Agrégation Externe

Anneaux principaux

On pourra consulter les ouvrages suivants.

P. Boyer, J. J. Risler : *Algèbre pour la licence 3. Groupes, anneaux, corps.* Dunod (2006).

F. Combes — *Algèbre et géométrie.* Bréal (2003).

S. Francinou, H. Gianella, S. Nicolas : *Exercices de mathématiques. Oraux X-ENS. Algèbre 1.* Cassini (2001).

S. Francinou, H. Gianella. *Exercices de mathématiques pour l'agrégation. Algèbre 1.* Masson (1994).

D. Perrin. *Cours d'algèbre.* Ellipses (1996).

A. Szpirglas. *Mathématiques L3. Algèbre.* Pearson (2009).

Pour ce problème, $\mathbb{A}$ désigne un anneau commutatif, unitaire, a priori intègre et on note :
- 0 et 1 les éléments neutres pour l'addition et la multiplication de $\mathbb{A}$, avec $0 \neq 1$;
- $\mathbb{A}^* = \mathbb{A} \setminus \{0\}$ l'ensemble des éléments non nuls de $\mathbb{A}$;
- $\mathbb{A}^\times$ le groupe multiplicatif des éléments inversibles (ou des unités) de $\mathbb{A}$.
- Deux éléments a, b de $\mathbb{A}$ sont dits associés s'il existe un élément inversible $u \in \mathbb{A}^\times$ tel que $b = ua$.
- Un élément p de $\mathbb{A}$ est dit irréductible si $p \neq 0$, p n'est pas inversible et :

$$(p = ab) \Rightarrow (a \text{ ou } b \text{ est inversible})$$

  (les seuls diviseurs de p sont les éléments inversibles ou les éléments de $\mathbb{A}$ associés à p).
- Un élément p de $\mathbb{A}$ est dit premier si $p \neq 0$, p n'est pas inversible et :

$$(p \text{ divise } ab) \Rightarrow (p \text{ divise } a \text{ ou } p \text{ divise } b)$$

Un élément premier dans $\mathbb{A}$ est irréductible, la réciproque n'étant pas acquise en général.
Pour les définitions qui suivent, l'anneau $\mathbb{A}$ n'est pas nécessairement intègre.
- Un idéal de $\mathbb{A}$ est un sous-ensemble I de $\mathbb{A}$ tel que :

$$\left\{ \begin{array}{l} I \text{ est un sous-groupe de } (\mathbb{A}, +) \\ \forall (a, b) \in I \times \mathbb{A},\ ab \in I \end{array} \right.$$

  (la deuxième condition se traduit en disant que I est absorbant pour le produit).
- Un idéal I de $\mathbb{A}$ est dit premier s'il est distinct de $\mathbb{A}$ et si $ab \in I$ si, et seulement si, $a \in I$ ou $b \in I$, ce qui équivaut à dire que l'anneau quotient $\dfrac{\mathbb{A}}{I}$ est intègre.
- Un idéal I de $\mathbb{A}$ est dit maximal s'il est distinct de $\mathbb{A}$ et si I et $\mathbb{A}$ sont les seuls idéaux de $\mathbb{A}$ qui contiennent I, ce qui équivaut à dire que l'anneau quotient $\dfrac{\mathbb{A}}{I}$ est un corps.

Un idéal maximal est premier, la réciproque n'étant pas acquise en général.

– I – Exemples d'anneaux principaux

On dit que l'anneau $\mathbb{A}$ est principal, s'il est intègre et si tout idéal de $\mathbb{A}$ est principal.
Les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$, pour $\mathbb{K}$ corps commutatif, sont connus pour être euclidiens et principaux.

1. Un corps est-il un anneau principal ?
2. Montrer que si l'anneau $\mathbb{A}$ (a priori non intègre) est isomorphe à un anneau $\mathbb{B}$ principal il est alors principal.
   Ce résultat peut être commode pour montrer qu'un anneau est principal.
3. Soit $\mathbb{K}$ un corps commutatif.
   On se propose de montrer que l'anneau quotient $\dfrac{\mathbb{K}[X, Y]}{(Y - X^2)}$ est principal.
   (a) Montrer que l'application :

$$\begin{array}{rccc} \varphi : & \mathbb{K}[X, Y] & \to & \mathbb{K}[X] \\ & P(X, Y) & \mapsto & P(X, X^2) \end{array}$$

   est un morphisme d'anneaux surjectif et préciser son noyau.
   (b) Montrer que l'anneau quotient $\dfrac{\mathbb{K}[X, Y]}{(Y - X^2)}$ est principal.
4.
   (a) Montrer que tout sous-anneau $\mathbb{A}$ de $\mathbb{Q}$ est principal.

