lemme d'Euclide et que tout élément non nul et non inversible de A s'écrive comme un produit d'éléments irréductibles.

Soit I, J des ensembles finis non vides, $\{p_i\}_{i\in I}$, $\{q_j\}_{j\in J}$ des familles d'éléments irréductibles de A indexées par I et J respectivement et telles que

$$\prod_{i\in I} p_i = \prod_{j\in J} q_j.$$

Il s'agit montrer qu'il existe une bijection $\psi\colon I \to J$ telle que pour tout $i \in I$, p_i et $q_{\psi(i)}$ sont associés.

Soit $A \subset I$ une partie de I maximale pour l'inclusion telle qu'il existe $B \subset J$ et une bijection $\psi\colon A \to B$ telle que pour tout $i \in A$, p_i et $q_{\psi(i)}$ sont associés (a priori, le cas $A = \varnothing$ n'est pas exclu). Si $A = I$ et $B = J$ on a terminé. Raisonnons par l'absurde et supposons $A \neq I$ ou $B \neq J$. Comme $\prod_{i\in A} p_i$ et $\prod_{j\in B} q_j$ sont associés, $\prod_{i\in I} p_i = \prod_{j\in J} q_j$, les éléments $\prod_{i\in I\setminus A} p_i$ et $\prod_{j\in J\setminus B} q_j$ sont associés. Si $A \neq I$ et $B = J$, on obtient que $\prod_{i\in I\setminus A} p_i$ est inversible. Ceci entraîne que pour tout $i \in I \setminus A$, p_i est inversible, ce qui contredit l'irréductibilité de p_i. De même on ne peut avoir $A = I$ et $B \neq J$. Il reste à examiner le cas $A \neq I$ et $B \neq J$. Soit $i_0 \in A \setminus I$. Comme $\prod_{i\in I\setminus A} p_i$ divise $\prod_{j\in J\setminus B} q_j$, l'élément irréductible p_{i_0} divise $\prod_{j\in J\setminus B} q_j$. Comme A vérifie le lemme d'Euclide, il existe $j_0 \in J$ tel que p_{i_0} divise q_{j_0}. Comme p_{i_0} et q_{j_0} sont irréductibles, ceci entraîne que p_{i_0} et q_{j_0} sont associés. On peut donc étendre ψ en une bijection $A \cup \{i_0\} \to B \cup \{j_0\}$ en posant $\psi(i_0) = j_0$. Ceci contredit la maximalité de A. Finalement, on a bien $A = I$ et $B = J$, ce qui conclut.

□

6.9.4 Tout anneau principal est factoriel

On va utiliser le théorème 42 pour montrer que tout anneau principal est factoriel : on sait déjà que tout anneau principal vérifie Euclide ; il suffit donc de montrer que dans un anneau principal tout élément non nul et non inversible est un produit d'éléments irréductibles.

Soit donc A un anneau principal. Montrons tout d'abord que tout élément a de A non nul et non inversible est divisible par un élément irréductible de A. Comme a est non inversible, aA est un idéal propre de A, et est donc contenu dans un idéal maximal $\mathfrak{M}$ de A. Comme A est principal, il existe $\pi \in A$ tel que $\mathfrak{M} = \pi A$. Comme l'idéal $\mathfrak{M}$ est maximal et contient $a \neq 0$, il est premier et non nul. Donc π est irréductible. Comme aA est contenu dans πA, π divise a.

