

BASES SUR  $\mathbb{Z}$  DES IDEAUX PRIMAIRES CANONIQUES D'UN  
CORPS  $K$  , EXTENSION DE  $\mathbb{Q}$  , CYCLIQUE , DE DEGRE  
PREMIER IMPAIR  $\ell$  , ET APPROXIMATIONS  $p$  - ADIQUES  
DES RACINES D'UN POLYNOME FONDAMENTAL  $f$  DE  $K$  .

Bases sur  $\mathbb{Z}$  des idéaux primaires canoniques d'un corps  $K$  , extension de  $\mathbb{Q}$  , cyclique , de degré premier impair  $\ell$  et approximations p-adiques des racines d'un polynome fondamental  $f$  de  $K$  .

## INTRODUCTION

L'objet de ce travail est la généralisation aux extensions de  $\mathbb{Q}$  , cycliques, de degré premier impair  $\ell$  ( $\ell \geq 5$ ) des résultats obtenus sur la construction de  $\mathbb{Z}$ -bases des idéaux primaires canoniques d'une extension cubique cyclique de  $\mathbb{Q}$  ([13], [14] et [15]).

Soit  $K$  une extension de  $\mathbb{Q}$  , cyclique , de degré premier impair  $\ell$  . Notons  $D_K$  son discriminant . Si  $\theta$  est un entier de trace 0 ou 1 , suivant que  $\ell$  divise ou ne divise pas  $D_K$  , on note  $f$  le polynome minimal de  $\theta$  sur  $\mathbb{Q}$  ([17]) ;  $f$  est appelé " polynome fondamental de  $K$  " ([16]) .

Désignons par  $E_K$  l'anneau des entiers de  $K$  .

Soit  $p$  un nombre premier . Nous savons ([7] ou [16]) que la décomposition de l'idéal  $pE_K$  , engendré par  $p$  dans  $K$  , est liée à celle de  $f$  sur  $\mathbb{Q}_p$  par les équivalences suivantes :

- $pE_K = \mathfrak{P} \Leftrightarrow f$  est irréductible sur  $\mathbb{Z}/p\mathbb{Z}$  , donc  $f$  est irréductible sur  $\mathbb{Q}_p$  .
- $pE_K = \mathfrak{P}^\ell \Leftrightarrow f$  est une puissance  $\ell^{\text{ième}}$  sur  $\mathbb{Z}/p\mathbb{Z}$  et  $f$  est irréductible sur  $\mathbb{Q}_p \Leftrightarrow p$  divise  $D_K$  .
- $pE_K = \mathfrak{P}_1 \times \mathfrak{P}_2 \times \dots \times \mathfrak{P}_\ell \Leftrightarrow f$  se factorise sur  $\mathbb{Q}_p$  .

Notons  $N(\mathfrak{P})$  la norme de l'idéal  $\mathfrak{P}$  ; les idéaux primaires canoniques ([6]) de  $K$  sont les idéaux  $\mathfrak{P}^k$  , où  $\mathfrak{P}$  est un idéal premier de degré un ,  $k$  est un entier quelconque si  $p = N(\mathfrak{P})$  ne divise pas  $D_K$  ,  $k = 1$  si  $p$  divise  $D_K$  .

Comme dans le cas cubique, la représentation des idéaux primaires canoniques de  $K$  par des bases sur  $\mathbb{Z}$  est liée au calcul effectif des approximations  $p$ -adiques, modulo  $p^k$ , pour tout entier  $k$ , des racines dans  $\mathbb{Q}_p$  d'un polynôme fondamental  $f$  de  $K$ .

Désignons par  $D(\theta)$  le discriminant du polynôme  $f$ .

Nous avons :  $|D(\theta)| = I^2(\theta) \times D_K$  ([12]).

Nous sommes amenés à distinguer trois catégories de nombres premiers  $p$  :

- (1) les diviseurs premiers  $p$  de  $D_K$ .
- (2) les nombres premiers  $p$  qui ne divisent pas  $D(\theta)$  et pour lesquels l'idéal  $pE_K$  se factorise dans  $K$ .
- (3) les nombres premiers  $p$  divisant  $D(\theta)$  et ne divisant pas  $D_K$ .

La première partie de ce mémoire est consacrée aux cas (1) et (2).

Dans le cas (1), nous indiquons une base sur  $\mathbb{Z}$  de l'idéal premier  $\mathfrak{P}$  tel que  $pE_K = \mathfrak{P}^{\ell}$ . Nous montrons, de plus, que  $f$  est irréductible au module  $p^2$  près. Il en résulte alors que  $f$  est irréductible sur  $\mathbb{Q}_p$  et que, pour tout entier  $k \geq 2$ , l'idéal  $\mathfrak{P}^k$  n'est pas un idéal canonique.

