6.4 Valuations dans un anneau factoriel

Si p est un nombre premier, on a rencontré en TD (*cf.* notamment l'exercice 6 de la feuille de TD n°2) la notion de valuation p-adique. Entre autres propriétés extrêmement utiles, cette notion vérifie par exemple que pour toute paire d'entiers, la valuation p-adique de leur produit est égale à la somme des valuations p-adiques de chacun d'entre eux. On a également vu une notion similaire de valuation sur les anneaux de séries formelles, avec des propriétés strictement analogues si l'anneau des coefficients est un anneau intègre.

On peut se demander dans quelle mesure cette notion existe pour d'autres anneaux intègres. Considérons par exemple le cas de $A = \mathbf{Z}[i\sqrt{3}]$ (*cf.* l'exercice 5 du TD n°2 pour la définition et les propriétés utiles). Comme 2 est un élément irréductible de A, on peut imaginer définir ainsi la notion de valuation 2-adique sur A : $v_2(0) = +\infty$ et pour $a \in A \setminus \{0\}$, $v_2(a)$ est le plus grand entier positif n tel que 2^n divise a. Notons que pour tout $a \in A \setminus \{0\}$ et $n \in \mathbf{N}$ tels que 2^n divise a, alors $4^n = N(2^n)$ divise $N(a)$ dans $\mathbf{Z}$, ce qui montre que $v_2(a)$ est bien définie. Cependant, 2 ne divise pas $1 + i\sqrt{3}$, en d'autres termes $v_2(1 + i\sqrt{3}) = 0$. Supposons en effet qu'il existe $b \in \mathbf{Z}[i\sqrt{3}]$ tel que $2b = 1 + i\sqrt{3}$. En prenant la norme, on en déduit aussitôt $N(b) = 1$, soit $b \in \{1, -1\}$, ce qui est contradictoire car $1 + i\sqrt{3} \notin \mathbf{Z}$. De même on voit que $v_2(1 + i\sqrt{3}) = 0$. Ainsi

$$v_2(1 + i\sqrt{3}) + v_2(1 - i\sqrt{3}) = 0$$

tandis que

$$v_2((1 + i\sqrt{3})(1 - i\sqrt{3})) = v_2(2^2) = 2$$

On perd donc la propriété évoquée ci-dessus sur $\mathbf{Z}$, ce qui limite considérablement l'intérêt de la valuation 2-adique sur $\mathbf{Z}[i\sqrt{3}]$.

Rappelons par ailleurs que $\mathbf{Z}[i\sqrt{3}]$ n'est pas factoriel. Dans ce qui suit, on va voir que la notion de valuation p-adique sur $\mathbf{Z}$ s'étend avec les propriétés voulues aux anneaux factoriels.

Soit A un anneau intègre. La relation « est associé à » est notée $\sim$ et est une relation d'équivalence sur A. Notons que pour tous éléments a, b de l'ensemble $A/\sim$, d'après la remarque qui suit la définition 63 du chapitre 2, on peut donner un sens à la condition « a divise b »

La relation $\sim$ induit une relation d'équivalence sur l'ensemble des éléments irréductibles de A. Soit $\mathscr{I}(A)$ l'ensemble quotient de l'ensemble des éléments irréductibles de A par cette relation d'équivalence. Dans la pratique, il est utile de travailler avec un système de représentants $\mathrm{Irr}(A) \subset A$ de $\mathscr{I}(A)$, que l'on pourra parfois (notamment pour alléger les notations) identifier à $\mathscr{I}(A)$.

Exemples. Si $A = \mathbf{Z}$, on peut prendre pour $\mathrm{Irr}(A)$ l'ensemble des nombres premiers (qui n'est autre que l'ensemble des éléments irréductibles positifs de $\mathbf{Z}$).

Si $\mathbf{K}$ est un corps et $A = \mathbf{K}[X]$, on peut prendre pour $\mathrm{Irr}(A)$ l'ensemble des polynômes irréductibles unitaire.

Si $\mathbf{K}$ est un corps et $A = \mathbf{K}[[X]]$, on peut prendre pour $\mathrm{Irr}(A)$ le singleton $\{X\}$.

Si p est un nombre premier et $A = \mathbf{Z}_{(p)}$, on peut prendre pour $\mathrm{Irr}(A)$ le singleton $\{p\}$.

