N° d'ordre 1153

THESE

présentée à

L'UNIVERSITE DES SCIENCES ET TECHNIQUES DE LILLE

pour obtenir

LE GRADE DE DOCTEUR DE 3ème CYCLE

Spécialité : MATHEMATIQUES PURES

par

José BONET

PARTIES GENERATRICES DANS UN ANNEAU DE POLYNOMES

CONSTRUCTIONS EFFECTIVES

Membres du Jury : Daniel LAZARD, Président
Nicole ZINN-JUSTIN, Rapporteur
Sabah FAKIR, Examinateur

Soutenue le 1er juillet 1985

A mes parents,

Je remercie vivement Madame Nicole ZINN-JUSTIN pour l'aide attentive et compétente qu'elle m'a apportée tout au long de l'élaboration du présent travail et d'avoir accepté de faire partie du jury.

Je remercie également Messieurs Daniel LAZARD et Sabah FAKIR pour leurs suggestions ainsi que d'avoir accepté de participer au jury et particulièrement Monsieur LAZARD pour les renseignements et les documents qu'il a bien voulu me fournir.

Je tiens aussi à remercier Madame Raymonde BERAT pour sa gentillesse et sa patience, ainsi que pour le soin apporté à la dactylographie de cette thèse. Mes remerciements vont également à toutes les personnes ayant participé à sa réalisation matérielle pour leur compétence et leur compréhension.

NOTATIONS

Nous noterons $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$ respectivement l'ensemble des entiers naturels, des entiers relatifs et des nombres rationnels.

Nous poserons $\mathbb{N}^{o} = \mathbb{N} - \{0\}$ (sauf chapitre I § 1 à 3 où $\mathbb{N}^{o} = \{0\}$). Pour $n \in \mathbb{N}$ (resp. $n \in \mathbb{N}^{o}$), $\mathbb{N}_n = \{x \in \mathbb{N} | x \leq n\}$ (resp. $\mathbb{N}_n^{o} = \{x \in \mathbb{N}^{o} | x \leq n\}$).

Pour A un anneau commutatif unitaire, nous poserons $A^{o} = A - \{0\}$ et A^{*} l'ensemble des éléments inversibles de A. Considérons M un A module. Pour U une partie de M (resp. de A), $\mathrm{mod}_A(U)$ (resp. $\mathrm{id}_A(U)$) est le sous A-module (resp. idéal) de M (resp. de A), engendré par U. Lorsqu'il n'y aura aucune ambiguïté, nous omettrons A en indice.

SOMMAIRE

INTRODUCTION

L'idée directrice du présent travail est d'établir une construction effective d'une décomposition primaire d'un idéal H de $A[X]$, où A est un anneau.

Pour ce faire, dans un premier temps, nous devons préciser l'anneau A sur lequel les opérations de base sont définies au moyen de procédés récursifs, et, dans un second temps, définir l'idéal H par une partie finie génératrice particulière qui nous permettra de décrire toutes les étapes du calcul.

Remarquons que la démarche suivie interdit l'utilisation de l'axiome du choix, ou toute méthode donnant une existence a priori : l'existence est subordonnée à une construction effective préalable.

Notre première étape est abordée au 1er chapitre. Ce qui nous amène à nous limiter aux ensembles finis ou dénombrables, et à faire un rappel sur les fonctions récursives, afin de pouvoir nous appuyer sur les travaux de D. Lazard concernant la notion d'anneau codable (cf. [LAZ 1], [LAZ 2]). Nous poursuivons par une étude des corps factoriels, introduits par A. Seidenberg sous la forme condition (F) (cf. [SE 1]) et définis par C.W. Ayoub dans [AY 1], pour lesquels il existe un algorithme pour déterminer la décomposition en produit de facteurs irréductibles dans l'anneau de polynômes en une indéterminée.

La seconde l'est au chapitre II, où nous utilisons l'article [AY 2] de C.W. Ayoub en y remplaçant l'anneau des entiers relatifs par un anneau principal algorithmique, défini au chapitre I, en nous limitant aux polynômes en une indéterminée. Nous y établissons une proposition (notée 23.3 p. 53) qui décrit complètement la structure d'une telle partie finie génératrice appelée séparante par C.W. Ayoub, dans le sens où, si $F \in A[X]$, nous pouvons alors

déterminer algorithmiquement si $F \in H$ ou non. Un résultat analogue a été établi indépendamment par D. Lazard dans [LAZ 3], pour les bases de Gröbner dans $K[X,Y]$, où K est un corps. Le chapitre III propose la généralisation au cas de polynômes en deux indéterminées sur un anneau.

Enfin le chapitre IV est consacré à une méthode de construction effective d'une décomposition primaire. Pour cela, nous suivons celle présentée par C.W. Ayoub dans [AY 1] qui s'est inspirée, comme elle l'indique des travaux de A. Seidenberg.

L'inconvénient est que c'est une méthode théorique. En effet, les parties finies des génératrices des idéaux intervenant à chaque étape ne sont pas données explicitement.

Par conséquent, l'originalité va constituer à présenter une méthode dans laquelle les idéaux construits le sont par des parties finies génératrices déterminées effectivement à partir de la partie finie génératrice séparante minimale de H, idéal dont nous cherchons une décomposition primaire. Pour l'instant, nous devons nous restreindre au cas où le contenu du polynôme de plus degré de cette partie est 1.

CHAPITRE I

ANNEAUX CODABLES

1. FONCTIONS RECURSIVES.

Pour plus de détails, se reporter à [LAC] ou [MY].

11. Fonctions initiales et opérations fondamentales.

Nous poserons, par convention, $\mathbb{N}^0 = \{0\}$, pour les § 1, § 2 et § 3.

Définitions des fonctions initiales.

11.1.- Pour tout $n \in \mathbb{N}$, $F^{(n)}$ est l'ensemble des applications de $\mathbb{N}^n$ dans $\mathbb{N}$.

Nous poserons $F = \bigcup_{n\in\mathbb{N}} F^{(n)}$.

11.2.- Application successeur.

C'est l'élément $\mathrm{suc} \in F^{(1)}$, défini par $\mathrm{suc} : \mathbb{N} \to \mathbb{N}$

$$x \to \mathrm{suc}(x) = x+1.$$

11.3.- Applications identiquement nulles.

Pour tout $n \in \mathbb{N}$, $0^{(n)}$ est l'élément de $F^{(n)}$ défini par

$$0^{(n)} : \mathbb{N}^n \longrightarrow \mathbb{N}$$
$$(x_1,\ldots,x_n) \to 0.$$

11.4.- Projections.

Pour tout $n \in \mathbb{N} - \{0\}$, définissons, pour $1 \leqslant i \leqslant n$, $\mathrm{pr}_i^{(n)} \in F^{(n)}$

$$pr_i^{(n)} : \mathbb{N}^n \longrightarrow \mathbb{N}$$
$$(x_1,\ldots,x_n) \longrightarrow x_i$$

Définitions des opérations fondamentales.

11.5.- Composition.

Pour tout $(n,m) \in \mathbb{N}^2$, $\Omega_c^{(n,m)} : F^{(n)} \times (F^{(m)})^n \longrightarrow F^{(m)}$

$$(\Psi,\chi_1,\ldots,\chi_n) \longrightarrow \varphi$$

où φ est définie par :

$$\forall x_1 \ldots \forall x_m \quad \varphi(x_1,\ldots,x_m) = \Psi[\chi_1(x_1,\ldots,x_m),\ldots,\chi_n(x_1,\ldots,x_m)].$$

11.6.- Récurrence.

Pour tout $n \in \mathbb{N}$, $\Omega_R^{(n)} : F^{(n)} \times F^{(n+2)} \longrightarrow F^{(n+1)}$

$$(\chi\ ,\ \Psi) \longrightarrow \varphi$$

où φ est définie par :

$$\forall x_1 \ldots \forall x_n \quad \forall k \quad \varphi(x_1,\ldots,x_n,0) = \chi(x_1,\ldots,x_n)$$
$$\varphi(x_1,\ldots,x_n,k+1) = \Psi[x_1,\ldots,x_n,k,\varphi(x_1,\ldots,x_n,k)].$$

11.7.- Opération μ.

(i) Pour tout $n \in \mathbb{N}$, définissons $F_\mu^{(n+1)}$ par $F_\mu^{(n+1)} \subset F^{(n+1)}$ et : $\forall \Psi \quad \Psi \in F_\mu^{(n+1)} \iff \forall x_1 \ldots \forall x_n \ \exists y \ \Psi(x_1,\ldots,x_n,y) = 0$.

(ii) Pour $\Psi \in F_\mu^{(n+1)}$, posons $\mu y[\Psi(x_1,\ldots,x_n,y) = 0]$, le plus petit $y \in \mathbb{N}$ tel que $\Psi(x_1,\ldots,x_n,y) = 0$.

(iii) Pour tout $n \in \mathbb{N}$, $\Omega_\mu^{(n)} : F_\mu^{(n+1)} \longrightarrow F^{(n)}$

$$\Psi \longrightarrow \varphi$$

où φ est définie par :

$\forall x_1 \ldots \forall x_n \qquad \psi(x_1,\ldots,x_n) = \mu y \left[\Psi(x_1,\ldots,x_n,y) = 0\right]$.

12. *Ensemble des fonctions récursives.*

Soit M une partie de F. Pour tout $n \in \mathbb{N}$, $M^{(n)} = M \cap F^{(n)}$ et nous définissons les conditions suivantes :

(i) $\text{suc} \in M^{(1)}$

(ii) $\forall\, n \in \mathbb{N} \quad 0^{(n)} \in M^{(n)}$

(iii) $\forall\, n \in \mathbb{N} - \{0\} \quad \forall\, i \in \mathbb{N}\ (1 \leqslant i \leqslant n)\ (\mathrm{pr}_i^{(n)} \in M^{(n)})$.

(iv) $\forall\, (n,m) \in \mathbb{N}^2, \quad \Omega_C^{(n,m)}\left[M^{(n)} \times (M^{(m)})^n\right] \subset M^{(m)}$

(v) $\forall\, n \in \mathbb{N} \quad \Omega_R^{(n)}\left[M^{(n)} \times M^{(n+2)}\right] \subset M^{(n+1)}$

(vi) $\forall\, n \in \mathbb{N} \quad \Omega_\mu^{(n)}\left[M^{(n+1)} \cap F_\mu^{(n+1)}\right] \subset M^{(n)}$.

Proposition 12.1.- L'intersection complète d'une famille de sous-ensembles de F_1 qui satisfont (i) à (vi), satisfait aussi (i) à (vi).

Définition 12.2.- L'ensemble F_R des fonctions récursives est l'intersection de tous les sous-ensembles de F qui satisfont (i) à (vi).

Quelques résultats élémentaires cités dans [LAC].

Proposition 12.3.- Les permutations, identifications et adjonctions de variables, ainsi que le remplacement de certaines variables par des constantes, transforment des fonctions récursives en fonctions récursives.

Proposition 12.4.- L'addition, la multiplication et l'exponentiation sont récursives.

Les applications constantes sont des fonctions récursives.

13. Sous-ensembles récursifs.

Sous-ensembles récursivement énumérables.

Définition 13.1.- Soit $n \in \mathbb{N}$. Nous dirons qu'un sous-ensemble E de $\mathbb{N}^n$ est récursif si sa fonction caractéristique 1_E est récursive.

Définition 13.2.- Soit $n \in \mathbb{N}$. Nous dirons qu'un sous-ensemble E de $\mathbb{N}^n$ est récursivement énumérable s'il est la projection d'un sous-ensemble récursif de $\mathbb{N}^{n+1}$, c'est-à-dire il existe F un sous-ensemble récursif de $\mathbb{N}^{n+1}$, tel que :

$$\forall x_1 \ldots \forall x_n \quad (x_1,\ldots,x_n) \in E \iff \exists y (x_1,\ldots,x_n,y) \in F.$$

Proposition 13.3.- Un sous-ensemble récursif est récursivement énumérable.

Démonstration :

Soit $n \in \mathbb{N}$ et considérons E un sous-ensemble récursif de $\mathbb{N}^n$. Posons $F = \{(x_1,\ldots,x_n,0) \mid (x_1,\ldots,x_n) \in E\}$. Donc $F \subset \mathbb{N}^{n+1}$; alors nous avons $1_F(x_1,\ldots,x_n,0) = 1_E(x_1,\ldots,x_n)$ et, pour $k \in \mathbb{N}$, $1_F(x_1,\ldots,x_n,k+1) = 0^{(n+2)}[x_1,\ldots,x_n,n,1_F(x_1,\ldots,x_n,n)]$.

Par conséquent, $1_F = \Omega_R^{(n)}(1_E, 0^{(n+2)})$.

Comme 1_E est une fonction récursive, 1_F est aussi une fonction récursive. Donc F est un sous-ensemble récursif de $\mathbb{N}^{n+1}$, dont la projection est E, et E est récursivement énumérable.

Remarque 13.4.- La réciproque de la proposition 13.3. n'est pas toujours vraie (cf. [LAC], théorème 1.II, p. 401).

Dans [LAC] (§ 1.5, p. 399-400), on trouvera des résultats élémentaires (dit de type "positif"), concernant ces ensembles.

En particulier, les sous-ensembles finis de $\mathbb{N}$ sont récursifs.

2. APPLICATIONS RECURSIVES SUR DES ENSEMBLES INFINIS DENOMBRABLES.

21. Numérotations sur un ensemble infini dénombrable.

Définition 21.1.- Soit A un ensemble infini dénombrable.

Nous appellerons numérotation de A, toute bijection de $\mathbb{N}$ sur A.

Proposition 21.2.- Soit A un ensemble infini dénombrable.

Considérons α_1 et α_2 deux numérotations de A. Pour que $\alpha_1^{-1} \circ \alpha_2$ soit récursive il faut et il suffit que $\alpha_2^{-1} \circ \alpha_1$ le soit.

D'où :

Définition 21.3.- Soit A un ensemble infini dénombrable. Nous dirons que deux numérotations α_1 et α_2 de A sont récursivement équivalentes si $\alpha_1^{-1} \circ \alpha_2$ est récursive.

Il est aisé de vérifier que c'est bien une relation d'équivalence sur l'ensemble des numérotations de A.

22. Applications récursives.

Définition 22.1.- Considérons deux ensembles infinis dénombrables A et A', munis, respectivement, des numérotations α et α'.

Une application $f : A \to A'$ est dite récursive relativement à (α,α') si $\alpha'^{-1} \circ f \circ \alpha$ est récursive.

Proposition 22.2.- Soient A et A' deux ensembles infinis dénombrables. Considérons α_1 et α_2 (resp. α'_1 et α'_2) deux numérotations de A (resp. de A'), récursivement équivalentes, et f une application de A dans A'.

Pour que f soit récursive relativement à (α_1,α'_1) il faut et il suffit que f soit récursive relativement à (α_2,α'_2).

23. *Sous-ensembles récursifs.*

Sous-ensembles récursivement énumérables.

Définition 23.1.- Soit A un ensemble infini dénombrable, muni d'une numérotation α. Un sous-ensemble B de A est dit récursif (resp. récursivement énumérable) relativement à α si $\alpha^{-1}(B)$ est un sous-ensemble récursif (resp. récursivement énumérable) de $\mathbb{N}$.

Proposition 23.2.- Soit A un ensemble infini dénombrable. Considérons α et α' deux numérotations récursivement équivalentes de A.

Pour qu'un sous-ensemble B de A soit récursif (resp. récursivement énumérable) relativement à α, il faut et il suffit que B le soit relativement à α'.

3. ENSEMBLES FINIS.

31.- Semi-fonctions semi-récursives.

Nous reprenons la définition donnée dans [LAC] § 1.9 p. 403-404 ; (rappelons que semi-fonction, de n variables, désigne une application d'un sous-ensemble E de $\mathbb{N}^n$ dans $\mathbb{N}$).

32.- Numérotation d'un ensemble fini.

Définition 32.1.- Soit A un ensemble fini de cardinal a.

Nous appellerons numérotation de A, toute bijection d'un sous-ensemble E de $\mathbb{N}$, tel que card(E) = a, sur A.

Considérons deux numérotations (α,E) et (α',E') de A. Désignons par $i_E : E \to \mathbb{N}$ (resp. $i_{E'} : E' \to \mathbb{N}$) l'injection canonique de E (resp. E') dans $\mathbb{N}$. Nous pouvons vérifier que $E \xrightarrow{\alpha} A \xrightarrow{\alpha'^{-1}} E' \xrightarrow{i_{E'}} \mathbb{N}$ est une semi-fonction semi-récursive si et seulement si $E' \xrightarrow{\alpha'} A \xrightarrow{\alpha^{-1}} E \xrightarrow{1_E} \mathbb{N}$ est une semi-fonction semi-récursive.

Dans ce cas, nous dirons que α et α' sont récursivement équivalentes.

33.- Applications récursives.

Définition 33.1.- Considérons A (resp. A') un ensemble fini de cardinal a (resp. a') et f une application de A dans A'. Posons α (resp. α') une numérotation de A (resp. A').

Alors f est dite récursive lorsque $E \xrightarrow{\alpha} A \xrightarrow{f} A' \xrightarrow{\alpha'^{-1}} E' \xrightarrow{i_{E'}} \mathbb{N}$ est une semi-fonction semi-récursive.

Comme dans le cas dénombrable infini, nous pouvons remplacer α et α' par des numérotations récursivement équivalentes.

Maintenant, comme tout sous-ensemble fini de $\mathbb{N}$ est récursif, tout sous-ensemble d'un ensemble fini muni d'une numérotation est récursif.

4. ANNEAUX CODABLES.

Dans la suite, dénombrable signifie infini dénombrable ou fini.

41. Définition.

Définition 41.1.- Nous appellerons anneau codable un anneau commutatif unitaire dénombrable A, muni d'une classe de numérotations récursivement équivalentes, qui satisfait les axiomes suivants :

(E0) pour une numérotation α de la classe dont est muni A, nous connaissons i et j dans $\mathbb{N}$ tels que $\alpha(i) = 0$ et $\alpha(j) = 1$.

(E1) l'addition est une application récursive de $A \times A$ dans A.

(E2) la multiplication est une application récursive de $A \times A$ dans A.

(E3) pour tout $n \in \mathbb{N}^o$, nous connaissons une application récursive $h^{(n)}$ de A^n dans l'ensemble des suites finies d'éléments de A^n, telle que $h^{(n)}(a_1,\ldots,a_n)$ soit une suite de solutions de l'équation $\sum_{i=1}^{n} a_i x_i = 0$, et que ces solutions engendrent le module de toutes les solutions.

(E4) pour tout $n \in \mathbb{N}^o$, nous connaissons une application récursive $k^{(n)}$ de A^{n+1} dans $A^n \cup \{\emptyset\}$ telle que :

(i) si $k^{(n)}(a_1,\ldots,a_n,b) = (c_1,\ldots,c_n)$ alors $\sum_{i=1}^{n} a_i c_i = b$;

(ii) si $k^{(n)}(a_1,\ldots,a_n,b) = \emptyset$ alors l'équation $\sum_{i=1}^{n} a_i x_i = b$ n'a pas de solution dans A^n.

Cette définition a été donnée par D. Lazard.

Proposition 41.2.- Soit A un anneau codable. Posons α la numérotation de A pour laquelle nous connaissons i et j dans $\mathbb{N}$ tels que $\alpha(i) = 0$ et $\alpha(j) = 1$.

Alors pour toute numérotation β de A, récursivement équivalente à α, nous connaissons s et r dans $\mathbb{N}$, tels que $\beta(s) = 0$ et $\beta(r) = 1$.

Proposition 41.3.- Soit A un anneau codable.

Alors l'application $A \longrightarrow A$ est récursive.

$$a \longrightarrow -a$$

Démonstration :

Considérons l'équation $1.x + a.y = 0$.

En utilisant $h^{(2)}$, nous pouvons déterminer $h^{(2)}(1,a) = ((x_1,y_1),\ldots,(x_s,y_s))$ une suite de solutions qui engendrent le module des solutions.

Maintenant, cherchons $k^{(s)}(y_1,\ldots,y_s,1)$, c'est-à-dire résoudre $\sum_{i=1}^{s} y_i.c_i = 1$.

Si $k^{(s)}(y_1,\ldots,y_s,1) = \emptyset$, alors cette équation n'a pas de solution. Donc nous ne pouvons trouver $b \in A$ tel que $1.b + a.1 = 0$, c'est-à-dire $b+a = 0$: absurde.

Donc $k^{(s)}(y_1,\ldots,y_s,1) = (c_1,\ldots,c_s)$.

Calculons alors $\sum_{i=1}^{s} (c_i.x_i + a.c_i.y_i)$

$$\sum_{i=1}^{s} (c_i.x_i + a.c_i.y_i) = \sum_{i=1}^{s} c_i(1.x_i + ay_i) = 0$$

et
$$\sum_{i=1}^{s} (c_i.x_i + a.c_i.y_i) = (\sum_{i=1}^{s} c_i.x_i) + a \sum_{i=1}^{s} c_i y_i$$

$$= (\sum_{i=1}^{s} c_i.x_i) + a$$

donc
$$(\sum_{i=1}^{s} c_i.x_i) + a = 0.$$

alors $-a = \sum_{i=1}^{s} c_i.x_i$.

Proposition 41.4.- Soit A un anneau codable. Posons A^* l'ensemble des éléments inversibles. Alors A^* est récursif.

Démonstration :

Nous devons établir que 1_{A^*} est une application récursive. Prenons $a \in A$ et $a \neq 0$, pour savoir si a est inversible ou pas, nous devons résoudre l'équation $a.x = 1$, c'est-à-dire déterminer $k^{(2)}(a,1)$.

Définissons $1 : A \to \mathbb{N}$; $id : A \to A$; et $1_A : A \cup \{\emptyset\} \to \mathbb{N}$

$a \mapsto 1$ $\quad$ $a \mapsto a$

ces applications sont, de façon évidente, récursives et nous avons :

$$1_{A^*} = \Omega_c^{(1,1)}\left[1_A, \Omega_c^{(2,1)}(k^{(2)}, id, 1)\right].$$

Donc 1_{A^*} est récursive.

42. *Application aux corps commutatifs.*

Proposition 42.1.- Soit K un corps commutatif dénombrable, muni d'une classe de numérotations récursivement équivalentes. Pour que K soit un anneau codable il faut et il suffit que K vérifie les axiomes (E0), (E1) et (E2) de la définition 41.1 et que les applications suivantes soient récursives :

$K \to K$ $\quad$ et $\quad$ $K^* \longrightarrow K^*$

$x \mapsto -x$ $\quad$ $x \longmapsto x^{-1}$.

Démonstration :

La condition nécessaire est évidente d'après les propositions 41.3 et 41.4.

La condition suffisante a été établie par D. Lazard.

43. Anneaux principaux algorithmiques.

Proposition 43.1.- Soit A un anneau principal dénombrable, muni d'une classe de numérotation récursivement équivalentes, qui vérifie les axiomes (E0), (E1) et (E2) de la définition 41.1.

Supposons de plus, que les applications suivantes sont récursives :

(i) $inv : A \to A \cup \{\emptyset\}$

telle que si $inv(a) = \emptyset$ alors a n'est pas inversible dans A.

si $inv(a) = b$ alors $a.b = 1$.

(ii) $p : (A^o)^2 \to A^4$

$(a,b) \to (c,d,e,f)$

telle que $a = e.(c.a+d.b)$ et $b = f.(c.a+d.b)$.

Alors A est un anneau codable.

Corollaire 43.1a.-

(i) l'anneau $\mathbb{Z}$ est codable ;

(ii) si K est un corps codable, alors $K[X]$ est un anneau codable.

Pour construire p, nous utilisons l'algorithme d'Euclide.

Définition 43.2.- Soit A un anneau principal dénombrable, muni d'une classe de numérotations récursivement équivalentes. Nous dirons que A est un anneau principal algorithmique que si A est un anneau codable pour lequel nous connaissons p une application récursive de $(A^o)^2$ dans A^4, telle que, si $p(a,b) = (c,d,e,f)$ alors $a = e.(c.a+d.b)$ et $b = f.(c.a+d.b)$.

43.3.- Remarquons que le transport par isomorphisme de cette propriété n'est possible que dans le cas d'un isomorphisme qui est une application récursive.

Proposition 43.4.- Soit A un anneau principal dénombrable, muni d'une classe de numérotations récursivement équivalentes.

Pour que A soit principal algorithmique, il faut et il suffit que A vérifie les hypothèses de la proposition 43.1.

Corollaire 43.4a.- Soit K un corps codable, alors $K[X]$ est un anneau principal algorithmique.

Proposition 43.5.- Soit A un anneau principal algorithmique.

Alors K, le corps des fractions de A, est un corps codable.

Démonstration :

Prenons α une numérotation de A, élément de la classe dont est muni A. Nous connaissons i et j dans $\mathbb{N}$ tels que $\alpha(i) = 0$ et $\alpha(j) = 1$.

Soit $x \in K$, si $x = 0$, x est représenté par $\frac{\alpha(i)}{\alpha(j)}$

sinon, x est représenté par $\frac{a}{b}$, a et b non nuls dans A. Nous pouvons déterminer $p(a,b) = (c,d,e,f)$ donc x est représenté par $\frac{e}{f}$ fraction irréductible. Posons $e = \alpha(s)$ et $f = \alpha(r)$.

Définissons $E \subset \mathbb{N}^2$ par

$(u,v) \in E$ si et seulement si $\frac{\alpha(u)}{\alpha(v)}$ est une fraction irréductible alors E est récursif (puisque p est récursive).

Dans ce cas, définissons $\Psi : K \to E$ par $\Psi(0) = (i,j)$ et, pour $x \neq 0$, $\Psi(x) = (s,r)$: c'est une bijection récursive.

Maintenant, nous pouvons déterminer $\psi : E \to \mathbb{N}$ bijection récursive. Posons $\beta = (\psi \circ \Psi)^{-1}$ alors β est une numérotation de K, définie par α.

K est muni de la classe des numérotations récursivement équivalentes à β.

Alors, de façon évidente, K vérifie la condition suffisante de la proposition 42.1, donc K est codable.

44. *Anneaux factoriels algorithmiques.*

Définition 44.1.- Soit A un anneau factoriel dénombrable, muni d'une classe de numérotations récursivement équivalentes. Posons Ξ l'ensemble des éléments irréductibles de A et $S_f(\Xi)$ l'ensemble des suites finies d'éléments de Ξ.

Nous dirons que A est un anneau factoriel algorithmique si A est un anneau codable qui vérifie :

(i) Ξ est récursif ;

(ii) nous connaissons une application récursive

$$\text{dec} : A^{\circ} - A^{*} \to A^{*} \times S_f(\Xi)$$

$$a \longmapsto (\varepsilon, \pi_1, \ldots, \pi_n)$$

telle que $a = \varepsilon . \prod_{i=1}^{n} \pi_i$.

(iii) nous connaissons une application récursive

$$\text{ass} : \Xi \times \Xi \to A^{*} \cup \{\emptyset\}$$

telle que : si $\text{ass}(\pi_1, \pi_2) = \emptyset$ alors π_1 et π_2 sont étrangers.

si $\text{ass}(\pi_1, \pi_2) = \varepsilon$ alors $\pi_2 = \varepsilon . \pi_1$.

44.2.- La remarque concernant le transport par isomorphisme est identique au cas des anneaux principaux algorithmiques.

45. *Anneaux de polynômes sur un anneau principal algorithmique.*

Théorème 45.1.- Soit A un anneau principal algorithmique. Alors $A[X]$ est un anneau codable.

C'est une conséquence du théorème plus général suivant :

Soit A un anneau noethérien codable alors $A[X]$ est un anneau codable (dû à Richman dont la démonstration est donnée par D. Lazard).

Rappelons maintenant la définition du contenu d'un polynôme.

Définition 45.2.- Soit A un anneau principal. Nous appellerons contenu de F, pour $F \in A[X]$, non nul, et nous le noterons $c(F)$, le p.g.c.d. des coefficients non nuls de F.

De façon évidente, nous avons :

Proposition 45.3.- Soit A un anneau principal algorithmique. Alors, l'application de $A[X] - \{0\}$ dans A, qui à F associe $c(F)$, est récursive.

Lorsque $c(F) = 1$, aux inversibles près, F est dit primitif, et nous avons les résultats suivants (cf. [BLW]) :

(i) pour tout $F \in A[X] - \{0\}$ et tout $a \in A^o$, $c(aF) = ac(F)$;

(ii) l'application $A[X]^o \longrightarrow A^o \times A[X]^o$

$$F \longmapsto (c(F), F_1)$$

telle que $F = c(F).F_1$ et F_1 primitif (donc $d^oF = d^oF_1$) est une application récursive.

(iii) le produit de deux polynômes primitifs est encore un polynôme primitif.

D'où :

Proposition 45.4.- Soit A un anneau principal algorithmique. Alors, quels que soient les éléments non nuls F et G de $A[X]$, $c(F.G) = c(F).c(G)$.

Proposition 45.5.- Soit A un anneau principal algorithmique. Considérons F un polynôme non constant de $A[X]$, pour lequel il existe deux éléments non constants g et h de $K[X]$, où K est le corps des fractions de A, tels que F = g.h. Alors nous pouvons déterminer explicitement deux polynômes primitifs non constants G et H de $A[X]$ tels que F = c(F).G.H.

Démonstration :

Posons a (resp. b) le produit des dénominateurs des coefficients non nuls de g (resp. de h), aussi $a.g \in A[X]$ (resp. $b.h \in A[X]$).

Comme l'application $L \longmapsto (c(L),L_1)$, où $L = c(L).L_1$ et L_1 primitif, est récursive, nous déterminons explicitement deux polynômes primitifs non constants G et H de $A[X]$ tels que $a.g = c(a.g).G$ et $b.h = c(b.h)H$.

Or F = g.h donc (a.b).F = (a.g).(b.h).

Alors, proposition 45.4, a.b.c(F) = c(a.g).c(b.b)

maintenant (a.b).F = c(a.g).c(b.h).G.H

donc (a.b).F = (a.b).c(F).G.H et F = c(F).G.H.

Théorème 45.6.- Soit A un anneau principal algorithmique. Alors nous pouvons déterminer q une application récursive de $(A[X]^o)^2$ dans $A[X]^3$ telle que :

si q(F,G) = (H,f,g) alors (i) F = H.f et G = H.g

(ii) pour tout $L \in A[X]^o$
si L divise F et G alors L divise H.

Démonstration :

Utilisons l'application récursive $L \to (c(L),L_1)$ où $L = c(L).L_1$

et L_1 primitif, pour obtenir $F = c(F).F_1$ et $G = c(G).G_1$.

Puisque A est un anneau principal algorithmique, nous connaissons p une application récursive de $(A^o)^2$ dans A^4, telle que si $p(a,b) = (c,d,e,f)$ alors $a = e.(c.a+d.b)$ et $b = f.(c.a+d.b)$.

Déterminons $p[c(F),c(G)] = (t,u,v,w)$.

1er cas : $d^oF = 0$ ou $d^oG = 0$

alors le p.g.c.d de F et de G dans $A[X]$ est $H = t.c(F)+u.c(G)$.

2ème cas : $d^oF \neq 0$ et $d^oG \neq 0$.

donc $d^oF_1 \neq 0$ et $d^oG_1 \neq 0$.

Posons K le corps des fractions de A, donc K est codable.

Alors, corollaire 43.4a, $K[X]$ est un anneau principal algorithmique.

Par conséquent, nous connaissons une application récursive p' de $(K[X]^o)^2$ dans $K[X]^4$ telle que si $p'(\alpha,\beta) = (\lambda,\mu,\gamma,\delta)$ alors $\alpha = \gamma.(\lambda.\alpha+\mu.\beta)$ et $\beta = \delta.(\lambda.\alpha+\mu.\beta)$.

Déterminons $p'(F_1,G_1) = (\lambda,\mu,\gamma,\delta)$ et posons $h = \lambda.F_1 + \mu.G_1$ donc $F_1 = \gamma.h$ et $G_1 = \delta.h$.

Nous pouvons alors utiliser la proposition 45.5 : nous pouvons déterminer des polynômes primitifs non constants F_2, G_2, H_1 de $A[X]$ tels que $F_1 = F_2.H_1$ et $G_1 = G_2.H_1$ (que nous obtenions H_1 dans les deux décompositions provient de la démonstration de la proposition 45.5).

Nous avions déterminé $p[c(F),c(G)] = (t,u,v,w)$

posons $s = t.c(F) + u.c(G)$. Donc $c(F) = s.v$ et $c(G) = s.w$.

D'où $F = (v.F_2).H$ et $G = (w.G_2).H$ en posant $H = s.H_1$.

Maintenant soit Δ un diviseur commun à F et à G dans $A[X]$.

Donc $F = \Delta.P$ et $G = \Delta.Q$ avec $P \in A[X]$ et $Q \in A[X]$.

Alors, proposition 45.4, $c(F) = c(\Delta).c(P)$ et $c(G) = c(\Delta).c(P)$, donc $c(\Delta)$ est un diviseur de s.

En outre, nous pouvons déterminer effectivement $\Delta = c(\Delta).\Delta_1$, $P = c(P).P_1$ et $Q = c(Q).Q_1$, où Δ_1, P_1 et Q_1 sont primitifs dans $A[X]$. Dans ce cas, $F_1 = P_1.\Delta_1$ et $G_1 = Q_1.\Delta_1$, donc $P_1.\Delta_1 = F_2.H_1$ et $Q_1.\Delta_1 = G_2.H_1$.

Comme F_2 et G_2 sont étrangers dans $K[X]$, en posant $p'(F_2,G_2) = (\lambda_2,\mu_2,\gamma_2,\delta_2)$ alors $\lambda_2.F_2 + \mu_2.G_2 = 1$ et $\gamma_2 = F_2$, $\delta_2 = G_2$. Calculons θ le produit des dénominateurs des coefficients non nuls de λ_2 et μ_2, alors $\theta \in A^o$, $\theta.\lambda_2 \in A[X]$ et $\theta.\mu_2 \in A[X]$. Posons $R = \theta.\lambda_2$ et $S = \theta.\mu_2$, nous obtenons :

$$\theta = R.F_2 + S.G_2$$

donc $\theta.H_1 = R.F_2.H_1 + S.G_2.H_1 = (R.P_1 + S.Q_1).\Delta_1$.

Comme H_1 et Δ_1 sont primitifs, nous en déduisons que Δ_1 est un diviseur de H_1. Par conséquent, $\Delta = c(\Delta).\Delta_1$ est un diviseur de $H = s.H_1$. Donc H est le p.g.c.d. de F et G, dans $A[X]$.

46.- Extensions simples d'un corps codable.

Proposition 46.1.- Soit K un corps codable. Alors toute extension transcendante simple $K(t)$ de K, est un corps codable.

Démonstration :

D'après le corollaire 43.4a, $K[X]$ est un anneau principal algorithmique.

Donc, proposition 43.5, $K(X)$ est un corps codable.

En outre, l'application de $K(X)$ dans $K(t)$ qui consiste à remplacer X par t est un isomorphisme récursif de corps.

Par conséquent, $K(t)$ est un corps codable.

Proposition 46.2.- Soit K un corps codable. Considérons $L = K[\theta]$ une extension monogène séparable de K, pour laquelle le polynôme minimal f de θ sur K est donné.

Alors L est un corps codable.

Démonstration :

Posons $n = d^{o}f$.

Tout élément $\alpha \in L$ peut être représenté par $\alpha = g(\theta)$ où $g \in K[X]$ et $d^{o}g < n$.

A partir d'une numérotation de K, nous pouvons alors en construire une pour L. Dans ce cas l'addition est récursive, ainsi que $L \longrightarrow L$

$$\alpha \longmapsto -\alpha.$$

De plus, puisque $K \subset L$ et K vérifie (EO), alors L vérifie (EO).

Considérons α et β deux éléments non nuls de L. Donc $\alpha = g(\theta)$ et $\beta = h(\theta)$, où g et h sont dans $K[X]$ et $d^{o}g < n$, $d^{o}h < n$.

Déterminons la division euclidienne $g.h = f.q + r$ avec $d^{o}r < n$. Alors $\alpha.\beta = r(\theta)$. Donc la multiplication est récursive.

Pour l'inverse, prenons $\alpha \in L$ et $\alpha \neq 0$, donc $\alpha = g(\theta)$ avec $g \in K[X]^{o}$ et $d^{o}g < n$. Donc g et f sont étrangers. Comme $K[X]$ est principal algorithmique, nous connaissons p application récursive telle que $p(g,f) = (u,o,\lambda,\mu)$ alors $u.g+v.f$ est le pgcd de g et f, donc $u.g+v.f = 1$.

Déterminons la division euclidienne $u = u_1.f + r_1$, avec $d^{o}r_1 < n$.

alors $\alpha.r_1(\theta) = 1$. Donc l'application $L^o \longrightarrow L^o$ est récursive.

$$\alpha \longmapsto \alpha^{-1}.$$

Par conséquent, la condition suffisante de la proposition 42.1 est vérifiée, d'où L est un corps codable.

5. CORPS FACTORIELS.

51. Définition.

Définition 51.1.- Soit K un corps commutatif dénombrable, muni d'une classe de numérotations récursivement équivalentes. Nous dirons que K est un corps factoriel si K est un corps codable et $K[X]$ est un anneau factoriel algorithmique.

Remarquons que cette définition est nécessaire, car le fait que K soit codable, bien que $K[X]$ soit codable et principal algorithmique (cf. corollaire 43.1a et 43.3a), n'entraîne pas en général que $K[X]$ soit factoriel algorithmique.

Proposition 51.2.- Soient K et K' deux corps commutatifs dénombrables, munis respectivement d'une classe de numérotations récursivement équivalentes. Supposons qu'il existe f un isomorphisme récursif de corps de K sur K'.

Pour que K soit factoriel, il faut et il suffit que K' le soit.

Démonstration :

Définissons $\bar{f} : K[X] \longrightarrow K'[X]$

$$\sum_{i=0}^{n} a_i X^i \longmapsto \sum_{i=0}^{n} f(a_i) X^i$$

alors $\bar{f}$ est un isomorphisme d'anneaux de $K[X]$ sur $K'[X]$.

De plus, c'est une application récursive, donc pour K soit factoriel il faut et il suffit que K' le soit.