(b) Montrer que l'anneau $\mathbb{D}=\left\{\dfrac{a}{10^m} \mid (a,m)\in\mathbb{Z}\times\mathbb{N}\right\}$ des nombres décimaux est principal.

5. On désigne par $\mathbb{K}$ le corps des fraction de l'anneau intègre $\mathbb{A}$.
On se donne une partie S de $\mathbb{A}^*$ qui contient 1 et qui est stable pour le produit.

   (a) Montrer que l'ensemble :
$$S^{-1}\mathbb{A}=\left\{\frac{a}{s} \mid a\in\mathbb{A} \text{ et } s\in S\right\}$$
   est un sous-anneau du corps $\mathbb{K}$ qui contient $\mathbb{A}$.

   (b) Montrer que si $\mathbb{A}$ est principal, il en est alors de même de $S^{-1}\mathbb{A}$.

   (c) Montrer que l'anneau $\mathbb{D}$ des nombres décimaux est principal.

   (d) Soit $\mathbb{K}$ un corps commutatif.
   Montrer que l'anneau $\mathbb{D}=\left\{\dfrac{P(X)}{X^n} \mid P\in\mathbb{K}[X] \text{ et } n\in\mathbb{N}\right\}$ est principal.

6. Soit $\mathbb{K}$ un corps commutatif.
On se propose de montrer que l'anneau quotient $\dfrac{\mathbb{K}[X,Y]}{(XY-1)}$ est principal.

   (a) Montrer que l'application :
$$\begin{array}{rccc} \varphi: & \mathbb{K}[X,Y] & \to & \mathbb{K}(X) \\ & P(X,Y) & \mapsto & P\left(X,\dfrac{1}{X}\right) \end{array}$$
   est un morphisme d'anneaux, puis préciser son noyau et son image.

   (b) Montrer que $\dfrac{\mathbb{K}[X,Y]}{(XY-1)}$ est principal.

7. Soit $\mathbb{K}$ un corps commutatif.
Montrer que les idéaux non réduit à $\{0\}$ de $\mathbb{K}[[X]]$ sont principaux de la forme (X^n). Donc $\mathbb{K}[[X]]$ est principal.

8. Soit $\mathbb{A}$ un anneau principal.

   (a) Montrer qu'un élément $p\in\mathbb{A}^*\setminus\mathbb{A}^\times$ est irréductible si, et seulement si, il est premier.

   (b) Montrer que, pour tout $p\in\mathbb{A}^*\setminus\mathbb{A}^\times$, on a :
$$((p) \text{ premier}) \Leftrightarrow (p \text{ premier}) \Leftrightarrow (p \text{ irréductible}) \Leftrightarrow ((p) \text{ maximal})$$

9. Soit $\mathbb{A}$ un anneau commutatif, unitaire et intègre. Montrer que :
$$(\mathbb{A}[X] \text{ est principal}) \Leftrightarrow (\mathbb{A} \text{ est un corps})$$

10. On se donne un entier naturel $n\geq 1$ et on note :
$$\mathbb{Z}\left[i\sqrt{n}\right]=\mathbb{Z}+i\sqrt{n}\mathbb{Z}=\left\{a+ib\sqrt{n} \mid (a,b)\in\mathbb{Z}^2\right\}$$
Pour $n=1$, il s'agit de l'ensemble $\mathbb{Z}[i]$ des entiers de Gauss.

   (a) Montrer que $\mathbb{Z}[i\sqrt{n}]$ est un sous-anneau de $\mathbb{C}$ stable par l'opération de conjugaison complexe.

   (b) Déterminer l'ensemble $\mathbb{Z}[i\sqrt{n}]^\times$ des éléments inversibles de $\mathbb{Z}[i\sqrt{n}]$.

   (c) Quels sont les entiers naturels $p\geq 2$ qui sont premiers dans $\mathbb{N}$ et réductibles dans $\mathbb{Z}[i\sqrt{n}]$?