Si x est un entier non nul et $A = \mathbf{Z}[\frac{1}{x}]$, on peut prendre pour $\mathrm{Irr}(A)$ l'ensemble des nombres premiers qui ne divisent pas x.

Théorème 13. *Soit A un anneau factoriel. Soit a un élément non nul de A. Alors il existe une unique famille presque nulle $(v_\pi(a)) \in \mathbf{N}^{(\mathscr{I}(A))}$ d'entiers indexée par $\mathscr{I}(A)$ telle que pour tout système $\mathrm{Irr}(A)$ de représentants d'irréductibles de A, on a*

$$a \sim \prod_{\pi \in \mathrm{Irr}(A)} \pi^{v_\pi(a)}.$$

Démonstration. Ce n'est qu'une traduction de la propriété d'unicité de la factorisation en irréductibles (*cf.* pour mémoire la définition 1). Les détails sont laissés à titre d'exercice. On pourra vérifier en particulier : soit $a \in A$ non nul qui s'écrit $\prod_{i=1}^{n} p_i$ où les p_i sont irréductibles, alors nécessairement pour tout $\pi \in \mathscr{I}(A)$ on a

$$v_\pi(a) = \mathrm{card}\{i \in \{1, \ldots, n\}, \quad p_i \in \pi\}.$$

□

Soit A un anneau factoriel et $\pi \in \mathscr{I}(A)$. En posant $v_\pi(0) = +\infty$, le théorème précédent permet de définir une fonction

$$\begin{array}{ccc} A & \longrightarrow & \mathbf{N} \cup \{+\infty\} \\ a & \longmapsto & v_\pi(a) \end{array}$$

appelée « valuation π-adique » et qui vérifie

$$\forall a \in A, \quad v_\pi(a) = +\infty \Leftrightarrow a = 0.$$

Théorème 14. *Soit A un anneau factoriel.*

1. *Soit $a, b \in A$. Alors a et b sont associés si seulement si pour tout $\pi \in \mathscr{I}(A)$, on a $v_\pi(a) = v_\pi(b)$.*
2. *Soit $a \in A$. Alors a est inversible si et seulement si pour tout $\pi \in \mathscr{I}(A)$, on a $v_\pi(a) = 0$.*
3. *Soit $a, b \in A$. Alors pour tout $\pi \in \mathscr{I}(A)$, on a*

$$v_\pi(ab) = v_\pi(a) + v_\pi(b).$$

4. *Soit $a, b \in A$. Alors a divise b si et seulement si pour tout $\pi \in \mathscr{I}(A)$, on a $v_\pi(a) \leqslant v_\pi(b)$.*

5. *Soit $a \in A$ un éléments non nul et $\pi \in \mathscr{I}(A)$. Alors*

$$v_\pi(a) = \mathrm{Max}\{n \in \mathbf{N}, \quad \pi^n \text{ divise } a\}.$$

Démonstration. Les trois premières assertions découlent facilement du théorème 13, et la dernière découle facilement de l'avant-dernière (vérifiez le).

Montrons l'avant-dernière assertion. Soit $a, b \in A$. Si $b = 0$, a divise toujours b et par ailleurs, pour tout $\pi \in \mathscr{I}(A)$, $v_\pi(b) = +\infty \geqslant v_\pi(a)$, donc le résultat est vrai.

Supposons désormais b non nul. Supposons que pour tout $\pi \in \mathscr{I}(A)$, on a $v_\pi(a) \leqslant v_\pi(b)$. Comme b est non nul, pour tout $\pi \in \mathscr{I}(A)$, on a $v_\pi(b) \in \mathbf{N}$ En particulier a est non nul. Rappelons qu'on a alors

$$a \sim \prod_{\pi \in \mathrm{Irr}(A)} \pi^{v_\pi(a)}$$

et

$$b \sim \prod_{\pi \in \mathrm{Irr}(A)} \pi^{v_\pi(b)}.$$

Ainsi

$$b \sim a \prod_{\pi \in \mathrm{Irr}(A)} \pi^{v_\pi(b) - v_\pi(a)}$$

ce qui montre que a divise b.