52. Cas d'un corps de fractions.

Proposition 52.1.- Soit A un anneau à la fois principal algorithmique et factoriel algorithmique. Posons K son corps des fractions.

Pour que $A[X]$ soit un anneau factoriel algorithmique, il faut et il suffit que K soit un corps factoriel.

Démonstration :

Supposons d'abord $A[X]$ anneau factoriel algorithmique. Prenons $F \in K[X]$, $F \neq 0$. Nous pouvons déterminer $a \in A^o$ (le pgcd des dénominateurs des coefficients de F) tel que $a.F \in A[X]$.

Par conséquent, $K[X]$ est un anneau factoriel algorithmique, c'est à-dire K est un corps factoriel.

Supposons maintenant K corps factoriel.

Prenons $F \in A[X]$. Nous pouvons déterminer le contenu $c(F)$ de F et $F_1 \in A[X]$ primitif tel que $F = c(F).F_1$.

En particulier, $F_1 \in K[X]$, donc nous pouvons déterminer une décomposition de F_1 en produit fini de facteurs irréductibles de $K[X]$:

$$F_1 = \prod_{j=1}^{k} f_{1,j}.$$

Nous pouvons déterminer, pour tout $j \in \mathbb{N}_k$, $a_{1,j} \in A^o$ tel que $a_{1,j}.f_{1,j} \in A[X]$. Déterminons $a_{1,j}.f_{1,j} = c(a_{1,j}.f_{1,j}).H_{1,j}$, avec $H_{1,j} \in A[X]$, primitif. Donc $H_{1,j}$ est irréductible dans $K[X]$, comme il est primitif, il reste irréductible dans $A[X]$.

Posons $a_1 = \prod_{j=1}^{k} a_{1,j}$. Alors :

$$a_1.F_1 = \prod_{j=1}^{k} (a_{1,j}.f_{1,j}) = \left(\prod_{j=1}^{k} c(a_{1,j}.f_{1,j})\right)\left(\prod_{j=1}^{k} H_{1,j}\right)$$

en passant aux contenus, nous obtenons $a_1 = \prod_{j=1}^{k} c(a_{1,j}.f_{1,j})$. Donc

$F_1 = \prod_{j=1}^{k} H_{1,j}$ avec $H_{1,j}$ irréductible dans $A[X]$.

En décomposant $c(F)$, nous en déduisons une décomposition en produit fini de facteurs irréductibles de $A[X]$ pour F.

Donc $A[X]$ est un anneau factoriel algorithmique.

53. *Propriétés des corps factoriels.*

Proposition 53.1. (*Kronecker*).- Soit K un corps factoriel. Alors tout anneau de polynômes sur K est un anneau factoriel algorithmique.

Démonstration :

Puisque K est un corps factoriel, $K[X]$ est un anneau factoriel algorithmique. Maintenant soit $n \in \mathbb{N}$ et $n > 1$. Alors $K[X_1,\ldots,X_n]$ est un anneau codable (cf. la remarque qui suit le théorème 45.1).

Considérons $F \in K[X_1,\ldots,X_n]$, non constant, alors nous pouvons écrire :

$$F = \sum_{(i_1,\ldots,i_n)\in I(F)} \alpha_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}$$ où $I(F)$ est une partie finie non vide de $\mathbb{N}^n$ et $\alpha_{i_1,\ldots,i_n} \in K^*$.

Prenons $m \in \mathbb{N}$, tel que $m > \max_{\substack{(i_1,\ldots,i_n)\in I(F) \\ \ell\in\mathbb{N}_n^o}} (i_\ell) > 0$ et définissons :

$$\psi : K[X_1,\ldots,X_n] \longrightarrow K[X]$$

$$G = \sum_{(j_1,\ldots,j_n)\in J(G)} \beta_{j_1\ldots j_n} X_1^{j_1}\ldots X_n^{j_n} \longrightarrow \psi(G) =$$

$$\sum_{(j_1,\ldots,j_n)\in J(G)} \beta_{j_1\ldots j_n} X^{j_1+j_2m+\ldots+j_nm^{n-1}}.$$

Donc ψ est une application récursive.

Considérons $G = \sum_{(j_1,\ldots,j_n)\in J(G)} \beta_{j_1\ldots j_n} X_1^{j_1}\ldots X_n^{j_n}$ et

$H = \sum_{(k_1,\ldots,k_n)\in J(H)} \gamma_{k_1,\ldots,k_n} X_1^{k_1}\ldots X_n^{k_n}$ dans $K[X_1,\ldots,X_n]$. Donc

$$G.H. = \sum_{\substack{(j_1,\ldots,j_n)\in J(G)\\(k_1,\ldots,k_i)\in J(H)}} \beta_{j_1\ldots j_n}.\gamma_{k_1\ldots k_n} X_1^{j_1+k_1}\ldots X_n^{j_n+k_n}$$

aussi $G.H = \sum_{(\ell_1,\ldots,\ell_n)\in J(GH)} \Big(\sum_{\substack{j_\nu+k_\nu=\ell_\nu\\ \text{pour } \nu\in\mathbb{N}_n^o}} \beta_{j_1\ldots j_n}.\gamma_{k_1\ldots k_n} \Big) X_1^{\ell_1}\ldots X_n^{\ell_n}$

d'où $\psi(GH) = \sum_{(\ell_1,\ldots,\ell_n)\in J(GH)} \Big(\sum_{\substack{j_\nu+k_\nu=\ell_\nu\\ \text{pour } \nu\in\mathbb{N}_n^o}} \beta_{j_1\ldots j_n}.\gamma_{k_1\ldots k_n} \Big) X^{\ell_1+\ell_2 m+\ldots+\ell_n m^{n-1}}$

$$= \sum_{(\ell_1,\ldots,\ell_n)\in J(GH)} \sum_{\substack{j_\nu+k_\nu=\ell_\nu\\ \text{pour } \nu\in\mathbb{N}_n^o}} \beta_{j_1\ldots j_n}.\gamma_{k_1\ldots k_n} X^{\ell_1+\ell_2 m+\ldots+\ell_n m^{n-1}} ;$$

or, pour $\nu \in \mathbb{N}_n^o$, $\ell_\nu = j_\nu + k_\nu$

donc $\psi(G,H) = \sum_{\substack{(j_1,\ldots,j_n)\in J(G)\\(k_1,\ldots,k_n)\in J(H)}} \beta_{j_1\ldots j_n}.\gamma_{k_1\ldots k_n} X^{j_1+k_1+(j_2+k_2)m+\ldots+(j_n+k_n)m^{n-1}}$

$$= \sum_{\substack{(j_1,\ldots,j_n)\in J(G)\\(k_1,\ldots,k_n)\in J(H)}} \beta_{j_1\ldots j_n}.\gamma_{k_1\ldots k_n} X^{j_1+j_2 m+\ldots+j_n m^{n-1}+k_1+\ldots+k_n m^{n-1}}$$

alors $\psi(G.H) = \psi(G).\psi(H)$.

Remarquons que pour F, $d^o\psi(F) < m\,\frac{m^n-1}{m-1}$.

De plus, pour $G = \sum_{(j_1,\ldots,j_n)\in J(G)} \beta_{j_1\cdots j_n} X_n^{j_1}\ldots X_n^{j_n} \in K[X_1,\ldots,X_n]$

tel que $\max_{\substack{(j_1,\ldots,j_n)\in J(G)\\ \ell\in\mathbb{N}_n^o}} (j_\ell) < m$, Ψ est une bijection récursive de l'ensemble de ces polynômes G sur l'ensemble des éléments de $K[X]$ de degré strictement inférieur à $m\frac{m^n-1}{m-1}$ (en effet, l'écriture en base m du degré est unique et dans ce cas, elle comporte au plus n termes).

Maintenant $\psi(F) \in K[X]$ et $K[X]$ est un anneau factoriel algorithmique, donc nous connaissons une application récursive qui nous permet de déterminer :

$\psi(F) = \varepsilon \prod_{\ell=1}^{k} h_\ell$ où $\varepsilon \in K^*$ et, pour tout $\ell \in \mathbb{N}_k^o$, h_ℓ est un élément irréductible unitaire de $K[X]$.

Or $d^o h_\ell \leqslant d^o\psi(F)$ donc $d^o h_\ell < m\frac{m^n-1}{m-1}$

posons $h_\ell = \sum_{j=0}^{\sigma(\ell)} a_{j\ell} X^j$ où $d^o h_\ell = \sigma(\ell)$ et $a_{j\ell} \in K$.

Pour $0 \leqslant j \leqslant \sigma(\ell)$, calculons $j = j_1 + j_2 m + \ldots + j_n m^{n-1}$: cette écriture est unique. Posons $H = \sum_{j=0}^{\sigma(\ell)} a_{j\ell} X_1^{j_1}\ldots X_n^{j_n}$ où $j_1,\ldots,j_n$ sont définis ci-dessus.

Donc $\psi(H_\ell) = h_\ell$.

Maintenant, $\psi(\varepsilon^{-1}F) = \varepsilon^{-1}\psi(F) = \prod_{\ell=1}^{k} h_\ell = \prod_{\ell=1}^{k} (H_\ell) = \psi(\prod_{\ell=1}^{k} H_\ell)$.

Or $d^o(\varepsilon^{-1}F) = d^oF < m\frac{m^{n-1}}{m-1}$, aussi $\varepsilon^{-1}F = \prod_{\ell=1}^{k} H_\ell$

et $F = \varepsilon \prod_{\ell=1}^{k} H_\ell$.

Vérifions que pour tout $\ell \in \mathbb{N}_k^o$, H_ℓ est irréductible dans $K[X_1,\ldots,X_n]$. Si non, nous pourrions écrire $H = G_1.G_2$ avec G_1 et G_2

non constants, alors $\psi(H_2) = \psi(G_1).\psi(G_2) = h_\ell$ avec $\psi(G_1)$ et $\psi(G_2)$ non constants, or h_ℓ est irréductible : contradiction. Alors H_ℓ est un polynôme irréductible de $K[X_1,\ldots,X_n]$. Par conséquent, en utilisant ψ nous pouvons décider, récursivement, si un élément de $K[X_1,\ldots,X_n]$ est irréductible ou non. Donc, l'ensemble des irréductibles de $K[X_1,\ldots,X_n]$ est récursif.

De plus, en utilisant ψ puis l'application récursive qui détermine une décomposition dans $K[X]$, nous définissons une application récursive qui détermine une décomposition dans $K[X_1,\ldots,X_n]$.

Enfin, pour vérifier que deux irréductibles sont associés ou non, nous comparons les termes de plus haut degré.

Corollaire 53.1a.- Soit K un corps factoriel. Alors toute extension transcendante simple $K(t)$ de K est un corps factoriel.

Démonstration :

Soit $F \in (K(t))[X]$, non nul et non constant.

Alors il existe $P \in K[X_1,X_2]$, de degré non nul en X_2, puisque F est non constant, et $Q \in K[X_1]$, tels que $F(X) = \frac{P(t,X)}{Q(t)}$.

Or, d'après la proposition 53.1., $K[X_1,X_2]$ est un anneau factoriel algorithmique, aussi nous connaissons une application récursive qui permet de déterminer $P(X_1,X_2) = \varepsilon \prod_{\ell=1}^{k} H_\ell(X_1,X_2)$ où $\varepsilon \in K^*$ et, pour tout $\ell \in \mathbb{N}_k^o$, H_ℓ est un polynôme irréductible de $K[X_1,X_2]$.

Or, le degré de P en X_2 est non nul, aussi il existe au moins un indice ℓ tel que le degré de H_ℓ en X_2 soit non nul.

Nous pouvons supposer que ce sont $H_1,\ldots,H_q$, avec $q \in \mathbb{N}_k^o$, les polynômes irréductibles H_ℓ, intervenant dans la décomposition de P, dont le degré en X_2 est non nul.

Posons $H = \varepsilon \prod_{\ell=q+1}^{k} H_\ell$ alors $H \in K[X_1]$,

d'où $F(X) = \frac{H(t)}{Q(t)} \prod_{\ell=1}^{q} H_\ell(t,X)$ et $\frac{H(t)}{Q(t)} \in K(t)$.

Maintenant t est transcendant sur K, aussi l'application suivante :

$$K[X_1,X_2] \to K[t,X]$$
$$G(X_1,X_2) \mapsto G(t,X)$$

est un isomorphisme récursif d'anneaux, donc, pour $\ell \in \mathbb{N}_q^o$, $H_\ell(t,X)$ est un élément irréductible de $K[t,X]$. Par conséquent, c'est un polynôme irréductible de $(K[t])[X]$.

Comme K est un corps explicitement donné, $K[X]$ est un anneau principal algorithmique. Or $K[t]$ est isomorphe à $K[X]$ et l'isomorphisme est récursif, donc, en utilisant la remarque 43.3, $K[t]$ est un anneau principal algorithmique.

Donc, si $H_\ell(t,X) = r(X).s(X)$ où r et s sont deux polynômes non constants de $(K(t))[X]$, d'après la proposition 45.5, nous pouvons déterminer explicitement R et S deux polynômes non constants de $(K[t])[X]$, tels que $H_\ell(t,X) = R(X).S(X)$: impossible car H_ℓ est irréductible dans $(K[t])[X]$.

Par conséquent, $H_\ell(t,X)$ est un polynôme irréductible de $(K(t))[X]$, et, donc l'ensemble des irréductibles de $(K(t))[X]$ est récursif.

De plus, nous avons défini une application récursive qui permet de déterminer une décomposition $F(X) = \frac{H(t)}{Q(t)} \prod_{\ell=1}^{q} H_\ell(t,X)$ de F en produit fini de facteurs irréductibles de $(K(t))[X]$.

Enfin, pour vérifier que deux irréductibles sont associés ou non, nous comparons les termes de plus haut degré.

Proposition 53.2.- Soit K un corps factoriel. Considérons $L = K[\theta]$ une extension algébrique monogène séparable de K, pour laquelle le polynôme minimal f de θ sur K soit donné.

Alors L est un corps factoriel.

Démonstration :

D'après la proposition 46.2, L est un corps codable.

Posons $s = d^{o}f$ et $\theta_1 = \theta, \theta_2, \ldots, \theta_s$ les conjugués deux à deux distints de θ sur K.

Soit $F(\theta,X) \in L[X]$, unitaire et non constant.

Calculons $F(\theta,X-\theta u)$ où u est une indéterminée sur K.

Puisque le polynôme minimal f de θ sur K est donné explicitement, nous **savons** effectivement calculer la norme $NF(\theta,X-\theta u)$ de $F(\theta,X-\theta u)$ sur K, définie par $NF(\theta,X-\theta u) = \prod_{i=1}^{s} F(\theta_i,X-\theta_i u)$.

Alors $NF(\theta,X-\theta u) \in K[u,X]$.

Or, d'après la proposition 53.1, $K[u,X]$ est un anneau principal algorithmique. Dans ce cas, nous connaissons une application récursive qui permet de déterminer une décomposition :

$$NF(\theta,X-\theta u) = \prod_{\ell=1}^{k} H_\ell(u,X)$$

où, pour tout $\ell \in \mathbb{N}_k^o$, $H_\ell(u,X)$ est un polynôme irréductible unitaire de $K[u,X]$.

Puisque u est transcendant sur K, en utilisant les propositions 46.1 et 46.2, le corps $K(u,\theta)$ est codable.

Donc $K(u,\theta)[X]$ est un anneau principal algorithmique.

Alors, nous connaissons une application récursive qui permet, pour tout $\ell \in \mathbb{N}_k^o$ d'exprimer $\Delta_\ell(\theta,u,X)$ le pgcd unitaire de $H_\ell(u,X)$ et de $F(\theta,X-\theta u)$ dans $(K(u,\theta))[X]$, comme combinaison linéaire de $H_\ell(u,X)$ et de $F(\theta,X-\theta u)$ dans $(K(u,\theta))[X]$:

$$\Delta_\ell(\theta,u,X) = u_\ell(\theta,u,X)F(\theta,X-u) + V_\ell(\theta,u,X)H_\ell(u,X).$$

S'il existe $\ell \in \mathbb{N}_k^o$, tel que $\Delta_\ell(\theta,u,X) = 1$. Sans nuire à la généralité, nous pouvons alors prendre $\ell = 1$. Donc :

$$1 = u_1(\theta,u,X)F(\theta,X-\theta u) + V_1(\theta,u,X)H_1(u,X)$$

alors $1 = \prod_{i=1}^{s} \left[U_1(\theta_i,u,X)F(\theta_i,X-\theta_i u) + V_1(\theta_i,u,X)H_1(u,X)\right]$

aussi, il existe $G_1 \in (K(\theta,u))[X]$ tel que :

$$1 = \prod_{i=1}^{s} \left[U_1(\theta_i,u,X)F(\theta_i,X-\theta_i u)\right] + G_1(\theta,u,X).H_1(u,X)$$

donc $1 = NU_1(\theta,u,X)NF(\theta,X-\theta u) + G_1(\theta,u,X).H_1(u,X)$.

Or $H_1(u,X)$ divise $NF(\theta,X-\theta u)$: contradiction.

Par conséquent, pour tout $\ell \in \mathbb{N}_k^o$, $\Delta_\ell(\theta,u,X) \neq 1$.

Deux cas se présentent :

1er cas : il existe $\ell \in \mathbb{N}_k^o$, tel que $\Delta_\ell(\theta,u,X) = F(\theta,X-\theta u)$.

Sans nuire à la généralité, prenons alors $\ell = 1$.
Nous allons montrer que $F(\theta,X)$ est irréductible dans $L[X]$.

Supposons le contraire :

$F(\theta,X) = g(\theta,X).h(\theta,X)$ où g et h sont deux polynômes unitaires de $L[X]$ avec $d^o g < d^o F$ et $d^o h < d^o G$.

Donc $NF(\theta,X-\theta u) = Ng(\theta,X-\theta u).Nh(\theta,X-\theta u)$.

Comme H_1 est un polynôme irréductible de $K[u,X]$, alors, par exemple, H_1 divise $Ng(\theta,X-\theta u)$ dans $K[u,X]$; aussi $F(\theta,X-\theta u)$ divise $Ng(\theta,X-\theta u)$ dans $(K(\theta,u))[X]$, c'est-à-dire :

$Ng(\theta,X-\theta u) = F(\theta,X-\theta u)G(\theta,u,X)$ avec $G(\theta,u,X) \in (K(\theta,u))[X]$.

Maintenant, il existe $a \in K[\theta,u]$ tel que $a.G(\theta,u,X) \in (K[\theta,u])[X]$, (prenons pour a le dénominateur commun des coefficients de G).

Or, $K[\theta,u] = (K[\theta])[u]$ est un anneau principal algorithmique, puisque $K[\theta]$ est un corps codable et u est une déterminée sur K, aussi, nous savons calculer le contenu d'un polynôme de $(K[\theta,u])[X]$ donc $c(aNg(\theta,X-\theta u)) = c(F(\theta,X-u))c(aG(\theta,u,X))$.

Aussi $a = c(aG(\theta,u,X))$, puisque $Ng(\theta,X-\theta u)$ et $F(\theta,X-\theta u)$ sont unitaires.

Maintenant nous pouvons déterminer $H(\theta,u,X) \in (K[\theta,u])[X]$ tel que

$aG(\theta,u,X) = c(aG(\theta,u,X))H(\theta,u,X) = aH(\theta,u,X)$

d'où $G(\theta,u,X) = H(\theta,u,X)$ et $G(\theta,u,X) \in (K[\theta,u])[X]$

et $Ng(\theta,X-\theta u) = F(\theta,X-\theta u).G(\theta,u,X)$ avec $G(\theta,u,X) \in (K[\theta,u])[X]$.

Cherchons les termes de plus haut degré en X et en u dans $Ng(\theta,X-\theta u)$: posons $m = d^{o}g$, alors ils sont donnés par $\prod_{i=1}^{s} (X-\theta_i u)^m$, puisque $Ng(\theta,X-\theta u) = \prod_{i=1}^{s} g(\theta_i,X-\theta_i u)$ et g unitaire.

Maintenant, cherchons les termes de plus haut degré en X et en u dans $F(\theta,X-\theta u).G(\theta,u,X)$:

posons $n = d^{o}F$ et $F(\theta,X) = \alpha_o + \alpha_1 X + \ldots + \alpha_{n-1}X^{n-1} + X^n$, où $\alpha_i \in L$; donc $F(\theta,X-\theta u) = \alpha_o + \alpha_1(X-u) + \ldots + \alpha_{n-1}(X-\theta u)^{n-1} + (X-\theta u)^n$.

Par conséquent, ils sont donnés par $(X-\theta u)^n G(\theta,u,X)$.

D'après l'égalité $Ng(\theta,X-\theta u) = F(\theta,X-\theta u)G(\theta,u,X)$, nous en déduisons que $(X-\theta u)^n$ divise $\prod_{i=1}^{s} [(X-\theta_i u)^m]$ dans $(K[\theta,u])[X]$,

c'est-à-dire, $\prod_{i=1}^{s} [(X-\theta_i u)^m] = (X-\theta_u)^n h(\theta,u,X)$

avec $h(\theta,u,X) \in (K[\theta,u])[X]$.

Faisons $u = 1$, nous obtenons :

$$\prod_{i=1}^{s} [(X-\theta_i)^m] = (X-\theta)^n h(\theta,1,X).$$

Or, f est le polynôme minimal de θ sur K, donc $f(X) = \prod_{i=1}^{s} (X-\theta_i)$ aussi $f^m(X) = (X-\theta)^n h(\theta,1,X)$.

maintenant θ est séparable, donc $f(X) = (X-\theta)f_1(\theta,X)$ avec $f_1(\theta,X)$ non divisible par $X-\theta$ dans $L[X]$.

Donc $(X-\theta)^m f_1^m(\theta,X) = (X-\theta)^n h(\theta,1,X)$

or $m = d^o g < d^o F = n$.

Alors, $f_1^m(\theta,X) = (X-\theta)^{n-m} h(\theta,1,X)$

comme $n-m > 0$ et $X-\theta$ irréductible, nous avons :

$X-\theta$ divise $f_1(\theta,X)$ dans $L[X]$: contradiction.

Par conséquent, $F(\theta,X)$ est un polynôme irréductible de $L[X]$.

<u>2ème cas</u> : pour tout $\ell \in \mathbb{N}_k^o$, $\Delta_\ell(\theta,u,X) \neq F(\theta,X-\theta u)$.

Pour $\ell = 1$, nous pouvons effectuer la division de $F(\theta,X-u)$ par $\Delta_1(\theta,u,X)$ dans $(K(\theta,u))[X]$; nous obtenons :

$$F(\theta,X-\theta u) = \Delta_1(\theta,u,X).Q_1(\theta,u,X) \quad \text{avec} \quad Q_1(\theta,u,X) \in (K(\theta,u))[X] .$$

de plus, Δ_1 et Q_1 sont unitaires et de degrés en X strictement inférieurs à celui de F.

Maintenant nous pouvons déterminer b et c dans $K[\theta,u]$ tels que $b\Delta_1(\theta,u,X) \in (K[\theta,u])[X]$ et $cQ_1(\theta,u,X) \in (K[\theta,u])[X]$.

donc $(bc)F(\theta,X-\theta u) = b\Delta_1(\theta,u,X).cQ_1(\theta,u,X)$.

Or $K[\theta,u]$ est un anneau principal algorithmique, aussi nous savons calculer le contenu d'un polynôme de $(K[\theta,u])[X]$.

Donc $bc = c(b\Delta_1(\theta,u,X)).c(c.Q_1(\theta,u,X))$ car F est unitaire.

Or, nous pouvons déterminer P et Q deux éléments primitifs de $(K[\theta,u])[X]$ tels que

$$b\Delta_1(\theta,u,X) = c(b\Delta_1(\theta,u,X))P(\theta,u,X)$$

$$cQ_1(\theta,u,X) = c(cQ_1(\theta,u,X))Q(\theta,u,X)$$

donc $F(\theta,X-u) = P(\theta,u,X).Q(\theta,u,X)$

avec P et Q dans $(K[\theta,u])[X]$, de degrés en X strictement inférieurs à celui de F.

Faisons alors $u = 0$, nous obtenons :

$$F(\theta,X) = p(\theta,X)q(\theta,X)$$

avec p et q dans $L[X]$ et de degrés strictement inférieurs à celui de F.

Il nous suffit alors de réappliquer le procédé à p et à q.

Ce procédé est fini, puisque le degré diminue à chaque pas, et nous obtenons

(i) une application récursive qui détermine une décomposition ;

(ii) cette même application décide si un élément est irréductible ou non donc l'ensemble des irréductibles est récursif.

Enfin, pour vérifier que deux irréductibles sont associés ou non, nous comparons les termes de plus haut degré.

54. *Formule d'interpolation de Newton.*

Définition 54.1.- Soit K un corps infini. Considérons $a_0,\ldots,a_n$ n+1 éléments de K, distincts deux à deux, et $b_0,\ldots,b_{n+1}$ n+1 éléments de K.

Définissons :

(i) pour tout $i \in \mathbb{N}_n$, $f(a_i) = b_i$;

(ii) pour tout $k \in \mathbb{N}_n^o$ et pour tout $i \in \{k,k+1,\ldots,n\}$,

$$f(a_0,\ldots,a_{k-1},a_i) = \frac{f(a_0,\ldots,a_{k-2},a_i) - f(a_0,\ldots,a_{k-2},a_{k-1})}{a_i - a_0} .$$

Proposition 54.2.- Soit K un corps infini. Considérons $a_0,\ldots,a_n$ n+1 éléments de K, deux à deux distincts, et $b_0,\ldots,b_n$ n+1 éléments de K.

Définissons $F \in K[X]$ par la formule d'interpolation de Newton :

$$F(X) = f(a_0)+f(a_0,a_1)(X-a_0)+\ldots+f(a_0,\ldots,a_k)(X-a_0)\ldots(X-a_{k-1})+\ldots+f(a_0,\ldots,a_n)(X-a_0)\ldots(X-a_{n-1}).$$

Alors F est l'unique élément de $K[X]$ qui vérifie $d^oF \leqslant n$

et, pour tout $i \in \mathbb{N}_n$, $F(a_i) = b_i$.

Une démonstration est donnée dans

[BLW], Hifssatz 2, § 23, p. 76.

Corollaire 54.2a.- Soit A un anneau commutatif unitaire et intègre, tel que card $A \geqslant \aleph_o$. Posons K son corps des fractions.

Considérons $F \in A[X]$, tel que $d^oF = n$, et $a_o,\ldots,a_n$ $n+1$ éléments distincts de A. Pour tout $i \in \mathbb{N}_n$, posons $b_i = F(a_i)$.

Alors :

(i) F est l'unique polynôme de $K[X]$ qui vérifie $d^oF \leqslant n$ et, pour tout $i \in \mathbb{N}_n$, $F(a_i) = b_i$.

(ii) pour tout $i \in \mathbb{N}$, $f(a_i) \in A$;

(iii) pour tout $k \in \mathbb{N}_n^o$, pour tout $i \in \{k,\ldots,n\}$

$$f(a_o,\ldots,a_{k-1},a_i) \in A.$$

Démonstration :

(i) et (ii) sont évidents.

(iii) d'après la proposition 54.2, nous avons :

$$F(X) = f(a_o) + f(a_o,a_1)(X-a_o)+\ldots+f(a_o,\ldots,a_k)(X-a_o)\ldots(X-a_{k-1})+\ldots$$
$$\ldots + f(a_o,\ldots,a_n)(X-a_o)\ldots(X-a_{n-1}).$$

Or, $F \in A[X]$, aussi, pour tout $k \in \mathbb{N}_n^o$, $f(a_o,\ldots,a_k) \in A$.

Maintenant, $f(a_o,\ldots,a_n) = \dfrac{f(a_o,\ldots,a_{n-2},a_n) - f(a_o,\ldots,a_{n-2},a_{n-1})}{a_n - a_{n-1}}$

donc $f(a_o,\ldots,a_{n-2},a_n) = f(a_o,\ldots,a_{n-1}) + (a_n-a_{n-1})f(a_o,\ldots,a_n)$

aussi $f(a_o,\ldots,a_{n-2},a_n) \in A$.

Ainsi, de proche en proche, le point (iii) est démontré.

55. *Exemples de corps factoriels.*

Lemme 55.1.- Soit A un anneau commutatif unitaire et intègre. Considérons $F \in A[X]$ avec $d^oF = n$. Posons s la partie entière de $\frac{n}{2}$.

Si F est réductible dans $A[X]$, alors F admet un diviseur $G \in A[X]$, tel que $d^oG \leqslant s$.

Lemme 55.2.- Soit A un anneau commutatif unitaire et intègre. Considérons $F \in A[X]$, un polynôme réductible. Si $G \in A[X]-\{0\}$ et G divise F dans $A[X]$, alors, pour tout $a \in A$ tel que $G(a) \neq 0$, $G(a)$ divise $F(a)$ dans A.

Proposition 55.3.- Soit A un anneau factoriel algorithmique tel que card $A^* < \aleph_o$ et card $A \geqslant \aleph_o$.

Alors pour tout élément a non nul et non inversible de A, nous pouvons déterminer explicitement tous les diviseurs de a dans A ; de plus, ils sont en nombre fini.

Démonstration :

Soit a un élément non nul et non inversible de A, alors nous connaissons une application récursive qui permet de déterminer une décomposition. $a = \prod_{j=1}^{k} \pi_j^{n_j}$ en produit fini de facteurs irréductibles de A. Alors tout diviseur d de a dans A est de la forme :

$$d = \varepsilon \prod_{j=1}^{k} \pi_j^{m_j} \quad \text{où} \quad \varepsilon \in A^* \quad \text{et} \quad 0 \leqslant m_j \leqslant n_j .$$

En fixant ε dans A^*, nous obtenons $\prod_{j=1}^{k} (n_j+1)$ diviseurs de a. Posons $\mathcal{D}(a)$ l'ensemble des diviseurs de a dans A ; alors en faisant varier ε dans A^*, nous obtenons tous les diviseurs de a dans A, or card $A^* < \aleph_o$, donc card $\mathcal{D}(a) = (\text{card } A^*).(\prod_{j=1}^{k} (n_j+1))$.

Proposition 55.4.- Soit A un anneau principal. Posons K son corps des fractions. Considérons $H \in A[X]$, irréductible dans $A[X]$.

Alors H est irréductible dans $K[X]$.

Ce résultat est démontré dans : [SZ] Théorème 5, p. 260.

Théorème 55.5.- Soit A un anneau factoriel algorithmique tel que $\text{card } A^* < \aleph_o$ et $\text{card } A = \aleph_o$.

Alors $A[X]$ est un anneau factoriel algorithmique.

Démonstration :

Posons K le corps des fractions de A.

Soit F un polynôme non nul et non inversible de $A[X]$.

Posons $n = d^oF$ et s la partie entière de $\frac{n}{2}$.

Considérons $a_o,\ldots,a_s$ $s+1$ éléments de A, deux à deux distincts. Calculons $F(a_o),\ldots,F(a_s)$. D'après la proposition 55.3, nous savons déterminer $\mathcal{D}_i$ l'ensemble des diviseurs de $F(a_i)$ dans A et $\text{card } \mathcal{D}_i < \aleph_o$.

Pour tout $i \in \mathbb{N}_s$, prenons $d_i \in \mathcal{D}_i$, et, d'après la proposition 53.2, nous savons déterminer explicitement l'unique $G \in K[X]$, tel que $d^oG \leqslant s$ et, pour tout $i \in \mathbb{N}_s$, $G(a_i) = d_i$.

Comme, pour tout $i \in \mathbb{N}_s$, $\text{card } \mathcal{D}_i < \aleph_o$, en faisant varier, pour tout $i \in \mathbb{N}_s$, d_i dans $\mathcal{D}_i$, nous construisons ainsi un nombre fini de polynômes G vérifiant :

pour $d_o,\ldots,d_s$ fixés, G est unique tel que $G \in K[X]$, $d^oG \leqslant s$ et, pour tout $i \in \mathbb{N}_s$, $G(a_i) = d_i$.

Maintenant, supposons que F soit réductible dans $A[X]$ et admette un diviseur $H \in A[X]$ tel que $d^oH = s$.

D'après le lemme 55.2, dès que $H(a_i) \neq 0$, alors $H(a_i)$ divise $F(a_i)$ dans A, donc $H(a_i) \in \mathcal{D}_i$.

Posons $G \in K[X]$, le polynôme construit par la proposition 54.2, tel que $d^oG \leqslant s$ et, pour tout $i \in \mathbb{N}_s$, $G(a_i) = H(a_i)$.

Or, d'après le corollaire 54.2a, H est l'unique polynôme de $K[X]$ vérifiant ces conditions, donc $G = H$.

Par conséquent, si F est réductible dans $A[X]$ et admet un diviseur dans $A[X]$ de degré s, alors celui-ci est parmi les polynômes G construits.

1er cas : aucun des polynômes G construits n'est dans $A[X]$, alors F n'admet pas de diviseur dans $A[X]$ de degré s aussi recommençons le procédé en remplaçant s par s-1.

2ème cas : il existe au moins un des polynômes G construits qui est dans $A[X]$. Posons alors $\mathcal{F}$ l'ensemble des polynômes G construits qui sont dans $A[X]$, donc $\mathcal{F} \neq \emptyset$ et card $\mathcal{F} < \aleph_o$.

Maintenant effectuons, dans $K[X]$, la division de F par tous les éléments de $\mathcal{F}$. Comme K est codable, le procédé est récursif et comme card $\mathcal{F} < \aleph_o$, il est fini.

Alors : - soit il n'existe aucun $G \in \mathcal{F}$ tel que $F = G.H$ où $H \in A[X]$, donc F n'admet aucun diviseur dans $A[X]$ de degré s.

Aussi recommençons en remplaçant s par s-1.

- Soit il existe $G \in \mathcal{F}$ tel que $F = G.H$ où $H \in A[X]$.

Or $d^oG \leqslant s$ donc $d^oH < n$.

Alors nous recommençons avec G et H où $d^oG \leqslant s < n$ et $d^oH < n$. Par conséquent, le procédé est fini. Ce qui nous permet de définir :

(i) une application récursive qui détermine une décomposition.

(ii) cette application décide si un élément est irréductible ou non donc l'ensemble des irréductibles est récursif.

Enfin, pour vérifier que deux éléments irréductibles sont associés ou non, nous comparons les termes de plus haut degré.

Corollaire 55.5a.- Soit A un anneau factoriel algorithmique tel que card $A^* < \aleph_0$ et card $A \geq \aleph_0$. Posons K le corps des fractions de A. Alors K est un corps factoriel.

Corollaire 55.5b - $\mathbb{Q}$ le corps des nombres rationnels est un corps factoriel .

Démonstration :

$\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$, qui est un anneau factoriel algorithmique tel que card $\mathbb{Z} \geq \aleph_0$ et $\mathbb{Z}^* = \{-1,+1\}$, aussi nous pouvons appliquer le corollaire 55.5a.

56. *Anneaux de polynômes sur* $\mathbb{Z}$.

Théorème 56.1.- L'anneau de polynômes en une indéterminée sur $\mathbb{Z}$, est un anneau factoriel algorithmmique.

Démonstration :

Nous utilisons la proposition 52.1. et le corollaire 55.5b.

57. *Corps finis*.

Théorème 57.1.- Tout corps fini, dont le nombre d'éléments est donné, est un corps factoriel.

Démonstration :

Nous faisons référence à l'algorithme de Berlekamp, présenté dans [BER] p. 146-150.

CHAPITRE II

PARTIES GENERATRICES SEPARANTES

L'objet de ce chapitre est de construire, pour H idéal de $A[X]$ où A est un anneau principal algorithmique, une partie génératrice qui permet de déterminer algorithmiquement si un élément quelconque de $A[X]$ est dans H ou non.

Nous adaptons, au cas d'un anneau principal algorithmique, les résultats établis par C.W. Ayoub dans [AY2], pour les anneaux de polynômes sur $\mathbb{Z}$, et, dans la proposition 23.3, nous caractérisons la structure des éléments de cette partie génératrice.

1. PARTIES TRIANGULAIRES ET PARTIES FINIES GENERATRICES SEPARANTES.

11. Notations.

Dans tout le chapitre, nous supposerons que A est un anneau principal algorithmique. Rappelons que dans ce cas, nous possédons une fonction récursive p de $(A^o)^2$ dans $(A^o)^4$, telle que si $p(a,b) = (c,d,e,f)$ alors $a = e.(c.a+d.b)$ et $b = f.(c.a+d.b)$, donc $c.a+d.b$ est le pgcd de a et de b dans A.

Pour tout $F \in A[X]^o$, nous poserons $F = \sum_{i \in I(F)} a_i.X^i$ où $I(F)$ est une partie finie non vide de $\mathbb{N}$, et, pour tout $i \in I(F)$, $a_i \in A^o$. Si nous posons $n = d^oF$, alors $n = \max I(F)$. Dans ce cas, a_n est appelé le coefficient directeur de F et $a_n.X^n$ le terme directeur de F.

Maintenant, pour U une partie de $A[X]$, nous poserons $\mathrm{mod}_A(U)$ le sous-A-module de $A[X]$ engendré par U, et $\mathrm{id}(U)$ l'idéal de $A[X]$ engendré par U.

12. Définitions.

Définition 12.1.- Soit U une partie de $A[X]$. Nous dirons que U est décalée si et seulement si :

(i) U est non vide et $0 \notin U$.

(ii) $\forall F \in U, \ \forall G \in U \quad F \neq G \implies d^oF \neq d^oG$.

Définition 12.2.- Soit T une partie de $A[X]$. Nous dirons que T est triangulaire si et seulement si

(i) T est décalée.

(ii) pour tout $F \in T$ et tout $G \in T$, posons $d^oF = k$ et $d^oG = \ell$. Si $k < \ell$, alors pour tout $j \in \mathbb{N}$ tel que $k < j < \ell$, il existe $F_j \in T$ pour lequel $d^oF_j = j$.

Proposition 12.3.- Soit T une partie finie décalée de $A[X]$. Posons $k = \min\{d^oF | F \in T\}$ et $m = \max\{d^oF | F \in T\}$. Pour que T soit triangulaire, il faut et il suffit que pour tout $j \in \mathbb{N}$ tel que $k \leqslant j \leqslant m$, il existe un unique $F_j \in T$ pour lequel $d^oF_j = j$.

