6.5 Valuations dans un anneau factoriel

On généralise ici la notion de valuation p-adique (p un nombre premier) sur $\mathbf{Z}$.

Soit A un anneau intègre. La relation « est associé à » est une relation d'équivalence sur A, qui 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 16. *Soit A un anneau factoriel.*

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

$$a = \alpha \prod_{\pi \in \mathrm{Irr}(A)} \pi^{\nu_\pi(a)}.$$

2. *Soit a un élément non nul de A. Alors a est inversible si et seulement si pour tout $\pi \in \mathscr{I}(A)$, on a $\nu_\pi(a) = 0$.*
3. *Soit $a, b \in A$ deux éléments non nuls. Alors pour tout $\pi \in \mathscr{I}(A)$, on a*

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

4. *Soit $a, b \in A$ deux éléments non nuls. Alors a divise b si et seulement si pour tout $\pi \in \mathscr{I}(A)$, on a $\nu_\pi(a) \leqslant \nu_\pi(b)$.*
5. *Soit $a \in A$ un éléments non nul et $\pi \in \mathscr{I}(A)$. Alors*

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

6. *Soit $a, b \in A$ deux éléments non nuls. Alors a et b sont associés si seulement si pour tout $\pi \in \mathscr{I}(A)$, on a $\nu_\pi(a) = \nu_\pi(b)$.*

Démonstration. La première assertion n'est qu'une traduction de la propriété d'unicité de la factorisation en irréductibles (*cf.* pour mémoire la définition 3). Les détails sont laissés à titre d'exercice. On pourra vérifier en particulier que si $a \in A$ non nul 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

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

La seconde et la troisième assertion découlent facilement de la première. L'avant-dernière assertion découle facilement de la quatrième, de même que la dernière, en se rappelant que deux éléments d'un anneau intègre sont associés si et seulement s'ils se divisent mutuellement.

Montrons la quatrième assertion. Soit $a, b \in A$ des éléments non nuls. Il existe $\alpha, \beta \in A^\times$ tels que

$$a = \alpha \prod_{\pi \in \mathrm{Irr}(A)} \pi^{\nu_\pi(a)}.$$

et

$$b = \beta \prod_{\pi \in \mathrm{Irr}(A)} \pi^{\nu_\pi(b)}.$$

Si pour tout $\pi \in \mathscr{I}(A)$, on a $\nu_\pi(a) \leqslant \nu_\pi(b)$, alors

$$b = a\beta\alpha^{-1} \prod_{\pi \in \mathrm{Irr}(A)} \pi^{\nu_\pi(b) - \nu_\pi(a)}$$

ce qui montre que a divise b.

Supposons à présent que a divise b. Soit $c \in A$ tel que $b = ca$. Soit $\pi \in \mathscr{I}(A)$. On a

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

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

Remarque. Pour tout $\pi \in \mathscr{I}(A)$ il est pratique d'étendre la fonction $\nu_\pi \colon A \setminus \{0\} \to \mathbf{N}$ en posant $\nu_\pi(0) = +\infty$.

Avec cette définition étendue, on vérifie alors que l'on peut dans l'énoncé du théorème précédent se passer de l'hypothèse que les éléments considérés sont non nuls, avec les conventions naturelles pour la somme et la relation d'ordre dans $\mathbf{N} \cup \{+\infty\}$. Par exemple, tout élément a de A divise 0, et on par ailleurs on a bien, pour tout $\pi \in \mathscr{I}(A)$, $\nu_\pi(a) \leqslant \nu_\pi(0) = +\infty$.

Il faut juste faire un peu attention pour l'énoncé de la première assertion avec $a = 0$ où la convention à prendre est $\pi^{+\infty} = 0$ pour tout $\pi \in \mathscr{I}(A)$ (et il n'y a plus unicité de α dans le cas $a = 0$).

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

6.6.1 pgcd, ppcm

Définition 17. 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.

Proposition 18. *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.

Théorème 19. *Soit A un anneau factoriel et $a, b \in A$.*

1. *a et b admettent un pgcd et un ppcm.*
2. *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

$$\nu_\pi(c) = \mathrm{Min}(\nu_\pi(a), \nu_\pi(b)) \ ;$$

(b) c est un ppcm de a et b si et seulement si pour tout $\pi \in \mathscr{I}(A)$ on a

$$\nu_\pi(c) = \mathrm{Max}(\nu_\pi(a), \nu_\pi(b)).$$

3. 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. Les deux premières assertions découlent de la quatrième assertion du théorème 16 (compte tenu de la remarque qui suit la démonstration de ce théorème).

Pour la troisième 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 troisième assertion vaut même si A est seulement intègre (*cf.* feuille de TD n°5).

6.6.2 Relations de Bézout

Définition 20. 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 21. *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.*

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.

6.6.3 Algorithme d'Euclide étendu dans un anneau euclidien

On utilisera le lemme élémentaire suivant.

Lemme 22. *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 22, 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, présenté ci-dessous, n'a pas ce défaut.

Plutôt que de donner directement les formules décrivant l'algorithme d'Euclide étendu, il est intéressant de reformuler l'algorithme d'Euclide sous forme matricielle, de laquelle l'algorithme étendu découlera assez naturellement.