Supposons à présent que a divise b. Soit $c \in A$ tel que $b = ca$. Comme b est non nul, on a $c \neq 0$. Soit $\pi \in \mathscr{I}(A)$. On a

$$v_\pi(b) = v_\pi(ca) = v_\pi(c) + v_\pi(a).$$

Comme $v_\pi(c) \in \mathbf{N}$, on a bien $v_\pi(b) \geqslant v_\pi(a)$. □

6.5 Plus grand commun diviseur, plus petit commun multiple ; cas des anneaux factoriels, principaux, euclidiens ; relations de Bézout, algorithme d'Euclide étendu

6.5.1 pgcd, ppcm

Définition 15. Soit A un anneau intègre et $a, b \in A$. Un pgcd de la paire $\{a, b\}$ est un élément $\delta \in A$ vérifiant les propriétés suivantes :

1. δ divise a et b ;
2. soit $d \in A$ qui divise a et b ; alors d divise δ.

Un ppcm de la paire $\{a, b\}$ est un élément $\mu \in A$ vérifiant les propriétés suivantes :

1. a et b divisent μ ;
2. soit $m \in A$ qui est divisible par a et b ; alors m est divisible par μ.

Exemple. Si a et b sont des éléments de A premiers entre eux, tout élément de $A^\times$ est un pgcd de a et b.

Si a et b sont des éléments associés de A, tout élément associé à a et b est un pgcd de a et b.

Pour tout élément a de A, tout élément associé à a est un pgcd de a et 0. En particulier, 0 est un pgcd de 0 et 0. Par ailleurs si a et b sont des éléments de A qui admettent 0 pour pgcd, alors 0 divise a et b, et donc $a = b = 0$.

Nous verrons en TD qu'en général, les pgcd et ppcm n'existent pas toujours. Par contre un pgcd ou un ppcm, s'ils existent, sont uniquement déterminés à association près. La démonstration de la proposition qui suit fait aussi l'objet d'un exercice de TD.

Proposition 16. *Soit A un anneau intègre et $a, b \in A$. On suppose que a et b admettent un pgcd δ (respectivement un ppcm μ).*

1. *Soit $c \in A$. Alors c est un pgcd (respectivement un ppcm) de a et b si et seulement si c est associé à δ (respectivement à μ).*
2. *Soit $\alpha \in A$. Alors $\alpha\delta$ (respectivement $\alpha\mu$) est un pgcd (respectivement un ppcm) de $\alpha\, a$ et $\alpha\, b$.*
3. *Soit $\alpha \in A \setminus \{0\}$ un diviseur commun de a et b. Alors $\frac{\delta}{\alpha}$ (respectivement $\frac{\mu}{\alpha}$) est un pgcd (respectivement un ppcm) de $\frac{a}{\alpha}$ et $\frac{b}{\alpha}$.*

   En particulier, si $\delta \neq 0$, (ou ce qui revient au même si $(a, b) \neq (0, 0)$), $\frac{a}{\delta}$ et $\frac{b}{\delta}$ sont premiers entre eux.

Dans un anneau factoriel, les pgcd et ppcm existent toujours.

Théorème 17. *Soit A un anneau factoriel et $a, b \in A$.*

1. *Soit $c \in A$. Alors :*
   (a) *c est un pgcd de a et b si et seulement si pour tout $\pi \in \mathscr{I}(A)$ on a*
   $$v_\pi(c) = \mathrm{Min}(v_\pi(a), v_\pi(b)) \ ;$$
   (b) *c est un ppcm de a et b si et seulement si pour tout $\pi \in \mathscr{I}(A)$ on a*
   $$v_\pi(c) = \mathrm{Max}(v_\pi(a), v_\pi(b)).$$
   En particulier a et b admettent un pgcd et un ppcm.
2. *Supposons en outre A principal. Alors :*
   (a) *c est un pgcd de a et b si et seulement si c engendre $aA + bA$;*
   (b) *c est un ppcm de a et b si et seulement si c engendre $aA \cap bA$.*

Démonstration. La première assertion découle de la quatrième assertion du théorème 14

Pour la seconde assertion, comme A est principal, il suffit de montrer que si c est un générateur de $aA + bA$ (respectivement $aA \cap bA$) alors c est un pgcd (resp. un ppcm) de a et b.

Supposons donc que c engendre $aA + bA$. En particulier cA contient aA et bA, donc c divise a et b. Soit $d \in A$ divisant a et b. Alors dA contient aA et bA, donc dA contient $aA + bA = cA$. Donc d divise c. Ainsi c est un pgcd de a et b.