(d) Montrer que, pour $n \geq 3$, 2 est irréductible non premier dans $\mathbb{Z}\left[i\sqrt{n}\right]$. Donc les anneaux $\mathbb{Z}\left[i\sqrt{n}\right]$ ne sont pas principaux pour $n \geq 3$.

11. Soient $\mathbb{A}$ un anneau principal et $I = (a)$ un idéal non trivial de $\mathbb{A}$ (i. e. $I \neq \{0\}$ et $I \neq \mathbb{A}$). Montrer que tous les idéaux de $\dfrac{\mathbb{A}}{I}$ sont principaux de la forme $\left(\overline{b}\right)$ où $b \in \mathbb{A}$ est un diviseur de a et l'anneau $\dfrac{\mathbb{A}}{(a)}$ est principal si, et seulement si, a est premier ou encore irréductible.

– II – Anneaux euclidiens

On appelle stathme sur un anneau $\mathbb{A}$ commutatif et intègre une application $\varphi : \mathbb{A}^* \to \mathbb{N}$.

On dit qu'un anneau commutatif et intègre $\mathbb{A}$ est euclidien, s'il existe un stathme φ tel que pour tout couple (a, b) d'éléments de $\mathbb{A}$ avec $b \neq 0$, il existe un couple (q, r) dans $\mathbb{A}^2$ tel que $a = bq + r$ avec $r = 0$ ou $r \neq 0$ et $\varphi(r) < \varphi(b)$.

On dit que q est un quotient et r un reste dans la division euclidienne de a par b.

On notera $(\mathbb{A}, \varphi)$ un tel anneau euclidien ou tout simplement $\mathbb{A}$, quand le stathme est fixé.

1. Montrer qu'un anneau euclidien $(\mathbb{A}, \varphi)$ est principal. Précisément, pour tout idéal I de $\mathbb{A}$ non réduit à $\{0\}$, il existe un élément a_0 dans $I \setminus \{0\}$ tel que $\varphi(a_0) = \min\limits_{a \in I \setminus \{0_{\mathbb{A}}\}} \varphi(a)$ et $I = (a_0)$.
2. Montrer que l'anneau $\mathbb{D}$ des nombres décimaux est euclidien pour le stathme φ défini, en utilisant l'écriture canonique d'un nombre décimal, par :
$$\forall a = n2^p5^q \in \mathbb{D}^*,\ \varphi(a) = |n|$$
3. Montrer que l'anneau $\mathbb{Z}\left[i\sqrt{n}\right]$ est euclidien uniquement pour $n = 1$ ou $n = 2$.
4. Effectuer la division euclidienne de $u = 11 + 7i$ par $v = 18 - i$ dans $\mathbb{Z}[i]$.
5. L'anneau des entiers de Gauss peut être utilisé pour caractériser les entiers naturels qui sont sommes de deux carrés d'entiers.
On note Σ_2 l'ensemble des entiers naturels qui s'écrivent comme somme de deux carrés, soit :
$$\Sigma_2 = \left\{n \in \mathbb{N} \mid \exists (a, b) \in \mathbb{Z}^2 \ ;\ n = a^2 + b^2\right\}$$
   (a) Montrer que Σ_2 est stable pour le produit.
   (b) Montrer qu'un nombre premier $p \geq 2$ est réductible dans $\mathbb{Z}[i]$ si, et seulement si, il est somme de deux carrés.
   (c) Soit $p \geq 2$ un nombre premier. Montrer que s'il existe un entier naturel q premier avec p tel que $pq \in \Sigma_2$, alors p est dans Σ_2.
   (d) Pour tout nombre premier impair p, on note :
$$C_p = \left\{x^2 \mid x \in \mathbb{F}_p^*\right\}$$
   l'ensemble des carrés de $\mathbb{F}_p^*$ et :
$$\Sigma_p = \left\{x \in \mathbb{F}_p^* \mid x^{\frac{p-1}{2}} - \overline{1}\right\}$$
   l'ensemble des racines du polynôme $X^{\frac{p-1}{2}} - \overline{1} \in \mathbb{F}_p[X]$.
      i. Montrer qu'il y a exactement $\dfrac{p-1}{2}$ carrés dans $\mathbb{Z}_p^*$ et $C_p = \Sigma_p$.
      ii. Montrer que $-\overline{1}$ est un carré dans $\mathbb{Z}_p$ si, et seulement si, p est congru à 1 modulo 4.

iii. Montrer qu'un nombre premier p est somme de deux carrés si, et seulement si, il est égal à 2 ou congru à 1 modulo 4.