Définition 12.4.- Soit T une partie finie triangulaire de $A[X]$. Posons $m = \max\{d^oF | F \in T\}$, aussi il existe un unique $F_m \in T$ tel que $d^oF_m = m$. Définissons $T^{(1)} \subset A[X]$ par :

$$T^{(1)} = T \cup \{X^jF_m | j \in \mathbb{N}^o\}.$$

Proposition 12.5.- Soit T une partie finie triangulaire de $A[X]$. Alors $T^{(1)}$ est une partie triangulaire de $A[X]$.

De plus, $\min\{d^oF | F \in T^{(1)}\} = \min\{d^oF | F \in T\}$.

Démonstration :

Posons $m = \max\{d^oF \mid F \in T\}$, alors il existe un unique $F_m \in T$ tel que $d^oF_m = m$. Aussi $T^{(1)} = T \cup \{X^jF_m \mid j \in \mathbb{N}^o\}$.

(i) démontrons que $T^{(1)}$ est décalée

comme $T \subset T^{(1)}$, $T^{(1)} \neq \emptyset$. De plus, pour tout $F \in T$, $F \neq 0$ et en particulier $F_m \neq 0$ donc $0 \notin T^{(1)}$.

Maintenant soient G_1 et G_2 dans $T^{(1)}$ tels que $d^oG_1 = d^oG_2$. Si $G_1 \in T$ et $G_2 \in T^{(1)} - T$ alors $d^oG_1 \leqslant m$ et $d^oG_2 \geqslant m+1$, donc $d^oG_1 < d^oG_2$.

Par conséquent, ou bien $G_1 \in T$ et $G_2 \in T$, or T est décalée, aussi $G_1 = G_2$.

ou bien $G_1 \in T^{(1)} - T$ et $G_2 \in T^{(1)} - T$, dans ce cas il existe j et k dans $\mathbb{N}^o$ tels que $G_1 = X^jF_m$ et $G_2 = X^kF_m$.
Comme $d^oG_1 = d^oG_2$ et $d^oF_m = m$, alors $m + j = m + k$
donc $j = k$ aussi $G_1 = G_2$.

Donc $T^{(1)}$ est décalée.

(ii) Soient G_1 et G_2 dans $T^{(1)}$, posons $d^oG_1 = k_1$, $d^oG_2 = k_2$ et supposons que $k_1 < k_2$.

1er cas : $G_1 \in T$ et $G_2 \in T$, puisque T est triangulaire, pour tout $j \in \mathbb{N}$ tel que $k_1 < j < k_2$, il existe $F_j \in T$ tel que $d^oF_j = j$, donc $F_j \in T^{(1)}$.

2ème cas : $G_1 \in T$ et $G_2 \in T^{(1)} - T$, donc $k_1 \leqslant m$ et il existe $j_2 \in \mathbb{N}^o$ tel que $G_2 = X^{j_2}F_m$. Soit $j \in \mathbb{N}$ tel que $k_1 < j < k_2$.

Si $j \leqslant m$ puisque T est triangulaire il existe $F_j \in T$, donc $F_j \in T^{(1)}$, tel que $d^oF_j = j$.

Sinon $j-m \in \mathbb{N}^o$ alors $X^{j-m}F_m \in T^{(1)}$ et $d^o(X^{j-m}F_m) = j$.

3ème cas : $G_1 \in T^{(1)} - T$ et $G_2 \in T^{(1)} - T$, alors il existe j_1 et j_2 dans $\mathbb{N}^o$ tels que $G_1 = X^{j_1}F_m$ et $G_2 = X^{j_2}F_m$. Donc $k_1 = m+j_1$ et $k_2 = m+j_2$; de plus $j_1 < j_2$.

Soit $j \in \mathbb{N}$ tel que $k_1 < j < k_2$.

Alors $j_1 < j-m < j_2$ donc $j-m \in \mathbb{N}^o$

aussi $X^{j-m}F_m \in T^{(1)}$ et $d^o(X^{j-m}F_m) = j$.

Par conséquent $T^{(1)}$ est triangulaire.

13. *Parties génératrices séparantes.*

Lemme 13.1.- Soit U une partie décalée de $A[X]$. Considérons $F \in \mathrm{mod}_A(U)$. Posons $F = \sum_{i=1}^{k} a_i.F_i$ avec $F_i \in U$.

Alors : $d^oF = \max\{d^oF_i \mid i \in \mathbb{N}^o_k \ ; \ a_i \neq 0\}$.

Lemme 13.2.- Soit T une partie finie triangulaire de $A[X]$ qui vérifie :

$$\forall F \in T \qquad X.F \in \mathrm{mod}_A(T^{(1)}).$$

Alors : $X.\mathrm{mod}_A(T^{(1)}) \subset \mathrm{mod}_A(T^{(1)})$.

Démonstration :

Posons $m = \max\{d^oF \mid F \in T\}$ et F_m l'unique élément de T de degré m. Alors $T^{(1)} = T \cup \{X^i.F_m \mid i \in \mathbb{N}\}$.

Prenons $G \in \mathrm{mod}_A(T^{(1)})$, alors $G = G_1 + G_2$ où $G_1 \in \mathrm{mod}_A(T)$ et $G_2 \in \mathrm{id}_{A[X]}(F_m)$.

Or, $X.G_1 \in \mathrm{mod}_A(T^{(1)})$ d'après l'hypothèse faite sur T et $X.G_2 \in \mathrm{id}_{A[X]}(F_m)$. Comme $\mathrm{id}_{A[X]}(F_m) \subset \mathrm{mod}_A(T^{(1)})$ alors le lemme est démontré.

Théorème 13.3.- Soit T une partie finie triangulaire de $A[X]$ qui vérifie :

$$\forall F \in T \qquad X.F \in \mathrm{mod}_A(T^{(1)}).$$

Posons $H = \mathrm{id}_{A[X]}(T)$. Nous avons les résultats suivants :

(i) $H = \mathrm{mod}_A(T^{(1)})$.

(ii) posons $m = \max\{d^oF \mid F \in T\}$ alors $\mathrm{mod}_A(T) = \{F \in H \mid d^oF \leq m\}$.

(iii) (a) Si $F \in T$ et $d^oF < m$ alors $X.F = \sum_{G \in T} a_F(G).G$, $a_F(G) \in A$.

(b) Les relations $XF - \sum_{G \in T} a_F(G).G = 0$ engendrent le $A[X]$ module des relations entre les éléments de T.

Démonstration :

(i) D'après le lemme 13.2, $\mathrm{mod}_A(T^{(1)})$ est un idéal de $A[X]$. contenu dans H et contenant T. Par définition de $H = \mathrm{id}_{A[X]}(T)$ alors $H = \mathrm{mod}_A(T^{(1)})$.

(ii) De façon évidente, $\mathrm{mod}_A(T) \subset \{F \in H \mid d^oF \leq m\}$.

Maintenant, soit $F \in H$ tel que $d^oF \leq m$.

Comme $H = \mathrm{mod}_A(T^{(1)})$, $F \in \mathrm{mod}_A(T^{(1)})$, alors, en utilisant le lemme 13.1, $F \in \mathrm{mod}_A(T)$.

(iii) (a) Soit $F \in T$ tel que $d^oF < m$ donc $X.F \in H$ et $d^o(XF) \leq m$ alors, d'après (ii), $XF = \sum_{G \in T} a_F(G).G$ avec $a_F(G) \in A$.

(b) Soit $\sum_{F \in T} x_F F = 0$ avec $x_F \in A[X]$.

Posons alors $d = \max\{d^o x_F \mid d^oF < m\}$.

Modulo les relations définies en (a), nous pouvons nous ramener à $d = 0$. Mais, lorsque $d = 0$, nous obtenons une relation à coefficients

dans A entre les éléments de $T^{(1)}$ et celle-ci est donc nulle.

Définition 13.4.- Soit H un idéal non nul de $A[X]$, admettant T une partie finie triangulaire de $A[X]$, comme partie génératrice.

Nous dirons que T est une partie finie génératrice séparante de H si et seulement si $H = \mathrm{mod}_A(T^{(1)})$.

2. ALGORITHME POUR CONSTRUIRE UNE PARTIE FINIE GENERATRICE SEPARANTE.

21. *Algorithme* Δ : *construction d'une partie finie génératrice triangulaire*.

21.1.- *Algorithme* Δ.

Entrée : U une partie finie non vide et non nulle de $A[X]$.

Sortie : T une partie finie triangulaire de $A[X]$.

Sous programme : p.

Début : $T = U - \{0\}$;

Tant que T possède deux éléments distincts de même degré faire :

Début Tq : n : = plus grand entier naturel j tel que T possède moins deux éléments de même degré j ;

q : = nombre d'éléments de T de degré n ;

$H_1,\ldots,H_q$ sont les q éléments de T de degré n;

pour tout $k \in \mathbb{N}_q^o$, a_k : = coefficient directeur de H_k ;

utiliser p pour déterminer $\alpha_1,\ldots,\alpha_q,\beta_1,\ldots,\beta_q$ que $\sum_{k=1}^{q} \alpha_k.a_k$ soit le pgcd des a_i dans A et $\beta_1,\ldots,\beta_q$ les quotients respectifs ;

d : = $\sum_{k=1}^{q} \alpha_k.a_k$; H : = $\sum_{k=1}^{q} \alpha_k.H_k$;

T : = $T - \{H_1,\ldots,H_q\}$; T : = $T \cup \{H, H_1-\beta_1.H,\ldots,H_q-\beta_q.H\}$;

Fin de Tq.

Ranger les éléments de T par ordre des degrés croissants ;

$s := \mathrm{card}(T)$; $F_1,\ldots,F_s$ sont les s éléments de T rangés dans l'ordre ;

pour tout $k \in \mathbb{N}_s^o$ $i_k := d^oF_k$; $j := 1$;

Tant que $j < s$ faire

Début Tq : si $i_{j+1} \neq i_j+1$ alors

début de si : $\ell := i_{j+1}-i_j$;

$T := T \cup \{X.F_j,\ldots,X^{\ell-1}.F_j\}$;

fin de si

$j := j + 1$;

Fin Tq.

Fin.

Proposition 21.2.- Soit U une partie finie non vide et non nulle de $A[X]$. Alors l'algorithme Δ appliqué à U s'arrête au bout d'un nombre fini d'opérations.

Notons $T = \Delta(U)$ le résultat de l'algorithme Δ appliqué à U. Alors T est une partie finie triangulaire de $A[X]$ telle que $\mathrm{id}_{A[X]}(U) = \mathrm{id}_{A[X]}(T)$.

Démonstration :

Pour le premier tant que, remarquons $d^o(H_k - \beta_k.H) < d^oH$, par conséquent, n décroît à chaque itération du premier tant que donc celui-ci s'arrête.

De plus, comme $\mathrm{id}_{A[X]}(H_1,\ldots,H_q) = \mathrm{id}_{A[X]}(H,H_1-\beta_1,\ldots,H_q-\beta_q.H)$, l'idéal engendré n'est pas modifié.

Ensuite, il est évident que le second tant que cesse (borné par s-1 itérations) et l'idéal engendré n'est pas modifié.

Par conséquent, l'algorithme Δ est fini et posons $T = \Delta(U)$ le résultat final, donc $id_{A[X]}(U) = id_{A[X]}(T)$.

De plus, il est facile de voir que T vérifie la proposition 12.3. Alors T est triangulaire et finie.

Corollaire 21.2a.- Soit U une partie finie non vide et non nulle de $A[X]$. Posons $T = \Delta(U)$. Alors :

$$\max\{d^oF \mid F \in T\} = \max\{d^oF \mid F \in U\}.$$

Corollaire 21.2b.- Soit U une partie fini non vide et non nulle de $A[X]$. Posons $T = \Delta(U)$. Alors :

$$mod_A(U) \subset mod_A(T).$$

Démonstration :

A chaque itération du premier tant que, nous remplaçons $H_1,\ldots,H_q$ par $H = \sum_{k=1}^{q} \alpha_k.H_k$ et $H_1-\beta_1.H,\ldots,H_q-\beta_q.H$.

Par conséquent, le A module engendré n'est pas modifié, après le premier tant que.

Comme pendant le second tant que, nous ajoutons des éléments, nous obtenons alors :

$$mod_A(U) \subset mod_A(T).$$

22. *Algorithme* R.

Soit $H \in A[X]$, nous poserons coef-dir(H) le coefficient directeur de H et ter-dir(H) le terme directeur de H.

22.1.- Algorithme R.

Entrées : T partie finie triangulaire de $A[X]$ et $H \in A[X]$.

Sortie : $R(T,H) \in A[X]$.

Début : Si $H = 0$ alors retourner 0 ;

Sinon

début : Si (il existe $F \in T^{(1)}$ avec $d^oF = d^oH$ et il existe $\gamma \in A$ tel que γ.coef-dir(F) = coef-dir(H)) alors retourner $R(T,H-\gamma.F)$;

Sinon retourner ter-dir(H)+R(T,H-ter-dir(H)) ;

fin.

Fin.

Proposition 22.2.- Soit T une partie finie triangulaire de $A[X]$. Alors, pour tout $H \in A[X]$, l'algorithme R s'arrête au bout d'un nombre fini d'opérations.

De plus, pour tout $H \in A[X]$, $R(T,H) \in H + \mathrm{mod}_A(T^{(1)})$ et $d^oR(T,H) \leq d^oH$.

Démonstration :

Pour $H = 0$, nous obtenons $R(T,0) = 0$: c'est fini.

Pour $H \neq 0$, 1er cas : la condition du si est remplie alors nous recommençons avec $H-\gamma.F$ tel que $d^o(H-\gamma.F) < d^oH$.

2ème cas : Sinon, nous recommençons avec H-ter-dir(H) tel que $d^o(H-\text{ter-dir}(H)) < d^oH$.

Par conséquent, à chaque étape, le degré décroît donc l'algorithme R cesse.

Pour le second résultat, procédons par récurrence.

Fixons $k = \inf\{d^oF \mid F \in T\}$. Considérons $H \in A[X]$, $H \neq 0$, tel que

$d^oH < k$. Alors la condition du si n'est pas remplie. Donc nous obtenons $R(T,H) = \text{ter-dir}(H) + R(T,H-\text{ter-dir}(H))$.

Mais $d^o(H-\text{ter-dir}(H)) < d^oH < k$, alors à chaque étape, la condition du si n'est pas remplie, d'où $R(T,H) = H$.

Nous en déduisons que pour tout $H \in A[X]$, $H \neq 0$ et $d^oH < k$, le second résultat est vrai.

Faisons alors l'hypothèse suivante : $n \geq k$, pour tout $H \in A[X]$, $H \neq 0$ et $d^oH < n$, $R(T,H) \in H + \text{mod}_A(T^{(1)})$ et $d^oR(T,H) \leq d^oH$.

Soit $G \in A[X]$, $G \neq 0$, $d^oG = n$.

- s'il existe $F \in T^{(1)}$ avec $d^oF = d^oG$ et s'il existe $\gamma \in A$ tel que $\gamma.\text{coef-dir}(F) = \text{coef-dir}(G)$ alors $R(T,G) = R(T,G-\gamma.F)$ mais $d^o(G-\gamma.F) < n$ aussi $R(T,G-\gamma.F) \in (G-\gamma.F) + \text{mod}_A(T^{(1)})$ et $d^oR(T,G-\gamma.F) \leq d^o(G-\gamma.F)$.
  Or, $F \in T^{(1)}$ alors $R(T,G) \in G + \text{mod}_A(T^{(1)})$ et $d^oR(T,G) \leq d^oG$.

- sinon $R(T,G) = \text{ter-dir}(G) + R(T,G-\text{ter-dir}(G))$.
  mais $d^o(G-\text{ter-dir}(G)) < n$ aussi nous avons
  $R(T,G-\text{ter-dir}(G)) \in (G-\text{ter-dir}(G)) + \text{mod}_A(T^{(1)})$ et
  $d^oR(T,G-\text{ter-dir}(G)) \leq d^o(G-\text{ter-dir}(G))$.
  Donc $R(T,G) \in G + \text{mod}_A(T^{(1)})$ et $d^oR(T,G) \leq d^oG$.

Corollaire 22.2a.- Soit T une partie finie triangulaire de $A[X]$. Pour tout $H \in A[X]$, pour que $H \in \text{mod}_A(T^{(1)})$ il faut et il suffit que $R(T,H) = 0$.

Démonstration :

Supposons d'abord $H \in \text{mod}_A(T^{(1)})$.

Comme $T^{(1)}$ est triangulaire, nous pouvons écrire :

$H = a_1.F_1 + \ldots + a_n.F_n$ avec $a_i \in A^o$, $F_i \in T^{(1)}$

et $d^oF_1 < \ldots < d^oF_n$.

D'après le lemme 13.1, $d^oH = d^oF_n$.

De plus, $a_n.\text{coef-dir}(F_n) = \text{coef-dir}(H)$. Donc la condition du si est remplie et nous obtenons $R(T,H) = R(T,H-a_nF_n) = R(T, \sum_{i=1}^{n-1} a_i.F_i)$.

A chaque itération, la condition du si est remplie et à la j-ème nous obtenons $R(T,H) = R(T, \sum_{i=1}^{n-j} a_i.F_i)$.

Par conséquent, à la n-ième, $R(T,H) = 0$.

Réciproquement, d'après le second résultat de 22.2, nous obtenons $H \in \text{mod}_A(T^{(1)})$.

23. *Algorithme* Θ : *construction d'une partie finie génératrice séparante.*

23.1.- *Algorithme* Θ .

Entrée : U une partie finie non vide et non nulle de $A[X]$.

Sortie : T une partie finie génératrice séparante de $id_{A[X]}(U)$.

Sous programmes : algorithme Δ, algorithme R.

Début : $T := \Delta(U)$;

S'il existe $F \in T$ tel que $R(T,X.F) \neq 0$

alors retourner $\Theta(T \cup \{R(T,X.F)\})$;

Sinon retourner T ;

Fin.

Théorème 23.2.- Soit H un idéal non nul de $A[X]$, donné par U un système fini de générateurs. Alors nous avons les résultats suivants :

(i) l'algorithme Θ appliqué à U s'arrête au bout d'un

nombre fini d'opérations.

(ii) Posons $T = \Theta(U)$ le résultat de l'algorithme Θ appliqué à U. Alors T est une partie finie génératrice séparante de H.

Démonstration :

(i) Posons $m = \max\{d^{o}F \mid F \in U\}$ et $M = \mathrm{mod}_A\{1, X, .., X^m\}$.

Alors M est un module libre de rang m sur A anneau principal, donc M est un A module noethérien.

De plus, $\mathrm{mod}_A(U) \subset M$.

Nous posons $T = \Delta(U)$ alors d'après le corollaire 21.2a, $\mathrm{mod}_A(T) \subset M$ et d'après le corollaire 21.2b, $\mathrm{mod}_A(U) \subset \mathrm{mod}_A(T)$.

Ensuite :

1er cas : La condition du si est remplie, alors $T_1 := \Delta(T \cup \{R(T, X.F)\})$ et nous recommençons.
Mais, en posant F_m l'unique élément de degré m de T, $F \neq F_m$; puisque $R(T, X.F) \neq 0$. Donc $d^{o}F < m$ et $d^{o}R(T, XF) \leq m$.
Par conséquent, $\mathrm{mod}_A(U) \subset \mathrm{mod}_A(T) \subset \mathrm{mod}_A(T_1) \subset M$.

2ème cas : Sinon l'algorithme cesse.

Donc, dans le 1er cas, nous construisons une chaîne croissante de sous A-modules de M, A module noethérien. Alors celle-ci est stationnaire et nous aboutissons au 2ème cas.

(ii) Posons $T = \Theta(U)$ le résultat final, alors, puisque l'algorithme cesse, pour tout $F \in T$, $R(T, X.F) = 0$ ce qui est équivalent à $X.F \in \mathrm{mod}_A(T^{(1)})$ (corollaire 22.2a).

D'après le théorème 13.3, T est donc une partie finie génératrice séparante de H. (Le fait que $H = \mathrm{id}_{A[X]}(T)$ provient de l'utilisation de l'algorithme Δ).

Corollaire 23.2a.- Soit H un idéal non nul de $A[X]$, donné par U un système fini de générateurs. Alors pour tout $F \in A[X]$, nous pouvons déterminer algorithmiquement si $F \in H$ ou si $F \notin H$.

Démonstration :

En utilisant l'algorithme Θ, nous obtenons $T = \Theta(U)$ une partie finie génératrice séparante de H. Donc $H = \mathrm{mod}_A(T^{(1)})$.

Déterminons alors $R(T,F)$. D'après le corollaire 22.2a, nous avons $F \in H$ si et seulement si $R(T,F) = 0$.

Les résultats de la proposition suivante ont été démontrés indépendamment par D. Lazard pour les bases de Gröbner dans le cas de deux indéterminées sur un corps (cf. [LAZ 3]).

Proposition 23.3.- Soit U une partie finie non vide et non nulle de $A[X]$.

Considérons $T = \Theta(U)$ et posons $T = \{F_1,\ldots,F_n\}$ rangée par ordre des degrés croissants. Alors :

(i) le pgcd dans $A[X]$ des éléments de T est égal à celui des éléments de U.

(ii) nous pouvons déterminer un polynôme primitif H de $A[X]$ et pour tout $i \in \mathbb{N}_n^o$ un polynôme unitaire H_i de $A[X]$ avec $d^oH_i = i-1$, tels que $F_i = c(F_i).H.H_i$, où $c(F_i)$ est le contenu de F_i.

(iii) pour tout $i \in \mathbb{N}_{n-1}^o$, $c(F_{i+1})$ divise $c(F_i)$.

Démonstration :

(i) Posons $U = \{G_1,\ldots,G_k\}$. D'après I, 45.6, puisque A est principal algorithmique, nous savons déterminer G (resp. F) le pgcd dans $A[X]$ des G_i (resp. des F_j).

Or pour tout $i \in \mathbb{N}_k^o$, $G_i = \sum_{j=1}^{n} \alpha_{i,j}.F_j$ avec $\alpha_{i,j} \in A[X]$,

et $F_j = \sum_{i=1}^{k} \beta_{j,i}.G_i$ avec $\beta_{j,i} \in A[X]$.

Donc $F = G$ aux inversibles de A près.

(ii) T est une partie finie génératrice séparante de $id_{A[X]}(U)$.

Donc, pour tout $F \in T$, $X.F \in mod_A(T^{(1)})$.

En particulier, $X.F_1 \in mod_A(T^{(1)})$. Mais $d^o(X.F_1) = 1+d^oF_1 = d^oF_2$.

donc $X.F_1 = a_{12}.F_2+a_{11}.F_1$ et $a_{12} \neq 0$.

Alors $a_{12}.F_2 = (X-a_{11}).F_1$.

En utilisant I, 45.3, nous pouvons déterminer $F_1 = c(F_1).H$ où $c(F_1)$ est le contenu de F_1 et $H \in A[X]$, primitif. Donc $d^oH = d^oF_1$.

Alors $a_{12}.F_2 = (X-a_{11}).c(F_1).H$. En passant aux contenus, nous obtenons $a_{12}.c(F_2) = c(F_1)$, d'où $F_2 = c(F_2).H.(X-a_{11})$.

Posons $H_1 = 1$ et $H_2 = X-a_{11}$.

Nous venons d'établir : $F_1 = c(F_1).H.H_1$

$F_2 = c(F_2).H.H_2$

avec H primitif, $d^oH = d^oF_1$, H_1 et H_2 unitaires, $d^oH_1 = 0$, $d^oH_2 = 1$ et $c(F_2)$ divise $c(F_1)$.

Faisons alors l'hypothèse suivante :

Soit $q \in \mathbb{N}_n^o$ et $q > 2$. Pour tout $i \in \mathbb{N}_{q-1}^o$, nous avons déterminer un polynôme unitaire $H_i \in A[X]$, $d^oH_i = i-1$ tel que $F_i = c(F_i).H.H_i$, et, pour tout $i \in \mathbb{N}_{q-2}^o$, $c(F_{i+1})$ divise $c(F_i)$.

Or $X.F_{q-1} \in mod_A(T^{(1)})$ et $d^o(X.F_{q-1}) = 1 + d^oF_{q-1} = d^oF_q$,

donc $X.F_{q-1} = a_{q-1,q}.F_q + a_{q-1,q-1}.F_{q-1} + \ldots + a_{q-1,1}.F_1$.

alors $a_{q-1,q}.F_q = (X-a_{q-1,q-1}).F_{q-1} - a_{q-1,q-2}.F_{q-2} - \dots - a_{q-1,1}.F_1$,

et $a_{q-1,q}.F_q = ((X-a_{q-1,q-1}).c(F_{q-1}).H_{q-1} - a_{q-1,q-2}.c(F_{q-2}) - \dots - a_{q-1,1}.c(F_1).H_1).H$.

Mais, pour tout $j \in \mathbb{N}^o_{q-2}$, $c(F_{q-1})$ divise $c(F_j)$, donc $c(F_j) = b_j.c(F_{q-1})$.

Alors :

$a_{q-1},q.F_q = c(F_{q-1}).((X-a_{q-1,q-1}).H_{q-1} - a_{q-1,q-2}.b_{q-2}.H_{q-2} - \dots - a_{q-1,1}.b_1.H_1).H$.

Posons $H_q = (X-a_{q-1,q-1}).H_{q-1} - a_{q-1,q-2}.b_{q-2}.H_{q-2} - \dots - a_{q-1,1}.b_1.H_1$, alors H_q est unitaire et $d^oH_q = 1 + d^oH_{q-1} = q-1$.

En passant aux contenus, nous obtenons $a_{q-1,q}.c(F_q) = c(F_{q-1})$. Par conséquent, $F_q = c(F_q).H.H_q$ avec H_q unitaire de degré $q-1$ et $c(F_q)$ divise $c(F_{q-1})$.

D'où les points (ii) et (iii) démontrés par récurrence.

Corollaire 23.3a.- Sous les mêmes notations et hypothèses que 23.3, posons, pour $i \in \mathbb{N}^o_{n-1}$, $c(F_i) = d_i.c(F_{i+1})$.

Alors pour tout $i \in \mathbb{N}^o_{n-1}$ et pour tout $k \in \mathbb{N}$, tel que $1 \leqslant k \leqslant n-i$, nous avons $H_{i+k} \in id_{A[X]}(d_i, H_{i+1})$.

Démonstration :

Fixons $i \in \mathbb{N}^o_{n-1}$. De façon évidente, $H_{i+1} \in id_{A[X]}(d_i, H_{i+1})$. Prenons $k \in \mathbb{N}$, $1 < k \leqslant n-i$ et faisons l'hypothèse suivante : pour tout $j \in \mathbb{N}$, $1 \leqslant j < k$, $H_{i+j} \in id_{A[X]}(d_i, H_{i+1})$.

Or $X.F_{i+k-1} \in mod_A(T^{(1)})$, donc nous avons :

$X.F_{i+k-1} = a_{i+k-1,i+k}.F_{i+k} + a_{i+k-1,i+k-1}.F_{i+k-1} + \dots + a_{i+k-1,1}.F_1$.

Isolons $a_{i+k-1,i+k}.F_{i+k}$ et simplifions par H (cf. 23.3). Nous obtenons :

$$a_{i+k-1,i+k}.c(F_{i+k}) = (X-a_{i+k-1,i+k-1}).c(F_{i+k-1}).H_{i+k-1} - a_{i+k-1,i+k-2}.c(F_{i+k-2}).H_{i+k-2}$$
$$- \ldots - a_{i+k-1,i+1}.c(F_{i+1}).H_{i+1} - a_{i+k-1,i}.c(F_i).H_i - \ldots$$
$$\ldots - a_{i+k-1,1}.c(F_1).H_1.$$

Utilisons 23.3 (iii) : pour $1 \leqslant j \leqslant i-1$, $c(F_j) = b_j.c(F_i)$

pour $i+1 \leqslant j \leqslant i+k-2$, $c(F_j) = b_j.c(F_{i+k-1})$.

D'où

$$a_{i+k-1,i+k}.c(F_{i+k}).H_{i+k} = c(F_{i+k-1})\left[(X-a_{i+k-1,i+k-1})H_{i+k-1}\right.$$
$$- a_{i+k-1,i+k-2}.b_{i+k-2}.H_{i+k-2} - \ldots -$$
$$\left. - a_{i+k-1,i+1}.b_{i+1}.H_{i+1}\right] - c(F_i).\left[a_{i+k-1,i}.H_i + \ldots\right.$$
$$\left. \ldots + a_{i+k-1,1}.b_1.H_1\right].$$

Or, $c(F_i) = d_i.c(F_{i+1}) = d_i.b_{i+1}.c(F_{i+k-1})$ et, en passant aux contenus, $a_{i+k-1,i+k}.c(F_{i+k}) = c(F_{i+k-1})$, donc

$$H_{i+k} = (X-a_{i+k-1,i+k-1})H_{i+k-1} - a_{i+k-1,i+k-2}.b_{i+k-2}.H_{i+k-2} - \ldots$$
$$- a_{i+k-1,i+1}.b_{i+1}.H_{i+1} - d_i.b_{i+1}\left[a_{i+k-1,i}.H_i + \ldots + a_{i+k-1,1}.b_1.H_1\right].$$

D'après l'hypothèse faite, $H_{i+k} \in id_{A[X]}(d_i, H_{i+1})$.

Par conséquent, pour tout $k \in \mathbb{N}$, $1 \leqslant k \leqslant n-i$, $H_{i+k} \in id_{A[X]}(d_i, H_{i+1})$.

Comme cela reste vrai pour tout $i \in \mathbb{N}^{o}_{n-1}$, le corollaire 23.3 est démontré.

Corollaire 23.3b.- Sous les mêmes notations et hypothèses que 23.3, nous avons :

(i) $c(F_n).H$ est le pgcd dans $A[X]$ des éléments de T ;

(ii) Pour que $d^{o}F_1 > 0$ il faut et il suffit que les éléments de U admettent un pgcd non constant dans $A[X]$.

Démonstration :

Le point (i) est une conséquence des points (ii) et (iii) de 23.3.

Le point (ii) est une conséquence du point (i) de 23.3b et du point (i) de 23.3.

Corollaire 23.3c.- Sous les mêmes notations et hypothèses que 23.3, pour tout $i \in \mathbb{N}_n^o$, nous pouvons déterminer $c(F_i) = b_i.c(F_n)$.
Alors :

(i) $\{b_1.H_1,\ldots,b_n.H_n\}$ est une partie finie génératrice séparante de $id_{A[X]}(b_1.H_1,\ldots,b_n.H_n)$.

(ii) $id_{A[X]}(U) = id_{A[X]}(T) = id_{A[X]}(c(F_n).H).id_{A[X]}(b_1.H_1,\ldots,b_n.H_n)$.
(Remarquons que $b_n = 1$).

Démonstration :

Pour le point (i), nous écrivons que T est une partie finie génératrice séparante de $id_{A[X]}(U)$, c'est-à-dire, pour tout $F \in T$, $X.F \in mod_A(T^{(1)})$. Nous divisons cette condition par $c(F_n).H$ et nous obtenons la même condition pour $\{b_1.H_1,\ldots,b_n.H_n\}$.

Le point (ii) se vérifie par un calcul simple.

Proposition 23.4.- Soit H un idéal non nul de $A[X]$, donné par U un système fini de générateurs. Posons $T = \Theta(U)$ et $k = \min\{d^oF \mid F \in T\}$.

(i) si $k > 0$ alors $H \cap A = \{0\}$.

(ii) sinon ; alors il existe un unique $F_o \in T$ tel que $d^oF_o = 0$ et $H \cap A = id_A(F_o)$.

Démonstration :

T est une partie finie génératrice séparante de H, donc $H = mod_A(T^{(1)})$.

(i) D'après la proposition 12.5, $\min\{d^oF \mid F \in T^{(1)}\} = \min\{d^oF \mid F \in T\}$, par conséquent, pour tout $G \in H$, $d^oG \geq k$. Donc $H \cap A = \{0\}$.

(ii) Donc $F_o \in A$ et $id_A(F_o) \subset H \cap A$.

Maintenant, soit $a \in H \cap A$, comme $H = mod_A(T^{(1)})$ et $T^{(1)}$ triangulaire, alors $a = b.F_o$. Donc $H \cap A = id_A(F_o)$.

3. PARTIES FINIES GENERATRICES SEPARANTES MINIMALES.

31. Invariants d'un idéal de $A[X]$.

Définition 31.1.- Soit H un idéal non nul de $A[X]$, donné avec U un système fini de générateurs. Définissons :

(i) $I_{-1} = \{0\}$.

(ii) Pour tout $j \in \mathbb{N}$, $I_j = \{a \in A \mid a\,X^j$ soit le terme directeur d'un $F \in H\} \cup \{0\}$.

Proposition 31.2.- Soit H un idéal non nul de $A[X]$, donné avec U un système fini de générateurs. Posons T la partie fini génératrice séparante de H obtenue par l'algorithme Θ appliqué à U. Alors nous avons les résultats suivants :

(i) Pour tout $j \in \mathbb{N}$, I_j est un idéal principal de A, engendré par le coefficient directeur de l'élément de degré j de $T^{(1)}$, lorsqu'il existe. De plus, pour tout $j \in \mathbb{N}$, $I_j \subset I_{j+1}$.

(ii) $\exists\, s \in \mathbb{N} \quad I_{s-1} \subset_{\neq} I_s \;\wedge\; \forall\, j \in \mathbb{N} \quad I_{s+j} = I_s$.

(iii) $\exists\, r \in \mathbb{N} \quad I_r \neq \{0\} \;\wedge\; \forall\, j \in \mathbb{N} \cup \{-1\} \quad j < r \Longrightarrow I_j = \{0\}$.

Démonstration :

(i) Il est clair que I_j est un idéal de A et, comme H est un idéal, $I_j \subset I_{j+1}$.

Posons $k = \min\{d^oF \mid F \in T\}$. Soit $j \in \mathbb{N}$ avec $j \geq k$, alors il existe $G \in T^{(1)}$ tel que $d^oG = j$. Posons a_j le coefficient directeur de G. En particulier, $a_j \in I_j$.

Prenons $a \in I_j^o$ alors il existe $F \in H$ tel que aX^j soit le terme directeur de F. Or $H = \mathrm{mod}_A(T^{(1)})$ et $T^{(1)}$ est triangulaire, aussi nous pouvons écrire $F = \sum_{i=1}^{q} \alpha_i G_i$ où pour tout $i \in \mathbb{N}_q^o$, $\alpha_i \in A$ et $G_i \in T^{(1)}$, de plus $d^oG_1 < \ldots < d^oG_q$.

Donc $d^oF = d^oG_q = j$. Comme $T^{(1)}$ est triangulaire, $G = G_q$.

Par conséquent, $a = \alpha_q a_j$. Alors, $I_j = A.a_j$.

(ii) Comme A est noethérien et que la suite $(I_j)_{j\in\mathbb{N}}$ est une suite croissante d'idéaux de A, elle est donc stationnaire.

Posons $\ell = \sup\{i \in \mathbb{N} \mid I_i \neq I_{i+1}\}$ et prenons $s = \ell+1$.

(iii) Puisque H est un idéal non nul de $A[X]$, il existe $i \in \mathbb{N}$ tel que $I_i \neq \{0\}$; prenons $r = \inf\{i \in \mathbb{N} \mid I_i \neq \{0\}\}$.

Corollaire 31.2a.- Sous les mêmes hypothèses et notations que dans 31.2, nous avons :

$$\{0\} = I_{r-1} \underset{\neq}{\subset} I_r \subset \ldots \subset I_{s-1} \underset{\neq}{\subset} I_s = I_{s+j} ,$$

pour tout $j \in \mathbb{N}$. De plus, les entiers r et s ne dépendent que de H.

Définition 31.3.- Soit H un idéal non nul de $A[X]$, donné par U un système fini de générateurs.

Nous poserons $r(H) = r$ et $s(H) = s$ où r et s sont les entiers naturels définis dans la proposition 31.2, ne dépendants que de H.

La proposition suivante va nous permettre de calculer effectivement $r(H)$ et de fixer un majorant effectif pour $s(H)$.

Proposition 31.4.- Soit H un idéal non nul de $A[X]$, donné par U un système fini de générateurs. Posons T la partie finie génératrice séparante de H obtenue par l'algorithme Θ appliqué à U. Alors, nous avons les résultats suivants :

(i) $r(H) = k(T)$

(ii) $s(H) \leqslant m(T)$

où $k(T) = \min\{d^oF \mid F \in T\}$ et $m(T) = \max\{d^oF \mid F \in T\}$.

Démonstration :

(i) d'après la définition de $k(T)$ il existe $G \in T$ tel que $d^oG = k(T)$. Donc $I_{k(T)} \neq \{0\}$ d'où $r(H) \leqslant k(T)$.

Maintenant soit $H \in H^o$, or $H = \mathrm{mod}_A(T^{(1)})$ et $T^{(1)}$ est triangulaire, aussi nous pouvons écrire :

$$H = \sum_{i=1}^{q} \alpha_i G_i \quad \text{où pour tout } i \in \mathbb{N}_q^o \ \alpha_i \in A^o \text{ et } G_i \in T^{(1)}$$
$$\text{et } d^oG_1 < \ldots < d^oG_q.$$

Aussi $d^oH = d^oG_q$. Comme $\min\{d^oF \mid F \in T\} = \min\{d^oF \mid F \in T^{(1)}\}$ alors $d^oG_q \geqslant k(T)$. Par conséquent, pour tout $H \in H^o$, $d^oH \geqslant k(T)$ donc $r(H) \geqslant k(T)$.

D'où, finalement, $r(H) = k(T)$.

(ii) Posons $m = m(T)$ et F_m l'unique élément de T de degré m.

Soit a_m le coefficient directeur de F_m.

D'après la proposition 31.2, $I_m = A.a_m$.

Considérons I_{m+j} où $j \in \mathbb{N}$.

Alors il existe $G \in T^{(1)}$ tel que $d^oG = m+j$. D'après la définition de $T^{(1)}$, $G = X^jF_m$; par conséquent, le coefficient directeur de G est a_m et, d'après la proposition 31.2, $I_{m+j} = Aa_m$.

Aussi, pour tout $j \in \mathbb{N}$, $I_{m+j} = I_m$

c'est-à-dire $s(H) \leqslant m(T)$, puisque $m = m(T)$.