Dans le cas (2), les congruences  $f(x) \equiv 0 \pmod{p}$  admettent, pour tout entier  $k$ ,  $\ell$  racines deux à deux distinctes modulo  $p^k$ , et chacune d'elles est l'approximation, modulo  $p^k$ , d'une racine  $p$ -adique de  $f$ .

Dans la seconde partie, nous étudions les nombres premiers  $p$  qui divisent  $D(\theta)$  sans diviser  $D_K$ . Nous montrons d'abord que  $I(\theta)$  et  $\sqrt{D_K}$  sont premiers entre eux, par suite les nombres premiers considérés sont les diviseurs premiers de  $I(\theta)$ . Nous montrons, de

plus, que, si  $I(\theta) \equiv 0 \pmod{p}$ , l'idéal  $pE_K$  se factorise dans  $K$  en un produit de  $\ell$  idéaux premiers deux à deux distincts.

Si la congruence fondamentale  $f(x) \equiv 0 \pmod{p}$  admet au moins une racine simple  $a$ , ce qui est toujours le cas pour  $\ell = 5$ , nous savons, à l'aide du lemme de Hensel ([3]) construire une suite d'entiers  $a_k$ , définis modulo  $p^k$ , de premier terme  $a$ , qui converge vers une racine de  $f$  dans  $\mathbb{Q}_p$ . A partir de cette suite, nous savons trouver les approximations, modulo  $p^k$ , des autres racines de  $f$  dans  $\mathbb{Q}_p$ .

Si  $\ell > 5$ , pour certains diviseurs premiers  $p$  de  $I(\theta)$ , il peut arriver que la congruence  $f(x) \equiv 0 \pmod{p}$  n'admette que des racines multiples. Nous donnons alors une méthode de construction d'une suite d'entiers  $a_k$ , ayant pour premier terme une racine multiple  $a$  et convergeant vers une racine de  $f$  dans  $\mathbb{Q}_p$ . A partir de cette suite, comme dans le cas d'une racine simple, nous construisons les approximations des autres racines de  $f$  dans  $\mathbb{Q}_p$ .

La troisième partie de ce travail est consacrée au cas particulier des corps de degré 5.

$K$  étant un corps cyclique de degré 5, nous donnons des conditions nécessaires et suffisantes, portant sur  $I(\theta)$  et sur le quadruplet d'entiers conjugués de  $\mathbb{Q}^{(5)}$  générateur de  $K$ , pour que la congruence fondamentale suivant un diviseur premier de  $I(\theta)$  admette :

- ou bien, une racine double et trois racines simples
- ou bien, deux racines doubles et une racine simple
- ou bien, une racine d'ordre 4 et une racine simple.

Nous donnons, pour terminer, quelques exemples de développements  $p$ -adiques.

PARTIE I

Représentation des idéaux  $\mathfrak{P}^k$  par des bases sur  $\mathbb{Z}$  dans les deux cas suivants :

- $p = N(\mathfrak{P})$  divise  $D_K$  .
- $p = N(\mathfrak{P})$  ne divise pas  $D(\theta)$  et  $p \in E_K$  se factorise dans  $K$  .

1.1.- Notations et rappels .

1) Notations .

Dans tout ce mémoire, les notations utilisées sont les suivantes :

$\ell$  : nombre premier impair ,  $\ell \geq 5$  .

$\mathbb{Q}^{\ell} = \mathbb{Q}(\epsilon^{\ell})$  :  $\ell^{\text{ième}}$  corps cyclotomique , engendré par  $\epsilon$  , racine primitive  $\ell^{\text{ième}}$  de l'unité .

Soit  $r$  un entier rationnel ,  $1 \leq r \leq \ell-1$  , tel que sa classe modulo  $\ell$  engendre le groupe multiplicatif  $(\mathbb{Z}/\ell\mathbb{Z})^*$  ; les éléments du groupe  $\text{Gal}(\mathbb{Q}^{\ell}/\mathbb{Q})$  sont les  $\ell-1$  automorphismes , notés  $\tau^i$  ,  $1 \leq i \leq \ell-1$  , définis par les égalités :  $\tau^i(\epsilon^k) = \epsilon^{r^i k}$  ,  $1 \leq i \leq \ell-1$  ,  $r^i k$  modulo  $\ell$  .

Pour des raisons de commodité d'écriture, pour tout  $\alpha \in \mathbb{Q}^{\ell}$ , le conjugué  $\tau^i(\alpha)$  de  $\alpha$  sera noté  $\alpha_j$  ,  $1 \leq j \leq \ell-1$  ,  $j \equiv r^i \pmod{\ell}$  .