(e) Montrer que si $n \in \Sigma_2 \setminus \{0\}$ admet un diviseur premier p congru à 3 modulo 4, alors p^2 divise n et $\dfrac{n}{p^2} \in \Sigma_2$.

(f) Montrer qu'un entier naturel non nul n est somme de deux carrés si, et seulement si, les éventuels diviseurs premiers de n congrus à 3 modulo 4 qui apparaissent dans sa décomposition en facteurs premiers y figurent avec un exposant pair (théorème de Fermat).

– III – Les anneaux $\mathbb{Z}[\omega]$, où ω est un entier quadratique

On se donne un nombre complexe $\omega = x + iy$ non réel (i. e. avec $x \in \mathbb{R}$ et $y \in \mathbb{R}^*$) et on note :

$$\mathbb{Z}[\omega] = \mathbb{Z} + \mathbb{Z}\omega = \left\{a + b\omega \mid (a, b) \in \mathbb{Z}^2\right\}$$

On dit qu'un nombre complexe ω est un entier quadratique, s'il est racine d'un polynôme de degré 2 à coefficients entiers.

1. Montrer que $\mathbb{Z}[\omega]$ est un anneau si, et seulement si, ω est un entier quadratique et dans ce cas :
   (a) $\mathbb{Z}[\omega]$ est stable par l'opération de conjugaison complexe $z \mapsto \overline{z}$;
   (b) $\mathbb{Z}[\omega] = \mathbb{Z}[\overline{\omega}]$;
   (c) pour tout entier relatif n, on a $\mathbb{Z}[\omega] = \mathbb{Z}[n + \omega]$;
   (d) il existe un nombre complexe $\omega' = x' + iy'$ tel que $x' \in [0, 1[$, $y' > 0$ et $\mathbb{Z}[\omega] = \mathbb{Z}[\omega']$;
   (e) l'application $\varphi : u \mapsto |u|^2$ définit un stathme sur $\mathbb{Z}[\omega]$.
2. Pour la suite, on suppose que $\omega = x + iy$ est un entier quadratique avec $x \in [0, 1[$, $y > 0$.
   Montrer que les seules valeurs possibles de ω sont :
   $$\omega = i\sqrt{n} \text{ ou } \omega = \frac{1 + i\sqrt{4n - 1}}{2} \text{ avec } n \in \mathbb{N}^*$$
3. Montrer que, pour $n \in \mathbb{N}^*$, $\mathbb{Z}[i\sqrt{n}]$ est isomorphe à l'anneau quotient $\dfrac{\mathbb{Z}[X]}{(X^2 + n)}$ et $\mathbb{Z}\left[\dfrac{1 + i\sqrt{4n - 1}}{2}\right]$ est isomorphe à l'anneau quotient $\dfrac{\mathbb{Z}[X]}{(X^2 - X + n)}$.
4. Montrer que pour tout nombre complexe z, il existe $q \in \mathbb{Z}[\omega]$ tel que :
   $$|z - q|^2 \leq \frac{1 + y^2}{4}$$
   ($y = \Im(\omega)$).
5. Montrer que si $\omega = x + iy$ est un entier quadratique avec $x \in [0, 1[$ et $y \in \left]0, \sqrt{3}\right[$, l'anneau $\mathbb{Z}[\omega]$ est alors euclidien pour le stathme :
   $$\varphi : u = a + b\omega \in \mathbb{Z}[\omega] \mapsto |u|^2$$
   On a donc montré que $\mathbb{Z}[\omega]$ est euclidien pour :
   $$\omega \in \left\{i, \sqrt{2}i, \frac{1 + i\sqrt{3}}{2}, \frac{1 + i\sqrt{7}}{2}, \frac{1 + i\sqrt{11}}{2}\right\}$$
   et qu'il n'est pas principal, donc non euclidien pour $\omega = i\sqrt{n}$ avec $n \geq 3$.
   On peut montrer que $\mathbb{Z}[\omega]$ n'est pas euclidien pour $\omega = \dfrac{1 + i\sqrt{4n - 1}}{2}$ avec $n \geq 4$ (mais pour certaines valeurs de n, il peut être principal non euclidien, c'est le cas pour $n = 5$, soit pour $\omega = \dfrac{1 + i\sqrt{19}}{2}$).