Corollaire 31.4a.- Sous les mêmes hypothèses et notations que 31.4, $k(T)$ est indépendant de la partie génératrice séparante T déterminée pour H.

32. *Définition et caractérisation des parties finies génératrices séparantes minimales.*

Définition 32.1.- Soit H un idéal non nul de $A[X]$, donné par U un système fini de générateurs. Une partie finie génératrice séparante T de H est dite minimale si et seulement si elle ne contient strictement aucune autre partie finie génératrice séparante de H.

Théorème 32.2.- Soit T une partie finie triangulaire de $A[X]$ et posons $H = id(T)$. Les assertions suivantes sont équivalentes :

(i) T est une partie génératrice séparante minimale de H ;

(ii) T est une partie génératrice séparante de H pour laquelle $m(T) = s(H)$.

(iii) T est une partie finie génératrice séparante de H qui vérifie il existe $F \in T$ de terme directeur aX^m où $a \in A^o$ et $m = m(T)$, mais il n'existe aucun $G \in T$ de terme directeur $\varepsilon\, a\, X^{m-1}$, où $\varepsilon \in A^*$.

Démonstration : Posons $m = m(T)$ et $s = s(H)$.

Supposons (i). D'après la proposition 31.4, $s \leqslant m$.

Si $m \neq s$ alors $I_m = I_{m-1}$.

Posons F_{m-1} l'unique élément de degré $m-1$ de T, alors il existe $\varepsilon \in A^*$ tel que εa_m soit le coefficient directeur de F_{m-1}.

Maintenant, posons $T' = \{F \in T | d^oF < m\}$ et nous allons démontrer que T' est une partie finie génératrice séparante de H.

D'abord, montrons que $\mathrm{mod}_A(T') = \{F \in H | d^oF < m\}$.

Nous savons que T est une partie finie triangulaire de $A[X]$, aussi $T' = T - \{F_m\}$ est une partie finie triangulaire de $A[X]$.

Comme $T' = \{F \in T | d^oF < m\}$, $\mathrm{mod}_A(T') \subset \{F \in H | d^oF < m\}$.

Prenons $H \in H$ tel que $d^oH < m$.

Or T est une partie finie génératrice séparante de H, donc $\mathrm{mod}_A(T) = \{F \in H | d^oF < m\}$. D'où $H \in \mathrm{mod}_A(T)$.

Aussi $H = \sum_{i=1}^{q} \alpha_i G_i$ où pour tout $i \in \mathbb{N}_q^o$ $\alpha_i \in A^o$ et $G_i \in T$, et, de plus, $d^oG_1 < \ldots < d^oG_q$; aussi $d^oH = d^oG_q$. Alors, nous avons : $m > d^oG_q > \ldots > d^oG_1$, aussi $G_i \in T'$ pour tout $i \in \mathbb{N}_q^o$ donc $H \in \mathrm{mod}_A(T')$. Par conséquent, $\mathrm{mod}_A(T') = \{F \in H | d^oF < m\}$.

Considérons $F_m - X(\varepsilon^{-1}F_{m-1})$; son terme de degré m est : $a_m - \varepsilon^{-1}(\varepsilon a_m) = 0$. Donc $d^o(F_m - X\varepsilon^{-1}F_{m-1}) < m$.

D'où $F_m - X(\varepsilon^{-1}F_{m-1}) \in \mathrm{mod}_A(T')$.

Comme $F_{m-1} \in T'$, nous en déduisons que $F_m \in \mathrm{id}(T')$.

Maintenant, $H = \mathrm{id}(T)$ et $T = T' \cup \{F_m\}$, aussi

$$H = \mathrm{id}(T').$$

Ensuite, montrons que pour tout $F \in T'$, $XF' \in \mathrm{mod}_A(T'^{(1)})$.

$$T'^{(1)} = T' \cup \{X^j F_{m-1} | j \in \mathbb{N}^o\}$$

donc $XF_{m-1} \in T'^{(1)}$ et $XF_{m-1} \in \mathrm{mod}_A(T'^{(1)})$.

Soit $F \in T'$ avec $F \neq F_{m-1}$, donc $d^oF < m-1$.

Aussi $d^o(XF) \leqslant m-1$.

Or $XF \in H$ et $\{H \in H \mid d^oH < m\} = \mathrm{mod}_A(T')$

donc $XF \in \mathrm{mod}_A(T')$; puisque $T' \subset T'^{(1)}$, nous avons $XF \in \mathrm{mod}_A(T'^{(1)})$. D'après le théorème 13.2, T' est une partie finie génératrice séparante de H. Mais $T' \underset{\neq}{\subset} T$ et T est minimale : contradiction.

Par conséquent, $s = m$, c'est-à-dire $s(H) = m(T)$.

Supposons (ii). Donc $I_m \neq I_{m-1}$; posons F_m l'unique élément de degré m de T et a_m son coefficient directeur.

S'il existe $G \in T$ tel que $d^oG = m-1$ et le terme directeur de G est $\varepsilon a_m X^{m-1}$ où $\varepsilon \in A^*$.

D'après la proposition 31.2, I_{m-1} est alors engendré par εa_m, c'est-à-dire $I_{m-1} = A.a_m$.

Or $I_m = A.a_m$, donc $I_m = I_{m-1}$: contradiction.

Par conséquent, il n'existe aucun $G \in T$ de terme directeur $\varepsilon a_m X^{m-1}$ où $\varepsilon \in A^*$.

Supposons (iii).

Posons F_m l'unique élément de T de degré m et a_m son coefficient directeur ; d'après la proposition 31.2, $I_m = A.a_m$.

De plus, I_{m-1} est engendré par le coefficient directeur a de l'unique élément de degré $m-1$ de T.

Or, d'après l'hypothèse faite, il n'existe aucun $\varepsilon \in A^*$ tel que $a = \varepsilon a_m$. Donc $I_m \neq I_{m-1}$ et $s(H) \leqslant m = m(T)$.

Or, nous savons que $m(T) \geqslant s(H)$, donc $s(H) = m(T)$.

Considérons T' une partie finie génératrice séparante de H telle que $T' \subset T$.

Si $m(T') < m(T)$. Posons F_o l'unique élément de degré $m(T')$ de T'.

$F_m \in H = \mathrm{mod}_A(T'^{(1)})$. Donc $F_m = \sum_{i=1}^{q} \alpha_i G_i$ où pour tout $i \in \mathbb{N}_q^o$ $\alpha_i \in A^o$ et $G_i \in T'^{(1)}$ et $d^oG_1 < \ldots < d^oG_q$ aussi $d^oG_q = d^oF_m = m(T) > m(T')$ donc $G_q = X^{m(T)-m(T')}F_o$.

Alors $a_m = \alpha_q a_o$ où a_o désigne le coefficient directeur de F_o.

Comme $m(T) - m(T') > 0$, $\alpha_q X^{m(T)-m(T')-1}F_o \in H$.

$$\begin{aligned} d^o(\alpha_q X^{m(T)-m(T')-1}F_o) &= m(T) - m(T') - 1 + d^oF_o \\ &= m(T) - m(T') - 1 + m(T') \\ &= m(T) - 1. \end{aligned}$$

De plus, le coefficient directeur de $\alpha_q X^{m(T)-m(T')-1}F_o$ est $\alpha_q a_o$ c'est-à-dire est a_m. Donc $a_m \in I_{m-1}$.

Or $I_m = A.a_m$ et $I_{m-1} \subset I_m$, donc $I_{m-1} = I_m$: contradiction.

Par conséquent $m(T) = m(T')$.

Maintenant, d'après le corollaire 31.4a, $k(T) = k(T')$.

De plus, d'après la proposition 12.3, puisque T' est triangulaire, pour tout $j \in \mathbb{N}$, tel que $k(T) \leqslant j \leqslant m(T)$, il existe un unique $G \in T'$ tel que $d^oG = j$.

Or $T' \subset T$ et T est triangulaire, aussi, pour tout $j \in \mathbb{N}$ tel que $k(T) \leqslant j \leqslant m(T)$, G est l'unique élément de degré j de T, par conséquent $T' = T$.

Donc T est une partie finie génératrice séparante minimale de H.

Proposition 32.3.- Soit H un idéal non nul de $A[X]$, donné par U un système fini de générateurs. Considérons T et T' deux parties finies génératrices séparantes minimales de H.

Pour qu'il existe $F \in T$ de terme directeur aX^n où $a \in A^o$ et $n \in \mathbb{N}$, il faut et il suffit qu'il existe $G \in T'$ de terme directeur $\varepsilon a X^n$ où $\varepsilon \in A^*$.

Démonstration :

D'après le corollaire 31.4a, nous savons que $k(T) = k(T')$. Considérons alors $n \in \mathbb{N}$ et $n \geqslant k(T)$. Posons $k = k(T)$.

De plus, d'après le théorème 32.2, nous avons $m(T) = m(T') = s(H)$ posons m cette valeur commune.

Soit $F \in T$ de terme directeur aX^n où $a \in A^o$ et $n \in \mathbb{N}$ tel que $k \leqslant n \leqslant m$.

Or $H = \mathrm{mod}_A(T'^{(1)})$, alors pour tout $G \in T'$, nous avons $XG \in \mathrm{mod}_A(T'^{(1)})$. Par conséquent, d'après le théorème 13.2, $\{H \in H \mid d^oH \leqslant m\} = \mathrm{mod}_A(T')$.

Donc $F \in \mathrm{mod}_A(T')$.

Alors $F = \sum_{i=1}^{q} \alpha_i G_i$ où pour tout $i \in \mathbb{N}_q^o$, $\alpha_i \in A^o$ et $G_i \in T'$, et $d^oG_1 < \ldots < d^oG_q$.

Donc $d^oF = d^oG_q$.

Alors G_q est l'unique élément de degré n de T'. Posons b son coefficient directeur, nous avons $a = \alpha_q b$.

Maintenant $G_q \in H$ et $H = \mathrm{mod}_A(T^{(1)})$, nous pouvons faire une démonstration identique et comme F est l'unique élément de T de degré n, nous avons $b = \beta.a$ avec $\beta \in A$.

Alors $\alpha_q.\beta = 1$, donc $\beta \in A^*$.

Nous en déduisons pour qu'il existe $F \in T$ de terme directeur aX^n où $a \in A^o$ et $n \in \mathbb{N}$, il faut et il suffit qu'il existe $G \in T'$ de terme directeur εaX^n où $\varepsilon \in A^*$.

Corollaire 32.3a.- Sous les mêmes notations et hypothèses que 32.3, pour qu'il existe $F \in T^{(1)}$ de terme directeur aX^n où $a \in A^o$ et $n \in N$, il faut et il suffit qu'il existe $G \in T'^{(1)}$ de terme directeur εaX^n où $\varepsilon \in A^*$.

Démonstration :

En effet, nous avons $m(T) = m(T') = m$, posons F_m (resp. G_m) l'unique élément de degré m de T (resp. de T') alors nous avons $T^{(1)} = T \cup \{X^j F_m \mid j \in \mathbb{N}^o\}$ et $T'^{(1)} = T' \cup \{X^j G_m \mid j \in \mathbb{N}^o\}$.

Corollaire 32.3b.- Soit H un idéal non nul de $A[X]$ dont U un système fini de générateurs est donné. Considérons T une partie finie génératrice séparante minimale de H et posons $T = \{F_1,\ldots,F_n\}$ où $d^oF_1 < \ldots < d^oF_n$ et posons $a_1,\ldots,a_n$ les coefficients directeurs respectifs de $F_1,\ldots,F_n$.

Alors $a_1,\ldots,a_n$ sont uniquement déterminés par H aux inversibles près.

Proposition 32.4.- Soit H un idéal non nul de $A[X]$ dont U un système fini de générateurs est donné. Considérons T et T' deux parties finies génératrices séparantes minimales de H.

Alors card T = card T'.

Démonstration :

D'après le théorème 32.2, nous avons $m(T) = m(T')$.

De plus, d'après le corollaire 31.4a, $k(T) = k(T')$.

Or, d'après la proposition 12.3, puisque T (resp. T') est une partie finie génératrice séparante de H, pour tout $j \in \mathbb{N}$ tel que $k(T) \leqslant j \leqslant m(T)$ (resp. $k(T') \leqslant j \leqslant m(T')$) il existe un unique $F_j \in T$ (resp. $G_j \in T$) tel que $d^oF_j = j$ ($d^oG_j = j$).

Par conséquent, card $T = m(T) - k(T) + 1$

et card $T' = m(T') - k(T') + 1$

Or, $m(T) = m(T')$ et $k(T) = k(T')$ aussi card T = card T'.

33. *Construction d'une partie génératrice séparante minimale.*

33.1.- *Algorithme* Λ.

Pour $F \in A[X]$, nous noterons coef-dir(F) son coefficient directeur.

Entrée : U une partie finie non vide et non nulle de $A[X]$.

Sortie : T partie finie génératrice séparante minimale de $H = id_{A[X]}(U)$.

Sous-programme : algorithme Θ

Début : $T := \Theta(U)$; $m := \max \{d^oF \mid F \in T\}$;

$T := \{F_1,\ldots,F_n\}$ rangée par ordre des degrés croissants ;

Si (coef-dir(F_n) = ε.coef-dir(F_{n-1}) où $\varepsilon \in A^*$)

alors retourner $\Lambda(\{F \in T \mid d^oF < m\})$.

Sinon retourner T.

Fin

Théorème 33.2.- Soit H un idéal non nul de $A[X]$ dont U un système fini de générateurs est donné.

Alors nous avons les résultats suivants :

(i) l'algorithme Λ appliqué à S s'arrête au bout d'un nombre fini d'opérations.

(ii) le résultat de l'algorithme Λ appliqué à U est une partie finie génératrice séparante minimale de H.

Démonstration :

(i) comme l'algorithme Θ est fini, l'opération $T := \Theta(U)$ est finie,

Ensuite : - la condition du si n'est pas réalisée, alors l'algorithme Λ cesse.

- la condition du si est réalisée, alors nous recommençons avec $T_1 = \{F \in T \mid d^oF < m\}$. Donc $\text{card}(T_1) = \text{card}(T)-1$.

Par conséquent, tant que la condition du si est réalisée nous construisons une suite strictement décroissante d'entiers naturels. Elle est donc finie.

Donc, l'algorithme Λ est fini.

(ii) Posons T le résultat final de l'algorithme Λ appliqué à U, et posons $T_o = \Theta(U)$. Donc T_o est une partie finie génératrice séparante de H.

1er cas : la condition du si est réalisée.

Alors $\text{coef-dir}(F_n) = \varepsilon.\text{coef-dir}(F_{n-1})$ où $\varepsilon \in A^*$

Mais $XF_{n-1} \in \text{mod}_A(T_o^{(1)})$, donc $XF_{n-1} = \alpha_n.F_n+\alpha_{n-1}.F_{n-1}+\ldots+\alpha_1.F_1$ (1).

Comme T_o est triangulaire, le terme directeur de XF_{n-1} est égal à celui de $\alpha_n.F_n$, c'est-à-dire $\text{coef-dir}(F_{n-1}).X^m = \alpha_n.\text{coef.dir}(F_n).X^m$.

Donc $1 = \alpha_n.\varepsilon$ (en simplifiant par $\text{coef-dir}(F_{n-1})$).

Multiplions (1) par ε et isolons F_n. Nous obtenons :

$$F_n = (\varepsilon.X - \varepsilon.\alpha_{n-1})F_{n-1} - \varepsilon.\alpha_{n-1}.F_{n-2} - \ldots - \varepsilon.\alpha_1.F_1.$$

Posons $T_1 = \{F \in T_o \mid d^oF < m\}$. Alors $F_n \in \text{mod}_A(T_1^{(1)})$.

Donc $H = \mathrm{mod}_A(T_1^{(1)})$, comme T_1 est triangulaire, c'est une partie finie génératrice séparante de H.

Par conséquent, l'algorithme Λ construit à chaque étape une partie finie génératrice séparante de H. Comme il est fini, nous aboutissons au :

2ème cas : la condition du si n'est pas réalisée, alors T, résultat final, est une partie finie génératrice séparante de H qui vérifie la condition (iii) du théorème 32.2, donc T est une partie finie génératrice séparante minimale de H.

CHAPITRE III

PARTIES FINIES GENERATRICES SEPARANTES DANS $A[X,Y]$, OU A EST UN ANNEAU PRINCIPAL ALGORITHMIQUE.

Nous allons prolonger à deux indéterminées ce que nous avons établi dans le chapitre II. Les modifications les plus importantes sont surtout relatives à des questions d'écriture avec ces deux indéterminées.

1 - PARTIES TRIANGULAIRES ET PARTIES FINIES GENERATRICES SEPARANTES.

11. Notations.

Dans tout ce chapitre, comme dans le chapitre II précédent, nous supposerons que A est un anneau principal algorithmique.

Posons PP(X,Y) l'ensemble des produits de puissances de X et de Y, c'est-à-dire, $PP(X,Y) = \{X^iY^j \mid i \in \mathbb{N}, j \in \mathbb{N}\}$.

Définissons sur PP(X,Y) l'ordre suivant :

pour tout i_1, tout j_1, tout i_2 et tout j_2 dans $\mathbb{N}$,

$X^{i_1}Y^{j_1} < X^{i_2}Y^{j_2}$ si et seulement si ou bien $j_1 < j_2$

ou bien $j_1 = j_2$ et $i_1 < i_2$.

Maintenant, il est aisé de voir que c'est un ordre total sur PP(X,Y) et que toute partie finie non vide de PP(X,Y) est bien ordonnée.

Pour tout F non nul de $A[X,Y]$, nous pouvons écrire :

$F = \sum_{m \in M(F)} a_m.m$ où M(F) est une partie finie non vide de

$PP(X,Y)$ et, pour tout $m \in M(F)$, $a_m \in A^o$.

Maintenant, d'après la remarque faite, $M(F)$ est bien ordonnée. Aussi soient $m_1,\ldots,m_n$ les éléments de $M(F)$, rangés dans l'ordre croissant. Posons, pour tout $i \in \mathbb{N}_n^o$, $a_i = a_{m_i}$, alors :

$$F = a_1.m_1 + a_2.m_2 + \ldots + a_n.m_n \quad . \qquad (1)$$

Définition 11.1.- m_n est appelé le monôme directeur de F et nous noterons $m_n = PP(F)$. De même, a_n (resp. $a_n.m_n$) est appelé le coefficient (resp. le terme) directeur de F.

Ecrivons $m_n = X^pY^q$, alors d'après la définition de l'ordre, q correspond au degré en Y de F. De plus, dans l'écriture (1) de F, les monômes sont rangés dans l'ordre croissant des puissances de Y, aussi nous en déduisons :

$$F = f_o(X) + f_1(X)Y + \ldots + f_q(X)Y^q$$

où, pour tout $i \in \mathbb{N}_q$, $f_i(X) \in A[X]$ et $f_q \neq 0$.

De plus, le degré de f_q en X est p. Par contre p n'est pas nécessairement le degré en X de F.

Définition 11.2.- q est appelé le Y-degré de F et noté $q = \deg_Y(F)$,

f_q (resp. f_qY^q) est appelé le Y-coefficient (resp. le Y-terme) directeur de F.

Rappelons que pour U une partie de $A[X,Y]$, nous noterons $\mathrm{mod}_A(U)$ (resp. $\mathrm{mod}_{A[X]}(U)$) le sous-A-module (resp. $A[X]$-module) de $A[X,Y]$, engendré par U, et, nous noterons $\mathrm{id}(U)$, l'idéal de $A[X,Y]$, engendré par U.

12. Parties décalées.

Définition 12.1.- Soit U une partie de $A[X,Y]$. Nous dirons que U est une partie décalée de $A[X,Y]$, si et seulement si U vérifie :

(i) $U \neq \emptyset$

(ii) $0 \notin U$

(iii) $\forall F \in U \ \forall G \in U \quad F \neq G \implies PP(F) \neq PP(G)$.

Remarquons que cette définition est identique à celle donnée dans le chapitre II (cf. définition 12.1).

13. Parties triangulaires.

Définition 13.1.- Soit T une partie de $A[X,Y]$. Nous dirons que T est triangulaire, si et seulement si T vérifie :

(i) T est décalée ;

(ii) pour tout $F \in T$ et pour tout $G \in T$, posons $PP(F) = X^{i_1}Y^{j_1}$ et $PP(G) = X^{i_2}Y^{j_2}$, et supposons $X^{i_1}Y^{j_1} < X^{i_2}Y^{j_2}$. Alors :

1er cas : $j_1 = j_2 = j$ et $i_1 < i_2$, aussi pour tout $i \in \mathbb{N}$ tel que $i_1 < i < i_2$, il existe $F_i \in T$ pour lequel $PP(F_i) = X^iY^j$.

2ème cas : $j_1 < j_2$, aussi pour tout $j \in \mathbb{N}$ tel que $j_1 < j < j_2$, il existe $F_j \in T$ et $i_3 \in \mathbb{N}$ pour lequel $PP(F_j) = X^{i_3}Y^j$.

Définition 13.2.- Soit T une partie triangulaire de $A[X,Y]$.

Pour tout $j \in \mathbb{N}$, définissons $T_{[Y^j]} = \{F \in T \mid \exists i \in \mathbb{N} \ PP(F) = X^iY^j\}$.

Proposition 13.3.- Soit T une partie finie triangulaire de $A[X,Y]$. Nous avons les résultats suivants :

(i) posons $k = \min\{\deg_Y(F) \mid F \in T\}$ et $m = \max\{\deg_Y(F) \mid F \in T\}$.

Alors pour tout $j \in \mathbb{N}$, $k \leqslant j \leqslant m$, il existe $F_j \in T$ tel que $\deg_Y(F) = j$.

(ii) pour tout $j \in \mathbb{N}$, $k \leqslant j \leqslant m$, $T_{[Y^j]} \neq \emptyset$ et $T_{[Y^j]}$ est une partie finie triangulaire de $A[X,Y]$.

(iii) pour tout $j \in \mathbb{N}$ tel que $j < k$ ou $j > m$, $T_{[Y^j]} = \emptyset$.

Démonstration :

(i) C'est une conséquence du 2ème cas point (ii) de la définition 13.1.

(ii) D'après (i), dans ce cas $T_{[Y^j]} \neq \emptyset$.

De plus, d'après le 1er cas point (ii) de la définition 13.1, alors $T_{[Y^j]}$ est une partie finie triangulaire.

(iii) C'est une conséquence de la définition de k et de m.

Définition 13.4.- Soit T une partie finie triangulaire de $A[X,Y]$.

Posons $k = \min\{\deg_Y(F) \mid F \in T\}$ et $m = \max\{\deg_Y(F) \mid F \in T\}$.

Définissons $T^{(1)}$ et $T^{(2)}$ par :

(i) $G \in T^{(1)}$ si et seulement si $G \in T$ ou bien il existe $j \in \mathbb{N}$, $k \leqslant j \leqslant m$, et $F \in T_{[Y^j]}$, de monôme directeur maximal dans $T_{[Y^j]}$, et il existe $i \in \mathbb{N}^o$, tels que $G = X^i F$.

(ii) $G \in T^{(2)}$ si et seulement si $G \in T^{(1)}$ ou bien il existe $F \in T^{(1)}$ pour lequel $\deg_Y(F) = m$, et il existe $j \in \mathbb{N}^o$ tel que $G = Y^j F$.

Proposition 13.5.- Soit T une partie finie triangulaire de $A[X,Y]$. Posons $k = \min\{\deg_Y(F) \mid F \in T\}$ et $m = \max\{\deg_Y(F) \mid F \in T\}$.

Considérons $E = \{\deg_Y(F) \mid F \in T^{(1)}\}$. Alors E admet un minimum et un maximum et nous avons :

(i) $\min\{\deg_Y(F) \mid F \in T^{(1)}\} = k$

(ii) $\max\{\deg_Y(F) \mid F \in T^{(1)}\} = m$.

Démonstration :

Soit $F \in T^{(1)}$ alors ou bien $F \in T$

aussi $k \leqslant \deg_Y(F) \leqslant m$,

ou bien il existe $j \in \mathbb{N}$, $k \leqslant j \leqslant m$,

et $G \in T_{[Y^j]}$, de monôme directeur maximal dans $T_{[Y^j]}$, et il existe $i \in \mathbb{N}^o$, tels que $F = X^i G$.

Par conséquent, $\deg_Y(F) = \deg_Y(G)$

donc $k \leqslant \deg_Y(F) \leqslant m$

c'est-à-dire E admet un minimum et un maximum.

Comme $T \subset T^{(1)}$ et pour tout $F \in T^{(1)}$, $k \leqslant \deg_Y(F) \leqslant m$,

nous avons $\min\{\deg_Y(F)/F \in T^{(1)}\} = k$

et $\max\{\deg_Y(F)/F \in T^{(1)}\} = m$.

Proposition 13.6.- Soit T une partie finie triangulaire de $A[X,Y]$.

Alors $T^{(1)}$ et $T^{(2)}$ sont des parties triangulaires de $A[X,Y]$.

Démonstration :

Posons $k = \min\{\deg_Y(F) \mid F \in T\}$ et $m = \max\{\deg_Y(F) \mid F \in T\}$.

Etudions $T^{(1)}$.

Nous avons $T \subset T^{(1)}$ aussi $T^{(1)} \neq \emptyset$. De plus, il est clair que $0 \notin T^{(1)}$ par construction.

Maintenant, soient G_1 et G_2 dans $T^{(1)}$, tels que $PP(G_1) = PP(G_2)$. Remarquons que, si $G_1 \in T$ et $G_2 \in T$, alors $G_1 = G_2$, puisque T est triangulaire. Nous avons donc à étudier les deux cas suivants :

* $G_1 \in T$ et $G_2 \notin T$, donc il existe $j \in \mathbb{N}$, $k \leqslant j \leqslant m$ et $F_2 \in T_{[Y^j]}$ de monôme directeur maximal dans $T_{[Y^j]}$, et il existe $\ell_2 \in \mathbb{N}^o$ tels que $G_2 = X^{\ell_2} F_2$.

donc $PP(G_1) = PP(G_2) = X^{\ell_2} PP(F_2)$

d'où $G_1 \in T_{[Y^j]}$. Ecrivons $PP(G_1) = X^{i_1}Y^j$ et $PP(F_2) = X^{i_2}Y^j$

d'après la propriété de F_2, $i_1 \leqslant i_2$. Or $i_1 = i_2 + \ell_2$

d'où $\ell_2 = 0$: contradiction, car $\ell_2 \in \mathbb{N}^o$.

Par conséquent, nous obtenons :

* $G_1 \notin T$ et $G_2 \notin T$, donc pour $t \in \{1,2\}$, il existe $j_t \in \mathbb{N}$, $k \leqslant j_t \leqslant m$, et $F_t \in T_{[Y^{j_t}]}$ de monôme directeur maximal dans $T_{[Y^{j_t}]}$, et il existe $\ell_t \in \mathbb{N}^o$, tels que $G_t = X^{\ell_t} F_t$.

Posons $PP(F_t) = X^{i_t}Y^{j_t}$; alors :

$$X^{i_1+\ell_1}Y^{j_1} = X^{i_2+\ell_2}Y^{j_2}.$$

Aussi $j_1 = j_2$, donc, d'après la maximalité du monôme directeur, $i_1 = i_2$ dans ce cas, nous avons $\ell_1 = \ell_2$ et $X^{i_1}Y^{j_1} = X^{i_2}Y^{j_2}$.

Or T est décalée, donc $F_1 = F_2$.

Par conséquent, $G_1 = G_2$.

D'où, finalement, $T^{(1)}$ est décalée.

Montrons maintenant que $T^{(1)}$ est triangulaire.

Soient G_1 et G_2 dans $T^{(1)}$ tels que $PP(G_1) < PP(G_2)$.

Posons $PP(G_1) = X^{i_1}Y^{j_1}$ et $PP(G_2) = X^{i_2}Y^{j_2}$. Donc :

1er cas : $j_1 = j_2 = j$ et $i_1 < i_2$. Soit $i \in \mathbb{N}$, tel que $i_1 < i < i_2$.

* Si $G_1 \in T$ et $G_2 \in T$, comme T est triangulaire, alors il existe $F_i \in T$ tel que $PP(F_i) = X^iY^j$ et $F_i \in T^{(1)}$.

* $G_1 \in T$ mais $G_2 \notin T$. Alors il existe $F_2 \in T_{[Y^j]}$ de monôme

directeur maximal dans $T_{[Y^j]}$, et il existe $\ell_2 \in \mathbb{N}^o$, tel que $G_2 = X^{\ell_2}F_2$.

Posons $PP(F_2) = X^{q_2}Y^j$, alors $i_2 = q_2+\ell_2$ et $i_1 \leqslant q_2$ puisque $G_1 \in T_{[Y^j]}$.

Pour $i_1 < i \leqslant q_2$, T est triangulaire aussi il existe $F_i \in T$ tel que $PP(F_i) = X^iY^j$ et $F_i \in T^{(1)}$.

Pour $q_2 < i < q_2+\ell_2$ alors $X^{i-q_2}F_2 \in T^{(1)}$ et $PP(X^{i-q_2}F_2) = X^iY^j$.

* $G_1 \notin T$ et $G_2 \notin T$. Donc pour $t \in \{1,2\}$, il existe $j_t \in \mathbb{N}$, $k \leqslant j_t \leqslant m$, et $F_t \in T_{[Y^{j_t}]}$ de monôme directeur maximal dans $T_{[Y^{j_t}]}$, et il existe $\ell_t \in \mathbb{N}^o$ tels que $G_t = X^{\ell_t}F_t$.

Or $j_1 = j_2 = j$, donc $PP(F_1) = PP(F_2)$ et $F_1 = F_2$ puisque T est décalée. Posons $PP(F_1) = PP(F_2) = X^qY^j$.

Alors $i_1 = q+\ell_1$ et $i_2 = q+\ell_2$.

donc pour $i_1 < i < i_2$, $\ell_1 < i-q < \ell_2$ et $X^{i-q}F_1 \in T^{(1)}$ avec $PP(X^{i-q}F_1) = X^iY^j$.

Par conséquent le premier cas est vérifié.

2ème cas : $j_1 < j_2$. Soit $j \in \mathbb{N}$, $j_1 < j < j_2$.

D'après la proposition 13.5, nous avons $k \leqslant j_1 < j < j_2 \leqslant m$.

Utilisons alors la proposition 13.3, il existe $F_j \in T$ tel que $\deg_Y(F_j) = j$, c'est-à-dire $PP(F) = X^{i_3}Y^j$ avec $i_3 \in \mathbb{N}$ et $F_j \in T^{(1)}$

aussi le second cas est vérifié.

Par conséquent, $T^{(1)}$ est une partie triangulaire.

Etudions maintenant $T^{(2)}$.

Pour démontrer que $T^{(2)}$ est décalée, il suffit d'utiliser une démonstration analogue au cas de $T^{(1)}$. Donc $T^{(2)}$ est décalée.

Démontrons maintenant que $T^{(2)}$ est triangulaire.

Soient G_1 et G_2 dans $T^{(2)}$, tels que $PP(G_1) < PP(G_2)$.

Posons $PP(G_1) = X^{i_1}Y^{j_1}$ et $PP(G_2) = X^{i_2}Y^{j_2}$.

L'étude du 1er cas $j_1 = j_2 = j$ et $i_1 < i_2$ est identique à celle faite pour $T^{(1)}$. Aussi passons directement au second cas :

2ème cas : $j_1 < j_2$ et soit $j_1 < j < j_2$.

* $G_1 \in T^{(1)}$ et $G_2 \in T^{(1)}$. Or $T^{(1)}$ est triangulaire, aussi il existe $F_j \in T^{(1)}$ tel que $PP(F_j) = X^{i_3}Y^j$ avec $i_3 \in \mathbb{N}$ et $F_j \in T^{(2)}$.

* $G_1 \in T^{(1)}$ et $G_2 \notin T^{(1)}$. Alors il existe $F_2 \in T^{(1)}$, tel que $\deg_Y(F_2) = m$, et il existe $\ell_2 \in \mathbb{N}^o$ tels que $G_2 = Y^{\ell_2}F_2$.

Donc $j_2 = m+\ell_2$. Or $G_1 \in T^{(1)}$ donc $j_1 \leqslant m$.

Aussi pour $j_1 \leqslant j \leqslant m$, il existe $F_j \in T^{(1)}$ tel que $PP(F_j) = X^{i_3}Y^j$ puisque $T^{(1)}$ est triangulaire.

Pour $m < j < j_2$ alors $0 < j-m < \ell_2$.

Aussi $Y^{j-m}F_2 \in T^{(2)}$ et $PP(Y^{j-m}F_2) = X^{i_2}Y^j$.

* $G_1 \notin T^{(1)}$ et $G_2 \notin T^{(1)}$. Alors pour $t \in \{1,2\}$, il existe $F_t \in T^{(1)}$ tel que $\deg_Y(F_t) = m$, et il existe $\ell_t \in \mathbb{N}^o$ tels que $G_t = Y^{\ell_t}F_t$ donc $PP(G_t) = X^{i_t}Y^{m+\ell_t}$ et $j_t = m+\ell_t$

aussi pour $j_1 < j < j_2$, nous avons $\ell_1 < j-m < \ell_2$

d'où $Y^{j-m}F_t \in T^{(2)}$ et $PP(Y^{j-m}F_t) = X^{i_t}Y^j$.

Par conséquent, $T^{(2)}$ est triangulaire.

14. *Parties finies génératrices séparantes.*

Lemme 14.1.- Soit B un anneau (commutatif unitaire). Considérons H un idéal de $B[X]$ et M un sous-B-module de $B[X]$, qui engendre H. Pour

qu'il existe $n \in \mathbb{N}$ tel que nous ayons $M = \{F \in H | d^oF \leq n\}$ il faut et il suffit que M vérifie :

(i) $\forall F \in M \quad d^oF \leq n$

(ii) $\forall F \in M \quad d^oF < n \implies X.F \in M.$

Démonstration :

Puisque $H = id_B(M)$, lorsque $M = \{F \in H | d^oF \leq n\}$ alors les conditions (i) et (ii) sont évidemment satisfaites.

Maintenant, supposons que M vérifie les conditions (i) et (ii). D'après (i), $M \subset \{F \in H | d^oF \leq n\}$.

Soit $F \in H^o$, tel que $d^oF \leq n$; puisque $H = id_B(M)$, nous pouvons écrire $F = \sum_{i=0}^{k} m_i.X^i$ où, pour tout $i \in \mathbb{N}_k$, $m_i \in M$.

Nous pouvons supposer k minimal.

Supposons $k \neq 0$, donc $m_k \neq 0$.

Si $d^om_k < n$, d'après (ii), $X.m_k \in M$. Donc $m_k.X^k \in M.X^{k-1}$.

Alors nous pouvons trouver $m'_o,\ldots,m'_{k-1}$ dans M tels que $F = \sum_{i=0}^{k-1} m'_i.X^i$.

Mais ceci contredit le caractère minimal de k, donc $d^om_k = n$.

Or, pour $i \in \mathbb{N}_k$, $d^o(m_i.X^i) = d^om_i + i < n+k$ et $d^o(m_k.X^k) = n+k$ donc $d^oF = n+k$; comme $k \neq 0$, $d^oF > n$: contradiction.

Par conséquent $k = 0$, donc $F = m_o$, c'est-à-dire $F \in M$, alors $M = \{F \in H | d^oF \leq n\}$.

Théorème 14.2.- Soit T une partie finie triangulaire de $A[X,Y]$. Supposons que T vérifie :

$$\forall F \in T \ , \quad XF \in mod_A(T^{(2)}) \wedge YF \in mod_A(T^{(2)}).$$

Posons H l'idéal de $A[X,Y]$ engendré par T. Alors, nous avons les résultats suivants :

(i) Posons $m = \max\{\deg_Y(F) \mid F \in T\}$. $\mathrm{mod}_A(T^{(1)}) = \{F \in H \mid \deg_Y(F) \leqslant m\}$.

(ii) $H = \mathrm{mod}_A(T^{(2)})$.

(iii) (a) Si $F \in T$ alors $XF = \sum_{G \in T^{(1)}} a_F(G,X).G$, $a_F(G,X) \in A$ tous nuls sauf un nombre fini et si, de plus, $\deg_Y(F) < m$ alors

$Y.F = \sum_{G \in T^{(1)}} a_F(G,Y).G$, $a_F(G,V) \in A$ tous nuls sauf un nombre fini.

(b) Les relations définies en (a) engendrent le $A[X]$ module des relations entre les éléments de T.

Démonstration :

(i) puisque $H = \mathrm{id}(T)$ nous avons $H = \mathrm{id}(\mathrm{mod}_{A[X]}(T))$.

Aussi, pour pouvoir utiliser le lemme 14.1, nous devons démontrer que $\mathrm{mod}_{A[X]}(T) = \mathrm{mod}_A(T^{(1)})$.

D'après la définition de $T^{(1)}$, nous avons $T^{(1)} \subset \mathrm{mod}_{A[X]}(T)$.

Maintenant soit $G \in \mathrm{mod}_{A[X]}(T)$. Alors $G = \sum_{F \in T} x_F F$ où $x_F \in A[X]$.

Ecrivons $x_F = a_o(F) + a_1(F)X + \ldots + a_{n(F)}(F)X^{n(F)}$ avec $a_i(F) \in A$.

Donc $G = \sum_{F \in T} \sum_{i=0}^{n(F)} a_i(F)X^i F$.

Par hypothèse, nous savons que $XF \in \mathrm{mod}_A(T^{(2)})$.

Ecrivons $XF = \alpha_1 G_1 + \ldots + \alpha_q G_q$ où $\alpha_i \in A$ et $G_i \in T^{(2)}$.

Or $T^{(2)}$ est triangulaire, aussi nous pouvons supposer $PP(G_1) < \ldots < PP(G_q)$, d'où $PP(XF) = PP(G_q)$ c'est-à-dire $\deg_Y(XF) = \deg_Y(G_q)$.

Or $\deg_Y(F) \leqslant m$ aussi $\deg_Y(XF) \leqslant m$ et $\deg_Y(G_q) \leqslant m$, ainsi que $\deg_Y(G_i) \leqslant m$ pour $i \in \mathbb{N}^o_{q-1}$. Donc, pour tout $i \in \mathbb{N}^o_q$, $G_i \in T^{(1)}$.