$K$  : extension cyclique de  $\mathbb{Q}$  , de degré  $\ell$  .

$E_K$  : anneau des entiers de  $K$  .

$G = \text{Gal}(K/\mathbb{Q}) = \langle \sigma \rangle$  . Pour tout  $\lambda \in K$  , on notera  $\lambda_i$  ,  $1 \leq i \leq \ell$  , le conjugué  $\sigma^i(\lambda)$  de  $\lambda$  . Les éléments  $\theta_u$  d'un  $\ell$ -uplet de conjugués irrationnels de  $K$  sont alors numérotés , modulo  $\ell$  , de façon que  $\sigma^h(\theta_u) = \theta_{u+h}$  .

2) Rappels ( [16] ).

- Résolvante de Lagrange d'un élément  $\theta_u$  .

Le groupe  $\hat{G}$  des caractères de  $G$  est un groupe cyclique

d'ordre  $\ell$  dont les éléments, notés  $\chi_k$ ,  $0 \leq k \leq \ell-1$ , sont définis par :

$$\chi_0(\sigma^h) = 1, \quad \chi_k(\sigma^h) = \epsilon^{hk}, \quad 1 \leq k \leq \ell-1, \quad h \in \mathbb{Z}, \quad h \pmod{\ell}.$$

La résolvante de Lagrange de l'élément  $\theta_u$  relativement au caractère  $\chi_k$  est l'élément du corps  $K\mathbb{Q}'$  (composé du corps  $K$  et du corps  $\mathbb{Q}'$ ) :

$$\langle \theta_u, \chi_k \rangle = \sum_{\varphi \in G} \chi_k(\varphi^{-1}) \varphi(\theta_u), \quad 0 \leq k \leq \ell-1, \quad u \pmod{\ell}.$$

- Choix d'un polynôme fondamental et d'une base de  $E_K$ .

Les corps cycliques  $K$ , de degré premier impair  $\ell$ , sont construits à partir des idéaux principaux  $\mathfrak{m}$  de  $\mathbb{Q}'$ , qui sont engendrés par la puissance  $\ell^{\text{ième}}$  d'une résolvante de Lagrange d'un élément primitif  $\theta$  de  $K$ .

J.J. PAYAN a établi l'équivalence suivante :

$$\mathfrak{m} = (\langle \theta, \chi_k \rangle^\ell), \quad 1 \leq k \leq \ell-1 \Leftrightarrow \mathfrak{m} = \mathfrak{n}^\ell \prod_{j=1}^{j=\ell-1} \mathfrak{A}_j^{j^*}$$

où :  $j^*$  est un entier déterminé par :  $1 \leq j^* \leq \ell-1$  et  $jj^* \equiv 1 \pmod{\ell}$ ,

$\mathfrak{n}$  est un idéal principal,

$\mathfrak{A}$  est un idéal premier, de degré un, dont la norme est sans facteur carré et est première à  $\ell$ , et  $\mathfrak{A}_j$  est le conjugué  $\tau^i(\mathfrak{A})$ ,  $j \equiv r^i \pmod{\ell}$ ,  $i = \{1, \dots, \ell-1\}$ .

En désignant par  $\lambda$  une base de l'idéal principal  $\mathfrak{n}$ , par  $\mu$

une base de l'idéal  $\prod_{j=1}^{\ell-1} \mathfrak{A}_j^{j^*}$ , nous avons :  $\mathfrak{m} = (\lambda^\ell \mu)$ .

Un corps  $K$  est dit unitaire s'il peut être construit à l'aide d'un nombre  $\mu \equiv 1 \pmod{\ell}$ . Dans ce cas, le  $\ell$ -uple de conjugués  $\{\theta_u\}$  construit avec  $\lambda = 1$ ,  $\mu$ ,  $s = 1$ , forme une base de  $E_K$ .

Un corps  $K$  est dit non unitaire s'il peut être construit à l'aide d'un nombre  $\mu \equiv \epsilon^h \pmod{\ell}$  ( $h \not\equiv 0 \pmod{\ell}$ ). Dans ce cas, si  $\{\theta_u\}$  désigne le  $\ell$ -uple de conjugués construit avec  $\lambda = \ell$ ,  $\mu$  et  $s = 0$ , les entiers  $\{1, \theta_{u+1}, \theta_{u+2}, \dots, \theta_{u+\ell-1}\}$  forment une base de  $E_K$ .

Comme , dans les deux cas , 1 et  $\ell-1$  des  $\theta_u$  forment une base de  $E_K$  , nous n'utiliserons , dans la suite , que les bases de la forme  $\{ 1, \theta_u, \dots, \theta_{u+\ell-2} \}$  ( $u+j$ , défini mod.  $\ell$ ) et plus particulièrement la base  $\{ 1, \theta_1, \dots, \theta_{\ell-1} \}$  .