Le cas d'un ppcm est laissé à titre d'exercice. □

Remarque. Le résultat sur le ppcm dans la seconde assertion vaut même si A est seulement intègre (*cf.* feuille de TD n°5).

6.5.2 Relations de Bézout

Définition 18. Soit A un anneau intègre et $a, b \in A$. Une *relation de Bézout* pour a et b est un couple $(u, v) \in A^2$ tel que $au + bv$ est un pgcd de a et b.

Remarque. En divisant une relation de Bézout $ua+bv = \delta$ par δ, on obtient que $uA+vA = A$. En particulier u et v sont nécessairement premiers entre eux.

Proposition 19. *Soit A un anneau intègre et $a, b \in A$. Alors il existe une relation de Bézout pour a et b si et seulement si l'idéal $aA + bA$ est principal.*

Démonstration. Exercice □

Ainsi, si A est principal, toute paire d'éléments de A admet une relation de Bézout. Dans la pratique, la détermination effective d'une telle relation (qui intervient par exemple lorsque l'on souhaite expliciter l'isomorphisme réciproque du théorème chinois) n'est pas un problème facile. Cependant, dans le cas particulier d'un anneau euclidien, et pour peu que la division euclidienne soit effective, on dispose d'une procédure efficace pour calculer des relations de Bézout.

6.5.3 Algorithme d'Euclide étendu dans un anneau euclidien

On utilisera le lemme élémentaire suivant.

Lemme 20. *Soit A un anneau intègre et α, β des éléments de A. On suppose qu'il existe $q, r \in A$ vérifiant*

$$\alpha = q\beta + r.$$

Alors la paire $\{\alpha, \beta\}$ admet un pgcd si et seulement si la paire $\{\beta, r\}$ admet un pgcd. En outre, dans ce cas, les paires $\{\alpha, \beta\}$ et $\{\beta, r\}$ ont les mêmes pgcd.

Démonstration. La relation de l'énoncé entraîne aussitôt que tout diviseur commun de α et β divise r, et que tout diviseur commun de β et r divise α. Ainsi les paires $\{\alpha, \beta\}$ et $\{\beta, r\}$ ont exactement les mêmes diviseurs communs. La définition d'un pgcd permet de conclure. □

Soit A un anneau euclidien et ν un stathme euclidien sur A. Soit $a, b \in A$. On décrit l'algorithme d'Euclide étendu, qui permet de calculer une relation de Bézout pour a et b (donc en particulier un pgcd de a et b). Il s'agit d'une extension immédiate de l'algorithme d'Euclide étendu sur $\mathbf{Z}$ et $\mathbf{K}[X]$ ($\mathbf{K}$ un corps) que vous avez très probablement déjà rencontrés dans vos études.

Notons que si $b = 0$, a est un pgcd de a et b et $a = 1 \cdot a + 0 \cdot b$ est une relation de Bézout pour a et b. Dans tout ce qui suit, on supposera que b est non nul.

Commençons par décrire l'algorithme d'Euclide « non étendu », qui permet de calculer un pgcd de a et b par divisions euclidiennes successives.

On initialise l'algorithme d'Euclide en posant $r_{-1} = a$ et $r_0 = b$. Ensuite, pour n entier positif, et tant que r_n est non nul, on écrit une division euclidienne de r_{n-1} par r_n :

$$r_{n-1} = q_n r_n + r_{n+1}.$$

En particulier, $r_{n+1} = 0$ ou $\nu(r_{n+1}) < \nu(r_n)$. On définit ainsi une suite $(r_n)_{n \geqslant -1}$ d'éléments de A qui est nécessairement une suite finie, car la suite $(\nu(r_n))_{n \geqslant 0}$, définie tant que r_n n'est pas nul, est une suite strictement décroissant d'entiers positifs. D'après le lemme 20, une récurrence immédiate montre que pour tout n tel que r_{n+1} est défini les paires $\{a, b\}$ et $\{r_n, r_{n+1}\}$ ont les mêmes pgcd. Ainsi si N est le plus grand entier positif n tel que $r_n \neq 0$, les paires $\{a, b\}$ et $\{r_N, r_{N+1}\} = \{r_N, 0\}$ ont les mêmes pgcd. En particulier r_N (le « dernier reste non nul ») est un pgcd de a et b.