Sinon $G_i = Y^{\ell}F_i$ avec $\ell \neq 0$ et $\deg_Y(F_i) = m$, aussi $\deg_Y(G_i) = m+\ell$ et $\deg_Y(G_i) > m$: impossible.

Par conséquent, $XF \in \mathrm{mod}_A(T^{(1)})$.

Par récurrence, pour tout $i \in \mathbb{N}^o$, $X^iF \in \mathrm{mod}_A(T^{(1)})$.

Alors $G \in \mathrm{mod}_A(T^{(1)})$ d'où, finalement, $\mathrm{mod}_{A[X]}(T) = \mathrm{mod}_A(T^{(1)})$.

Maintenant, soit $G \in \mathrm{mod}_{A[X]}(T)$, donc $G \in \mathrm{mod}_A(T^{(1)})$ aussi $G = \alpha_1F_1 + \ldots + \alpha_qF_q$ avec $\alpha_i \in A$ et $F_i \in T^{(1)}$.
Or, d'après la proposition 13.5, pour tout $i \in \mathbb{N}^o_q$, $\deg_Y(F_i) \leqslant m$.
Comme $\alpha_i \in A$, nous en déduisons que $\deg_Y(G) \leqslant m$ et, ceci pour tout $G \in \mathrm{mod}_{A[X]}(T)$,

Considérons $F \in T$ tel que $\deg_Y(F) < m$.

D'après l'hypothèse faite, nous savons que $YF \in \mathrm{mod}_A(T^{(2)})$, c'est-à-dire que $YF = \alpha_1F_1 + \ldots + \alpha_qF_q$ où $\alpha_i \in A$ et $F_i \in T^{(2)}$.
Comme $T^{(2)}$ est triangulaire, nous pouvons supposer que $PP(F_1) < \ldots < PP(F_q)$ alors $PP(YF) = PP(F_q)$ donc $\deg_Y(F_q) = \deg_Y(YF)$ aussi $\deg_Y(F_q) \leqslant m$.
Par conséquent, pour tout $i \in \mathbb{N}^o_q$, $\deg_Y(F_i) \leqslant m$, ce qui implique que $F_i \in T^{(1)}$, pour tout $i \in \mathbb{N}^o_q$. Donc $YF \in \mathrm{mod}_A(T^{(1)})$, par suite $YF \in \mathrm{mod}_{A[X]}(T)$.

Considérons maintenant $G \in \mathrm{mod}_{A[X]}(T)$, alors $G = \sum_{F \in T} x_F F$ et supposons $\deg_Y(G) < m$. Posons $F_1, \ldots, F_q$ les éléments de T pour lesquels $x_F \neq 0$ dans $G = \sum_{F \in T} x_F F$ et posons $x_{F_i} = x_i$, dans ce cas.

Puisque T est triangulaire, nous pouvons supposer $PP(F_1) < \ldots < PP(F_q)$.

Donc $\deg_Y(F_1) \leqslant \ldots \leqslant \deg_Y(F_q)$ et $\deg_Y(F_q) = \deg_Y(G)$.

Aussi, pour tout $i \in \mathbb{N}^o_q$, $\deg_Y(F_i) < m$, donc $YF_i \in \mathrm{mod}_{A[X]}(T)$.

Or $YG = \sum_{i=1}^{q} x_i\, YF_i$ aussi $YG \in \mathrm{mod}_{A[X]}(T)$.

Finalement, $\mathrm{mod}_{A[X]}(T)$ vérifie les conditions du lemme 14.1 aussi $\mathrm{mod}_{A[X]}(T) = \{F \in H \mid \deg_Y(F) \leqslant m\}$.

Comme $\mathrm{mod}_A(T^{(1)}) = \mathrm{mod}_{A[X]}(T)$, nous avons $\mathrm{mod}_A(T^{(1)}) = \{F \in H \mid \deg_Y(F) \leqslant m\}$

(ii) $H = \mathrm{id}(T)$. Posons $M = \mathrm{mod}_A(T^{(1)})$

donc $H = \mathrm{id}(M)$.

Or M est un $A[X]$ module, puisque $\mathrm{mod}_A(T^{(1)}) = \mathrm{mod}_{A[X]}(T)$.

Aussi, nous avons $H = \sum_{j \in \mathbb{N}} Y^j.M$, c'est-à-dire que H est engendré comme A module, par $\bigcup_{j \in \mathbb{N}} Y^j.T^{(1)}$.

Soit $G \in T^{(1)}$: * Si $\deg_Y(G) = m$, alors, par définition, pour tout $j \in \mathbb{N}$, $Y^jG \in T^{(2)}$.

* Sinon, $\deg_Y(G) < m$ et $YG \in \mathrm{mod}_A(T^{(1)})$

donc $YG \in \mathrm{mod}_A(T^{(2)})$. Supposons que $Y^jG \in \mathrm{mod}_A(T^{(2)})$.

Aussi $Y^jG = \alpha_1 G_1 + \ldots + \alpha_q G_q$ avec $\alpha_\ell \in A$ et $G_\ell \in T^{(2)}$.

1er cas : $\deg_Y(G_\ell) < m$ alors $G_\ell \in T^{(1)}$ et $YG_\ell \in \mathrm{mod}_A(T^{(1)})$.

2ème cas : $\deg_Y(G_\ell) \geqslant m$ alors $G_\ell = Y^{k(\ell)}F_\ell$ où $k(\ell) \in \mathbb{N}$

et $F_\ell \in T^{(1)}$ tel que $\deg_Y(F_\ell) = m$.

ainsi $YG_\ell = Y^{k(\ell)+1}F_\ell$, or, par définition, $Y^{k(\ell)+1}F_\ell \in T^{(2)}$

aussi $YG_\ell \in T^{(2)}$.

Maintenant $Y^{j+1}G = Y(Y^jG) = \alpha_1 YG_1 + \ldots + \alpha_q YG_q$

donc $Y^{j+1}G \in \mathrm{mod}_A(T^{(2)})$.

Nous en déduisons que pour tout $j \in \mathbb{N}$ et pour $G \in T^{(1)}$, $Y^jG \in \mathrm{mod}_A(T^{(1)})$.

Par conséquent $\bigcup_{j \in \mathbb{N}} Y^j.T^{(1)} \subset \mathrm{mod}_A(T^{(2)})$.

Comme $T^{(2)} \subset H$, de façon évidente, nous obtenons $H = \mathrm{mod}_A(T^{(2)})$.

(iii) La démonstration de cette propriété est identique à la démonstration donnée pour une indéterminée au théorème 13.3. du chapitre II.

Définition 14.3.- Soit H un idéal non nul de $A[X,Y]$, amettant T une partie finie triangulaire de $A[X,Y]$ comme partie génératrice.

Nous dirons que T est une partie finie génératrice séparante de H si et seulement si $H = \mathrm{mod}_A(T^{(2)})$.

2. ALGORITHME POUR DETERMINER UNE PARTIE FINIE GENERATRICE SEPARANTE.

21. Algorithme Δ : construction d'une partie finie génératrice triangulaire.

21.1.- Algorithme Δ.

Entrée : U partie finie non vide et non nulle de $A[X,Y]$.

Sortie : T partie finie triangulaire de $A[X,Y]$.

Sous-programme : fonction récursive p.

Début : $T := U - \{0\}$;

Tant que T possède deux éléments de même monôme directeur faire

Début tq : X^iY^j est le plus grand monôme directeur pour lequel il existe au moins deux éléments de T de même monôme directeur ;

q =: nombre d'éléments de T de monôme directeur X^iY^j ;

$H_1,\ldots,H_q$ sont les q éléments de T de monôme directeur X^iY^j ;

pour tout $k \in \mathbb{N}_q^o$, a_k := coefficient directeur de H_k ;

utiliser p pour déterminer $\alpha_1,\ldots,\alpha_k,\beta_1,\ldots,\beta_k$ dans A tels que $\sum_{k=1}^{q} \alpha_k.a_k$ est le p.g.c.d. des a_k dans A

et $\beta_1,\ldots,\beta_k$ sont les quotients respectifs ;

$d := \sum_{k=1}^{q} \alpha_k.a_k$; $H := \sum_{k=1}^{q} \alpha_k.H_k$;

$T := T - \{H_1,\ldots,H_q\}$;

$T := T \cup \{H, H_1-\beta_1.H, \ldots, H_k-\beta_k.H\}$;

Fin tq.

Ranger les éléments de T par ordre des degrés croissants ;

$s := \text{card}(T)$; $T := \{F_1,\ldots,F_s\}$;

pour tout $k \in \mathbb{N}_s^o$ $PP(F_k) := X^{i_k} Y^{j_k}$;

$\ell := 1$;

Tant que $\ell < s$ faire

Début tq : si $j_k = j_{k+1}$ alors

début de si : $h := i_{k+1} - i_k$;

si $h > 1$ alors $T := T \cup \{XF_k, \ldots, X^{h-1}F_k\}$;

fin de si

sinon

début : $h := j_{k+1} - j_k$;

si $h > 1$ alors $T := T \cup \{YF_k, \ldots, Y^{h-1}F_k\}$;

fin de sinon.

Fin de tq.

Fin.

Proposition 21.2.- Soit U une partie finie non vide et non nulle de $A[X,Y]$.

Nous avons les résultats suivants :

(i) l'algorithme Δ appliqué à U s'arrête au bout d'un nombre fini d'opérations.

(ii) posons $T = \Delta(U)$ le résultat final. Alors T est une partie finie triangulaire de $A[X]$ telle que

$$id_{A[X]}(U) = id_{A[X]}(T).$$

Démonstration :

Elle est identique à la démonstration de la proposition 21.2 du chapitre II.

Nous avons d'ailleurs le même type de conséquences.

Corollaire 21.2a.- Soit U une partie finie non vide et non nulle de $A[X,Y]$. Posons T la partie finie triangulaire obtenue par l'algorithme Δ appliqué à U. Alors :

$$\max\{\deg_Y(F) \mid F \in T\} = \max\{\deg_Y(F) \mid F \in U\}.$$

Corollaire 21.2b.- Soit U une partie finie non vide et non nulle de $A[X,Y]$. Posons T la partie finie triangulaire obtenue par l'algorithme Δ appliqué à U. Alors :

$$\mathrm{mod}_{A[X]}(U) \subset \mathrm{mod}_{A[X]}(T).$$

22. *Algorithme* R.

Soit T une partie finie triangulaire de $A[X,Y]$. Comme dans le chapitre II sous paragraphe 22, cet algorithme nous permettra de décider, pour $F \in A[X,Y]$, si $F \in \mathrm{mod}_A(T^{(2)})$ ou si $F \notin \mathrm{mod}_A(T^{(2)})$.

Maintenant si nous regardons les premiers pas de l'algorithme R dans le cas d'une indéterminée au chapitre II, pour $F \in A[X]$, nous devons d'abord déterminer s'il existe $G \in T^{(1)}$ tel que $d^oG = d^oF$.

Donc, dans le cas de deux indéterminées, qui nous intéresse maintenant, pour $F \in A[X,Y]$, il nous faut déterminer s'il existe $G \in T^{(2)}$ tel que $PP(G) = PP(F)$, ce qui est un peu moins facile et nécessite un algorithme préliminaire R_o, qui nous permettra de dire, pour i et j dans $\mathbb{N}$, s'il existe ou non $G \in T^{(2)}$ tel que $PP(G) = X^iY^j$.

Définition 22.1.- Soit T une partie finie triangulaire de $A[X,Y]$.

Pour $j \in \mathbb{N}$, définissons :

(i) $T^{(2)}_{[Y^j]} = \{F \in T^{(2)} \mid \exists\, i \in \mathbb{N} \quad PP(F) = X^iY^j\}$

(ii) $\omega(j) = \inf\{i \in \mathbb{N} \mid \exists\, F \in T^{(2)}_{[Y^j]} \quad PP(F) = X^iY^j\}$.

(iii) $\tau(j) = \max\{i \in \mathbb{N} \mid \exists\, F \in T_{[Y^j]} \quad PP(F) = X^iY^j\}$.

Remarque : $T_{[Y^j]}$ est définie à la définition 13.2.

Proposition 22.2.- Soit T une partie finie triangulaire de $A[X,Y]$. Posons $k = \min\{\deg_Y(F) \mid F \in T\}$ et $m = \max\{\deg_Y(F) \mid F \in T\}$.

Nous avons les résultats suivants :

(i) pour tout $j \in \mathbb{N}$ et $j < k$, $T^{(2)}_{[Y^j]} = \emptyset$ donc $\omega(j)$ n'est pas défini.

(ii) pour tout $j \in \mathbb{N}$ et $j \geqslant k$, $T^{(2)}_{[Y^j]} \neq \emptyset$.

(iii) pour tout $j \in \mathbb{N}$ et $k \leqslant j \leqslant m$,

$$\omega(j) = \inf\{i \in \mathbb{N} \mid \exists\ F \in T_{[Y^j]},\ PP(F) = X^iY^j\}.$$

(iv) pour tout $j \in \mathbb{N}$ et $j \geqslant m$, $\omega(j) = \omega(m)$

et $\omega(m) = \inf\{i \in \mathbb{N} \mid \exists\ F \in T_{[Y^m]},\ PP(F) = X^iY^m\}$, d'après (iii).

(v) pour tout $j \in \mathbb{N}$, $\tau(j)$ est défini lorsque $k \leqslant j \leqslant m$.

Démonstration :

Lorsque nous construisons $T^{(1)}$ à partir de T, nous prenons les éléments de T plus certains éléments de T multipliés par une puissance de X donc $\min\{\deg_Y(F) \mid F \in T^{(1)}\} = k$. De plus, nous construisons $T^{(2)}$ à partir de $T^{(1)}$, en prenant tous les éléments de $T^{(1)}$, plus les éléments de degré en Y égal à m, multipliés par une puissance de Y.

Aussi $\min\{\deg_Y(F) \mid F \in T^{(2)}\} = k$ et pour tout $j \in \mathbb{N}$, $j \geqslant k$, il existe $F \in T^{(2)}$ tel que $\deg_Y(F) = j$. D'où les points (i) et (ii) sont vérifiés.

Passons maintenant aux autres résultats :

(iii) soit $j \in \mathbb{N}$ tel que $k \leqslant j \leqslant m$.

Alors, d'après la proposition 13.3, $T_{[Y^j]} \neq \emptyset$.

De plus, comme $T \subset T^{(2)}$, alors $T_{[Y^j]} \subset T^{(2)}_{[Y^j]}$.

Aussi $\omega(j) \leqslant \inf\{i \in \mathbb{N} \mid \exists\ F \in T_{[Y^j]}\ \ PP(F) = X^iY^j\}$.

Maintenant, d'après ce que nous avons rappelé relativement à la construction de $T^{(1)}$ et de $T^{(2)}$, nous avons en fait :

$$\omega(j) = \inf\{i \in \mathbb{N} \mid \exists\ F \in T_{[Y^j]}\ \ PP(F) = X^iY^j\}.$$

(iv) Soit $j \in \mathbb{N}$ tel que $j \geqslant m$.

Considérons $G \in T^{(2)}_{[Y^j]}$ et posons $PP(G) = X^iY^j$.

Comme $j \geqslant m$, il existe $F \in T^{(1)}$, tel que $\deg_Y(F) = m$, et il existe $\ell \in \mathbb{N}$ tels que $G = Y^\ell F$ donc $PP(F) = X^iY^m$.

Dans la proposition 13.3, nous avons démontré que $T_{[Y^m]}$ est triangulaire. Posons F_o l'unique élément de $T_{[Y^m]}$ tel que $PP(F_o) = X^{\omega(m)}Y^m$; alors $Y^\ell F_o \in T^{(2)}$ or $PP(Y^\ell F_o) = X^{\omega(m)}Y^{\ell+m} = X^{\omega(m)}Y^j$; aussi $Y^\ell F_o \in T^{(2)}_{[Y^j]}$. Donc $\omega(m) \geqslant \omega(j)$.

Maintenant, soit $G_o \in T^{(2)}_{[Y^j]}$ tel que $PP(G_o) = X^{\omega(j)}Y^j$.

Or $G_o = Y^{\ell_o}F$ avec $PP(F) = X^{\omega(j)}Y^m$.

Donc $F \in T^{(2)}_{[Y^m]}$ et $\omega(j) \geqslant \omega(m)$, car $\omega(m) = \inf\{i \in \mathbb{N} \mid \exists F \in T^{(2)}_{[Y^m]}\ PP(F) = X^iY^m\}$ d'où $\omega(j) = \omega(m)$.

(v) Cela provient de la proposition 13.3.

23.3.- Algorithme R_o.

Entrées : T partie finie triangulaire de $A[X,Y]$,
i et j deux entiers naturels.

Sortie : Un élément de $T^{(2)}$ de PP égal à X^iY^j s'il existe
0 sinon.

Début : $T := \{F_1,\ldots,F_n\}$ rangée par ordre croissant des PP ;
$m := \deg_Y(F_n)$; $PP(F_n) = X^{\omega}Y^{m}$;
Si $j > m$ alors retourner $Y^{j-m}.R_o(T,i,m)$
Si $j = m$ et $i \geq \omega$ alors retourner $X^{i-\omega}.F_n$.
$k := 1$;
Tant que $PP(F_k) < X^i.Y^j$ faire $k := k+1$;
Si $PP(F_k) = X^i.Y^j$ alors retourner F_k ;
Si $k = 1$ alors retourner 0
$k := k-1$; $PP(F_k) := X^{\alpha}.Y^{\beta}$;
Si $\beta < j$ alors retourner 0 ;
Sinon retourner $X^{i-\alpha}.F_k$;

Fin.

Proposition 22.4.- Soit T une partie finie triangulaire de $A[\underline{X},\underline{Y}]$. Considérons i et j dans $\mathbb{N}$. Alors :

(i) l'algorithme R_o appliqué à i et j s'arrête au bout d'un nombre fini d'opérations.

(ii) Si $R_o(T,i,j) \neq 0$ alors $R_o(T,i,j) \in T^{(2)}$.

Démonstration :

1er cas : $j = m$ et $i \geq \omega$ alors $R_o(T,i,m) = X^{i-\omega}.F_n$
donc l'algorithme cesse et $R_o(T,i,m) \in T^{(2)}$.

2ème cas : $j = m$ et $i < \omega$ ou $j < m$.

Dans ce cas, le nombre d'itérations du Tant que est borné par n, donc l'algorithme cesse. De plus, le Tant que détermine le F_k de PP maximum, pour j fixé.

En outre, nous obtenons soit 0 soit un élément de $T^{(1)}$ ($T^{(1)} \subset T^{(2)}$).

3ème cas : $j > m$. Pour déterminer $R_o(T,i,m)$, nous utilisons soit le 1er cas, soit le 2ème cas, donc l'algorithme cesse.

De plus, nous obtenons soit O, soit un élément de $T^{(1)}$ de PP maximum, donc $Y^{j-m}R_o(T,i,m) \in T^{(2)}$.

22.5.- *Algorithme* R.

Entrées : T une partie finie triangulaire de $A[X,Y]$, et $H \in A[X,Y]$.

Sortie : $R(T,H) \in A[X,Y]$.

Sous-programme : algorithme R_o.

Début : Si $H = 0$ alors retourner 0 ;

Sinon

Début : $X^i.Y^j := PP(H)$; $a :=$ coefficient directeur de H ;

Si $R_o(T,i,j) = 0$ alors retourner $a.X^iY^j + R(T,H-a.X^iY^j)$;

Sinon

début : $F := R_o(T,i,j)$; $b :=$ coefficient directeur de F ;

Si $a = b.\gamma$ alors retourner $R(T,H-\gamma.F)$;

Sinon retourner $a.X^iY^j + R(T,H-a.X^iY^j)$;

fin de sinon.

Fin de sinon.

Fin.

Proposition 22.6.- Soit T une partie finie triangulaire de $A[X,Y]$. Pour tout $H \in A[X,Y]$ nous avons les résultats suivants :

(i) l'algorithme R appliqué à H s'arrête au bout d'un nombre fini d'opérations.

(ii) $R(T,H) \in H + \mathrm{mod}_A(T^{(2)})$ et si $R(T,H) \neq 0$, $PP(R(T,H)) \lesssim PP(H)$.

Démonstration :

Pour $H = 0$ c'est évident ;

Pour $H \neq 0$ nous établissons une démonstration par récurrence identique à celle de la proposition 22.2 correspondante du chapitre II.

De plus, nous avons le même corollaire :

Corollaire 22.6a.- Soit T une partie finie triangulaire de $A[X,Y]$. Pour que $H \in \mathrm{mod}_A(T^{(2)})$ il faut et il suffit que $R(T,H) = 0$.

23. *Algorithme* Δ : *construction d'une partie finie génératrice séparante.*

23.1.- *Algorithme* Θ.

Entrée : U une partie finie non vide et non nulle de $A[X,Y]$.

Sortie : T une partie finie génératrice séparante de $\mathrm{id}_{A[X]}(U)$.

Sous-programmes : algorithme Δ, algorithmes R_o et R.

Début : $T := \Delta(U)$;

s'il existe $F \in T$ tel que $R(T,X.F) \neq 0$

alors retourner $\Theta(T \cup \{R(T,X.F)\})$;

s'il existe $F \in T$ tel que $R(T,Y.F) \neq 0$

alors retourner $\Theta(T \cup \{R(T,Y.F)\})$;

retourner T ;

Fin.

Théorème 23.2.- Soit H un idéal non nul de $A[X,Y]$, donné par U un système fini de générateurs. Alors, nous avons les résultats suivants :

(i) l'algorithme Θ appliqué à U cesse au bout d'un nombre fini d'opérations.

(ii) posons $T = \Theta(U)$ le résultat final. Alors T est une partie finie génératrice séparante de H.

Démonstration :

Pour (i) la démonstration est identique à celle du théorème 23.2 du chapitre II, avec les modifications suivantes :

$m = \max \deg_Y(F) | F \in U$ et $M = \mathrm{mod}_{A[X]}(1, Y, \ldots, Y^m)$.

Pour (ii) c'est identique avec la conclusion $H = \mathrm{mod}_A(T^{(2)})$.

c.q.f.d.

Corollaire 23.2a.- Soit H un idéal non nul de $A[X,Y]$, dont un système fini U de générateurs est donné. Alors pour tout $F \in A[X,Y]$, nous pouvons déterminer algorithmiquement si $F \in H$ ou si $F \notin H$.

Démonstration :

Posons T la partie finie génératrice séparante de H, obtenue par l'algorithme Θ appliqué à U.

Par conséquent, $H = \mathrm{mod}_A(T^{(2)})$.

Or, d'après le corollaire 22.6a, soit $F \in A[X,Y]$, pour que $F \in \mathrm{mod}_A(T^{(2)})$, c'est-à-dire $F \in H$, il faut et il suffit que $R(T,H) = 0$.

Par conséquent, pour tout $F \in A[X,Y]$, nous pouvons déterminer, en utilisant l'algorithme R, si $F \in H$ ou si $F \notin H$.

3 - PARTIES FINIES GENERATRICES SEPARANTES MINIMALES.

31. *Invariants d'un idéal de* $A[X,Y]$.

Définition 31.1.- Soit H un idéal non nul de $A[X,Y]$, dont un système fini U de générateurs est donné. Définissons :

(i) $T_{-1} = \{0\}$.

(ii) pour tout $j \in \mathbb{N}$,

$T_j = \{f \in A[X] \mid fY^j$ soit le Y terme directeur d'un $F \in H\} \cup \{0\}$.

Proposition 31.2.- Soit H un idéal non nul de $A[X,Y]$, dont U un système fini de générateurs est donné. Alors nous avons les résultats suivants :

(i) pour tout $j \in \{-1\} \cup \mathbb{N}$, T_j est un idéal de $A[X]$

(ii) pour tout $j \in \mathbb{N}$, $T_j \subset T_{j+1}$

(iii) $\exists\, r \in \mathbb{N} \quad T_r \neq \{0\} \wedge \forall j \in \{-1\} \cup \mathbb{N} \quad j < r \implies T_j = \{0\}$.

(iv) $\exists\, s \in \mathbb{N} \quad T_{s-1} \subsetneq T_s \wedge \forall j \in \mathbb{N} \quad T_{s+j} = T_s$.

Démonstration :

Comme H est un idéal de $A[X,Y]$ et que nous avons pris la précaution de mettre 0, pour tout $j \in \mathbb{N}$, T_j est un idéal. $T_{-1} = \{0\}$ donc c'est un idéal.

Soit $f \in T_j$, alors fY^j est le Y terme directeur de $F \in H$. Mais $YF \in H$ et son terme directeur est fY^{j+1}, donc $f \in T_{j+1}$. D'où $T_j \subset T_{j+1}$.

Par conséquent (i) et (ii) sont vérifiés.

Démontrons (iv), $A[X]$ est un anneau noethérien, donc la chaîne croissante des idéaux T_j est stationnaire. Donc l'ensemble $\{i \in \mathbb{N} \mid T_i \neq T_{i+1}\}$ est fini. Posons $\ell = \sup\{i \in \mathbb{N} \mid T_i \neq T_{i+1}\}$ et prenons $s = \ell+1$ donc $T_{s-1} \subsetneq T_s$ et pour $j \in \mathbb{N}$ $T_{s+j} = T_s$.

Passons à (iii), considérons les idéaux $T_{-1}, T_o, T_1, \ldots, T_s$. Comme H est non nul, alors il existe $i \in \mathbb{N}_s$ tel que $T_i \neq \{0\}$. Alors posons $r = \inf\{i \in \mathbb{N}_s \mid T_i \neq \{0\}$.

Corollaire 31.2a.- Sous les mêmes hypothèses et notations que dans 31.2, nous avons $\{0\} = T_{r-1} \subsetneq T_r \subset \ldots \subset T_{s-1} \subsetneq T_s = T_{s+j}$, pour tout $j \in \mathbb{N}$. De plus, les entiers r et s ne dépendent que de H.

Définition 31.3.- Soit H un idéal non nul de $A[X,Y]$, donné avec U un système fini de générateurs. Alors nous poserons $r = r(H)$ et $s = s(H)$, les entiers r et s définis à la proposition 31.2.

32. *Caractérisation des parties finies génératrices séparantes.*

Définition 32.1.- Soit T une partie finie triangulaire de $A[X,Y]$. Nous définissons :

(i) $k(T) = \min\{\deg_Y(F) \mid F \in T\}$ et $m(T) = \max\{\deg_Y(F) \mid F \in T\}$.

(ii) pour tout $j \in \mathbb{N}$ et $k(T) \leqslant j \leqslant m(T)$,

$U_j = \{g \in A[X] \mid gY^j$ soit le Y terme directeur d'un $G \in T\}$.

Proposition 32.2.- Soit T une partie finie triangulaire de $A[X,Y]$. Alors, pour tout $j \in \mathbb{N}$ et $k(T) \leqslant j \leqslant m(T)$, U_j est une partie finie triangulaire de $A[X]$.

Démonstration :

Soit $j \in \mathbb{N}$, tel que $k(T) \leqslant j \leqslant m(T)$

donc $U_j \neq \emptyset$. De plus, $0 \notin U_j$.

Soient g_1 et g_2 dans U_j tels que $d^o g_1 = d^o g_2$ ($g_1 \in A[X]$ et $g_2 \in A[X]$).

Alors il existe G_1 et G_2 dans T pour lesquels $g_1 Y^j$ et $g_2 Y^j$ sont leurs Y termes directeurs respectifs. Puisque $d^o g_1 = d^o g_2$, alors $PP(G_1) = PP(G_2)$. Mais T est triangulaire, donc décalée aussi $G_1 = G_2$. Donc $g_1 = g_2$ et U_j est décalée.

Maintenant soient g_1 et g_2 dans U_j tels que $d^o g_1 < d^o g_2$, et considérons $i \in \mathbb{N}$, tel que $d^o g_1 < i < d^o g_2$.

Or il existe G_1 et G_2 dans T tels que $g_1 Y^j$ et $g_2 Y^j$ soient leurs Y termes directeurs respectifs.

Posons $PP(G_1) = X^{i_1} Y^{j_1}$ et $PP(G_2) = X^{i_2} Y^{j_2}$

alors $j_1 = j_2 = j$ et $i_1 = d^o g_1$, $i_2 = d^o g_2$.

Aussi $i_1 < i_2$. Comme T est triangulaire, il existe $G \in T$, tel que $PP(G) = X^i Y^j$. Posons alors $g Y^j$ le Y terme directeur de G. Nous avons $d^o g = i$ et $g \in U_j$.

Comme T est finie, U_j est finie.

Par conséquent, U_j est une partie finie triangulaire de $A[X]$.

Proposition 32.3.- Soit T une partie finie triangulaire de $A[X,Y]$. Posons $H = id(T)$. Pour que T soit une partie finie génératrice séparante de H, il faut et il suffit que T vérifie :

(i) $\forall F \in T \quad YF \in mod_A(T^{(2)})$;

(ii) pour tout $j \in \mathbb{N}$, $k(T) \leqslant j \leqslant m(T)$,

U_j est une partie finie génératrice séparante de T_j, où T_j est défini à la définition 31.1.

Démonstration :

Supposons d'abord T partie finie génératrice séparante de H. Donc $H = mod_A(T^{(2)})$, aussi pour tout $F \in T$, $YF \in mod_A(T^{(2)})$

Soit $j \in \mathbb{N}$ tel que $k(T) \leqslant j \leqslant m(T)$. De façon évidente, $U_j \subset T_j$.

Considérons $f \in T_j$ et $f \neq 0$. Alors $f Y^j$ est le Y terme directeur d'un élément F de H. Nous pouvons écrire $F = \alpha_1 G_1 + \ldots + \alpha_q G_q$ où $\alpha_i \in A$ et $G_i \in T^{(2)}$. Comme $T^{(2)}$ est triangulaire, nous pouvons supposer $PP(G_1) < \ldots < PP(G_q)$.

Donc $PP(G_q) = PP(F)$. Or $\deg_Y(F) = j$ et $j \leqslant m(T)$, donc pour tout $i \in \mathbb{N}_q^o$, $\deg_Y(G_i) \leqslant m(T)$, d'où, pour tout $i \in \mathbb{N}_q^o$, $G_i \in T^{(1)}$.

Alors pour tout $i \in \mathbb{N}_q^o$, $G_i = X^{\ell(x)}F_i$ avec $F_i \in T$ et $\ell(x) \in \mathbb{N}$. Notons $G_r,\ldots,G_q$ les G_i qui vérifient $\deg_Y(G_i) = j$ et f_iY^j le Y terme de F_i. Aussi $f\,Y^j = (\alpha_r X^{\ell(r)}f_r + \ldots + \alpha_q X^{\ell(q)}f_q)Y^j$.

C'est-à-dire $f = \alpha_r X^{\ell(r)}f_r + \ldots + \alpha_q X^{\ell(q)}f_q$.

Or $f_i \in U_j$ pour $r \leqslant i \leqslant q$.

Donc $T_j = id_{A[X]}(U_j)$.

Nous savons, d'après la proposition 32.2, que U_j est une partie finie triangulaire de $A[X]$. Il nous reste donc à démontrer que U_j est séparante.

Posons $U_j = \{g_1,\ldots,g_n\}$; comme U_j est triangulaire, nous pouvons supposer $d^og_1 < d^og_2 < \ldots < d^og_n$. De plus, pour tout $i \in \mathbb{N}_{n-1}^o$, $d^og_{i+1} = 1 + d^og_i$.

Donc $U_j^{(1)} = U_j \cup \{X^ig_n \mid i \in \mathbb{N}^o\}$ (cf. définition 12.4, chapitre II).

Posons, pour tout $i \in \mathbb{N}_n^o$, G_i l'élément de T pour lequel g_iY^j est son Y terme directeur. En posant $d^og_i = q_i$, nous avons alors $PP(G_i) = X^{q_i}Y^j$. Prenons $i \in \mathbb{N}^o$ et $i < n$ et considérons g_i.

Comme T est une partie finie génératrice séparante de H, nous savons que $XG_i \in \mathrm{mod}_A(T^{(2)})$.

Or $PP(XG_i) = X^{q_i+1}Y^j = X^{q_{i+1}}Y^j = PP(G_{i+1})$.

Par conséquent, puisque $T^{(2)}$ est triangulaire, nous avons :

$$XG_i = a_{i+1}G_{i+1} + a_iG_i + \ldots + a_1G_1 + \sum_{\substack{G\in T(2) \\ \deg_Y(G)<j}} a_G.G$$

où les $a_G \in A$ et sont nuls sauf pour un nombre fini d'entre eux.

Alors $Xg_i = a_{i+1}g_{i+1} + \ldots + a_1g_1$

c'est-à-dire $Xg_i \in \mathrm{mod}_A(U_j^{(1)})$ et ceci pour tout $i \in \mathbb{N}^o$ tel que $i < n$.

Pour g_n, il est évident que $Xg_n \in U_j^{(1)}$.

Par conséquent, U_j est une partie finie triangulaire génératrice de T_j, qui vérifie : pour tout $g \in U_j$, $Xg \in \mathrm{mod}_A(U_j^{(1)})$.

Alors, d'après le théorème 13.2 du chapitre II, U_j est une partie finie génératrice séparante de T_j.

Réciproquement, supposons que T soit une partie finie triangulaire de $A[X,Y]$ qui vérifie : (i) $\forall F \in T \quad YF \in \mathrm{mod}_A(T^{(2)})$

(ii) pour tout $j \in \mathbb{N}$, $k(T) \leqslant j \leqslant m(T)$, U_j est une partie finie génératrice séparante de T_j.

Puisque $H = \mathrm{id}(T)$, T est triangulaire et $k(T) = \min\{\deg_Y(F) \mid F \in T\}$, alors pour tout $H \in H$, $\deg_Y(H) \geqslant k(T)$.

Considérons $F \in T$ pour lequel $\deg_Y(F) = k(T)$.

Posons $f\,Y^{k(T)}$ son Y terme directeur, alors $f \in U_{k(T)}$.

Posons $U_{k(T)} = \{g_1,\ldots,g_n\}$. Or $Xf \in U_{k(T)}^{(1)}$, aussi nous avons $Xf = a_1g_1 + \ldots + a_{n-1}g_{n-1} + hg_n$ avec $h \in A[X]$, en supposant $d^og_1 < \ldots < d^og_n$. Posons G_i l'élément de T dont le Y terme directeur est $g_iY^{k(T)}$, pour tout $i \in \mathbb{N}_n^o$. Posons $H = XF - (a_1G_1 + \ldots + a_{n-1}G_{n-1} + h\,G_n)$.

Alors $\deg_Y(H) < k(T)$. Mais $H \in H$, donc $H = 0$.

Aussi $XF = a_1G_1 + \ldots + a_{n-1}G_{n-1} + h\,G_n$.

Ecrivons $h = \sum_{i=0}^{p} \alpha_i X^i$. Or $G_n \in T_{[Y^{k(T)}]}$ et son monôme directeur est maximal dans $T_{[Y^{k(T)}]}$, aussi pour tout $i \in \mathbb{N}$, $X^iG_n \in T^{(1)}$.

Par conséquent $XF \in \mathrm{mod}_A(T^{(1)})$; d'où $XF \in \mathrm{mod}_A(T^{(2)})$.

Faisons maintenant l'hypothèse suivante : pour $q \in \mathbb{N}$ et $k(T) \leqslant q < m(T)$, pour tout $j \in \mathbb{N}$, $k(T) \leqslant j \leqslant q$ et tout $F \in T$, tel que $\deg_Y(F) = j$, alors $XF \in \mathrm{mod}_A(T^{(2)})$.

Considérons $G \in T$ tel que $\deg_Y(G) = q+1$.

Posons $g\,Y^{q+1}$ le Y terme directeur de G. Alors $g \in U_{q+1}$.

Posons $U_{q+1} = \{g_1,\ldots,g_n\}$. Or $Xg \in U_{q+1}^{(1)}$, donc nous avons $Xg = a_1g_1 + \ldots + a_{n-1}g_{n-1} + h\,g_n$ avec $h \in A[X]$, en supposant $d^0g_1 < \ldots < d^0g_n$. Posons, pour tout $i \in \mathbb{N}_n^0$, G_i l'élément de T dont le Y terme directeur est g_iY^{q+1}.

Posons $H = XG - (a_1G_1 + \ldots + a_{n-1}G_{n-1} + h\,G_n)$.

Alors $\deg_Y(H) < q+1$, c'est-à-dire $\deg_Y(H) \leqslant q$.

Or $H \in H$, donc $H = \sum_{F \in T} x_F F$ avec $x_F \in A[X,Y]$.

Aussi $H = \sum_{\substack{F\in T \\ \deg_Y(F)\leqslant q}} x_F F + \sum_{\substack{F\in T \\ \deg_Y(F)>q}} x_F F$.

Si $\sum_{\substack{F\in T \\ \deg_Y(F)>q}} x_F F \neq 0$ alors $\deg_Y(H) > q$: contradiction.

Par conséquent, $H = \sum_{\substack{F\in T \\ \deg_Y(F)\leqslant q}} x_F F$.

Mais $x_F \in A[X,Y]$, aussi $x_F = b_o(F,X) + b_1(F,X)Y + \ldots + b_{p(F)}(F,X)Y^{p(F)}$ où $b_i(F,X) \in A[X]$.

Donc $H = \sum_{\substack{F \in T \\ \deg_Y(F) \leq q}} \sum_{i=0}^{p(F)} b_i(F,X)Y^i F$.

Maintenant, puisque $\deg_Y(F) \leq q$, alors $XF \in \mathrm{mod}_A(T^{(2)})$ et, par récurrence, pour tout $i \in \mathbb{N}$, $X^i F \in \mathrm{mod}_A(T^{(2)})$.

Par conséquent, $b_i(F,X)F \in \mathrm{mod}_A(T^{(2)})$.

De plus, pour tout $F \in T$, $YF \in \mathrm{mod}_A(T^{(2)})$.

Alors, par récurrence, pour tout $j \in \mathbb{N}$ et tout $F \in T^{(2)}$, $Y^j F \in \mathrm{mod}_A(T^2)$.

Donc $b_i(F,X)Y^i F \in \mathrm{mod}_A(T^{(2)})$.

Par suite $H \in \mathrm{mod}_A(T^{(2)})$.

Or $XG = H + a_1 G_1 + \ldots + a_{n-1} G_{n-1} + hG_n$.