Nous choisissons pour polynome fondamental  $f$  de  $K$ : le polynome minimal , à coefficients dans  $\mathbb{Q}$  , de ces  $\theta_u$  .

- Calcul de  $D_K$  .

Le discriminant  $D_K$  se calcule à l'aide d'une base d'entiers : (I-1)

$$D_K = \begin{vmatrix} 1 & \dots & \dots & \dots & 1 \\ \theta_u & & & & \theta_{u+\ell-1} \\ \vdots & & & & \vdots \\ \theta_{u+\ell-2} & & & & \theta_{u+\ell-3} \end{vmatrix}^2 = [\ell^{2(1-s)} m]^{l-1} = M^{l-1}$$

en posant  $M = \ell^{2(1-s)} m$  , avec  $s = 1$  pour un corps unitaire ,  $s = 0$  sinon , et  $m = p_1 \times p_2 \times \dots \times p_n$  , les  $p_i$  étant des nombres premiers , deux à deux distincts , congrus à +1 modulo  $\ell$  .

- Calcul de  $D(\theta)$  ( [10] ) .

$$D(\theta) = (-1)^{\frac{\ell(\ell-1)}{2}} D_\ell^2 ,$$

où  $D_\ell$  est le déterminant de Vandermonde d'ordre  $\ell$  :

$$\text{ligne } i \geq 2 \rightarrow \begin{vmatrix} 1 & \dots & 1 & \dots & 1 \\ \vdots & & & & \vdots \\ \vdots & & \theta_j^{i-1} & & \vdots \\ \vdots & & & & \vdots \\ \theta_1^{\ell-1} & & \uparrow & & \theta_\ell^{\ell-1} \end{vmatrix} = D_\ell = \prod_{1 \leq i < j \leq \ell} (\theta_j - \theta_i)$$

colonne  $j \geq 1$

- Relation entre  $D(\theta)$  et  $D_K$  .

Le quotient  $I(\theta) = \sqrt{\frac{|D(\theta)|}{D_K}}$  est un entier, appelé " indice de  $\theta$  " .

$$\text{Nous avons donc : } |D(\theta)| = I^2(\theta) \times D_K \quad (1-2)$$

- Expression des racines de  $f$  en fonction de l'une d'entre elles .

Pour tout  $u$  ,  $1 \leq u \leq \ell$  , et pour tout  $h$  ,  $1 \leq h \leq \ell-1$  , il existe un entier rationnel  $d_h$  , divisant  $I(\theta)$  et un polynome  $g_h$  ,  $g_h \in \mathbb{Z}[X]$  , de degré inférieur ou égal à  $\ell-1$  , tel que :

$$d_h \theta_{u+h} = g_h(\theta_u) \quad (1 \leq h \leq \ell-1) \quad (1-3)$$

La méthode théorique pour déterminer les polynomes  $g_h$  est la suivante :

$u$  étant un entier ,  $1 \leq u \leq \ell$  , pour tout  $j$  ,  $2 \leq j \leq \ell-1$  , on exprime  $\theta_u^j$  dans la base  $\{ 1, \theta_u, \dots, \theta_{u+\ell-2} \}$  et on considère les  $\ell-2$  égalités obtenues comme un système de  $\ell-2$  équations à  $\ell-2$  inconnues :  $\theta_{u+1}, \theta_{u+2}, \dots, \theta_{u+\ell-2}$  . Ce système est un système de Cramer , car son déterminant  $\Delta$  est égal , en valeur absolue , à  $I(\theta)$  . Par les formules de Cramer , on obtient alors  $\Delta \theta_{u+h}$  ,  $2 \leq h \leq \ell-2$  , sous la forme d'un polynome en  $\theta_u$  , à coefficients entiers rationnels , de degré inférieur ou égal à  $\ell-1$  . Les formules (1-3) pour  $h = 1, \dots, \ell-2$  s'en déduisent par simplification éventuelle par le p.g.c.d de  $I(\theta)$  et des coefficients du polynome. On trouve enfin  $g_{\ell-1}$  , en utilisant :  $\theta_{u+\ell-1} = s - \theta_u - \sum_{h=1}^{\ell-2} \theta_{u+h}$  .

1.2.- Idéaux primaires canoniques de  $K$  .

Soit  $\mathfrak{J}$  un idéal de  $K$  . On notera  $\mathfrak{J}_u$  ,  $u \text{ mod. } \ell$  , les conjugués  $\sigma^u(\mathfrak{J})$  de l'idéal  $\mathfrak{J}$  .