Il est possible de calculer une relation de Bézout pour a et b à partir de l'algorithme d'Euclide en « remontant » les divisions euclidiennes. Si cette méthode est assez efficace lorsque le nombre d'étapes dans l'algorithme d'Euclide est petit, elle possède en particulier l'inconvénient pratique de nécessiter de « garder en mémoire » toutes les étapes de l'algorithme. L'algorithme d'Euclide étendu, que l'on présente maintenant, n'a pas ce défaut.

Plutôt que de donner directement les formules de cet algorithme, expliquons l'idée qui permet de les retrouver facilement. Elle consiste à construire récursivement, pour n allant de -1 à N, une combinaison linéaire de a et b (ici et dans ce qui suit, « combinaison linéaire » s'entend à coefficients dans A) égale à r_n. Ainsi pour $n = N$, on obtiendra la relation de Bezout cherchée. Pour $n = -1$ et $n = 0$, de telles combinaisons sont données « gratuitement » par

$$a.1 + b.0 = r_{-1} = a \quad \text{et} \quad a.0 + b.1 = r_0 = b$$

(mais en fait toutes autres combinaisons linéaire de a et b égales à a d'une part et b d'autre part conviendraient pour initialiser l'algorithme) Supposons à présent que pour un

$n \in \{0, \ldots, N-1\}$ on connaisse $(u_{n-1}, v_{n-1}) \in A^2$ et $(u_n, v_n) \in A^2$ tels que

$$a.u_{n-1} + b.v_{n-1} = r_{n-1} \quad \text{et} \quad a.u_n + b.v_n = r_n$$

Toute combinaison linéaire de deux combinaisons linéaires de a et b est encore une combinaison linéaire de a et b. L'idée pour déterminer une combinaison linéaire de a et b égale à r_{n+1} est de partir d'une combinaison linéaire de r_{n-1} et r_n égale à r_{n+1} En effet, si $(\alpha_n, \beta_n) \in A^2$ vérifie $\alpha_n r_{n-1} + \beta_n r_n = r_{n+1}$, en ajoutant α_n fois la première des combinaisons ci-dessus à β_n fois la seconde, on obtiendra une combinaison linéaire de a et b égale à r_{n+1}. Or une combinaison linéaire de r_{n-1} et r_n égale à r_{n+1} intervient naturellement dans l'algorithme d'Euclide : la division euclidienne $r_{n-1} = q_n r_n + r_{n+1}$ se réécrit $1.r_{n-1} + (-q_n).r_n = r_{n+2}$.

On obtient ainsi la description suivante de l'algorithme d'Euclide étendu. On initialise l'algorithme en posant $r_{-1} := a$, $u_{-1} := 1$, $v_{-1} := 0$, $r_0 := b$, $u_0 := 0$, $v_0 := 1$. Ensuite, pour n entier positif, et tant que r_n est non nul, on écrit une division euclidienne de r_{n-1} par r_n :

$$r_{n-1} = q_n r_n + r_{n+1}$$

ce qui définit r_{n+1}. En outre on pose

$$u_{n+1} := u_{n-1} - q_n\, u_n, \quad v_{n+1} := v_{n-1} - q_n\, v_n.$$

Désignant toujours par N est plus grand entier positif n que $r_n \neq 0$, on a alors, pour tout entier n vérifiant $-1 \leqslant n \leqslant N$

$$r_n = u_n r_{-1} + v_n r_0$$

en particulier

$$\mathrm{pgcd}(a, b) = r_N = u_N r_{-1} + v_N r_0.$$

La proposition suivante, dont la démonstration est proposée en exercice de TD, permet d'achever la description de l'algorithme de décodage des codes BCH (section 4.8.5).

Proposition 21. *On reprend les notations ci-dessus (en particulier $b \neq 0$) en supposant en outre que $A = \mathbf{K}[X]$, où $\mathbf{K}$ est un corps. Alors :*