Lemme 43. *Soit $(\mathcal{I}_n)_{n\in\mathbf{N}}$ une suite croissante (pour l'inclusion) d'idéaux de A. Alors la suite est stationnaire, en d'autres termes il existe $n \in \mathbf{N}$ tel que pour tout $m \geqslant n$ on a $\mathcal{I}_m = \mathcal{I}_n$.*

Démonstration. Soit $n \in \mathbf{N}$. Comme A est principal, il existe $a_n \in A$ tel que $\mathcal{I}_n = a_n A$. Soit $\mathcal{I} := \cup_{n\in\mathbf{N}} \mathcal{I}_n$. Comme la suite $(\mathcal{I}_n)$ est croissante, on peut montrer que $\mathcal{I}$ est un idéal de A (faites-le !). Comme A est principal, il existe $b \in A$ tel que $\mathcal{I} = bA$. En particulier $b \in \cup_{n\in\mathbf{N}} \mathcal{I}_n$. Soit $n \in \mathbf{N}$ tel que $b \in \mathcal{I}_n$. Montrons que pour tout $m \geqslant n$ on a $\mathcal{I}_m = \mathcal{I}$, ce qui conclura. Soit $m \geqslant n$. Par croissance de la suite d'idéaux, on a $b \in \mathcal{I}_m = a_m A$. Comme $\mathcal{I} = bA$ est l'idéal engendré par b, on en déduit $\mathcal{I} = bA \subset \mathcal{I}_m$. Mais par définition de $\mathcal{I}$, on a $\mathcal{I}_m \subset \mathcal{I}$. Donc finalement $\mathcal{I}_m = \mathcal{I}$. □

Soit alors $a \in A$ un élément non nul et non inversible. Montrons que a est un produit d'éléments irréductibles. D'après le résultat précédent, il existe un élément irréductible π_1 tel que π_1 divise a. Soit $a_1 = \frac{a}{\pi_1}$. En particulier, a_1 est non nul. Si a_1 est inversible, a est irréductible et on a terminé. Sinon, il existe un élément irréductible π_2 de A qui divise a_1. Si $a_2 = \frac{a_1}{\pi_2}$ est inversible, on a terminé. Sinon, il existe un élément irréductible π_3 de A qui divise a_2... Il s'agit de voir que ce procédé se termine, en utilisant le lemme ci-dessus.

En fait on va associer à a deux suites $(\pi_n)_{n\geqslant 1}$ et $(a_n)_{n\geqslant 0}$ d'éléments de A telles que $a_0 = a$ et pour tout $n \in \mathbf{N} \setminus \{0\}$ on a : π_n est irréductible ou $\pi_n = 1$,

$$a = a_n \prod_{i=1}^{n} \pi_i, \text{et} \quad a_{n+1}\pi_{n+1} = a_n$$

On construit cette suite par récurrence en commençant comme indiqué ci-dessus pour (a_1, π_1). Supposons la suite $(a_i, \pi_i)_{i\leqslant n}$ construite. Si a_n est inversible, on pose $\pi_{n+1} = 1$

et $a_{n+1} = a_n$ Sinon, il existe un élément irréductible π_{n+1} de A qui divise a_n et on pose $a_{n+1} = \frac{a_n}{\pi_{n+1}}$

Pour tout $n \in \mathbf{N}$, posons $\mathcal{I}_n := a_n A$. Soit $n \in \mathbf{N}$. L'égalité $a_{n+1}\pi_{n+1} = a_n$ montre que $a_n \in a_{n+1}A$, d'où $a_n A \subset a_{n+1}A$. Ainsi la suite $(\mathcal{I}_n)$ est croissante. D'après le lemme ci-dessus, il existe $n_0 \in \mathbf{N}$ tel que $a_{n_0}A = a_{n_0+1}A$. Ainsi a_{n_0} et a_{n_0+1} sont associés. Comme $a_{n_0+1}\pi_{n_0+1} = a_{n_0}$ et un élément irréductible n'est pas inversible, on voit que π_{n_0+1} n'est pas irréductible. D'après la construction de la suite (a_n, π_n) ceci montre que a_{n_0} est inversible. Comme $a = a_{n_0} \prod_{i=1}^{n_0} \pi_i$, ceci conclut la démonstration.