Pour $i \in \mathbb{N}_{n-1}^o$, $G_i \in T$. De plus, $G_n \in T_{[Y^{q+1}]}$ et est de monôme directeur maximal dans $T_{[Y^{q+1}]}$, donc, pour tout $i \in \mathbb{N}$, $X^i G_n \in T^{(1)}$, aussi $hG_n \in \mathrm{mod}_A(T^{(1)})$.

Comme $T \subset T^{(1)} \subset T^{(2)}$, nous en déduisons que $XG \in \mathrm{mod}_A(T^{(2)})$.

Nous venons d'établir que l'hypothèse est vérifiée pour $k(T)$ et si elle est vérifiée pour q, tel que $k(T) \leq q < m(T)$, alors elle est vérifiée pour $q+1$.

Par conséquent, elle est vraie pour tout $j \in \mathbb{N}$, tel que $k(T) \leq j \leq m(T)$ c'est-à-dire, pour tout $F \in T$, $XF \in \mathrm{mod}_A(T^{(2)})$.

Comme nous avions déjà, pour tout $F \in T$, $YF \in \mathrm{mod}_A(T^{(2)})$, nous sommes placés dans les conditions du théorème 14.2, aussi T est une partie finie génératrice séparante de $H = \mathrm{id}(T)$.

33. *Définition et caractérisation des parties finies génératrices séparantes minimales.*

Proposition 33.1.- Soit H un idéal non nul de $A[X,Y]$, dont U un système fini de générateurs est donné. Posons T la partie finie génératrice séparante, obtenue par l'algorithme Θ appliqué à U. Alors, nous avons les résultats suivants :

(i) $k(T) = r(H)$;

(ii) $s(H) \leqslant m(T)$.

Démonstration :

(i) Il est évident que $T_{k(T)} \neq \{0\}$ puisque $k(T) = \min\{\deg_Y(F) \mid F \in T\}$. Aussi $U_{k(T)} \neq \emptyset$ et, proposition 32.3, $U_{k(T)}$ est une partie finie génératrice séparante de $T_{k(T)}$. Aussi $r(H) \leqslant k(T)$.

Maintenant, pour tout $H \in H$, $\deg_Y(H) \geqslant k(T)$. D'où $r(H) = k(T)$.

(ii) Posons $m = m(T)$ et soit $j \in \mathbb{N}$.

Considérons T_{m+j}.

Soit f non nul dans T_{m+j}. Posons F l'élément de H dont le Y terme directeur est $f Y^{m+j}$. Donc $F \in \mathrm{mod}_A(T^{(2)})$.

Aussi $F = a_1 G_1 + \ldots + a_n G_n$ avec $a_i \in A$ et $G_i \in T^{(2)}$.

Posons $G_p, \ldots, G_n$ les éléments G_i de cette décomposition qui vérifient $\deg_Y(G_i) = m+j$, et posons, pour $p \leqslant i \leqslant n$, $g_i Y^{m+j}$ le Y terme directeur de G_i,

Posons maintenant $PP(G_i) = X^{\ell_i} Y^{m+j}$.

Alors, en utilisant l'algorithme R_o (cf. Proposition 22.4), nous pouvons déterminer $F_i \in T$, r_i et s_i dans $\mathbb{N}$, tels que $G_i = X^{r_i} Y^{s_i} F_i$. D'où $PP(F_i) = X^{\ell_i - r_i} Y^{m+j-s_i}$.

Posons $f_i Y^{m+j-s_i}$ le Y-terme directeur de F_i. Alors $g_i = X^{r_i} f_i$.

Par conséquent, $f = a_1 X^{r_1} f_1 + \ldots + a_n X^{r_n} f_n$.

De plus, comme $\deg_Y(G_i) = m+j$ alors $\deg_Y(G_i) \geqslant m$, aussi $s_i = j$,

Donc $PP(F_i) = X^{\ell_i - r_i} Y^m$ et $f_i \in U_m$.

D'où $f \in id_{A[X]}(U_m)$.

Or, proposition 32.3, $id_{A[X]}(U_m) = T_m$,

donc $T_{m+j} = T_m$ (nous avions déjà $T_m \subset T_{m+j}$).

Par conséquent, $s(H) \leqslant m$, c'est-à-dire $s(H) \leqslant m(T)$.

Définition 33.2.- Soit H un idéal non nul de $A[X,Y]$, donné avec U un système fini de générateurs. Une partie finie génératrice séparante T de H est dite minimale si et seulement si elle ne contient strictement aucune autre partie finie génératrice séparante de H.

Théorème 33.3.- Soit T une partie finie triangulaire de $A[X,Y]$ et posons $H = id(T)$. Les assertions suivantes sont équivalentes :

(i) T est une partie finie génératrice séparante minimale de H.

(ii) T est une partie finie génératrice séparante de H, et :

(a) $s(H) = m(T)$;

(b) pour tout $j \in \mathbb{N}$, $k(T) \leqslant j \leqslant m(T)$, U_j est une partie finie génératrice séparante minimale de T_j.

(iii) T est une partie finie génératrice séparante de H et :

(a) il existe $F \in T$ tel que $\deg_Y(F) = m(T)$ et, en posant $aX^iY^{m(T)}$ son terme directeur, où $a \in A^o$ et $i \in \mathbb{N}$, alors il n'existe aucun $G \in T$ tel que $\deg_Y(G) = m(T) - 1$ et G a pour terme directeur $\varepsilon aX^iY^{m(t)-1}$, où $\varepsilon \in A^*$.

(b) pour tout $j \in \mathbb{N}$, $k(T) \leqslant j \leqslant m(T)$, U_j est une partie finie génératrice séparante minimale de T_j.

Démonstration :

Elle est du même type que la démonstration donnée pour le théorème 32,2 du chapitre II. C'est-à-dire :

d'abord, nous supposons (i) vérifiée.

Si $s(H) \neq m(T)$, d'après la proposition 33.1, $s(H) < m(T)$.

Posons alors $T' = \{F \in T | \deg_Y(F) < m(T)\}$ et nous démontrons, en utilisant le théorème 14.2, que T' est une partie finie génératrice séparante de H : ce qui contredit le caractère minimal de T.

Donc $s(H) = m(T)$.

De même, s'il existe $j \in \mathbb{N}$, $k(T) \leqslant j \leqslant m(T)$, pour lequel U_j n'est pas minimale, posons $q = \inf\{j \in \mathbb{N} | k(T) \leqslant j \leqslant m(T)$ et U_j non minimale$\}$. En utilisant l'algorithme Λ du chapitre II (cf. Théorème 33.2, chapitre II), nous savons déterminer V_q une partie finie génératrice séparante minimale à partir de U_q, pour T_q.

Posons $T' = \{F \in T | \deg_Y(F) \neq q\} \cup W$

où $W = \{F \in T | F$ a pour Y-terme directeur $f Y^q$ où $f \in V_q\}$.

Donc $T' \subsetneq T$ et en utilisant le théorème 14.2, nous démontrons que T' est une partie finie génératrice séparante de H, ce qui contredit le caractère minimal de T.

Donc, pour tout $j \in \mathbb{N}$, $k(T) \leqslant j \leqslant m(T)$, U_j est une partie finie génératrice séparante minimale de T_j. Par conséquent, (ii) est vérifiée.

Supposons maintenant (ii) vérifiée.

En particulier, $s(H) = m(T)$, aussi $T_{m(T)-1} \neq T_{m(T)}$.
Si, pour tout $F \in T$ tel que $\deg_Y(F) = m(T)$, nous posons $aX^iY^{m(T)}$ son terme directeur, et qu'il existe $G \in T$ de terme directeur $\varepsilon aX^iY^{m(T)-1}$, où $\varepsilon \in A^*$.

Posons $F_1,\ldots,F_p$ les p éléments F_ℓ de T qui vérifient $\deg_Y(F_\ell) = m(T)$. Posons, pour tout $\ell \in \mathbb{N}_p^o$, $a\ X^{i_\ell}Y^{m(T)}$ le terme directeur de F_ℓ, et G_ℓ l'élément de T de terme directeur $\varepsilon_\ell a_\ell X^{i_\ell}Y^{m(T)-1}$, où $\varepsilon_\ell \in A^*$.

Puisque T est triangulaire, nous pouvons supposer $PP(F_1) < \ldots < PP(F_p)$.

Considérons $H_1 = F_1 - Y\,\varepsilon_1^{-1}G_1$ alors $PP(H_1) < PP(F_1)$.
Donc $\deg_Y(H_1) < m(T)$. Posons $f_1Y^{m(T)}$ (resp. $g_1Y^{m(T)-1}$) le Y-terme directeur de F_1 (resp. de G_1). Alors $f_1 = \varepsilon_1^{-1}g_1$.

D'où $f_1 \in T_{m(T)-1}$.

Faisons l'hypothèse suivante : pour $q \in \mathbb{N}_{p-1}^o$, pour tout $j \in \mathbb{N}_q^o$, posons $f_jY^{m(T)}$ le Y-terme directeur de F_j, alors $f_j \in T_{m(T)-1}$.

Considérons F_{q+1} et $f_{q+1}Y^{m(T)}$ son Y-terme directeur.

Posons $H_{q+1} = F_{q+1} - Y\,\varepsilon_{q+1}^{-1}G_{q+1}$.
Donc $PP(H_{q+1}) < PP(F_{q+1})$, aussi $PP(H_{q+1}) = PP(F_q)$.

Par conséquent, nous pouvons écrire $H_{q+1} = \alpha_qF_q + \ldots + \alpha_1F_1 + H_o$ où $\alpha_i \in A$ et $\deg_Y(H_o) < m(T)$.

Alors $f_{q+1} = \varepsilon_{q+1}^{-1}g_{q+1} + \alpha_qf_q + \ldots + \alpha_1f_1$.

Donc $f_{q+1} \in T_{m(T)-1}$.

Par conséquent, pour tout $q \in \mathbb{N}_p^o$, $f_q \in T_{m(T)-1}$.

Or $U_{m(T)} = \{f_1,\ldots,f_p\}$ et $T_{m(T)} = id_{A[X]}(U_{m(T)})$.

Donc $T_{m(T)} \subset T_{m(T)-1}$, c'est-à-dire $T_{m(T)} = T_{m(T)-1}$: contradiction, puisque $s(H) = m(T)$.

Par conséquent, le point (a) de (iii) est vérifié et le point (b) est conservé.

Enfin, supposons (iii) vérifiée.

D'après (a), nous avons $T_{m(T)} \neq T_{m(T)-1}$, aussi $s(H) \geqslant m(T)$. Donc $s(H) = m(T)$ (nous avons toujours $s(H) \leqslant m(T)$, d'après la proposition 33.1).

Considérons alors T' une partie finie génératrice séparante de H, telle que $T' \subset T$. Donc $m(T') \leqslant m(T)$.

La démonstration est alors identique à celle du théorème 32.2 du chapitre II :

- si $m(T') < m(T)$ nous aboutissons à une contradiction.
- donc $m(T') = m(T)$, et, grâce au caractère triangulaire, nous démontrons alors que $T' = T$.

Donc T est minimale.

Proposition 33.4.- Soit H un idéal non nul de $A[X,Y]$, donné avec U un système fini de générateurs. Considérons T et T' deux parties finies génératrices séparantes minimales de H.

Pour qu'il existe $F \in T$ de terme directeur $a X^i Y^j$, où $a \in A^o$, $i \in \mathbb{N}$ et $j \in \mathbb{N}$, il faut et il suffit qu'il existe $G \in T'$, de terme directeur $\varepsilon a X^i Y^j$, où $\varepsilon \in A^*$.

Démonstration identique à celle donnée pour la proposition 32.3 du chapitre II.

Corollaire 33.4a.- Sous les mêmes notations et hypothèses que dans 33.4., pour qu'il existe $F \in T^{(2)}$ de terme directeur aX^iX^j, où $a \in A^o$, $i \in \mathbb{N}$, $j \in \mathbb{N}$, il faut et il suffit qu'il existe $G \in T'^{(2)}$, de terme directeur $\varepsilon\, aX^iX^j$, où $\varepsilon \in A^*$.

34. *Construction d'une partie finie génératrice séparante minimale.*

34.1.- *Algorithme* Λ.

Entrée : U partie finie non vide et non nulle de $A[X,Y]$.

Sortie : T partie finie génératrice séparante minimale de $H = id_{A[X,Y]}(U)$.

Sous programme : algorithme Θ.

Début : $T := \Theta(U)$; $m := \max\{d^oF \mid F \in T\}$;

S'il existe $F \in T$ et $G \in T$ tels que $F \neq G$,

ter-direct(F) = ε.ter-direct(G) où $\varepsilon \in A^*$ alors retourner $(T-T_{[Y^m]})$.

Sinon retourner T.

Fin.

Remarque :

Rappelons que $T_{[Y^m]} = \{F \in T \mid \exists i \in \mathbb{N} \quad PP(F) = X^iY^m\}$.

Théorème 34.2.- Soit H un idéal non nul de $A[X,Y]$, dont U un système fini de générateurs est donné. Nous avons les résultats suivants :

(i) l'algorithme Λ cesse au bout d'un nombre fini d'opérations ;

(ii) le résultat est une partie finie génératrice séparante minimale de H.

Démonstration :

Elle est identique à la démonstration du théorème 33.2 du chapitre II.

CHAPITRE IV

DECOMPOSITION PRIMAIRE - METHODE EFFECTIVE

Dans un premier paragraphe, nous rappelons la définition d'une décomposition primaire ainsi que le théorème d'existence dans le cas noethérien, dont une démonstration est donnée dans [SZ]. Remarquons que cela constitue une démarche classique.

Par contre, d'un point de vue constructiviste, il suffit de donner la définition d'un idéal primaire, établir ses différentes caractérisations, puis donner la définition d'une décomposition primaire. Enfin, l'existence de celle-ci est assurée par sa construction effective.

C'est ce que nous ferons dans les paragraphes suivants, en nous inspirant de la méthode proposée par C.W. Ayoub dans [AY 1]. Celle-ci consiste d'abord à décomposer l'idéal étudié en une intersection finie d'idéaux particuliers de deux types, dont des parties finies génératrices sont déterminées, puis, pour chacun de ces deux types, déterminer une décomposition primaire. C'est dans cette seconde étape que notre travail trouve son originalité.

1 - EXISTENCE D'UNE DECOMPOSITION PRIMAIRE.

11. Idéaux primaires.

Définition 11.1.- Soit A un anneau commutatif unitaire. Considérons Q un idéal de A. Nous dirons que Q est un idéal primaire de A si et seulement si :

$$\forall\, a \in A\ \forall\, b \in A\ \langle ab \in Q \wedge b \notin Q \rangle \implies \langle \exists m \in \mathbb{N}^{o}\ a^{m} \in Q \rangle .$$

Proposition 11.2.- Soit A un anneau commutatif unitaire. Considérons Q un idéal primaire de A. Posons $P = \sqrt{Q}$ alors nous avons les résultats suivants :

(i) P est un idéal premier de A ;

(ii) $\forall\, a \in A\ \forall\, b \in A\ \langle ab \in Q \wedge b \notin Q \rangle \implies \langle a \in P \rangle$

12. Caractérisation des idéaux primaires.

Théorème 12.1.- Soit A un anneau commutatif unitaire. Considérons P et Q deux idéaux de A. Alors les assertions suivantes sont équivalentes :

(i) Q est un idéal primaire de A de racine P.

(ii) Q et P vérifient :

(*) $Q \subset P$.

(**) $\forall\, x \in P\ \exists\, m \in \mathbb{N}^{o}\ x^{m} \in Q$.

(***) $\forall\, a \in A\ \forall\, b \in A\ \langle ab \in Q \wedge b \notin Q \rangle \implies \langle a \in P \rangle$

(iii) Q et P vérifient :

(*) $Q \subset P$.

(**) $\forall\, x \in P\ \exists\, m \in \mathbb{N}^{o}\ x^{m} \in Q$.

(***) $\forall\, a \in A\ \forall\, b \in A\ \langle ab \in Q \wedge b \notin P \rangle \implies \langle a \in Q \rangle$

13. Décomposition primaire.

Définition 13.1.- Soit A un anneau commutatif unitaire. Nous dirons qu'un idéal H de A admet une décomposition primaire si et seulement s'il

existe un entier naturel n non nul et n idéaux primaires de A, $Q_1,\ldots,Q_n$ tels que $H = \bigcap_{i=1}^{n} Q_i$.

Posons alors $P_i = \sqrt{Q_i}$, pour $i \in \mathbb{N}_n^o$, alors $P_1,\ldots,P_n$ sont appelés idéaux premiers de A associés à H.

Définition 13.2.- Soit A un anneau commutatif unitaire. Soit H un idéal de A admettant une décomposition primaire. Nous dirons qu'une décomposition primaire $H = \bigcap_{i=1}^{n} Q_i$ est réduite si et seulement si, en posant, pour tout $i \in \mathbb{N}_n^o$, $P_i = \sqrt{Q_i}$, nous avons :

(i) $\forall\, i \in \mathbb{N}_n^o \quad \forall\, j \in \mathbb{N}_n^o \quad i \neq j \implies P_i \neq P_j$

(ii) $\forall\, j \in \mathbb{N}_n^o \quad \bigcap_{\substack{i=1 \\ i\neq j}}^{n} Q_i \not\subset Q_j$.

Proposition 13.3.- Soit A un anneau commutatif unitaire. Soit H un idéal de A. Si H admet une décomposition primaire alors H admet une décomposition primaire réduite.

Définition 13.4.- Soit A un anneau commutatif unitaire. Considérons H un idéal de A admettant une décomposition primaire réduite.

Alors les éléments minimaux dans l'ensemble des idéaux premiers associés à H sont appelés idéaux premiers isolés associés à H ; ceux qui ne sont pas isolés sont dits immergés.

Théorème 13.5. (*Lasker-Noether*)

Soit A un anneau noethérien. Alors tout idéal de A admet une décomposition primaire réduite.

14. Localisation.

Proposition 14.1.- Soient A un anneau noethérien et H un idéal de A. Considérons P un idéal premier de A, associé à H. Posons ψ l'homéomorphisme canonique de A dans le localisé A_P.

Si K est la composante P primaire de H_P alors $\psi^{-1}(K)$ est la composante P primaire de H.

Démonstration.

cf. [BOU].

2 - RESULTATS PRELIMINAIRES.

21. Multiplicités.

Les notions introduites et les résultats énoncés ici, sont tirés des références [SAM] et [SER].

Proposition 21.1.- Un anneau artinien est de dimension zéro.

Cf. [SER] p. III - 1.

Proposition 21.2.- Soit A un anneau local artinien, d'idéal maximal M. Posons m la longueur de A. Considérons H un idéal A, primaire pour M.

Alors $P_H(n) = m$ pour n assez grand, où P_H est le polynôme de Hilbert-Samuel.

Cf. [SAM] p. 28, théorème 5.

Corollaire 21.2a.- Pour un anneau local artinien, la multiplicité coïncide avec la longueur.

En effet, la multiplicité est définie comme étant le coefficient du terme de plus haut degré du polynôme de Hilbert-Samuel.

22. Relèvement des éléments d'un anneau quotient.

Proposition 22.1.- Soit A un anneau codable. Prenons α une numérotation de A. Alors nous avons les résultats :

(i) pour tout $a \in A$, nous pouvons déterminer une numérotation β de $A_{/A.a}$.

(ii) $A_{/A.a}$ étant numéroté par β, nous pouvons déterminer une fonction récursive $\rho_a : A_{/A.a} \to A$, telle que si $s : A \to A_{/A.a}$ est la surjection canonique, alors, pour tout $\omega \in A_{/A.a}$, $s \circ \rho_a(\omega) = \omega$.

Démonstration :

Pour $b \in A$, nous voulons déterminer la classe de b modulo a, nous devons donc résoudre l'équation $x-ay = 0$, ce que nous savons faire récursivement en utilisant (E 3) (cf. I, définition 41.1).

S l'ensemble des solutions est défini par un système fini de générateurs et S_b l'ensemble des solutions de $x-ay = b$ est défini par

$$S_b = (b,0) + S.$$

Donc la classe de b modulo a est la projection de la première composante de S_b.

Nous pouvons déterminer récursivement $k_b = \inf\{n \mid \exists z \in A \ (\alpha(n),z) \in S_b\}$

En rangeant les k_b par ordre croissant nous numérotons alors $A/A.a$.

Posons β cette numérotation.

Maintenant soit $\omega \in A_{/A.a}$, $\omega = \beta(i)$ pour $i \in \mathbb{N}$.

D'après ce qui précède i correspond à un unique k_b.

Alors $\rho_a(\omega) = \alpha(k_b)$, ce qui est bien récursif.

Remarque 22.2.- Si nous remplaçons α dans 21.1 par α' numérotation récursivement équivalente, alors β' la numérotation de $A_{/A.a}$ construite à partir de α', est récursivement équivalente à β.

Proposition 22.3.- Soit A un anneau codable. Pour tout $a \in A$, l'anneau quotient $A_{/A.a}$ est un anneau codable.

Démonstration :

Prenons α une numérotation de A, dans la classe dont est muni A. D'après 22.2, la démonstration est indépendante de ce choix.

Nous devons établir les axiomes (E0) à (E4) de I, définition 41.1 (page 10).

(E0) est évidemment vérifié.

Pour (E1), prenons ω_1 et ω_2 dans $A_{/A.a}$ alors $\omega_1 = \beta(i_1)$ et $\omega_2 = \beta(i_2)$, avec $\alpha(i_1)$ (resp. $\alpha(i_2)$) représentant de ω_1 (resp. de ω_2) et i_1 (resp. i_2) plus petit indice.

Déterminons $\alpha(i_1) + \alpha(i_2) = \alpha(j)$ puisque A est codable. Alors nous avons $\omega_1 + \omega_2 = \beta(k_{\alpha(j)})$ où

$k_{\alpha(j)} = \inf\{n \mid \exists z \in A \ \ \alpha(n),z) \in S_{\alpha(j)}\}$.

Donc (E1) est vérifié. Pour (E2) la démonstration est identique.

Posons à (E3). Considérons $\omega_1,\ldots,\omega_n$ dans $A_{/A.a}$ et nous devons déterminer un système fini de générateurs de l'ensemble des solutions de l'équation $\sum_{i=1}^{n} \omega_i.x_i = 0$, dans $A_{/A.a}$.

Or, pour tout $i \in \mathbb{N}_n^o$, $\omega_i = \beta(j_i)$, donc c'est équivalent à déterminer un système fini de générateurs de l'ensemble des solutions de l'équation $\sum_{i=1}^{n} \alpha(j_i).y_i + a.z = 0$, ce qui est possible en utilisant (E3) pour A codable et déterminer pour chaque composante d'un générateur le plus petit indice de sa classe, ce qui est récursif, donc (E3) est vérifié.

Pour (E4) la démonstration est identique.

Par conséquent, $A_{/A.a}$ est un anneau codable.

Définition 22.4.- Soit A un anneau codable. Nous dirons que A est fortement factoriel si :

(FF1) A est à la fois principal algorithmique et factoriel algorithmique ;

(FF2) $A[X]$ est un anneau factoriel algorithmique ;

(FF3) Pour tout π irréductible de A, le corps quotient $A_{/A.\pi}$ est un corps factoriel.

Proposition 22.5.- Soit A un anneau fortement factoriel. Alors son corps des fractions est un corps factoriel.

Démonstration :

Cf. I, 52.1.

Proposition 22.6.- $\mathbb{Z}$, l'anneau des entiers relatifs, est un anneau fortement factoriel.

Démonstration :

De façon évidente, $\mathbb{Z}$ est un anneau à la fois principal algorithmique et factoriel algorithmique. Pour (FF2) cf. I, 56.1 et pour (FF3) cf. I, 57.1.

23. *Décomposition primaire d'un idéal dans un anneau à la fois principal algorithmique et factoriel algorithmique.*

Les résultats de ce sous-paragraphe sont élémentaires, mais proposent une méthode simple de détermination explicite de la décomposition primaire pour des exemples connus.

Dans ce qui suit, A est un anneau à la fois principal algorithmique et factoriel algorithmique. Notons p la fonction récursive associée à A principal algorithmique (cf. I, 43.2) et dec la fonction récursive associée à A factoriel algorithmique (cf. I, 44.1).

Algorithme DPØ.

Entrée : H idéal de A, donné par U un système fini de générateurs.

Sortie : une décomposition primaire de H.

Sous-programmes : p, dec.

Début : Si $U = \{0\}$ alors retourner $\{0\}$.

Sinon

Début : $r := \mathrm{card}(U)$; $U := \{a_1,\ldots,a_r\}$;

Tant que $j \leq r$ faire

Début Tq : si $a_j = 0$ alors $U := U - a_j$;

$j := j+1$;

Fin Tq.

Utiliser p pour déterminer a le pgcd des éléments de U ;

Utiliser dec pour déterminer la décomposition en produit fini de facteurs irréductibles de a ; $\mathrm{dec}(a) := \varepsilon \prod_{i=1}^{n} \pi_i^{k_i}$;

Retourner $\bigcap_{i=1}^{n} \mathrm{id}_A(\pi_i^{k_i})$.

Fin.

Fin.

23.1.- Il est facile de vérifier que le résultat de DPØ est bien une décomposition primaire de H.

Pour tout $i \in \mathbb{N}_n^o$, $\mathrm{id}_A(\pi_i^{k_i})$ est un idéal primaire de A de racine $\mathrm{id}_A(\pi_i)$.

Proposition 23.2.- Nous avons les résultats suivants :

(i) l'anneau $\mathbb{Z}$ des entiers relatifs possède un algorithme DPØ ;

(ii) soit K un corps factoriel. Alors $K[X]$ possède un algorithme DPØ.

24. *Résultats sur les transporteurs.*

La proposition qui suit est essentielle pour la décomposition d'un idéal sous forme d'intersection.

Proposition 24.1.- Soit A un anneau commutatif et unitaire. Considérons H un idéal de A. S'il existe $v \in A$ pour lequel il existe $n \in \mathbb{N}^o$ tel que $H : id_A(v^n) = H : id_A(v^{n+1})$ alors nous avons :

$$H = (H + id_A(v^n)) \cap (H : id_A(v^n)).$$

Démonstration :

Soit $v \in A$ pour lequel il existe $n \in \mathbb{N}^o$ tel que $H : id_A(v^n) = H : id(v^{n+1})$. Nous avons $H \subset H : id_A(v^n)$ aussi $H \subset (H + id_A(v^n)) \cap (H : id_A(v^n))$.

De plus, puisque $H \subset H : id_A(v^n)$, nous avons :
$(H + id_A(v^n)) \cap (H : id_A(v^n)) = H + id_A(v^n) \cap (H : id_A(v^n))$.

Maintenant, soit $y \in id_A(v^n) \cap (H : id_A(v^n))$, alors il existe $a \in A$ tel que $y = av^n$ et $yv^n \in H$.

D'où $yv^n = av^{2n} = av^{n-1}.v^{n+1}$ car $n \in \mathbb{N}^o$ et $av^{n-1} \in H : id_A(v^{n+1})$. Or $H : id_A(v^{n+1}) = H : id_A(v^n)$,

donc $av^{n-1} \in H : id_A(v^n)$, c'est-à-dire $av^{n-1}.v^n \in H$, d'où $yv^{n-1} \in H$ et $y \in H : id_A(v^{n-1})$.

Faisons l'hypothèse de récurrence suivante :

Pour $k \in \mathbb{N}$ et $k < n$, $yv^{n-k} \in H$.

Donc $av^n.v^{n-k} \in H$, aussi $av^{n-k-1}.v^{n+1} \in H$ c'est-à-dire $av^{n-k-1} \in H : id_A(v^{n+1})$, or $H : id_A(v^{n+1}) = H : id_A(v^n)$ aussi $av^{n-k-1} \in H : id_A(v^n)$, donc $av^n.v^{n-k-1} \in H$ c'est-à-dire $yv^{n-k-1} \in H$.

Par conséquent, l'hypothèse de récurrence est vraie pour $k = 1$ et si elle l'est pour k, elle l'est pour $k+1$.

Nous en déduisons que $y \in H$, aussi :

$$H = (H + id_A(v^n)) \cap (H : id_A(v^n)).$$

Proposition 24.2.- Soit A un anneau noethérien. Considérons H un idéal de A, $v \in A$ et T un idéal de A contenu dans la racine de H. Posons $K = T + id_A(v)$. Pour que $H : K = H$ il faut et il suffit que $H : id_A(v) = H$.

Démonstration :

Supposons d'abord $H : id_A(v) = H$. Comme $K = H + id_A(v)$, $H : K = (H : T) \cap (H : id_A(v)) = (H : T) \cap H$.

Or $H \subset H : T$, aussi $H : K = H$.

Supposons maintenant $H : K = H$.

Pour $n \in \mathbb{N}^o$, faisons l'hypothèse suivante $H : K^n = H$.

Alors $H : K^{n+1} = (H : K^n) : K = H : K = H$.

Aussi pour tout $n \in \mathbb{N}^o$, $H : K^n = H$.

Maintenant, puisque A est noetherien et, pour tout $m \in \mathbb{N}^o$, $H : id_A(v^m) \subset H : id_A(v^{m+1})$, il existe un entier non nul k tel que $H : id_A(v^k) = H : id_A(v^{k+1})$.

Alors d'après la proposition 24.1, $H = (H + id_A(v^k)) \cap (H : id_A(v^k))$.

En outre, $K = T + id_A(v)$ et $T \subset \sqrt{H}$,

aussi $K \subset \sqrt{H} + \sqrt{id_A(v)}$. Mais $\sqrt{id_A(v)} = \sqrt{id_A(v^k)}$,

donc $K \subset \sqrt{H} + \sqrt{id_A(v^k)} \subset \sqrt{\sqrt{H} + \sqrt{id_A(v^k)}}$.

Or $\sqrt{\sqrt{H} + \sqrt{id_A(v^k)}} = \sqrt{H + id_A(v^k)}$

donc $K \subset \sqrt{H + id_A(v^k)}$.

Comme A est noethérien, alors il existe un entier naturel non nul q tel que $K^q \subset H + id_A(v^k)$.

Or, nous avons démontré plus haut que $H = H : K^q$,

donc $H = [(H + id_A(v^k)) \cap (H : id_A(v^k))] : K^q$

et $H = [(H + id_A(v^k)) : K^q] \cap [(H : id_A(v^k)) : K^q]$.

Mais $K^q \subset H + id_A(v^k)$ aussi $(H + id_A(v^k)) : K^q = A$.

Par conséquent $H = (H : id_A(v^k)) : K^q$

d'où $H = (H : K^q) : id_A(v^k)$

et $H = H : id_A(v^k)$, puisque $H : K^q = H$.

Maintenant soit $x \in H : id_A(v)$, alors $xv \in H$, aussi en particulier, $xv \in H : id_A(v^k)$, donc $xv^{k+1} \in H$.

Or $H : id_A(v^{k+1}) = H : id_A(v^k)$, donc $x \in H : id_A(v^k)$.

Comme $H = H : id_A(v^k)$, alors $x \in H$, par conséquent :

$$H = H : id_A(v).$$

Corollaire 24.2a.- Soient A un anneau noethérien et H un idéal de A.

Considérons v_1 et v_2 deux éléments de A tels que $v_1 - v_2 \in \sqrt{H}$.

Pour que $H : id_A(v_1) \supsetneq H$ il faut et il suffit que $H : id_A(v_2) \supsetneq H$.

Démonstration :

Posons $K = \sqrt{H} + id_A(v_1)$; puisque $v_1 - v_2 \in \sqrt{H}$, $\sqrt{H} + id_A(v_2) = K$.

D'après la proposition 24.2, $H : id_A(v_1) = H$ équivaut à $H : K = H$.

Or, pour la même raison, $H : K = H$ équivaut à $H : id_A(v_2) = H$.

Par conséquent, pour que $H : id_A(v_1)$ il faut et il suffit que $H : id_A(v_2) = H$, donc pour que $H : id_A(v_1) \supsetneq H$ il faut et il suffit que $H : id_A(v_2) \supsetneq H$.

Proposition 24.3.- Soit B un anneau commutatif et unitaire. Considérons H un idéal de B et u un élément de B, pour lequel il existe $n \in \mathbb{N}^o$, tel que $u^n \in H$. Pour tout $i \in \mathbb{N}_{n-1}$, posons $H_i = H : id_B(u^i) + id_B(u)$. Soit $v \in B$; si, pour tout $i \in \mathbb{N}_{n-1}$, nous avons $H_i : id_B(v) = H_i$, alors $H : id_B(v) = H$.

Démonstration :

Supposons d'abord $n = 1$. Donc $H_o = H : id_B(u^o) + id_B(u)$. Or $u^o = 1$ et $u^1 = u$, aussi $u \in H$ et $H_o = H$.

Par conséquent, soit $v \in B$, tel que $H_o : id_B(v) = H_o$, alors $H : id_B(v) = H$.

Maintenant, supposons $n \neq 1$. Faisons l'hypothèse suivante : la proposition est vraie pour $n-1$.

Considérons $v \in B$, pour lequel, pour tout $i \in \mathbb{N}_{n-1}$, $H_i : id_B(v) = H_i$. Soit $x \in H : id_B(v)$. Comme $H_o = H + id_B(u)$, nous avons $H \subset H_o$, aussi $H : id_B(v) \subset H_o : id_B(v)$. Or $H_o = H_o : id_B(v)$, donc $H : id_B(v) \subset H_o$, et, en particulier $x \in H_o$, c'est-à-dire $x = h + au$, avec $h \in H$ et $a \in B$.

D'où $xv = hv + auv$.

Puisque $x \in H : id_B(v)$, alors $xv \in H$, et, comme $h \in H$, nous en déduisons que $auv \in H$, c'est-à-dire $a \in H : id_B(uv)$.

Posons $T = H : id_B(u)$. Comme $u^n \in H$ alors $u^{n-1} \in T$.

Posons alors $T_j = T : id_B(u^j) + id_B(u)$, pour $j \in \mathbb{N}_{n-2}$.

Aussi $T_j = (H : id_B(u)) : id_B(u^j) + id_B(u) = H : id_B(u^{j+1}) + id_B(u)$.

Donc $T_j = H_{j+1}$.

Par conséquent, pour tout $j \in \mathbb{N}_{n-2}$,

$$T_j : id_B(v) = H_{j+1} : id_B(v) = H_{j+1} = T_j.$$

Appliquons alors l'hypothèse :

$$T : id_B(v) = T.$$

Donc $H : id_B(uv) = H : id_B(u)$. Or $a \in H : id_B(uv)$, donc $a \in H : id_B(u)$ et $au \in H$. Comme $x = h + au$ avec $h \in H$, nous obtenons $x \in H$.

Or, ceci est vrai pour tout $x \in H : id_B(v)$,

donc $H : id_B(v) = H$.

Proposition 24.4.- Soit A un anneau commutatif et unitaire.

Considérons H et K deux idéaux de A, pour lesquels il existe $n \in \mathbb{N}^o$ tel que $H : K^n = H : K^{n+1}$.

Posons $r = \inf \{\ell | \ell \in \mathbb{N} \ ; \ H : K^\ell = H : K^{\ell+1}\}$. Alors pour tout $m \in \mathbb{N}^o$, dès que $m \geq r$, nous avons $H : K^m = H : K^r$.

Démonstration :

Posons $E = \{\ell | \ell \in \mathbb{N} \ ; \ H : K^\ell = H : K^{\ell+1}\}$. Comme $n \in E$, $E \neq \emptyset$ et nous pouvons considérer $r = \inf E$. Nous avons $H : K^{r+1} = H : K^r$.

Faisons l'hypothèse suivante : pour $m \in \mathbb{N}$, $m \geq 1$,

$H : K^{r+m} = H : K^r$;

$H : K^{r+m+1} = (H : K^{r+m}) : K = (H : K^r) : K = H : K^{r+1} = H : K^r$.

c.q.f.d.

25. *Transporteur d'un idéal de* $A[X]$ *par un élément irréductible de* A, *où* A *est un anneau à la fois principal algorithmique et factoriel algorithmique.*

Dans ce qui suit, A est un anneau à la fois principal algorithmique, dont nous notons p la fonction récursive associée, et factoriel algorithmique, dont nous notons dec la fonction récursive associée, (cf. I. 43.2 et 44.1).

Proposition 25.1.- Soit H un idéal non nul de $A[X]$, donné par U un système fini de générateurs. Posons $T = \{F_1,\ldots,F_n\}$ la partie génératrice séparante minimale de H, obtenue à partir de U, avec pour $i \in \mathbb{N}^o_{n-1}$, $d^oF_{i+1} = 1 + d^oF_i$

Considérons π un élément irréductible de A.
Pour que $H : id_{A[X]}(\pi) \supsetneq H$, il faut et il suffit que π soit un facteur irréductible de $c(F_1)$ le contenu de F_1, où F_1 est l'élément de plus bas degré de T.

Démonstration :

D'après II, 23.3, nous avons, pour tout $i \in N^o_n$, $F_i = c(F_i).H.H_i$ où H est un polynôme primitif de $A[X]$, H_i est un polynôme unitaire de degré i-1 de $A[X]$.

Alors $H_1 = 1$ et $F_1 = c(F_1).H$.
Utilisons dec pour déterminer $c(F_1) = \varepsilon.\prod_{i=1}^{k} \pi_i^{\alpha_i}$, $\varepsilon \in A^*$, $\alpha_i \neq 0$.
Par conséquent, $H : id_{A[X]}(\pi_i) \supsetneq H$.

Maintenant, considérons π un élément irréductible de A, étranger avec π_i, pour tout $i \in \mathbb{N}^o_k$.

Déterminons $p(\pi,c(F_1))$. Alors $p(\pi,c(F_1)) = (u,v,\pi,c(F_1))$ puisque π est étranger avec $c(F_1)$.

Donc $1 = u.\pi + v.c(F_1)$ (*)

Prenons $G \in H : id_{A[X]}(\pi)$, donc $\pi.G \in H$.

En particulier, $\pi.G = g.H$ avec $g \in A[X]$.

Passons aux contenus, $\pi.c(G) = c(g)$ car H est primitif.

Donc $g = \pi.g_1$ avec $g_1 \in A[X]$, et $G = g_1.H$.

Multiplions (*) par G :

$G = u.(\pi.G) + v.c(F_1).g_1.H$

d'où $G = u.(\pi.G) + (v.g_1).(c(F_1).H)$

c'est-à-dire $G = u.(\pi.G) + (v.g_1).F_1$.