6. Montrer que l'ensemble des éléments inversibles de $\mathbb{Z}[\omega]$ est :

$$\mathbb{Z}[\omega]^{\times} = \left\{u \in \mathbb{Z}[\omega] \mid |u|^2 = 1\right\}$$

soit :

$$\mathbb{Z}[i]^{\times} = \{-1, 1, -i, i\}$$

$$\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]^{\times} = \left\{-1, 1, \frac{1+i\sqrt{3}}{2}, -\frac{1+i\sqrt{3}}{2}, \frac{1-i\sqrt{3}}{2}, -\frac{1-i\sqrt{3}}{2}\right\}$$

et :

$$\mathbb{Z}[\omega]^{\times} = \{-1, 1\}$$

pour $\omega = i\sqrt{n}$ ou $\omega = \dfrac{1+i\sqrt{4n-1}}{2}$ avec $n \geq 2$.

7. Montrer que l'anneau $\mathbb{Z}\left[\dfrac{1+i\sqrt{19}}{2}\right]$ n'est pas euclidien.

8. Le résultat qui suit nous donne une pseudo division euclidienne dans $\mathbb{Z}\left[\dfrac{1+i\sqrt{19}}{2}\right]$.

   (a) Montrer que pour tout $z \in \mathbb{C}$, il existe $u \in \mathbb{Z}\left[\dfrac{1+i\sqrt{19}}{2}\right]$ tel que :

   $$|z-u| < 1 \text{ ou } |2z-u| < 1$$

   (b) Montrer que, pour u, v dans $\mathbb{Z}\left[\dfrac{1+i\sqrt{19}}{2}\right]$ avec $v \neq 0$, il existe q, r dans $\mathbb{Z}\left[\dfrac{1+i\sqrt{19}}{2}\right]$ tels que :

   $$\left\{\begin{array}{l} u = qv + r \\ |r|^2 < |v|^2 \end{array}\right. \text{ ou } \left\{\begin{array}{l} 2u = qv + r \\ |r|^2 < |v|^2 \end{array}\right.$$

   (c) Montrer que si 2 ne divise pas $u \in \mathbb{Z}\left[\dfrac{1+i\sqrt{19}}{2}\right]$, il existe alors deux éléments u_1 et u_2 de $\mathbb{Z}\left[\dfrac{1+i\sqrt{19}}{2}\right]$ tels que :

   $$2u_1 + u \cdot u_2 = 1$$

   (relation de Bézout).

9. Montrer que l'anneau $\mathbb{Z}\left[\dfrac{1+i\sqrt{19}}{2}\right]$ est principal et non euclidien.

10. Montrer que l'anneau $\mathbb{K}[[X]]$ est euclidien pour le stathme :

$$\varphi : S \in \mathbb{K}[[X]] \setminus \{0\} \mapsto \varphi(S) = \mathrm{val}(S)$$

11. Montrer que si l'anneau $\mathbb{A}$ est isomorphe à un anneau $\mathbb{B}$ principal [resp. euclidien], il est alors principal [resp. euclidien].

12. Montrer que l'anneau quotient $\dfrac{\mathbb{C}[X,Y]}{(Y-X^2)}$ est euclidien (donc aussi principal et factoriel).

13. On désigne par $\mathbb{K}$ le corps des fraction de l'anneau intègre $\mathbb{A}$.
On se donne une partie S de $\mathbb{A}^*$ qui contient 1 et qui est stable pour le produit, c'est-à-dire que pour tout (a, b) dans S^2, le produit ab est dans S.

(a) Montrer que l'ensemble :

$$S^{-1}\mathbb{A} = \left\{ \frac{a}{s} \mid a \in \mathbb{A} \text{ et } s \in S \right\}$$

est un sous-anneau du corps $\mathbb{K}$ qui contient $\mathbb{A}$.

(b) Montrer que si $\mathbb{A}$ est principal, il en est alors de même de $S^{-1}\mathbb{A}$.

(c) Montrer que si $\mathbb{A}$ est euclidien, il en est alors de même de $S^{-1}\mathbb{A}$.

14.