Soit  $p$  un nombre premier naturel . Les décompositions possibles de l'idéal  $pE_K$  , engendré par  $p$  dans  $K$  , sont :



-  $pE_K = \mathfrak{P}$ ,  $\mathfrak{P}$  idéal premier de degré  $\ell$ ; ce cas se produit si et seulement si  $f$  est irréductible sur  $\mathbb{Z}/p\mathbb{Z}$ , donc aussi sur  $\mathbb{Q}_p$ .

-  $pE_K = \mathfrak{P}^\ell$ ,  $\mathfrak{P}$  idéal premier de degré un; ce cas se produit si et seulement si  $p$  divise  $D_K$  ou encore si et seulement si  $f(x) \equiv (x-c)^\ell \pmod{p}$  et  $f(x) \not\equiv (x-c)^\ell \pmod{p^2}$ .  $f$  est alors irréductible dans  $\mathbb{Q}_p$ .

-  $pE_K = \prod_{u=1}^{u=\ell} \mathfrak{P}_u$ , les idéaux  $\mathfrak{P}_u$  étant des idéaux premiers,

de degré un, deux à deux distincts; ce cas se produit si et seulement si  $f(x) \equiv \prod_{u \text{ mod. } \ell} (x-c_u) \pmod{p}$  avec au moins deux racines de  $f$

$\pmod{p}$   $c_u$  et  $c_{u'}$  non congrues mod.  $p$ ;  $f$  se factorise alors dans  $\mathbb{Q}_p$ .

C'est ce dernier cas qui nous intéresse plus particulièrement dans ce travail.

En 1965, au cours d'un exposé (non publié) intitulé "Bases arithmétiques de certains idéaux de corps abéliens de degré premier", J.J. PAYAN a donné le résultat suivant :

Définition 1.1 :

On appelle idéal canonique un idéal entier  $\mathfrak{J}$  de  $K$  dont la décomposition est de la forme :  $\mathfrak{J} = \prod_{i=1}^{i=r} \mathfrak{P}_i^{k_i}$ , où les  $\mathfrak{P}_i$  sont des idéaux

premiers, de degré un, de normes  $p_i$  deux à deux distinctes.  $k_i$  est un entier supérieur ou égal à 1 si  $p_i$  ne divise pas  $D_K$ ,  $k_i = 1$  si  $p_i$  divise  $D_K$ .

Proposition 1.1 :

Soit  $\mathfrak{J}$  un idéal canonique, de norme  $q$ ; pour tout entier  $j$ ,  $1 \leq j \leq \ell$ , il existe un entier rationnel  $c_j$ , défini de façon unique au module  $q$  près, tel que  $\theta_j \equiv c_j \pmod{\mathfrak{J}}$ . Ces entiers  $c_j$  ont les propriétés suivantes :

- (i)  $f(c_j) \equiv 0 \pmod{q}$ ,  $1 \leq j \leq \ell$ , et  $\sum_{j=1}^{\ell} c_j \equiv s \pmod{q}$
- (ii)  $\{q, \theta_i - c_i, 1 \leq i \leq \ell-1\}$  est une base sur  $\mathbb{Z}$  de l'idéal  $\mathfrak{J}$ .

Remarques :

- 1°)  $\mathfrak{J} \cap \mathbb{Z} = q\mathbb{Z}$ .
- 2°) L'idéal  $\mathfrak{J}$  de base  $\{q, \theta_i - c_i, 1 \leq i \leq \ell-1\}$  sera noté  $\mathfrak{J} = (q, \theta_i - c_i, 1 \leq i \leq \ell-1)$ .
- 3°) On obtient encore une base sur  $\mathbb{Z}$  de  $\mathfrak{J}$ , en remplaçant dans la base précédente l'un quelconque des  $\theta_i - c_i, 1 \leq i \leq \ell-1$ , par  $\theta_\ell - c_\ell$ .
- 4°)  $\theta_i \equiv c_i \pmod{\mathfrak{J}} \Rightarrow \sigma^h(\theta_i) = \theta_{i+h} \equiv c_i \pmod{\sigma^h(\mathfrak{J}) = \mathfrak{J}_h}$ .  
( $i+h \pmod{\ell}$ )

D'où :  $\mathfrak{J}_h = (q, \theta_{i+h} - c_i, 1 \leq i \leq \ell-1)$ ,  $1 \leq h \leq \ell$ ,  $i+h \pmod{\ell}$ .  
 Mais  $\theta_i = \sigma^h(\theta_{i+\ell-h})$  ( $i+\ell-h \pmod{\ell}$ ) avec  $\theta_{i+\ell-h} \equiv c_{i+\ell-h} \pmod{\mathfrak{J}}$   
 d'où :  $\mathfrak{J}_h = (q, \theta_i - c_{i+\ell-h}, 1 \leq i \leq \ell-1)$ ,  $1 \leq h \leq \ell$ ,  $i+\ell-h \pmod{\ell}$ .