1. *pour tout entier n vérifiant $1 \leqslant n \leqslant N+1$, on a*

$$\deg(r_n) < \deg(r_{n-1}) \ ;$$

2. *pour tout entier n vérifiant $1 \leqslant n \leqslant N$, on a*

$$\deg(r_{n-1}) = \deg(q_n) + \deg(r_n) \ ;$$

3. *On suppose en outre que $\deg(a) \geqslant \deg(b)$; alors pour tout entier n vérifiant $1 \leqslant n \leqslant N$, on a*

$$\deg(v_n) = \deg(r_{-1}) - \deg(r_{n-1}).$$

Soit t un entier strictement positif. Appliquons ce qui précède dans le cas où a est de degré $2t$ et b de degré $2t-1$, en conservant les même notations. Soit m le plus petit entier n compris entre 1 et $N+1$ tel que $\deg(r_n) < t$. En particulier $\deg(r_{m-1}) > t$ et

$$\deg(v_m) = \deg(r_{-1}) - \deg(r_{m-1}) \leqslant 2t - t = t$$

Ainsi, on a

$$v_m b = r_m \pmod{a}$$

avec $\deg(v_m) \leqslant t$ et $\deg(r_m) < t$.

6.5.4 pgcd, ppcm d'une famille finie d'éléments

Les notions de pgcd et de ppcm d'une paire d'éléments s'étendent au cas d'une famille finie d'éléments, avec des énoncés strictement analogues. Les démonstrations sont essentiellement identiques.

Définition 22. Soit A un anneau intègre, I un ensemble fini non vide et $\{a_i\}_{i\in I}$ une famille d'éléments de A indexée par I.

Les éléments de la famille $\{a_i\}_{i\in I}$ sont dits premiers entre eux si les seuls diviseurs communs à tous les a_i sont les inversibles de A.

Un pgcd de la famille $\{a_i\}_{i\in I}$ est un élément $\delta \in A$ vérifiant les propriétés suivantes :

1. pour tout $i \in I$, δ divise a_i ;
2. soit $d \in A$ tel que pour tout $i \in I$, δ divise a_i ; alors d divise δ.

Un ppcm de la famille $\{a_i\}_{i\in I}$ est un élément $\mu \in A$ vérifiant les propriétés suivantes :

1. pour tout $i \in I$, a_i divise μ ;
2. soit $m \in A$ tel que pour tout $i \in I$, a_i divise m ; alors μ divise m.

Proposition 23. *Soit A un anneau intègre, I un ensemble fini non vide et $\{a_i\}_{i\in I}$ une famille d'éléments de A indexée par I. On suppose que la famille $\{a_i\}_{i\in I}$ admet un pgcd δ (respectivement un ppcm μ).*

1. *Soit $c \in A$. Alors c est un pgcd (respectivement un ppcm) de la famille $\{a_i\}_{i\in I}$ si et seulement si c est associé à δ (respectivement à μ).*
2. *Soit $\alpha \in A$. Alors $\alpha\delta$ (respectivement $\alpha\mu$) est un pgcd (respectivement un ppcm) de la famille $\{\alpha a_i\}_{i\in I}$.*
3. *Soit $\alpha \in A \setminus \{0\}$ un diviseur commun à tous les a_i. Alors $\frac{\delta}{\alpha}$ (respectivement $\frac{\mu}{\alpha}$) est un pgcd (respectivement un ppcm) de la famille $\{\frac{a_i}{\alpha}\}_{i\in I}$.*
   En particulier, si $\delta \neq 0$, (ou ce qui revient au même si les a_i ne sont pas tous nuls) les éléments de la famille $\{\frac{a_i}{\delta}\}_{i\in I}$ sont premiers entre eux.
4. *δ est un pgcd de la famille $\{a_i\}_{i\in I} \cup \{0\}$.*

Théorème 24. *Soit A un anneau factoriel, I un ensemble fini non vide et $\{a_i\}_{i\in I}$ une famille d'éléments de A indexée par I.*

1. *Soit $c \in A$. Alors :*
   (a) *c est un pgcd de la famille $\{a_i\}_{i\in I}$ si et seulement si pour tout $\pi \in \mathscr{I}(A)$ on a*
   $$v_\pi(c) = \mathrm{Min}_{i\in I}(v_\pi(a_i)) \ ;$$
   (b) *c est un ppcm de la famille $\{a_i\}_{i\in I}$ seulement si pour tout $\pi \in \mathscr{I}(A)$ on a*
   $$v_\pi(c) = \mathrm{Max}_{i\in I}(v_\pi(a_i)).$$
   En particulier la famille $\{a_i\}_{i\in I}$ admet un pgcd et un ppcm.
2. *Supposons en outre A principal. Alors :*
   (a) *c est un pgcd de la famille $\{a_i\}_{i\in I}$ si et seulement si c engendre l'idéal $\sum_{i\in I} a_i A$;*
   (b) *c est un ppcm de la famille $\{a_i\}_{i\in I}$ si et seulement si c engendre $\cap_{i\in I} a_i A$.*

Remarque. De même que dans le cas du ppcm de deux éléments, la toute dernière assertion du théorème précédent vaut dans un anneau intègre quelconque.