(a) Montrer que l'ensemble :

$$\mathbb{A} = \left\{ \frac{P(X)}{X^n} \mid P \in \mathbb{C}[X] \text{ et } n \in \mathbb{N} \right\}$$

est un anneau euclidien.

(b) Montrer que l'anneau quotient $\dfrac{\mathbb{C}[X,Y]}{(XY-1)}$ est euclidien.

– IV –Anneaux factoriels

On dit que l'anneau $\mathbb{A}$ est factoriel s'il est intègre et si tout élément a non nul et non inversible s'écrit de manière unique (à permutation et association près) comme produit d'éléments irréductibles.

1. Montrer que l'anneau $\mathbb{A}$ est factoriel si, et seulement si, il est intègre et :
   (a) toute suite croissante d'idéaux principaux de $\mathbb{A}$ est stationnaire (un anneau factoriel est noethérien) ;
   (b) tout élément irréductible de $\mathbb{A}$ est premier.
2. Montrer que dans un anneau factoriel, un élément est irréductible si, et seulement si, il est premier.
3. Montrer que les anneaux $\mathbb{Z}[i\sqrt{n}]$ ne sont pas factoriels pour $n \geq 3$.
4. Montrer qu'un anneau principal est factoriel.

– V –Anneaux à pgcd

L'anneau $\mathbb{A}$ est supposé intègre.

Soient $r \in \mathbb{N} \setminus \{0,1\}$ et $a_1, \cdots, a_r$ dans $\mathbb{A}^*$. On dit que ces éléments admettent un plus grand commun diviseur s'il existe $\delta \in \mathbb{A}^*$ tel que :

$$\begin{cases} \forall k \in \{1, \cdots, r\}, \ \delta \text{ divise } a_k \\ \text{tout diviseur commun à } a_1, \cdots, a_r \text{ divise } \delta \end{cases}$$

En cas d'existence, on note $\operatorname{pgcd}(a_1, \cdots, a_r)$ ou $a_1 \wedge \cdots \wedge a_r$ un plus grand commun diviseur de $a_1, \cdots, a_r$.

Dans le cas où $\operatorname{pgcd}(a_1, \cdots, a_r)$ est inversible, on dit que $a_1, \cdots, a_r$ sont premiers entre eux.

On dit que l'anneau commutatif, unitaire et intègre $\mathbb{A}$ est un anneau à pgcd si deux éléments quelconques a, b de $\mathbb{A}^*$ admettent un pgcd.

1. Montrer qu'un anneau principal $\mathbb{A}$ est un anneau à pgcd. Précisément, pour toute famille $\{a_1, \cdots, a_r\}$ de $r \geq 2$ éléments de $\mathbb{A}^*$, il existe un élément δ de $\mathbb{A}^*$ tel que :

$$(a_1, \cdots, a_r) = (\delta)$$

cet élément s'écrit :

$$\delta = \sum_{k=1}^{r} u_k a_k \tag{1}$$

où $u_1, \cdots, u_r$ sont des éléments de $\mathbb{A}$ et δ est un pgcd de $a_1, \cdots, a_r$.

2. Soient $\mathbb{A}$ un anneau factoriel et a, b deux éléments non nuls et non inversibles de $\mathbb{A}$. En notant :

$$a = u \prod_{k=1}^{r} p_k^{m_k}, \; b = v \prod_{k=1}^{r} P_k^{n_k}$$

les décompositions de a et b en facteurs irréductibles, où u, v sont inversibles, les p_k sont irréductibles deux à deux non associés et les n_k, m_k sont des entiers naturels (certains de ces entiers pouvant être nuls).
Montrer que :

$$(a \text{ divise } b) \Leftrightarrow (\forall k \in \{1, \cdots, r\}, \; m_k \leq n_k)$$

3. Montrer qu'un anneau factoriel $\mathbb{A}$ est un anneau à pgcd. Précisément, pour :

$$a = u \prod_{k=1}^{r} p_k^{m_k}, \; b = v \prod_{k=1}^{r} P_k^{n_k}$$

dans $\mathbb{A}^*$, où u, v sont inversibles, les p_k sont irréductibles deux à deux non associés et les n_k, m_k sont des entiers naturels (certains de ces entiers pouvant être nuls), on a :

$$a \wedge b = \prod_{k=1}^{r} p_k^{\min(m_k, n_k)}$$