Cas particulier : Idéal primaire canonique .

Un idéal entier  $\mathfrak{J}$  de  $K$  est un idéal primaire canonique si et seulement si  $\mathfrak{J} = \mathfrak{P}^k$ , où  $\mathfrak{P}$  est un idéal premier de degré un ;  $k$  est un entier quelconque si  $p = N(\mathfrak{P})$  ne divise pas  $D_K$ ,  $k = 1$  si  $p$  divise  $D_K$ .

Il résulte de la proposition I.1 le :

Corollaire I.1 :

Soit  $\mathfrak{P}^k$  un idéal primaire canonique . Pour tout entier  $j$ ,  $1 \leq j \leq \ell$ , il existe un entier rationnel  $a_{j,k}$ , défini de façon unique modulo  $p^k$ , tel que  $\theta_j \equiv a_{j,k} \pmod{\mathfrak{P}^k}$  et  $\{p^k, \theta_i - a_{i,k}, 1 \leq i \leq \ell-1\}$  est une base sur  $\mathbb{Z}$  de  $\mathfrak{P}^k$ .

Pour construire effectivement des  $\mathbb{Z}$ -bases des idéaux  $\mathfrak{P}^k$ , nous précisons comment nous obtenons les entiers  $a_{i,k}$ . Pour cela, nous distinguons les trois cas suivants :

- $p = N(\mathfrak{P})$  divise  $D_K$
- $p = N(\mathfrak{P})$  ne divise pas  $D(\theta)$
- $p = N(\mathfrak{P})$  divise  $D(\theta)$  et ne divise pas  $D_K$ .

1.3.- Cas où  $p = N(\mathfrak{P})$  divise  $D_K$ .

Dans ce cas bien connu, nous avons les résultats suivants :

Proposition 1.2 :

Soit  $p$  un diviseur premier de  $D_K$  et soit  $\mathfrak{P}$  l'idéal premier tel que  $pE_K = \mathfrak{P}^\ell$ . Alors  $\{ p, \theta_i - c, 1 \leq i \leq \ell-1 \}$  est une  $\mathbb{Z}$ -base de l'idéal  $\mathfrak{P}$ .

Démonstration :

$$D_K \equiv 0 \pmod{p} \Leftrightarrow f(x) \equiv (x-c)^\ell \pmod{p} \Leftrightarrow pE_K = \mathfrak{P}^\ell.$$

D'après la proposition 1.1, pour tout  $i$ ,  $1 \leq i \leq \ell$ , il existe  $c_i \in \mathbb{Z}$ , unique mod.  $p$ , tel que  $\theta_i \equiv c_i \pmod{\mathfrak{P}}$  et  $\{ p, \theta_i - c_i, 1 \leq i \leq \ell-1 \}$  est une base sur  $\mathbb{Z}$  de  $\mathfrak{P}$ . Alors :  $0 \equiv f(c_i) \equiv (c - c_i)^\ell \pmod{p}$ , d'où :  $c \equiv c_i \pmod{p}$ ,  $1 \leq i \leq \ell$ , et on a bien  $\mathfrak{P} = (p, \theta_i - c, 1 \leq i \leq \ell-1)$ .

Proposition 1.3 :

Si  $D_K \equiv 0 \pmod{p}$  et si  $\mathfrak{P}$  est l'idéal premier tel que  $pE_K = \mathfrak{P}^\ell$ , alors :

- (i) Pour tout  $i$ ,  $1 \leq i \leq \ell$ ,  $\theta_i$  n'est pas congru à un entier rationnel modulo l'idéal  $\mathfrak{P}^2$ .
- (ii) La congruence  $f(x) \equiv 0 \pmod{p^2}$  n'a pas de solution et  $f$  est irréductible modulo  $p^2$ .

Démonstration : ( Nous raisonnons par l'absurde )

- (i) S'il existe un entier  $i$ ,  $1 \leq i \leq \ell$ , et  $a \in \mathbb{Z}$  tels que  $\theta_i \equiv a \pmod{\mathfrak{P}^2}$ , alors, pour tout  $h$ ,  $1 \leq h \leq \ell$ ,  $\sigma^h(\theta_i) = \theta_{i+h} \equiv a \pmod{\mathfrak{P}^2}$  ( $h+i \pmod{\ell}$ ), soit :  $\theta_u \equiv a \pmod{\mathfrak{P}^2}$ ,  $1 \leq u \leq \ell$ . Par suite, pour

tout  $\lambda \in K$ , il existe  $x \in \mathbb{Z}$  tel que  $\lambda \equiv x \pmod{\mathfrak{p}^2}$ . Or  $p \in \mathfrak{p}^2$ , on aurait alors :  $\lambda \equiv r \pmod{\mathfrak{p}^2}$  avec  $0 \leq r < p$ , d'où  $\text{card. } E_K/\mathfrak{p}^2 = p$ , ce qui est impossible, car  $\text{card. } E_K/\mathfrak{p}^2 = N(\mathfrak{p}^2) = p^2$ .