6.9.5 Tout anneau factoriel qui vérifie Bezout est principal

Soit A un anneau factoriel vérifiant le théorème de Bezout. On va montrer que A est principal. Comme A est factoriel, A est intègre. Il reste à démontrer que tout idéal de A est principal, c'est à dire est engendré par un élément.

Commençons par montrer que tout idéal de A engendré par un nombre fini d'éléments est principal. Soit $a, b \in A$ et I l'idéal engendré par a et b. Si $a = b = 0$, $I = \{0\} = 0\,A$. Sinon a et b admettent un pgcd δ non nul. Montrons que $aA + bA = \delta A$. Comme δ divise a et b, on a $aA \subset \delta A$ et $bA \subset \delta A$, donc $aA + bA \subset \delta A$. Par ailleurs $\alpha := \frac{a}{\delta}$ et $\beta := \frac{b}{\delta}$ sont premiers entre eux. Comme A vérifie le théorème de Bezout, on a $\alpha A + \beta A = A$. Ainsi il existe $(u, v) \in A^2$ tels que $\alpha u + \beta v = 1$. En multipliant la relation précédente par δ, on obtient $\delta \in aA + bA$. Comme δA est l'idéal engendré par δ, on en déduit l'inclusion $\delta A \subset aA + bA$, d'où finalement l'égalité $aA + bA = \delta A$.

Ainsi tout idéal de A engendré par deux éléments est principal. Une récurrence facile montre alors que tout idéal de A engendré par un nombre fini d'éléments est principal.

Montrons ensuite que dans un anneau factoriel toute suite croissante (pour l'inclusion) d'idéaux principaux est stationnaire. Soit $(a_n) \in A^{\mathbf{N}}$ une suite d'éléments de A telle que la suite d'idéaux $(a_n A)_{n\in\mathbf{N}}$ est croissante pour l'inclusion. En d'autres termes, pour tout $n \in \mathbf{N}$, a_{n+1} divise a_n. Pour tout élément irréductible π de A, on obtient alors que la suite d'entiers positifs $(v_\pi(a_n))_{n\in\mathbf{N}}$ est décroissante, donc stationnaire. Par ailleurs, pour tout élément irréductible π de A qui ne divise pas a_0, $(v_\pi(a_n))_{n\in\mathbf{N}}$ est la suite nulle. On en déduit qu'il existe $N_0 \in \mathbf{N}$ tel que pour tout élément irréductible π de A la suite $(v_\pi(a_n))_{n\geqslant N_0}$ est constante (égale à disons ν_π). Soit $a = \prod_{\pi\in\mathscr{I}(A)} \pi^{\nu_\pi}$. Alors pour tout $n \geqslant N_0$, a_n et a, ayant les mêmes valuations adiques, sont associés. Ainsi pour tout $n \geqslant N_0$, on a $a_n A = aA$, ce qui conclut.

Montrons enfin que tout idéal I de A est principal. Soit I un idéal de A. On construit par récurrence une suite (I_n) d'idéaux de A contenus dans I de la façon suivante : soit $a_0 \in I$. On pose $I_0 = a_0 A$. Pour $n \in \mathbf{N}$, supposons l'idéal I_n construit. Si $I_n = I$, on pose $I_{n+1} = I$; sinon, il existe $a_{n+1} \in I \setminus I_n$; on pose alors $I_{n+1} = I_n + a_{n+1}A$; notons que dans ce dernier cas, I_{n+1} contient strictement I_n. Il est immédiat que (I_n) est croissante, et on montre par une récurrence facile que pour tout $n \geqslant 0$, I_n est engendré par un nombre fini d'éléments, donc est principal d'après un résultat montré ci-dessus. Toujours d'après un

résultat montré ci-dessus, la suite (I_n) est stationnaire, en particulier il existe $n_0 \in \mathbf{N}$ tel que $I_{n_0} = I_{n_0+1}$. D'après la construction de (I_n) on a alors $I = I_{n_0}$, donc I est principal.