Définition 25. Soit A un anneau intègre, I un ensemble fini non vide et $\{a_i\}_{i\in I}$ une famille d'éléments de A indexée par I. Une *relation de Bézout* pour la famille $\{a_i\}_{i\in I}$ est une famille $\{u_i\}_{i\in I}$ d'éléments de A indexée par I telle que $\sum_{i\in I} a_i u_i$ est un pgcd de la famille $\{a_i\}_{i\in I}$.

Proposition 26. *Soit A un anneau intègre, I un ensemble fini non vide et $\{a_i\}_{i\in I}$ une famille d'éléments de A indexée par I. Alors il existe une relation de Bézout pour la famille $\{a_i\}_{i\in I}$ si et seulement si l'idéal $\sum_{i\in I} a_i A$ est un idéal principal.*

6.6 Valuations, pgcd et ppcm dans le corps des fractions d'un anneau factoriel

Lemme 27. *Soit A un anneau factoriel et $x \in \mathrm{Frac}(A)$. Soit $\pi \in \mathscr{I}(A)$. Soit $(a,b) \in A \times A \setminus \{0\}$ tel que $x = \frac{a}{b}$. Alors l'élément $v_\pi(a) - v_\pi(b) \in \mathbf{N} \cup \{+\infty\}$ ne dépend que de x et pas du choix d'un tel couple (a,b), et coïncide avec $v_\pi(x)$ si $x \in A$.*

Démonstration. Soit $(c,d) \in A \times A \setminus \{0\}$ tel que $x = \frac{c}{d}$. On a donc $\frac{a}{b} = \frac{c}{d}$, d'où $ad = bc$. On en déduit $v_\pi(a) + v_\pi(d) = v_\pi(b) + v_\pi(c)$. Comme $v_\pi(b), v_\pi(d) \in \mathbf{N}$, on obtient bien la relation
$$v_\pi(a) - v_\pi(b) = v_\pi(c) - v_\pi(d).$$
□

Définition 28. Soit A un anneau factoriel et $x \in \mathrm{Frac}(A)$. Soit $\pi \in \mathscr{I}(A)$. Soit $(a,b) \in A \times A \setminus \{0\}$ tel que $x = \frac{a}{b}$. Alors

$$v_\pi(x) := v_\pi(a) - v_\pi(b)$$

est appelé la valuation π-adique de x

Remarque. On obtient ainsi une fonction

$$\begin{array}{ccc} \mathrm{Frac}(A) & \longrightarrow & \mathbf{Z} \cup \{+\infty\} \\ x & \longmapsto & v_\pi(x) \end{array}$$

qui étend la fonction v_π précédemment définie sur A. En outre, soit $x \in \mathrm{Frac}(A)$ et $\pi \in \mathscr{I}(A)$. Alors on a $v_\pi(x) = +\infty$ si et seulement si $x = 0$.

Notons que si A est un anneau intègre la relation d'équivalence « est associé à » s'étend aux élément de $\mathrm{Frac}(A)$: deux éléments x, y de $\mathrm{Frac}(A)$ seront dits A-associés s'il existe un élément $\alpha \in A^\times$ vérifiant $x = \alpha y$. On note $\sim_A$ la relation de A-association. La dénomination « A-associés » (et non simplement « associés ») est là pour éviter les confusions possibles venant du fait qu'il n'y a en général pas unicité de l'anneau intègre A dont le corps des fractions est $\mathrm{Frac}(A)$. Par exemple $\frac{1}{2}$ et $-\frac{1}{2}$ sont $\mathbf{Z}$-associés, tandis que $\frac{1}{2}$ et 2 sont $\mathbf{Q}$-associées mais pas $\mathbf{Z}$-associés.