Pour tout élément $\alpha \in A$, on note $M(\alpha)$ la matrice $\begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix}$. Pour tout couple (β, γ) d'éléments de A, on a alors

$$(\beta, \gamma) \cdot M(\alpha) = (\gamma, \beta + \alpha\gamma)$$

Ainsi, en reprenant les notations ci-dessus, et en posant, pour tout entier n vérifiant $-1 \leqslant n \leqslant N$, $R_n = (r_n, r_{n+1})$, on a pour tout n vérifiant $-1 \leqslant n \leqslant N-1$ la relation

$$R_{n+1} = R_n \cdot M(-q_{n+1}).$$

Pour tout $0 \leqslant n \leqslant N$, posons $M_n := M(-q_0)M(-q_1)\dots M(-q_n)$ et soit U_n le premier vecteur colonne de M_n. On a alors

$$R_n = R_{-1} \cdot M_n$$

soit en particulier $r_n = R_{-1} \cdot U_n$. Pour $n = N$ on obtient bien, à partir des coefficients de U_n, une relation de Bézout pour a et b (rappelons que $R_{-1} = (a, b)$).

Au vu de la relation de récurrence $M_n := M_{n-1}M(-q_n)$ il est facile d'expliciter une relation de récurrence pour calculer les U_n. On pose $U_{-1} =: \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $U_0 =: \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Pour tout $0 \leqslant n \leqslant N$, on a alors $M_n = (U_n, U_{n+1})$ avec $U_{n+1} = U_{n-1} - q_n U_n$.

En écrivant, pour tout entier n vérifiant $-1 \leqslant n \leqslant N$, $U_n =: \begin{pmatrix} u_n \\ v_n \end{pmatrix}$, on obtient finalement la description suivante de l'algorihtme d'Euclide étendu.

On initialise l'algorithme d'Euclide étendu 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 23. *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 $\deg(r_m) < t$.

6.6.4 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, et dont les démonstrations sont essentiellement identiques.

Définition 24. 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 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. 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 26. *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. *La famille $\{a_i\}_{i\in I}$ admet un pgcd et un ppcm.*
2. *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*
   $$\nu_\pi(c) = \mathrm{Min}_{i\in I}(\nu_\pi(a_i)) \ ;$$
   (b) *c est un ppcm de la famille $\{a_i\}_{i\in I}$ seulement si pour tout $\pi \in \mathscr{I}(A)$ on a*
   $$\nu_\pi(c) = \mathrm{Max}_{i\in I}(\nu_\pi(a_i)).$$
3. *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 dernière assertion du théorème précédent vaut dans un anneau intègre quelconque.

Définition 27. 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 28. *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.*

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

Lemme 29. *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'entier $\nu_\pi(a) - \nu_\pi(b)$ ne dépend que de x et pas du choix d'un tel couple (a,b).*

Définition 30. 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

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

est appelé la valuation π-adique de x

Remarque. Soit $x \in \mathrm{Frac}(A)$ et $\pi \in \mathscr{I}(A)$. Alors $\nu_\pi(x) \in \mathbf{N} \cup \{+\infty\}$, et on a $\nu_\pi(x) = +\infty$ si et seulement si $x = 0$.

Notons que si A est un anneau intègre la relation d'équivalence « est associé à » s'étend aussitôt 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 $x = \alpha y$. La dénomination « A-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 $\mathrm{Frac}(A)$.

Théorème 31. *Soit A un anneau factoriel.*

1. *Soit x un élément non nul de $\mathrm{Frac}(A)$. Alors $\nu_\pi(x)$ est nul pour tout élément $\pi \in \mathscr{I}(A)$ sauf un nombre fini. Par ailleurs, pour tout système $\mathrm{Irr}(A)$ de représentants d'irréductibles de A, il existe un unique $\alpha \in A^\times$ vérifiant*

$$x = \alpha \prod_{\pi \in \mathrm{Irr}(A)} \pi^{\nu_\pi(x)}.$$

   Cette dernière formule s'étend au cas $x = 0$ avec la convention $\pi^{+\infty} = 0$ (sans unicité de α).

2. *Soit $x \in \mathrm{Frac}(A)$. Alors $x \in A$ si et seulement si pour tout $\pi \in \mathscr{I}(A)$, on a $\nu_\pi(x) \geqslant 0$.*

3. *Soit $x, y \in \mathrm{Frac}(A)$. Alors pour tout $\pi \in \mathscr{I}(A)$, on a*

$$\nu_\pi(xy) = \nu_\pi(x) + \nu_\pi(y).$$

4. *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*

$$\nu_\pi(x) = \nu_\pi(y).$$

Définition 32. 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

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

et

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

On appelle A-pgcd de la famille $\{a_i\}_{i\in I}$ tout élément de $\mathrm{Frac}(A)$ qui est A-associé à 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 33. *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. Les conditions suivantes sont équivalentes :*

1. *pour tout $i \in I$, $a_i \in A$;*
2. *tout pgcd de la famille $\{a_i\}_{i\in I}$ est dans A ;*
3. *un pgcd de la famille $\{a_i\}_{i\in I}$ est dans A.*