(ii) S'il existe  $a \in \mathbb{Z}$  tel que  $f(a) \equiv 0 \pmod{p^2}$ ,  $(f(a))_{E_K} \equiv 0 \pmod{p^2 E_K = \mathfrak{p}^{2\ell}}$ . Nous avons :  $a \equiv c \pmod{p}$ , d'où  $a - \theta_i \equiv 0 \pmod{\mathfrak{p}}$ ,  $1 \leq i \leq \ell$ , et  $(a - \theta_i)_{E_K} = \mathfrak{p} \times \mathfrak{S}_i$ ,  $1 \leq i \leq \ell$ . Comme  $f(x) = \prod_{i=1}^{\ell} (x - \theta_i)$ ,  $(f(a))_{E_K} = \left( \prod_{i=1}^{\ell} (a - \theta_i) \right)_{E_K} = \prod_{i=1}^{\ell} (a - \theta_i)_{E_K} = \mathfrak{p}^{\ell} \prod_{i=1}^{\ell} \mathfrak{S}_i \equiv 0 \pmod{\mathfrak{p}^{2\ell}}$ , d'où :  $\prod_{i=1}^{\ell} \mathfrak{S}_i \equiv 0 \pmod{\mathfrak{p}^{\ell}}$ . L'idéal premier  $\mathfrak{p}$  divisant le produit  $\prod \mathfrak{S}_i$ , il existe au moins un entier  $i$ ,  $1 \leq i \leq \ell$ , tel que  $\mathfrak{p}$  divise  $\mathfrak{S}_i$ . Pour cet entier  $i$ , on aurait  $a - \theta_i \equiv 0 \pmod{\mathfrak{p}^2}$ , ce qui est impossible d'après (i).

On déduit de cette proposition le :

Théorème 1.1 :

Si  $D_K \equiv 0 \pmod{p}$ , la congruence  $f(x) \equiv 0 \pmod{p^k}$  n'a pas de solution pour tout entier  $k > 1$  et  $f$  est irréductible dans  $\mathbb{Q}_p$ .

1.4.- Cas où  $p = N(\mathfrak{p})$  ne divise pas  $D(\theta)$ .

Soit  $p$  un nombre premier ne divisant pas  $D(\theta)$ . On suppose que  $f$  n'est pas irréductible sur  $\mathbb{Z}/p\mathbb{Z}$ . Nous savons alors que  $pE_K$  est décomposé en un produit de  $\ell$  idéaux premiers, de degré un, deux à deux distincts et conjugués. Soit  $\mathfrak{p}$  l'un de ces idéaux premiers. Pour tout entier  $k \geq 1$ ,  $\mathfrak{p}^k$  étant un idéal primaire canonique, nous avons :  $\theta_i \equiv a_{i,k} \pmod{\mathfrak{p}^k}$ ,  $1 \leq i \leq \ell$ , et  $\mathfrak{p}^k = (p^k, \theta_i - a_{i,k}, 1 \leq i \leq \ell-1)$  avec  $a_{i,k} \in \mathbb{Z}$ ,  $f(a_{i,k}) \equiv 0 \pmod{p^k}$  et  $\sum_{i=1}^{\ell} a_{i,k} \equiv s \pmod{p^k}$ , (corollaire 1.1). D'autre part, entre les  $\theta_u$ , nous avons les relations :

(1-3)  $d_h \theta_{u+h} = g_h(\theta_u)$ ,  $1 \leq h \leq \ell-1$ ,  $1 \leq u \leq \ell$ ,  $u+h \pmod{\ell}$ ,

où  $d_h$  divise  $l(\theta)$ . Nous avons alors : pour tout  $h$ ,  $1 \leq h \leq \ell-1$ ,

$$d_h (\theta_{h+1} - a_{h+1,k}) = g_h(\theta_1) - d_h a_{h+1,k} \equiv 0 \pmod{\mathfrak{P}^k}$$

avec  $\theta_1 \equiv a_{1,k} \pmod{\mathfrak{P}^k}$ . Il en résulte :

$$g_h(a_{1,k}) - d_h a_{h+1,k} \equiv 0 \pmod{\mathfrak{P}^k \cap \mathbb{Z}} \text{ avec } \mathfrak{P}^k \cap \mathbb{Z} = p^k \mathbb{Z},$$

d'où  $d_h a_{h+1,k} \equiv g_h(a_{1,k}) \pmod{p^k}$ . Comme  $p$  ne divise pas  $D(\theta)$ ,  $p$  ne divise pas  $d_h$ , pour tout  $h$ , et les congruences précédentes déterminent  $a_{h+1,k}$ ,  $1 \leq h \leq \ell-1$ , de façon unique modulo  $p^k$ , si  $a_{1,k}$  est connu.