Théorème 29. *Soit A un anneau factoriel.*

1. *Soit x un élément non nul de $\mathrm{Frac}(A)$. Alors pour tout élément $\pi \in \mathscr{I}(A)$ sauf un nombre fini, $v_\pi(x)$ est nul. Par ailleurs, pour tout système $\mathrm{Irr}(A)$ de représentants d'irréductibles de A, on a*
$$x \sim_A \prod_{\pi \in \mathrm{Irr}(A)} \pi^{v_\pi(x)}.$$
Cette dernière formule s'étend au cas $x = 0$ avec la convention $\pi^{+\infty} = 0$
2. *Soit $x, y \in \mathrm{Frac}(A)$. Alors x et y sont A-associés si et seulement si pour tout $\pi \in \mathscr{I}(A)$, on a*
$$v_\pi(x) = v_\pi(y).$$
3. *Soit $x \in \mathrm{Frac}(A)$. Alors $x \in A$ si et seulement si pour tout $\pi \in \mathscr{I}(A)$, on a $v_\pi(x) \geqslant 0$.*
4. *Soit $x, y \in \mathrm{Frac}(A)$. Alors pour tout $\pi \in \mathscr{I}(A)$, on a*
$$v_\pi(xy) = v_\pi(x) + v_\pi(y).$$

Démonstration. Exercice a priori sans difficulté. On notera bien que pour tous $x, y \in \mathrm{Frac}(A)$ vérifiant $x \sim_A y$, alors $x \in A$ si et seulement si $y \in A$. □

Définition 30. Soit A un anneau factoriel, I un ensemble fini non vide et $\{a_i\}_{i\in I}$ une famille d'éléments non nuls de $\mathrm{Frac}(A)$ indexée par I.

Pour $\pi \in \mathscr{I}(A)$, soit

$$N_\pi := \mathrm{Min}_{i\in I}(v_\pi(a_i))$$

et

$$M_\pi := \mathrm{Max}_{i\in I}(v_\pi(a_i)).$$

On appelle A-pgcd de la famille $\{a_i\}_{i\in I}$ tout élément de $\mathrm{Frac}(A)$ qui est A-associé à $\prod_{\pi\in\mathscr{I}(A)} \pi^{N_\pi}$ (avec la convention $\pi^{+\infty} = 0$).

On appelle A-ppcm de la famille $\{a_i\}_{i\in I}$ tout élément de $\mathrm{Frac}(A)$ qui est A-associé à $\prod_{\pi\in\mathscr{I}(A)} \pi^{M_\pi}$ (avec la même convention que ci-dessus).

Proposition 31. *Soit A un anneau factoriel, I un ensemble fini non vide et $\{a_i\}_{i\in I}$ une famille d'éléments de* $\mathrm{Frac}(A)$ *indexée par I.*

1. *Supposons que pour tout $i \in I$, on a $a_i \in A$. Alors tout A-pgcd (resp. tout A-ppcm) de $\{a_i\}_{i\in I}$ est un pgcd (resp. un A-ppcm) de de $\{a_i\}_{i\in I}$*
2. *Les conditions suivantes sont équivalentes :*
   (a) *pour tout $i \in I$, $a_i \in A$;*
   (b) *tout A-pgcd de la famille $\{a_i\}_{i\in I}$ est dans A ;*
   (c) *un A-pgcd de la famille $\{a_i\}_{i\in I}$ est dans A.*

Démonstration. Exercice a priori sans difficulté. □

On a des énoncés analogues à certains énoncés de la proposition 23.

Proposition 32. *Soit A un anneau factoriel, I un ensemble fini non vide et $\{a_i\}_{i\in I}$ une famille d'éléments de* $\mathrm{Frac}(A)$ *indexée par I. Soit δ un A-pgcd (resp. un A-ppcm) de la famille $\{a_i\}_{i\in I}$.*

1. *Soit $\alpha \in \mathrm{Frac}(A)$. Alors $\alpha\delta$ (respectivement $\alpha\mu$) est un A-pgcd (respectivement un A-ppcm) de la famille $\{\alpha a_i\}_{i\in I}$.*
2. *Soit $\alpha \in \mathrm{Frac}(A) \setminus \{0\}$. Alors $\frac{\delta}{\alpha}$ (respectivement $\frac{\mu}{\alpha}$) est un A-pgcd (respectivement un A-ppcm) de la famille $\{\frac{a_i}{\alpha}\}_{i\in I}$.*
3. *δ est A-un pgcd de la famille $\{a_i\}_{i\in I} \cup \{0\}$.*

Démonstration. Là encore, exercice a priori sans difficulté. □