Donc $G \in H$ et $H : id_{A[X]}(\pi) = H$.

La proposition 25.1 est ainsi démontrée.

Corollaire 25.1a.- Sous les mêmes notations et hypothèses que 24.1, nous pouvons déterminer explicitement tous les éléments irréductibles π de A tels que $H : id_{A[X]}(\pi) \not\supseteq H$.

De plus, ils sont en nombre fini, aux inversibles près.

Maintenant, nous allons donner un algorithme qui permet de déterminer un système fini de générateurs du transporteur $H : id_{A[X]}(\pi)$.

Algorithme transporteur.

Entrées : U une partie finie non vide et non nulle de $A[X]$ et π un élément irréductible de A.

Sortie : Un système fini de générateurs de $id_{A[X]}(U) : id_{A[X]}(\pi)$.

Sous-programme : p application récursive associée à A principal algorithmique.

Début : $T := \Lambda(U)$; $T = \{F_1,\ldots,F_n\}$ rangée par ordre croissant des degrés ;

Tant que $i \leq n$ faire c_i := contenu de F_i ;

si F_1 divise π alors retourner $\{1\}$;

sinon $t := \max\{i \mid i \in \mathbb{N}_n^o ; \pi \text{ divise } c_i\}$;

retourner $\{F_{1/\pi}, \ldots, F_{t/\pi}, F_{t+1}, \ldots, F_n\}$;

Fin.

Proposition 25.2.- Considérons H un idéal non nul de $A[X]$, donné par U un système fini de générateurs et π un élément irréductible.

Alors l'algorithme transporteur détermine une partie finie génératrice séparante minimale de $H : \mathrm{id}_{A[X]}(\pi)$.

Démonstration :

1er cas : F_1 divise π, alors :

ou bien $F_1 \in A^*$ donc $H = A[X]$ et $H : \mathrm{id}_{A[X]}(\pi) = A[X]$.

ou bien $F_1 = \varepsilon.\pi$ avec $\varepsilon \in A^*$ donc $H : \mathrm{id}_{A[X]}(\pi) = A[X]$.

Dans ce cas, $\{1\}$ est bien une partie finie génératrice séparante minimale de $H : \mathrm{id}_{A[X]}(\pi)$.

2ème cas : F_1 ne divise pas π.

Supposons d'abord que pour tout $i \in \mathbb{N}_n^o$, π ne divise pas c_i. Donc $t = 0$.

De plus, π est étranger avec c_1 le contenu de l'élément de plus bas degré de T. Nous utilisons alors la proposition 25.1 :

$$H : \mathrm{id}_{A[X]}(\pi) = H$$

d'où $\{F_1, \ldots, F_n\}$ est une partie finie génératrice séparante minimale de $H : \mathrm{id}_{A[X]}(\pi)$ et, comme $t = 0$, c'est ce que détermine l'algorithme transporteur.

Supposons maintenant qu'il existe $j \in \mathbb{N}_n^o$ tel que π divise c_j. D'après II. 23.3, nous savons que, pour tout $i \in \mathbb{N}_{n-1}^o$, c_{i+1} divise c_i. Donc, nous pouvons définir $t = \max \{i | i \in \mathbb{N}_n^o \ ; \ \pi \text{ divise } c_i\}$ et :

- pour $i \leqslant t$, π divise c_i
- pour $i > t$, π est étranger avec c_i ;

D'après II, 23.3, $F_i = c_i.H.H_i$ avec $H \in A[X]$, primitif et $d^oH = d^oF_1$, et $H_i \in A[X]$, unitaire et $d^oH_i = i-1$.

Donc $\{F_{1/\pi}, \ldots, F_{t/\pi}, F_{t+1}, \ldots, F_n\} \subset H : id_{A[X]}(\pi)$.

Maintenant, soit $G \in H : id_{A[X]}(\pi)$, alors $\pi.G \in H$, donc : $\pi.G = a_1.F_1 + \ldots + a_{n-1}F_{n-1} + P.F_n$, où $a_j \in A$ et $P \in A[X]$.
Posons $L = A_{/A.\pi}$. Dans $L[X]$, nous obtenons :

$$0 = \bar{a}_{t+1}.\bar{F}_{t+1} + \ldots + \bar{a}_{n-1}\bar{F}_{n-1} + \bar{P}.\bar{F}_n$$

c'est-à-dire

$$0 = \bar{a}_{t+1}.\bar{c}_{t+1}.\bar{H}.\bar{H}_{t+1} + \ldots + \bar{a}_{n-1}.\bar{c}_{n-1}.\bar{H}.\bar{H}_{n-1} + \bar{P}.\bar{c}_n.\bar{H}.\bar{H}_n.$$

Or H est primitif donc $\bar{H} \neq 0$, aussi :

$$0 = \bar{a}_{t+1}.\bar{c}_{t+1}.\bar{H}_{t+1} + \ldots + \bar{a}_{n-1}.\bar{c}_{n-1}.\bar{H}_{n-1} + \bar{P}.\bar{c}_n.\bar{H}_n.$$

ce que nous écrivons

$$\bar{a}_{t+1}.\bar{c}_{t+1}.\bar{H}_{t+1} + \ldots + \bar{a}_{n-1}.\bar{H}_{n-1} = -\bar{P}.\bar{c}_n.\bar{H}_n \qquad (*).$$

Or H_j est unitaire, donc $\bar{H}_j \neq 0$ et $d^o\bar{H}_j = d^oH_j = j-1$.
Si $\bar{P} \neq 0$ alors $d^o(\bar{P}.\bar{H}_n) \geqslant n-1$, or le degré du premier membre de (*) est strictement inférieur à $n-1$: contradiction.

Par conséquent, $\bar{P} = 0$, c'est-à-dire $P = \pi.Q$, et le premier membre de (*) est identiquement nul. Remarquons que $d^{o}\bar{H}_{j+1} = 1+d^{o}\bar{H}_{j}$, alors en utilisant le même type de raisonnement, nous obtenons :

pour tout $j \in \mathbb{N}$, $t+1 \leqslant j \leqslant n$, $\bar{a}_j = 0$, c'est-à-dire $a_j = \pi.b_j$.

Par conséquent,

$$G = a_1.(F_{1/\pi} + \ldots + a_t.(F_{t/\pi}) + b_{t+1}.F_{t+1} + \ldots + b_{n-1}.F_{n-1} + Q.F_n$$

et H : $\mathrm{id}_{A[X]}(\pi) = \mathrm{id}_{A[X]}(F_{1/\pi},\ldots,F_{t/\pi},F_{t+1},\ldots,F_n)$.

Donc l'algorithme transporteur détermine un système fini de générateurs de H : $\mathrm{id}_{A[X]}(\pi)$. Vérifions que c'est une partie finie génératrice séparante minimale :

nous avons $T = \{F_1,\ldots,F_n\}$ partie finie génératrice séparante minimale de H.

(i) pour $i < t$, $X.F_i = a_{i,i+1}.F_{i+1} + \ldots + a_{i,1}.F_1$

donc $X.(F_{i/\pi}) = a_{i,i+1}.(F_{i+1/\pi}) + \ldots + a_{i,1}.(F_{1/\pi})$

(ii) pour $i = t$, $X.F_t = a_{t,t+1}.F_{t+1} + a_{t,t}.F_t + \ldots + a_{t,1}.F_1$.

Or, pour $1 \leqslant j \leqslant t$, π divise F_j ; mais π ne divise pas F_{t+1}, donc π divise $a_{t,t+1}$. Alors :

$$X.(F_{t/\pi}) = (a_{t,t+1/\pi}).F_{t+1} + a_{t,t}.(F_{t/\pi}) + \ldots + a_{t,1}.(F_{1/\pi}) .$$

(iii) pour $i > t$, $X.F_i = a_{i,i+1}.F_{i+1} + \ldots + a_{i,1}.F_1$

$$= a_{i,i+1}.F_{i+1} + \ldots + a_{i,t+1}.F_{t+1}$$

$$+ (a_{i,t}.\pi).(F_{t/\pi}) + \ldots + (a_{i,1}.\pi).(F_{1/\pi}).$$

Par conséquent, d'après II, 13.2, l'algorithme transporteur détermine une partie finie génératrice séparante minimale de H : $\mathrm{id}_{A[X]}(\pi)$.

3 - PREMIERE ETAPE : DECOMPOSITION EN IDEAUX DE TYPE (I) ET DE TYPE (II).

Dans ce paragraphe, nous supposons que A est un anneau à la fois principal algorithmique dont nous notons p la fonction récursive associée, et factoriel algorithmique dont nous notons dec la fonction récursive associée.

31. Idéaux de type (I) et idéaux de type (II).

D'après le corollaire 25.1a, nous sommes en mesure de déterminer explicitement, pour H un idéal non nul de $A[X]$, donné par U un système fini de générateurs, tous les éléments π irréductibles de A, tels que $H : \mathrm{id}_{A[X]}(\pi) \not\supseteq H$.

Nous allons étudier ici deux cas particuliers qui interviennent dans la première étape de la méthode de détermination d'une décomposition primaire.

Proposition 31.1.- Soit H un idéal propre non nul de $A[X]$, donné par U un système fini de générateurs. Les assertions suivantes sont équivalentes :

(i) pour tout élément irréductible π de A, $H : \mathrm{id}_{A[X]}(\pi) = H$;

(ii) H vérifie : $(a)_o$ $\sqrt{H} \cap A = \{0\}$.

$(b)_o$ posons $S = A - \{0\}$. Pour tout $s \in S$,

$$H : \mathrm{id}_{A[X]}(s) = H.$$

Démonstration :

Supposons (i). Soit $s \in S$, en utilisant dec, nous pouvons déterminer $s = \varepsilon . \prod_{j=1}^{k} \pi_j$, où $\varepsilon \in A^*$ et π_j élément irréductible de A.

Alors $(b)_o$ se démontre par récurrence sur k, puisque pour $k = 1$ c'est vrai.

Maintenant soit $a \in \sqrt{H} \cap A$. Supposons $a \neq 0$. Alors il existe $\ell \in \mathbb{N}^o$ tel que $a^\ell \in H$. Posons $m = \inf\{i | a^i \in H\}$, donc $m \neq 0$.

Nous avons $a^{m-1} \in H$: $id_{A[X]}(a)$. Mais $a \in S$ donc $a^{m-1} \in H$: contradiction. D'où $a = 0$.

Réciproquement, (1) est une conséquence de $(b)_o$.

Définition 31.2.- Soit H un idéal propre non nul de $A[X]$, donné par U un système fini de générateurs.

Nous dirons que H est de type (I) si et seulement s'il vérifie l'une des deux assertions équivalentes de 31.1.

Théorème 31.3.- Soit H un idéal propre non nul de $A[X]$, donné par U un système fini de générateurs.

Pour que H soit un idéal de type (I), il faut et il suffit que la partie génératrice séparante minimale de H, obtenue à partir de U, soit réduite à un élément primitif de $A[X]$, non constant.

Démonstration :

Supposons H idéal de type (I). Posons $T = \{F_1, \ldots, F_n\}$ la partie finie génératrice séparante minimale de H, obtenue à partir de U, rangée par ordre des degrés croissants. D'après II, 23.3, nous pouvons déterminer, pour tout $i \in \mathbb{N}_n^o$,

$F_i = c(F_i).H.H_i$ où $H \in A[X]$, primitif et $d^oH = d^oF_1$

$H_i \in A[X]$, unitaire et $d^oH_i = i-1$

$c(F_{i+1})$ divise $c(F_i)$.

Si $c(F_1) \notin A^*$, alors, d'après 25.1, H ne peut être de type (I). Donc $c(F_1) \in A^*$, alors $c(F_i) \in A^*$ pour tout $i \in \mathbb{N}_n^o$. Comme T est minimale alors $n = 1$. De plus, $d^oH \neq 0$ (sinon $H = A[X]$: impossible).

D'où $T = \{H\}$.

Réciproquement, $T = \{H\}$ où $H \in A[X]$, primitif non constant. Donc $c(H) \in A^*$, alors, d'après 25.1, pour tout π irréductible de A, $H : id_{A[X]}(\pi) = H$. Donc H est de type (I).

Nous allons supposer de plus que $A[X]$ est un anneau factoriel algorithmique, dont nous notons $dec_{A[X]}$ la fonction récursive associée. Dans ce cas, nous pouvons déterminer une décomposition primaire d'un idéal de type (I).

31.4.- Algorithme DP type (I).

Entrée : H un idéal de type (I), donné par U un système fini de générateurs.

Sortie : une décomposition primaire de H.

Sous-programmes : algorithme Λ, $dec_{A[X]}$.

Début : $T := \Lambda(U)$; $T = \{H\}$;

utiliser $dec_{A[X]}$ pour déterminer $H = \prod_{i=1}^{n} h_i^{k_i}$ une décomposition en produit fini de facteurs irréductibles de $A[X]$;

retourner $\bigcap_{i=1}^{n} id_{A[X]}(h_i^{k_i})$;

Fin.

Proposition 31.5.- Soit H un idéal de type (I) de $A[X]$, donné par U un système fini de générateur.

Alors le résultat de l'algorithme DP type (I) appliqué à H est une décomposition primaire de H, où pour tout $i \in \mathbb{N}_n^o$, $id_{A[X]}(h_i^{k_i})$ est un idéal primaire de $A[X]$ dont la racine est $id_{A[X]}(h_i)$.

De plus, cette décomposition primaire est réduite.

Proposition 31.6.- Soit H un idéal non nul de $A[X]$, donné par U un système fini de générateurs.

Alors les assertions suivantes sont équivalentes :

(i) il existe un unique élément irréductible π de A, aux inversibles près qui vérifie :

$$H : \mathrm{id}_{A[X]}(\pi) \not\supseteq H \text{ et } \pi \in \sqrt{H} \ ;$$

(ii) H vérifie : (a) $\sqrt{H} \cap A = \mathrm{id}_A(\pi)$;

(b) posons $S = A - \mathrm{id}_A(\pi)$. Pour tout $s \in S$,

$$H : \mathrm{id}_{A[X]}(s) = H.$$

Démonstration :

Supposons (i) vérifiée. Donc pour tout θ élément irréductible de A, étranger avec π, nous avons $H : \mathrm{id}_{A[X]}(\theta) = H$. Pour $s \in S$, en utilisant dec, nous pouvons déterminer $s = \prod_{j=1}^{k} \theta_j$ où θ_j irréductible et étranger avec π.

Donc (b) se démontre par récurrence sur k.

Nous avons $\pi \in \sqrt{H}$. En raisonnant par l'absurde (cf. 31.1), (a) est vérifiée.

Réciproquement, d'après (a), $\pi \in \sqrt{H}$ et d'après (b), pour tout θ irréductible et étranger avec π, nous avons

$$H : \mathrm{id}_{A[X]}(\theta) = H.$$

Si $H : \mathrm{id}_{A[X]}(\pi) = H$, en utilisant $\pi \in \sqrt{H}$, nous obtenons une contradiction. Donc $H : \mathrm{id}_{A[X]}(\pi) \not\supseteq H$ et (ii) est vérifiée.

Définition 31.7.- Soit H un idéal non nul de $A[X]$, donné par U un système fini de générateurs.

Nous dirons que H est un idéal de type (II) si et seulement s'il vérfie l'une des sdeux assertions équivalentes de 31.6.

Théorème 31.8.- Soit H un idéal non nul de $A[X]$, donné par U un système fini de générateurs.

Pour que H soit un idéal de type (II), il faut et il suffit que le pgcd des éléments de U dans $A[X]$ soit une constante et que l'élément de degré nul dans la partie finie génératrice séparante minimale de H, obtenue à partir de U, soit une puissance d'un élément irréductible de A, à la multiplication par un inversible près.

Démonstration :

Supposons d'abord H idéal de type (II).

Posons T la partie finie génératrice séparante minimale de H obtenue à partir de U et posons π l'élément irréductible de A associé à H défini en 31.5.

Posons alors $T = \{F_1,\ldots,F_n\}$ rangée par ordre des degrés croissants. Comme $\pi \in \sqrt{H}$, il existe $m \in \mathbb{N} - \{0\}$, tel que $\pi^m \in H$. Puisque T est séparante minimale, $\pi^m = a.F_1$. Donc, il existe $r \in \mathbb{N} - \{0\}$ et $\varepsilon \in A^*$ tels que $F_1 = \varepsilon.\pi^r$. Maintenant, d'après II, 23.3, pour tout $i \in \mathbb{N}_n^o$ $F_i = c(F_i).H.H_{i-1}$ où H est la partie primitive du pgcd $(F_1,\ldots,F_n)$ et $d^oH = d^oF_1$, alors $H = 1$. Comme pgcd(U) = pgcd(T) (cf. II, 23.3), alors le pgcd des éléments de U dans $A[X]$ est une constante.

Réciproquement, posons $T = \{F_1,\ldots,F_n\}$ rangée par ordre croissant des degrés, la partie génératrice séparante minimale de H obtenue à partir de U. Alors le pgcd des F_i dans $A[X]$ est une constante.

Par conséquent, pour tout $i \in \mathbb{N}_n^o$, $F_i = c(F_i).H_i$ où H_i est unitaire.

En particulier, $H_1 = 1$ et $c(F_1) = \varepsilon.\pi^r$ avec π irréductible de A. Donc $\pi \in \sqrt{H}$ et, d'après la proposition 25.1, π est l'unique irréductible de A qui vérifie $H : \mathrm{id}_{A[X]}(\pi) \not\supseteq H$. Donc H est de type (II).

32. *Décomposition d'un idéal en une intersection finie d'idéaux de type (I) et de type (II).*

Proposition 32.1.- Soit H un idéal non nul de $A[X]$, donné par U un système fini de générateurs. Posons $T = \{F_1,\ldots,F_n\}$ la partie finie génératrice séparante minimale de H, obtenue à partir de U, rangée par ordre des degrés croissants.

Nous pouvons déterminer $F_1 = c(F_1).H$ où $c(F_1)$ est le contenu de F_1 et H un polynôme primitif, et nous pouvons déterminer $c(F_1) = \varepsilon.\prod_{j=1}^{k} \pi_j^{r_j}$ une décomposition en produit de facteurs irréductibles de A.

Alors : pour tout $j \in \mathbb{N}_k^o$, $H : \mathrm{id}_{A[X]}(\pi_j^{r_j}) = H : \mathrm{id}_{A[X]}(\pi_j^{r_j+1})$.

De plus :

(i) $r_j = \inf\{\ell \mid \ell \in \mathbb{N} ; H : \mathrm{id}_{A[X]}(\pi_j^{\ell}) = H : \mathrm{id}_{A[X]}(\pi_j^{\ell+1})\}$;

(ii) pour tout $\ell \in \mathbb{N}$, dès que $\ell \geq r_j$,

$$H : \mathrm{id}_{A[X]}(\pi_j) = H : \mathrm{id}_{A[X]}(\pi_j^{r_j}).$$

Démonstration :

D'après II, 23.3, nous avons, pour tout $i \in \mathbb{N}_n^o$, $F_i = c(F_i).H.H_i$ où H est primitif, $d^oH = d^oF_1$ et H_i est unitaire, $d^oH_i = i-1$.

De plus, pour tout $i \in \mathbb{N}_{n-1}^o$, $c(F_{i+1})$ divise $c(F_i)$.

Posons $t_j = \max\{\ell \mid \ell \in \mathbb{N}_n^o$; π_j divise $c(F_\ell)\}$.

Alors pour $\ell \leq t_j$, π_j divise $c(F_\ell)$ et pour $\ell > t_j$, π_j ne divise pas $c(F_\ell)$.

Par conséquent, l'exposant de la plus grande puissance de π_j divisant $c(F_\ell)$, pour $\ell \leq t_j$, est toujours inférieur ou égal à r_j.

Alors, en appliquant r_j fois l'algorithme transporteur, nous obtenons $b_1.H.H_1,\ldots,b_{t_j}.H.H_{t_j},c(F_{t_j+1}).H.H_{t_j+1},\ldots,c(F_n).H.H_n$ comme système fini de générateurs, dont les contenus sont étrangers avec π_j, pour $H : \mathrm{id}_{A[X]}(\pi_j^{r_j})$.

Si nous l'appliquons encore une fois, nous avons $t = 0$ où t est l'indice maximum tel que π_j divise le contenu correspondant, alors le système générateur est inchangé et, donc, $H : \mathrm{id}_{A[X]}(\pi_j^{r_j+1}) = H : \mathrm{id}_{A[X]}(\pi_j^{r_j})$.

De plus, pour $\ell < r_j$, $\dfrac{c(F_1)}{\pi_j^{\ell}}$ est divisible par π_j et $\dfrac{c(F_1)}{\pi_j^{\ell}}.H$ est un générateur de $H : \mathrm{id}_{A[X]}(\pi_j^{\ell})$.

Dans ce cas $\dfrac{c(F_1)}{\pi_j^{\ell+1}}.H \in H : \mathrm{id}_{A[X]}(\pi_j^{\ell+1})$ mais $\dfrac{c(F_1)}{\pi_j^{\ell+1}}.H \notin H : \mathrm{id}_{A[X]}(\pi_j^{\ell})$.

Par conséquent (i) est vérifié et, d'après la proposition 24.4, (ii) l'est également.

Corollaire 32.1a.- Sous les mêmes notations et hypothèses que 32.1, nous avons, pour tout $j \in \mathbb{N}_k^o$:

(i) $H = (H + \mathrm{id}_{A[X]}(\pi_j^{r_j})) \cap (H : \mathrm{id}_{A[X]}(\pi_j^{r_j}))$

et nous connaissons un système fini de générateurs pour chacun des deux idéaux.

(ii) pour tout élément irréductible π de A, tel que, pour tout $i \in \mathbb{N}_k^o$ et $i \neq j$, π est étranger avec π_i, alors :

$$(H : \mathrm{id}_{A[X]}(\pi_j^{r_j})) : \mathrm{id}_{A[X]}(\pi) = H : \mathrm{id}_{A[X]}(\pi_j^{r_j}).$$

(iii) pour tout $i \in \mathbb{N}_k^o$, dès que $i \neq j$, nous avons

$$(H : \mathrm{id}_{A[X]}(\pi_j^{r_j})) : \mathrm{id}_{A[X]}(\pi_i) \not\supseteq H : \mathrm{id}_{A[X]}(\pi_j^{r_j}).$$

Démonstration :

Le point (i) est une conséquence de la proposition 23.1.

Un système fini de générateurs de $H + \mathrm{id}_{A[X]}(\pi_j^{r_j})$ est $T \cup \{\pi_j^{r_j}\}$ et un système fini de générateurs de $H : \mathrm{id}_{A[X]}(\pi_j^{r_j})$ est déterminé en utilisant r_j fois l'algorithme transporteur.

Pour (ii), prenons π irréductible de A, étranger avec π_i pour tout $i \in \mathbb{N}_n^o$. D'après la proposition 24.1, $H : \mathrm{id}_{A[X]}(\pi) = H$,

donc $(H : \mathrm{id}_{A[X]}(\pi_j^{r_j})) : \mathrm{id}_{A[X]}(\pi) = H : \mathrm{id}_{A[X]}(\pi_j^{r_j})$.

De plus, $(H : \mathrm{id}_{A[X]}(\pi_j^{r_j})) : \mathrm{id}_{A[X]}(\pi_j) = H : \mathrm{id}_{A[X]}(\pi_j^{r_j+1}) = H : \mathrm{id}_{A[X]}(\pi_j^{r_j})$.
Par conséquent, (ii) est vérifiée.

Passons à (iii). Si $(H : \mathrm{id}_{A[X]}(\pi_j^{r_j})) : \mathrm{id}_{A[X]}(\pi_i) = H : \mathrm{id}_{A[X]}(\pi_j^{r_j})$.
Considérons $F \in H : \mathrm{id}_{A[X]}(\pi_i)$. En particulier $F \in (H : \mathrm{id}_{A[X]}(\pi_j^{r_j})) : \mathrm{id}_{A[X]}(\pi_i)$
donc $F \in H : \mathrm{id}_{A[X]}(\pi_j^{r_j})$. Or π_i et π_j sont étrangers, donc, en utilisant p,

nous pouvons déterminer $1 = u.\pi_i + v.\pi_j^{r_j}$.

Alors $F = u.(\pi_i.F) + v.(\pi_j^{r_j}.F)$ donc $F \in H$;

Par conséquent $H : \mathrm{id}_{A[X]}(\pi_i) = H$: impossible.

Nous en déduisons que $(H : \mathrm{id}_{A[X]}(\pi_j^{r_j})) : \mathrm{id}_{A[X]}(\pi_i) \not\supseteq H : \mathrm{id}_{A[X]}(\pi_j^{r_j})$.

Théorème 32.2.- Soit H un idéal non nul de $A[X]$, donné par U un système fini de générateurs. Posons $T = \{F_1,\ldots,F_n\}$ la partie finie génératrice séparante minimale de H obtenue à partir de U, rangée par ordre des degrés croissants.

D'après II, 23.3, nous pouvons déterminer, pour tout $i \in \mathbb{N}_n^o$; $F_i = c(F_i).H.H_i$, avec $H \in A[X]$, primitif et $d^oH = d^oF_1$, et $H_i \in A[X]$, H_i unitaire et $d^oH_i = i-1$.

De plus, en utilisant dec, nous pouvons déterminer $c(F_1) = \varepsilon.\prod_{j=1}^{k} \pi_j^{r_j}$ une décomposition en produit fini de facteurs irréductibles.

Alors $H = id_{A[X]}(H) \cap (\bigcap_{j=1}^{k} (H + id_{A[X]}(\pi_j^{r_j})))$

avec $id_{A[X]}(H)$ idéal de type (I)

et, pour tout $j \in \mathbb{N}_k^o$, $H + id_{A[X]}(\pi_j^{r_j})$ idéal de type (II).

Démonstration : Elle se fait par récurrence sur k.

D'après le corollaire 32.1a, nous avons :

$$H = (H + id_{A[X]}(\pi_k^{r_k})) \cap (H : id_{A[X]}(\pi_k^{r_k})).$$

D'après le corollaire 32.1a, point (iii), nous avons

$$(H : id_{A[X]}(\pi_k^{r_k})) : id_{A[X]}(\pi_{k-1}) \supsetneq H : id_{A[X]}(\pi_k^{r_k}).$$

De plus, comme $H : id_{A[X]}(\pi_{k-1}^{r_{k-1}}) = H : id_{A[X]}(\pi_{k-1}^{r_{k-1}+1})$ (cf. 32.1),

alors $(H : id_{A[X]}(\pi_k^{r_k})) : id_{A[X]}(\pi_{k-1}^{r_{k-1}}) = (H : id_{A[X]}(\pi_k^{r_k})) : id_{A[X]}(\pi_{k-1}^{r_{k-1}+1})$.

Donc

$$H : id_{A[X]}(\pi_k^{r_k}) = (H : id_{A[X]}(\pi_k^{r_k}) + id_{A[X]}(\pi_{k-1}^{r_{k-1}})) \cap ((H : id_{A[X]}(\pi_k^{r_k})) : id_{A[X]}(\pi_{k-1}^{r_{k-1}})).$$

Or $H + id_{A[X]}(\pi_{k-1}^{r_{k-1}}) \subset H : id_{A[X]}(\pi_k^{r_k}) + id_{A[X]}(\pi_{k-1}^{r_{k-1}})$.

Soit $F \in H : id_{A[X]}(\pi_k^{r_k})$. Comme π_k et π_{k-1} sont étrangers, en utilisant p, nous pouvons déterminer $1 = u.\pi_k^{r_k} + v.\pi_{k-1}^{r_{k-1}}$.

Donc $F = u.(\pi_k^{r_k}.F) + \pi_{k-1}^{r_{k-1}}.(v.F)$ et $F \in H + id_{A[X]}(\pi_{k-1}^{r_{k-1}})$.

Par conséquent $H + id_{A[X]}(\pi_{k-1}^{r_{k-1}}) = H : id_{A[X]}(\pi_k^{r_k}) + id_{A[X]}(\pi_{k-1}^{r_{k-1}})$.

D'où :

$$H = (H + id_{A[X]}(\pi_k^{r_k})) \cap (H + id_{A[X]}(\pi_{k-1}^{r_{k-1}})) \cap (H : id_{A[X]}(\pi_k^{r_k}.\pi_{k-1}^{r_{k-1}})).$$

De plus, d'après le corollaire 32.1a, les uniques π irréductibles de A, aux inversibles près, tels que :

$$(H : id_{A[X]}(\pi_k^{r_k}.\pi_{k-1}^{r_{k-1}})) : id_{A[X]}(\pi) \neq H : id_{A[X]}(\pi_k^{r_k}.\pi_{k-1}^{r_{k-1}})$$

sont $\pi_1,\ldots,\pi_{k-2}$.

Alors, par récurrence sur k, nous obtenons :

$$H = (H : id_{A[X]}(\pi_1^{r_1} \ldots \pi_k^{r_k})) \cap (\bigcap_{j=1}^{k} (H + id_{A[X]}(\pi_j^{r_j}))).$$

Or $F_1 = c(F_1).H$ et $c(F_1) = \varepsilon.\pi_1^{r_1}\ldots\pi_k^{r_k}$

donc $H \in H : id_{A[X]}(\pi_1^{r_1}\ldots\pi_k^{r_k})$.

Maintenant soit $F \in H : id_{A[X]}(\pi_1^{r_1}\ldots\pi_k^{r_k})$
alors $(\pi_1^{r_1}\ldots\pi_k^{r_k}).F \in H$.

En particulier $(\pi_1^{r_1}\ldots\pi_k^{r_k}).F = g.H$.

Passons aux contenus : $(\pi_1^{r_1}\ldots\pi_k^{r_k}).c(F) = c(g)$ car H est primitif, d'où $F = c(F).g_1.H$ $(g = c(g).g_1)$.

Par conséquent, $H : \mathrm{id}_{A[X]}(\pi_1^{r_1} \ldots \pi_k^{r_k}) = \mathrm{id}_{A[X]}(H)$.

Donc le théorème 32.2 est démontré, car, de plus, $\mathrm{id}_{A[X]}(H)$ est un idéal de type (I) d'après le théorème 31.3, et, pour tout $j \in \mathbb{N}_k^o$, $H + \mathrm{id}_{A[X]}(\pi_j^{r_j})$ est un idéal de type (II) d'après le théorème 31.8.

4 - *THEOREME DE DECOMPOSITION PRIMAIRE.*

Dans ce paragraphe, nous supposons que A est un anneau fortement factoriel (cf. définition 22.4).

41. *Etude d'un cas particulier.*

Considérons H un idéal non nul de $A[X]$, donné par U un système fini de générateurs. Posons $T := \Lambda(U)$ et $T := \{F_1, \ldots, F_n\}$ rangée par ordre des degrés croissants.

D'après II, 23.3, pour tout $i \in \mathbb{N}_n^o$, nous avons $F_i = c(F_i).H.H_i$ où :

(i) H est un polynôme primitif de $A[X]$ tel que $d^oH = d^oF_1$;

(ii) H_i est un polynôme unitaire de $A[X]$ tel que $d^oH_i = i-1$

(iii) $c(F_i)$ est le contenu de F_i et $c(F_{i+1})$ divise $c(F_i)$.

Alors, en utilisant le théorème 32.2 du paragraphe précédent, nous obtenons

$$H = \mathrm{id}_{A[X]}(H) \cap \left[\bigcap_{j=1}^{k} (H + \mathrm{id}_{A[X]}(\pi_j^{r_j}))\right]$$

avec $c(F_1) = \prod_{j=1}^{k} \pi_j^{r_j}$, π_j irréductible de A et $r_j \in \mathbb{N}^o$.

Supposons qu'il existe $j \in \mathbb{N}_k^o$ pour lequel $r_j = 1$.
Dans ce cas, posons $\pi := \pi_j$ et $T := H + \mathrm{id}_{A[X]}(\pi)$.

Proposition 41.1.- Sous les notations et hypothèses précédentes, posons $t := \max\{\ell \mid \pi \text{ divise } c(F_\ell)\}$. Nous avons les résultats suivants :

(i) si $t = n$ alors $T = \mathrm{id}_{A[X]}(\pi)$;

(ii) sinon, posons $L := A_{/A.\pi}$ et $\bar{T} := T_{/\mathrm{id}_{A[X]}(\pi)}$.

Alors $\bar{T} = \mathrm{id}_{L[X]}(\bar{H}.\bar{H}_{t+1})$ où $\bar{H}$ (resp. $\bar{H}_{t+1}$) est la classe modulo π de H (resp. de H_{t+1}).

Démonstration :

(i) c'est évident car $c(F_n)$ divise $c(F_i)$ pour tout $i \in \mathbb{N}_n^o$ et $\pi \in T$.

(ii) il est clair que $T = \mathrm{id}_{A[X]}(\pi, F_2, \ldots, F_n)$.
Dans $L[X]$, $\bar{F}_i = 0$ pour $i \leq t$ et $\bar{F}_i = \bar{H}.\bar{H}_i$ pour $i > t$.

Maintenant, d'après II, 23.3a, pour tout $k \in \mathbb{N}$, $1 \leq k \leq n-t$, nous avons $H_{t+k} \in \mathrm{id}_{A[X]}(d_t, H_{t+1})$ où d_t est défini par : $c(F_t) = d_t.c(F_{t+1})$. Par définition de t, $c(F_{t+1})$ est étranger avec π, donc π divise d_t. Nous en déduisons que $\bar{H}_{t+k} \in \mathrm{id}_{L[X]}(\bar{H}_{t+1})$.

Par conséquent $\bar{T} = \mathrm{id}_{L[X]}(\bar{H}.\bar{H}_{t+1})$.

Proposition 41.2.- Sous les mêmes notations et hypothèses que 41.1, nous savons que L est un corps factoriel. Alors il est muni d'un algorithme DPØ (cf. Proposition 23.2).

Par conséquent, $\bar{H}.\bar{H}_{t+1} = \prod_{j=1}^{r} \phi_j^{\gamma_j}$ étant une décomposition en produit fini de facteurs irréductibles de $L[X]$, nous déterminons explicitement une décomposition primaire $\bar{T} = \bigcap_{j=1}^{r} \mathrm{id}_{L[X]}(\phi_j^{\gamma_j})$ et, pour tout $j \in \mathbb{N}_r^o$, la

racine de $id_{L[X]}(\bar{\psi}_j^{\gamma_j})$ est $id_{L[X]}(\bar{\psi}_j)$.

Corollaire 41.2a.- Sous les mêmes notations et hypothèses que 41.2, déterminons $\bar{H}.\bar{H}_{t+1} = \prod_{j=1}^{r} \bar{\psi}_j^{\gamma_j}$ une décomposition en produit fini de facteurs irréductibles de $L[X]$, puis, pour tout $j \in \mathbb{N}_r^o$, déterminons P_j polynôme unitaire de $A[X]$ tel que $\bar{P}_j = \bar{\psi}_j$, (ce qui est possible en utilisant la proposition 22.1).

Alors (i) $T = \bigcap_{j=1}^{r} id_{A[X]}(\pi, P_j^{\gamma_j})$;

(ii) c'est une décomposition primaire de T ;

(iii) la racine de $id_{A[X]}(\pi, P_j^{\gamma_j})$ est l'idéal premier $id_{A[X]}(\pi, P_j)$.

Démonstration :

Le point (i) est une conséquence de $\pi \in T$ et du résultat de 42.1.

Démontrons que $\sqrt{id_{A[X]}(\pi, P_j^{\gamma_j})} = id_{A[X]}(\pi, P_j)$.

De façon évidente, $id_{A[X]}(\pi, P_j) \subset \sqrt{id_{A[X]}(\pi, P_j^{\gamma_j})}$.

Soit $G \in \sqrt{id_{A[X]}(\pi, P_j^{\gamma_j})}$, donc il existe $m \in \mathbb{N}^o$, tel que

$$G^m = \pi.Q_1 + P_j^{\gamma_j}.Q_2 .$$

Modulo π, nous obtenons $\bar{G}^m = \bar{P}_j^{\gamma_j}.\bar{Q}_2$. Or $\bar{P}_j$ est irréductible dans $L[X]$, donc $\bar{P}_j$ divise $\bar{G}$, c'est-à-dire $G \in id_{A[X]}(\pi, P_j)$.

Maintenant, considérons G_1 et G_2 dans $A[X]$ tels que

$G_1.G_2 \in id_{A[X]}(\pi,P_j^{\gamma_j})$ mais $G_1 \notin id_{A[X]}(\pi,P_j)$.

Donc $G_1.G_2 = \pi.Q_1 + P_j^{\gamma_j}.Q_2$.

Modulo π, nous obtenons $\bar{G}_1.\bar{G}_2 = \bar{P}_j^{\gamma_j}.\bar{Q}_2$, or $\bar{P}_j$ est irréductible dans $L[X]$ anneau factoriel et $\bar{P}_j$ ne divise pas $\bar{G}_1$, donc $\bar{P}_j^{\gamma_j}$ divise $\bar{G}_2$.

Par conséquent, $G_2 \in id_{A[X]}(\pi,P_j^{\gamma_j})$.

D'après le théorème 12.1, $id_{A[X]}(\pi,P_j^{\gamma_j})$ est un idéal primaire dont la racine est l'idéal premier $id_{A[X]}(\pi,P_j)$.

Nous en déduisons que $T = \bigcap_{j=1}^{r} id_{A[X]}(\pi,P_j^{j})$ est une décomposition primaire de T, déterminée explicitement.

42. Caractérisation des idéaux premiers.

Nous utilisons les résultats du sous-paragraphe 41, pour établir

Théorème 42.1.- Soit H un idéal propre non nul de $A[X]$, donné par U un système fini de générateurs. Pour que H soit un idéal premier de $A[X]$, il faut et il suffit qu'il soit de l'un des trois types suivants :

(i) $H = id_{A[X]}(\pi)$ où π est un élément irréductible de A ;

(ii) $H = id_{A[X]}(H)$ où H est polynôme irréductible non constant de $A[X]$.

(iii) $H = id_{A[X]}(\pi,P)$ où π est un élément irréductible de A et et P un polynôme unitaire non constant de $A[X]$, irréductible modulo π.

Démonstration :

Supposons d'abord H idéal premier de $A[X]$ et posons $T := \Lambda(U)$. Posons alors $T := \{F_1,\dots,F_n\}$ rangée par ordre des degrés croissants.

En posant $c(F_1) = \prod_{j=1}^{k} \pi_j^{r_j}$ et H la partie primitive du pgcd des éléments de T, nous avons, d'après le théorème 32.2 :

$$H = id_{A[X]}(H) \cap (\bigcap_{j=1}^{k} (H + id_{A[X]}(\pi_j^{r_j}))).$$

Or H est premier donc il est égal à l'un de ces idéaux.

1er cas : $H = id_{A[X]}(H)$.

Comme H est un idéal premier alors H est un polynôme non constant irréductible de $A[X]$.

2ème cas : Il existe $j \in \mathbb{N}_k^o$ tel que $H = H + id_{A[X]}(\pi_j^{r_j})$.

Donc $\pi_j^{r_j} \in H$. Or H est un idéal premier alors $\pi_j \in H$.

Dans ce cas, F_1 est associé à π_j.

Si π_j divise $c(F_n)$ alors $H = id_{A[X]}(\pi_j)$.

Sinon, posons $t = \max\{\ell \mid \pi_j \text{ divise } c(F_\ell)\}$, donc $t < n$.

Comme H est un idéal de type (II) (car $H = H + id_{A[X]}(\pi_j^{r_j})$) alors $H = 1$ (cf. théorème 31.8).

Utilisons alors le corollaire 41.2a,

$$H = \bigcap_{i=1}^{r} id_{A[X]}(\pi_j, P_i^{\gamma_i})$$

où $H_{t+1} = \prod_{i=1}^{r} P_i^{\gamma_i}$ modulo π_j et P_i polynôme unitaire non constant, irréductible modulo π_j.

Or H est premier donc il existe $i \in \mathbb{N}_r^o$ tel que

$$H = id_{A[X]}(\pi_j, P_i^{\gamma_i})$$

la racine de cet idéal étant $id_{A[X]}(\pi_j, P_i)$ (cf. corollaire 41.2a) alors $H = id_{A[X]}(\pi_j, P_i)$.

Par conséquent, la condition est nécessaire.

Remarquons que le calcul de ces générateurs est effectif pour chaque cas. En effet, nous savons calculer le pgcd dans $A[X]$ ainsi que la partie primitive d'un polynôme. De plus, dans le second cas, $k = 1$, car pour $\ell \neq j$, π_ℓ est étranger avec π_j. Enfin, $r = 1$, donc P_i est l'unique facteur irréductible modulo π_j de H_{t+1}.

Réciproquement, dans les cas (i) et (ii), H est de façon évidente un idéal premier.

Dans le cas (iii), un calcul modulo π montre que H est premier (il est possible d'effectuer le relèvement car $\pi \in H$).

Corollaire 42.1a.- Soit H un idéal propre non nul de $A[X]$, donné par U un système fini de générateurs. Pour que H soit un idéal maximal de $A[X]$, il faut et il suffit qu'il existe π élément irréductible de A et P polynôme unitaire non constant de $A[X]$, irréductible modulo π tel que $H = id_{A[X]}(\pi, P)$.

Démonstration :

Supposons H idéal maximal, il est donc premier. Nous pouvons alors utiliser le théorème 42.1.

Examinons les trois cas de ce théorème, et uniquemeent ceux-ci, car H premier est une condition nécessaire.

(i) donne un idéal premier non maximal ;

(ii) $H = id_{A[X]}(H)$ où H polynôme irréductible non constant de $A[X]$.

Il est donc primitif. Prenons π élément irréductible de A, donc nous pouvons considérer P unitaire non constant de $A[X]$, facteur irréductible modulo π de H. Alors $H \subsetneq id_{A[X]}(\pi,P)$. Par conséquent, H n'est pas maximal.

Enfin (iii). $H = id_{A[X]}(\pi,P)$. Supposons $H \subsetneq K$ où K idéal de $A[X]$. Donc il existe $F \in K$ et $F \notin H$. Alors, posons $L = A_{/A.\pi}$, L est un corps codable d'où $L[X]$ est principal algorithmique (cf. I, 43a, p. 14). Par conséquent, modulo π, $1 = U.F + V.P$. Donc $1 \in K$ et H est un idéal maximal.

D'où le corollaire 42.1a est démontré.

43. Lien avec la multiplicité.

Considérons H un idéal propre non nul de $A[X]$ donné par U un système fini de générateurs.

Posons $T := \Lambda(U)$ et $T = \{F_1,\ldots,F_n\}$ rangée par ordre des degrés croissants.

D'après II. 23.3, nous pouvons déterminer, pour tout $i \in \mathbb{N}_n^o$, $F_i = c(F_i).H.H_i$ où $H \in A[X]$ primitif tel que $d^oH = d^oF_1$, $H_i \in A[X]$ unitaire tel que $d^oH_i = i-1$ et $c(F_i)$ est le contenu de F_i.

De plus, pour tout $i \in \mathbb{N}_{n-1}^o$, $c(F_{i+1})$ divise $c(F_i)$ et nous posons $d_i = c(F_i)/c(F_{i+1})$.

Déterminons $c(F_1) = \varepsilon . \prod_{j=1}^{k} \pi_j^{r_j}$ où $\varepsilon \in A^*$ et π_j élément irréductible de A. Fixons $j \in \mathbb{N}_n^o$ et posons :

$$\pi := \pi_j, \quad \alpha := r_j \quad \text{et} \quad t = \max\{\ell \mid \pi \text{ divise } c(F_\ell)\}.$$

Proposition 43.1.- Soit P un élément unitaire de $A[X]$, irréductible modulo π. Pour que $H \subset id_{A[X]}(\pi,P)$ il faut et il suffit que $(t = n)$ ou $(P$ divise H modulo $\pi)$ ou (il existe $i \in \mathbb{N}_t^o$ tel que π divise d_i et P divise H_{i+1} modulo $\pi)$.

Démonstration :

Si $t = n$ ou si P divise H modulo π, c'est évident.

Supposons qu'il existe $i \in \mathbb{N}_t^o$ tel que π divise d_i et P divise H_{i+1} modulo π. Or, pour $j \leqslant i$, d_i divise $c(F_j)$ et pour $j > i$, $H_j \in id_{A[X]}(d_i,H_{i+1})$, donc, pour $j \leqslant i$, π divise F_j et, pour $j > i$, P divise H_j modulo π.

Par conséquent $H \subset id_{A[X]}(\pi,P)$.

Réciproquement, $t < n$ et P ne divise par H modulo π.

Comme $t = \max\{\ell \mid \pi$ divise $c(F_\ell)\}$ alors π divise d_t. Maintenant, $F_{t+1} = c(F_{t+1}).H.H_{t+1}$. Or π ne divise pas $c(F_{t+1})$ donc P divise $H.H_{t+1}$ modulo π. D'où P divise H_{t+1} modulo π. Alors nous prenons $i = t$.

Plaçons-nous dans les conditions de 43.1. Posons $\mathcal{P} = id_{A[X]}(\pi,P)$, $B = A[X]/_H$ et $\bar{\mathcal{P}} = \mathcal{P}/_H$.

Proposition 43.2.- Le localisé $B_{\bar{\mathcal{P}}}$ est un anneau local noethérien d'idéal maximal l'idéal engendré par les images de π et $\mathcal{P}$.

De plus, $B_{\bar{\mathcal{P}}} = A[X]_{\mathcal{P}}/_{H_{\mathcal{P}}}$.

Proposition 43.3.- Pour que $B_{\bar{\mathcal{P}}}$ soit artinien il faut et suffit que $t < n$ et P ne divise pas H modulo π.

Démonstration :

Supposons d'abord $t < n$ et P ne divise pas H modulo π.

Donc $H \notin id_{A[X]}(\pi)$. Pour démontrer que $B_{\overline{P}}$ est artinien, il nous suffit de démontrer que tout idéal premier de $B_{\overline{P}}$ est maximal. Mais un idéal premier de $B_{\overline{P}}$ est de la forme $(K/H)_{\overline{P}}$ où K est un idéal premier de $A[X]$ tel que $H \subset K \subset P$.

Comme $H \notin id_{A[X]}(\pi)$, d'après le théorème 42.1, soit $K = id_{A[X]}(h)$ où h élément irréductible de $A[X]$, soit $K = id_{A[X]}(\pi,Q)$ où Q élément unitaire de $A[X]$, irréductible modulo π.

Si $K = id_{A[X]}(h)$ alors h divise H. Comme P divise h modulo π, nous obtenons une contradiction. Donc $K = id_{A[X]}(\pi,Q)$; comme celui-ci est maximal d'après le corollaire 42.1a, alors $K = P$. Donc tout idéal premier de $B_{\overline{P}}$ est maximal. c.q.f.d.

Supposons maintenant $t \neq n$. Donc $H \subset id_{A[X]}(\pi) \subsetneq P$.

Or $(id_{A[X]}(\pi)/H)_{\overline{P}}$ est un idéal premier de $B_{\overline{P}}$, qui n'est donc pas maximal. Alors $B_{\overline{P}}$ n'est pas artinien.

Enfin, supposons P divise H modulo π. En utilisant $dec_{A[X]}$, nous pouvons déterminer $H = \prod_{j=1}^{r} h_j$ où h_j élément irréductible de $A[X]$. Comme P est irréductible modulo π, il existe $j \in \mathbb{N}_r^o$ tel que P divise h_j modulo π. Donc $H \subset id_{A[X]}(h_j) \subsetneq P$. Or $(id_{A[X]}(h_j)/H)_{\overline{P}}$ est un idéal premier de $B_{\overline{P}}$, qui n'est donc pas maximal. Alors $B_{\overline{P}}$ n'est pas artinien.

Maintenant, d'après la proposition 24.1, nous avons :

$$H = (H + id_{A[X]}(\pi^{\alpha})) \cap (H : id_{A[X]}(\pi^{\alpha})).$$

Posons $T = H + id_{A[X]}(\pi^{\alpha})$; c'est un idéal de type (II) d'après le théorème 31.8.

Proposition 43.4.- Considérons P un élément unitaire de $A[X]$, irréductible modulo π. Pour que $T \subset id_{A[X]}(\pi,P)$ il faut et il suffit que $H \subset id_{A[X]}(\pi,P)$.

Dans ce cas, soit γ tel que $T : id_{A[X]}(P^\gamma) = T : id_{A[X]}(P^{\gamma+1})$. Alors, nous avons :

(i) $T = (T + id_{A[X]}(P^\gamma)) \cap (T : id(P^\gamma))$;

(ii) $T + id_{A[X]}(P^\gamma)$ est un idéal primaire de racine $P = id_{A[X]}(\pi,P)$.

De plus, c'est la composante P-primaire de H.

Démonstration :

(i) est une conséquence de la proposition 24.1.

(ii) $\sqrt{T + id_{A\,X}(P^\gamma)} = \sqrt{\sqrt{T} + id_{A[X]}(P)} \subset id_{A[X]}(\pi,P)$

or $\pi^\alpha \in T$ donc $\sqrt{T + id_{A[X]}(P^\gamma)} = P$.

Maintenant, soient F et G dans $A[X]$, tels que $F.G \in T + id_{A[X]}(P^\gamma)$ mais $G \notin P$. Nous pouvons supposer G irréductible modulo π. Donc G est étranger avec P modulo π, c'est-à-dire $1 = U.G + V.P$ modulo π, donc $1 - U.G \in P$. Comme $P = \sqrt{T + id_{A[X]}(P^\gamma)}$, nous pouvons utiliser le corollaire 24.2a et $(T + id_{A[X]}(P^\gamma)) : id_{A[X]}(U.G) = T + id_{A[X]}(P^\gamma)$.

Or $T + id_{A[X]}(P^\gamma) \subset (T + id_{A[X]}(P^\gamma)) : id_{A[X]}(G) \subset (T + id_{A[X]}(P^\gamma)) : id_{A[X]}(U.G)$.

Donc $T + id_{A[X]}(P^\gamma) = (T + id_{A[X]}(P^\gamma)) : id_{A[X]}(G)$.

Par conséquent, $F \in T + id_{A[X]}(P^\gamma)$ et $T + id_{A[X]}(P^\gamma)$ est un idéal primaire de racine P.

Comme $(H : id_{A[X]}(\pi^\alpha)) : id_{A[X]}(\pi) = H : id_{A[X]}(\pi^\alpha)$, c'est la composante P-primaire de H.

Corollaire 43.4a.- Sous les mêmes hypothèses et notations que 43.4, posons $B = A[X]_{/H}$ et $\bar{P} = P_{/H}$.

Alors γ est égale à la longueur de la chaîne croissante d'idéaux $(T : \mathrm{id}_{A[X]}(P^S)_{/H})_{\bar{P}}$.

Démonstration :

Nous avons $(T : \mathrm{id}_{A[X]}(P^S)_{/H})_{\bar{P}} = T_P : \mathrm{id}_{A[X]}(P^S)_{P/H_P}$

et la longueur de cette chaîne détermine l'exposant r de l'image de P qui engendre la composante $\bar{P}$ primaire de $T_{P/H_P} = (T_{/H})_{\bar{P}}$ dans $B_{\bar{P}}$. Or, son image réciproque est la composante $\bar{P}$-primaire de $T_{/H}$ dans B, d'après la proposition 14.1. Comme celle-ci correspond à la composante P-primaire de T qui est $T + \mathrm{id}_{A[X]}(P^\gamma)$ d'après la proposition 43.4, γ est donc égal à cet exposant r, c'est-à-dire γ est égale à la longueur de la chaîne.

Corollaire 43.4b.- Sous les mêmes hypothèses et notations que 43.4a, supposons de plus que $t < n$ et P ne divise pas H modulo π.

Alors $B_{\bar{P}}$ est un anneau local artinien et γ est majoré par la multiplicité de $B_{\bar{P}}$.

Démonstration :

D'après la proposition 43.3, $B_{\bar{P}}$ est un anneau local artinien. D'après le corollaire 21.2a, sa multiplicité est égale à sa longueur. En outre, γ est égal à la longueur de la chaîne croissante d'idéaux $(T : \mathrm{id}_{A[X]}(P^S)_{/H})_{\bar{P}}$ de $B_{\bar{P}}$, donc γ est majoré par la multiplicité de $B_{\bar{P}}$.

44. Calcul de la multiplicité.

Considérons H un idéal propre non nul de $A[X]$, donné par U un système fini de générateurs.

Nous conservons les notations introduites au début du sous-paragraphe 43.

Supposons alors $t < n$ et $H = 1$.

Le calcul présenté ici est une adaptation de celui proposé par D. Lazard dans [LAZ 3] pour démontrer les points iv) et v)

Soit P un élément unitaire de $A[X]$, irréductible modulo π et posons $\mathcal{P} = id_{A[X]}(\pi, P)$.

Proposition 44.1.- Pour $i \in \mathbb{N}^{o}_{n-1}$, posons $B_i = A[X]/id_{A[X]}(d_i, H_{i+1})$.

(i) Si $id_{A[X]}(d_i, H_{i+1}) \subset \mathcal{P}$, posons $\bar{\mathcal{P}}_i = \mathcal{P}/id_{A[X]}(d_i, H_{i+1})$.
alors $(B_i)_{\bar{\mathcal{P}}_i} = (B_i)_{\mathcal{P}}$.

(ii) Sinon $(B_i)_{\mathcal{P}} = \{0\}$.

Démonstration :

En considérant la localisation en $\mathcal{P}$ de $A[X]$ modules, nous avons

$$(B_i)_{\mathcal{P}} = A[X]_{\mathcal{P}}/id_{A[X]}(d_i, H_{i+1})_{\mathcal{P}}$$

(i) puisque $id_{A[X]}(d_i, H_{i+1}) \subset \mathcal{P}$, alors $(B_i)_{\bar{\mathcal{P}}_i} = A[X]_{\mathcal{P}}/id_{A[X]}(d_i, H_{i+1})_{\mathcal{P}}$;

(ii) comme $id_{A[X]}(d_i, H_{i+1}) \not\subset \mathcal{P}$, alors

ou bien d_i est étranger avec π,

ou bien P ne divise pas H_{i+1} modulo π,

donc, dans $A[X]_P$, l'idéal localisé $id_{A[X]}(d_i,H_{i+1})_P$ contient un élément inversible, d'où $id_{A[X]}(d_i,H_{i+1})_P = A[X]_P$ et $(B_i)_P = \{0\}$.

Proposition 44.2.- Conservons les notations de 44.1. Nous avons, en désignant par $mult_P$ la multiplicité :

(i) $$mult_P\ B_{\bar{P}} = \sum_{i=1}^{n-1} mult_P(B_i)_P \quad ;$$

(ii) pour tout $i \in \mathbb{N}^o_{n-1}$, $mult_P(B_i)_P = \alpha_i.\beta_i$ où α_i est l'exposant de la plus grande puissance de π qui divise d_i et β_i celui de la plus grande puissance de P qui divise H_{i+1} modulo π.

Démonstration :

(i) Puisque $H = 1$, H est engendré par $c(F_1),c(F_2).H_2,\ldots,c(F_n).H_n$. De plus,

$$\begin{aligned} c(F_{n-1}) &= d_{n-1}.c(F_n) \\ &\vdots \\ c(F_i) &= d_i.\ \ldots\ .d_{n-1}.c(F_n) \\ &\vdots \\ c(F_1) &= d_1.\ \ldots\ .d_{n-1}.c(F_n). \end{aligned}$$

Posons $T_1 = id_{A[X]}(d_1,H_2)$ et, pour $2 \leq i \leq n-1$,

$$T_i = id_{A[X]}(H_{i+1}) + d_i.T_{i-1}.$$

Pour $2 \leq i \leq n-1$, considérons :

$$0 \longrightarrow A[X]/T_{i-1} \longrightarrow A[X]/T_i \longrightarrow A[X]/id_{A[X]}(d_i,H_{i+1}) \longrightarrow 0$$

où $A[X]/T_{i-1} \to A[X]/T_i$ est la multiplication par d_i, bien définie car $T_i = id_{A[X]}(H_{i+1}) + d_i.T_{i-1}$ et $A[X]/T_i \to A[X]/id_{A[X]}(d_i,H_{i+1})$

est l'homomorphisme surjectif canonique puisque $T_i \subset id_{A[X]}(d_i, H_{i+1})$.

Maintenant soit $F \in A[X]$ tel que $d_i.F = 0$ dans $A[X]/T_i$ donc $d_i.F \in T_i$, c'est-à-dire $d_i.F = G_1.H_{i+1} + d_i.G_2$ avec $G_2 \in T_{i-1}$. Alors d_i divise G_1 et $F = g_1.H_{i+1} + G_2$.

Or, $H_{i+1} \in T_{i-1}$ (cf. II, démonstration 23.3a, prendre $i := i-1$ et $k := 2$ dans le calcul final de H_{i+k}) donc $F \in T_{i-1}$ et la multiplication par d_i est injective.

Maintenant la suite est exacte, car l'image dans $A[X]/T$ est engendrée par d_i, c'est donc $id_{A[X]}(d_i) + T_i/T_i$, et le noyau est $id_{A[X]}(d_i, H_{i+1})/T_i = id_{A[X]}(d_i) + T_i/T_i$.

En utilisant l'additivité de la multiplicité pour les suites exactes (cf. [SER]) nous obtenons $mult_P(A[X]/T_{n-1})_P = \sum_{i=1}^{n-1} mult_P(B_i)_P$ puisque $B_i = A[X]/id_{A[X]}(d_i, H_{i+1})$.

Maintenant $H = c(F_n).T_{n-1}$. Nous pouvons donc définir la multiplication par $c(F_n)$ de $A[X]/T_{n-1}$ dans $A[X]/H$. C'est un homorphisme injectif. En localisant suivant P, puisque π ne divise pas $c(F_n)$ $(t < n)$, alors $c(F_n)$ devient inversible et la multiplication par $c(F_n)$ devient un isomorphisme.

Par conséquent, $mult_{\bar{P}} B_{\bar{P}} = \sum_{i=1}^{n-1} mult_P(B_i)_P$.

(ii) Nous reprenons la démonstration de D. Lazard pour le point v) dans [LAZ 3], avec α_i exposant de la plus grande puissance de π divisant d_i et β_i celui de la plus grande puissance de P divisant H_{i+1} modulo π.

Donc $mult_P(B_i)_P = \alpha_i.\beta_i$.

45. *Décomposition primaire.*

Soit H un idéal propre non nul de $A[X]$, donné par U un système fini de générateurs. Posons $T := \Lambda(U)$ et $T := \{F_1,\dots,F_n\}$ rangée par ordre des degrés croissants.

D'après II, 23.3, nous pouvons déterminer, pour tout $i \in \mathbb{N}_n^o$, $F_i = c(F_i).H.H_i$, où $H \in A[X]$ primitif tel que $d^oH = d^oF_1$, $H_i \in A[X]$ unitaire tel que $d^oH_i = i-1$, et $c(F_i)$ est le contenu de F_i.

De plus, pour tout $i \in \mathbb{N}_{n-1}^o$, $c(F_{i+1})$ divise $c(F_i)$ et posons $d_i = c(F_i)/c(F_{i+1})$.

Déterminons $c(F_1) = \varepsilon.\prod_{j=1}^{k} \pi_j^{r_j}$ où $\varepsilon \in A^*$ et π_j élément irréductible de A.

Fixons $j \in \mathbb{N}_n^o$. Posons $\pi := \pi_j$, $\alpha := r_j$ et $t = \max\{\ell \mid \pi \text{ divise } c(F_\ell)\}$.

Proposition 45.1.- Supposons $t < n$ et $H = 1$.

Soit P un élément unitaire de $A[X]$, irréductible modulo π, tel que $H \subset \mathrm{id}_{A[X]}(\pi,P)$. Posons $P = \mathrm{id}_{A[X]}(\pi,P)$.

La composante P-primaire de H est $H + \mathrm{id}_{A[X]}(\pi^\alpha,P^\gamma)$ où γ est majoré par $\sum_{i=1}^{n-1} \alpha_i.\beta_i$ où α_i est l'exposant de la plus grande puissance de π divisant d_i et β_i celui de la plus grande puissance de P divisant H_{i+1} modulo π.

Démonstration :

Nous utilisons la proposition 43.4, le corollaire 43.4b et la proposition 44.2.

Corollaire 45.1a.- Sous les mêmes notations et hypothèses que 45.1, posons $T = H + id_{A[X]}(\pi^{\alpha})$. Alors

$T = \bigcap (T + id(P^{\gamma}))$ est une décomposition primaire de T, où l'intersection porte sur les P unitaires de $A[X]$, irréductibles modulo π, pour lesquels il existe $j \in \mathbb{N}_t^o$ tel que π divise d_j et P divise H_{i+1} modulo π et $\gamma = \sum_{i=1}^{n-1} \alpha_i.\beta_i$.

Démonstration :

D'après la proposition 43.1, et, puisque $t < n$ et $H = 1$, pour que $H \subset id_{A[X]}(\pi,P)$ il faut et il suffit qu'il existe $j \in \mathbb{N}_t^o$ tel que π divise d_i et P divise H_{i+1} modulo π.

Maintenant, nous utilisons la proposition 45.1 pour majorer γ par $\sum_{i=1}^{n-1} \alpha_i.\beta_i$. Mais, d'après la proposition 24.4, nous pouvons prendre $\gamma = \sum_{i=1}^{n-1} \alpha_i.\beta_i$. Alors $T = (T + id_{A[X]}(P^{\gamma})) \cap (T : id_{A[X]}(P^{\gamma}))$.

En outre, $t < n$ donc $T \not\subset id_{A[X]}(\pi)$ et $P = id_{A[X]}(\pi,P)$ est maximal (cf. corollaire 42.1a) donc nous déterminons ainsi toutes les composantes primaires de T.

Corollaire 45.1b.- Soit H un idéal de type (II) de $A[X]$, donné par U un système fini de générateurs. Dans ce cas $H = 1$ et $F_1 = \pi^{\alpha}$ (cf. théorème 31.8). Supposons $t < n$.

Alors, nous pouvons déterminer explicitement une décomposition primaire de H.

45.2.- D'après le théorème 32.2, nous avons :

$$H = id_{A[X]}(H) \cap (\bigcap_{j=1}^{k} (H + id_{A[X]}(\pi_j^{r_j}))$$

et $H_j = H + id_{A[X]}(\pi_j^{r_j})$ est un idéal de type (II) de $A[X]$ dont une partie finie génératrice est $U_j = T \cup \{\pi_j^{r_j}\}$.

Déterminons alors $T_j := \Lambda(U_j)$, dans ce cas ses éléments sont de la forme $\pi_j^{s_{ji}}.H_{j,i}$ pour $i \in \mathbb{N}_{n(j)}^{o}$ où $r_j = s_{j,1} \geq s_{j,2} \geq \ldots \geq s_{j,n(j)}$ et $H_{j,i} \in A[X]$ unitaire tel que $d^{o}H_{j,i} = i-1$.

Supposons $c(F_n) = 1$. Donc, en posant $t_j = \max\{\ell \mid s_\ell \neq 0\}$, nous avons $t_j < n(j)$, pour tout $j \in \mathbb{N}_k^o$. Alors nous pouvons utiliser le corollaire 45.1b et déterminer explicitement une décomposition primaire de H_j. D'où l'algorithme suivant pour déterminer une décomposition primaire de H lorsque $c(F_n) = 1$.

45.3.- *Algorithme de décomposition primaire.*

Entrée : H un idéal propre non nul de $A[X]$ donné par U un système fini de générateurs, tel que si $T := \Lambda(U)$, alors le contenu du terme de plus haut degré de T est 1.

Sortie : une décomposition primaire de H.

Sous-programmes : algorithme Λ, algorithme DP type (I).

Début : $T := \Lambda(U)$; $T := \{F_1,\ldots,F_n\}$ rangée par ordre des degrés croissants (donc $c(F_n) = 1$) ;

$c(F_1) = \varepsilon.\prod_{j=1}^{k} \pi_j^{r_j}$; $H :=$ partie primitive $\text{pgcd}(F_1,\ldots,F_n)$

(ici $H := \text{pgcd}(F_1,\ldots,F_n)$ puisque $c(F_n) = 1$) ;

pour tout $j \in \mathbb{N}_k^o$ $U_j := T \cup \{\pi_j^{r_j}\}$; $H_j := id_{A[X]}(U_j)$;

Utiliser DP type (I) pour déterminer $\bigcap_{i=1}^{\ell} id_{A[X]}(h_i^{m_i})$ une décomposition primaire de $id_{A[X]}(H)$;

Pour tout $j \in \mathbb{N}_k^o$ $T_j := \Lambda(U_j)$; $T_j := \{\pi_j^{s_{j,i}}.H_{j,i}\}_{i\in\mathbb{N}_{n(j)}^o}$

(ici $s_{j,n(j)} = 0$) ;

Pour tout $j \in \mathbb{N}_k^o$ pour tout $i \in \mathbb{N}_{n(j)-1}^o$, $\alpha_{j,i} = s_{j,i} - s_{j,i+1}$ et $\beta_{j,i}$ est l'exposant de la plus grande puissance de P divisant $H_{j,i+1}$ où $P \in A[X]$, unitaire, irréductible modulo π_j, ;

$\gamma_j(P) = \sum_{i=1}^{n(j)-1} \alpha_{j,i}.\beta_{j,i}$;

Retourner $(\bigcap_{i=1}^{\ell} id_{A[X]}(h_i^{m_i})) \cap (\bigcap_{j=1}^{k} (\bigcap_{P} (H_j + id_{A[X]}(P^{\gamma_j(P)}))))$.

Fin.

Remarque 45.4.- La détermination de chaque T_j augmente le temps de calcul, et les $\alpha_{j,i}$ (resp. $\beta_{j,i}$) déterminés explicitement à partir des $s_{j,i}$ (resp. $H_{j,i}$) dépendent de d_i et H_{i+1}, mais le lien direct n'est pas aisé à établir pour l'instant sauf pour le cas particulier traité dans le sous-paragraphe 46, qui permet d'envisager l'amélioration de cet algorithme.

46. *Cas où* $c(F_2)$ *est une puissance d'un* π_j.

Nous reprenons les notations introduites au début du sous-paragraphe 45. Supposons $t < n$.

Proposition 46.1.- Pour que $\pi^{\alpha}.X^{q+1} \in \mathrm{mod}_A(\pi^{\alpha},\ldots,\pi^{\alpha}.X^q, c(F_2).H.H_2)$ où $q := d^oH$, il faut et il suffit que H soit unitaire et $c(F_2) = \pi^{s_2}$ où $s_2 \in \mathbb{N}^o$ et $s_2 \leq \alpha$.

Démonstration :

Supposons $\pi^{\alpha}.X^{q+1} \in \mathrm{mod}_A(\pi^{\alpha},\ldots,\pi^{\alpha}.X^{q},c(F_2).H.H_2)$

donc $\pi^{\alpha}.X^{q+1} = a_o.\pi^{\alpha} + \ldots + a_q.\pi^{\alpha}.X^{q} + a_{q+1}.c(F_2).H.H_2$

d'où $a_{q+1}.c(F_2).H.H_2 = \pi^{\alpha}.(X^{q+1} - \sum_{i=0}^{q} a_i X^i)$

en passant aux contenus nous obtenons $a_{q+1}.c(F_2) = \pi^{\alpha}$, donc $c(F_2) = \pi^{s_2}$,

et $H.H_2 = X^{q+1} - \sum_{i=0}^{q} a_i.X^i$, donc H est unitaire.

Réciproquement $H = X^q - \sum_{i=0}^{q-1} c_i.X^i$ et $c(F_2) = \pi^{s_2}$ où $s_2 \leq \alpha$.

Or $H_2 = X-a$ donc $c(F_2).H.H_2 = \pi^{s_2}.X^q(X-a) + \pi^{s_2}.(X-a)\sum_{i=0}^{q-1} c_i.X^i$.

Donc :

$$\pi^{\alpha}.X^{q+1} - \pi^{\alpha-s_2}.c(F_2).H.H_2 = \pi^{\alpha}.a.X^q - \pi^{\alpha}(X-a)\sum_{i=0}^{q-1} c_i.X^i$$

$$= \pi^{\alpha}(a-c_{q-1})X^q + \sum_{i=1}^{q-1}(a.c_i - c_{i-1})\pi^{\alpha}.X^i + (a.c_o)\pi^{\alpha},$$

d'où $\pi^{\alpha}.X^{q+1} \in \mathrm{mod}_A(\pi^{\alpha},\ldots,\pi^{\alpha}.X^{q},c(F_2).H.H_2)$.

Corollaire 46.1a.- Supposons les conditions de 46.1 vérifiées.

Alors $n = t+1$.

Démonstration :

En effet, $c(F_{i+1})$ divise $c(F_i)$; comme $c(F_2) = \pi^{s_2}$ alors $c(F_i) = \pi^{s_i}$ pour $2 \leq i \leq n$ et $s_n \leq \ldots \leq s_2 \leq \alpha$. Or $t < n$ donc $s_n = 0$ et $c(F_n) = 1$, ainsi que $c(F_j) = 1$ pour tout $j > t$. Mais $s_t \neq 0$ et T minimale donc $n = t+1$.

Corollaire 46.1b.- Supposons les conditions de 46.1 vérifiées. Alors $\{\pi^{\alpha},\ldots,\pi^{\alpha}.X^{q},c(F_2).H.H_2,\ldots,c(F_t).H.H_t,H.H_{t+1}\}$ est une partie finie génératrice séparante minimale de $H + id_{A[X]}(\pi^{\alpha})$.

Démonstration :

Il nous suffit de démontrer que $c(F_1).H.H_1 \in mod_A(\pi^{\alpha},\ldots,\pi^{\alpha}.X^{q})$, puisque T est séparante. Or $H_1 = 1$ et π^{α} divise $c(F_1)$, donc $c(F_1) = b.\pi^{\alpha}$ Posons $H = X^{q} + \sum_{i=0}^{q-1} c_i.X^{i}$, alors

$$c(F_1).H.H_1 = b(\pi^{\alpha}.X^{q}) + \sum_{i=0}^{q-1} (b.c_i).(\pi^{\alpha}.X^{i}) \qquad \text{c.q.f.d.}$$

Corollaire 46.1c.- Supposons les conditions de 46.1 vérifiées. Alors $H + id_{A[X]}(\pi^{\alpha}) = \bigcap (H + id_{A[X]}(\pi^{\alpha},P^{\gamma}))$ est une décomposition primaire de $H + id_{A[X]}(\pi^{\alpha})$ où l'intersection porte sur les P unitaires de $A[X]$, irréductibles modulo π tels que (P divise H modulo π) ou (il existe $j \in \mathbb{N}_t^o$ tel que π divise d_j et P divise H_{j+1} modulo π), et $\gamma = \sum_{i=1}^{t} \alpha_i.(\beta+\beta_i)$ où α_i l'exposant de la plus grande puissance de divisant d_i, β_i celui de la plus grande puissance de P divisant H_{i+1} modulo π et β celui de celle de P divisant H modulo π.

Démonstration :

D'après ce qui précède nous pouvons utiliser le corollaire 45.1a, en prenant $\{\pi^{\alpha},\ldots, .X^{q},c(F_2).H.H_2,\ldots,c(F_t).H.H_t,H.H_{t+1}\}$ comme partie finie génératrice séparante minimale. Posons d_i' les quotients respectifs de deux contenus consécutifs et α_i' l'exposant de la plus grande puissance de π divisant d_i', alors :

$$d'_1 = 1,\ldots,d'_{q-1} = 1,\quad d'_q = \pi^{\alpha-s_2},\ldots,d'_{q+1} = \pi^{s_t}$$

$$= d_1 \quad ,\ldots, \quad = d_t$$

$$\alpha'_1 = 0,\ldots,\alpha'_q = 0,\quad \alpha'_{q+1} = \alpha_1 \ ,\ldots,\alpha'_{q+1} = \alpha_t \ .$$

Prenons P unitaire de $A[X]$ irréductible modulo π.

Posons $\beta'_1,\ldots,\beta'_q,\beta'_{q+1},\ldots,\beta'_{q+t}$ les exposants respectifs de la plus grande puissance de P divisant respectivement $X,\ldots,X^q,H.H_2,\ldots,H.H_{t+1}$.

Donc $\beta'_{q+i} = \beta+\beta_i$ où β (resp. β_i) est l'exposant de la plus grande puissance de P divisant H (resp. H_{i+1}) modulo π.

Par conséquent, d'après le corollaire 45.1a, $\gamma = \sum_{i=1}^{q+t} \alpha'_i.\beta'_i$ et $\gamma = \sum_{i=1}^{t} \alpha_i.(\beta+\beta_i)$.

B I B L I O G R A P H I E

[AY 1] C.W. AYOUB - *The decomposition theorem for ideals in polynomial rings,* Journal of Algebra, 76 (1982), p. 99-110.

[AY 2] C.W. AYOUB - *On constructing bases for ideals in polynomial rings over the integers,* Journal of Number Theory, 17 (1983), p. 204-225.

[BER] E.R. BERLEKAMP - *Algebraic Coding Theory,* Mac Graw Hill, NY (1968).

[LAC] D. LACOMBE - *La théorie des fonctions récursives et ses applications,* Bull. Soc. Math. France, 88 (1960), p. 392-468.

[LAZ 1] D. LAZARD - *Algorithmes fondamentaux en algèbre commutative,* Soc. Math. France, Astérisque 38-39 (1976), p. 131-138.

[LAZ 2] D. LAZARD - *Commutative algebra and Computer algebra,* Lect. Notes in Comp. Sciences n° 144 (1982), p. 40-48.

[LAZ 3] D. LAZARD - *Ideal basis and Primary Decomposition. Case of two variables,* A paraître dans Jour. Symb. Computation.

[M.Y.] M. MACHTEY, P. YOUNG - *An introduction to the general theory algorithms,* North Holland, NY.

[RIC] F. RICHMANN - *Constructive aspects of noetherian rings,* Proc. Amer. Math. Soc., 44 (1974), p. 436-441.

[SAM] P. SAMUEL - *La notion de multiplicité en Algèbre et en Géométrie algébrique,* 1ère thèse - Gauthier-Villars, Paris (1951).

[S.Z.] P. SAMUEL, O. ZARISKI - *Commutative Algebra,* Vol. 1, Van Nostrand, Princeton (1958).

[SE 1] A. SEIDENBERG - *Construction in Algebra,* Trans. Amer. Math. Soc., 197 (1974).

[SE 2] A. SEIDENBERG - *Constructions in a polynomial ring over the ring of integer,* Amer. Jour. Math., 100 (1978).

[BLW] B.L. VAN DER WAERDEN - *Moderne Algebra,* 2ème ed., Vol. 1, Frederik Ungar Publishing C°, NY (1943).

[BOU] N. BOURBAKI - *Algèbre commutative. Chap. 4.* Hermann, Paris (1961).

RÉSUMÉ

Les principaux objectifs de ce travail sont d'abord de déterminer pour H, idéal de $A[X]$ où A est un anneau fortement factoriel, T une partie finie génératrice séparante au sens où, pour $F \in A[X]$, nous déterminons algorithmiquement si $F \in H$ ou non, et, utilisant T, de construire une décomposition primaire de H, pour laquelle nous avons effectivement déterminer une partie finie génératrice des composantes primaires ainsi que de leurs racines.

Au premier chapitre, je précise la notion d'anneau fortement factoriel, en me référant aux travaux de D. Lazard sur les anneaux codables dans lesquels les calculs classiques de l'algèbre sont effectifs et j'étudie, en reprenant les travaux de Krönecker, Van der Waerden et Seidenberg, les corps pour lesquels la décomposition en produit de facteurs irréductibles est effective dans les anneaux de polynômes.

Le premier objectif est atteint aux chapitres II et III pour $A[X]$ et $A[X,Y]$, où j'adapte à A anneau principal algorithmique, un résultat établi pour $\mathbb{Z}$ par C.W. Ayoub, et au chapitre II, je donne un théorème précisant la structure de ces parties finies génératrices séparantes.

Le second l'est au chapitre IV pour lequel je m'inspire d'un article de C.W. Ayoub mais j'établis une méthode de recherche effective des parties finies génératrices des composantes primaires, ainsi que pour leurs racines, dont les calculs sont bornés dès que l'on utilise une partie finie génératrice séparante minimale.

MOTS CLES : Anneaux principaux, polynômes, idéaux, algorithmes, parties finies génératrices, décomposition primaire.