De plus, si  $i \neq j$ ,  $a_{i,k} \not\equiv a_{j,k} \pmod{p}$ . Car si  $a_{i,k} \equiv a_{j,k} \pmod{p}$ , comme  $\mathfrak{P}^k \subset \mathfrak{P}$ , on aurait  $\theta_i \equiv a_{i,k} \equiv a_{j,k} \equiv \theta_j \pmod{\mathfrak{P}}$ , par suite  $D_\ell = \prod_{1 \leq i < j \leq \ell} (\theta_j - \theta_i) \in \mathfrak{P} \cap \mathbb{Z}$  et  $\sqrt{|D(\theta)|} = |D_\ell| \equiv 0 \pmod{p}$ , ce qui est contraire à l'hypothèse.

Nous avons donc obtenu la :

Proposition 1.4 :

Si  $D(\theta) \not\equiv 0 \pmod{p}$  et si  $f$  n'est pas irréductible sur  $\mathbb{Z}/p\mathbb{Z}$ , pour tout entier  $k$ , la congruence  $f(x) \equiv 0 \pmod{p^k}$  admet  $\ell$  racines. Ces racines sont deux à deux incongrues mod.  $p$  (donc aussi mod.  $p^k$ ) et si  $a_{1,k}$  est l'une de ces racines, les autres racines  $a_{h+1,k}$ ,  $1 \leq h \leq \ell-2$ , sont déterminées par les congruences :

$$d_h a_{h+1,k} \equiv g_h(a_{1,k}) \pmod{p^k}, \quad \sum_{h=1}^{h=\ell} a_{h,k} \equiv s \pmod{p^k}.$$

Comme, pour tout  $k \geq 1$ ,  $\mathfrak{P}^{k+1} \subset \mathfrak{P}^k$ , nous avons  $a_{i,k+1} \equiv a_{i,k} \pmod{p^k}$ , ce qui montre que les  $\ell$  suites  $\{a_{i,k}\}$ ,  $1 \leq i \leq \ell$ , convergent  $p$ -adiquement ([3]), lorsque  $k$  tend vers l'infini, vers les racines de  $f$  dans  $\mathbb{Z}_p$ .

On désigne par  $\theta_i$ ,  $1 \leq i \leq \ell$ , les racines dans  $\mathbb{Q}_p$  du polynôme  $f$  et on les associe aux racines réelles de  $f$  de la façon suivante :

on choisit arbitrairement  $\theta_1$  associée à  $\theta_1$ , alors les racines  $\theta_{h+1}$  associées à  $\theta_{h+1}$ ,  $1 \leq h \leq \ell-1$ , sont définies par les relations :

$d_h \theta_{h+1} = g_h(\theta_1)$ . Avec ces notations, la suite  $\{a_{i,k}\}$  converge vers  $\theta_i$ , et le nombre rationnel  $a_{i,k}$  sera appelé "approximation p-adique modulo  $p^k$  de  $\theta_i$ ".

De plus, choisissons dans  $\mathbb{Q}_p$  la distance  $d$  définie de la façon suivante :

pour tout  $(\lambda, \mu) \in \mathbb{Q}_p^2$ ,  $d(\lambda, \mu) = \left(\frac{1}{p}\right)^n$  si  $\lambda \neq \mu$  et  $\lambda - \mu = p^n \eta$ ,  $\eta$  unité p-adique,  $d(\lambda, \mu) = 0$  si  $\lambda = \mu$ . Comme, pour tout  $i$  et tout  $j$  tels que  $i \neq j$ ,  $a_{i,1} \not\equiv a_{j,1} \pmod{p}$ ,  $d(\theta_j, \theta_i) = 1$ .

Par suite :

Théorème 1.2 :

Si  $D(\theta) \not\equiv 0 \pmod{p}$  et si  $f$  n'est pas irréductible dans  $\mathbb{Z}/p\mathbb{Z}$ , l'équation  $f(x) \equiv 0$  admet  $\ell$  racines dans  $\mathbb{Z}_p$  et la distance p-adique de deux quelconques des racines est 1.

Théorème 1.3 :

Si  $D(\theta) \not\equiv 0 \pmod{p}$  et si  $f$  n'est pas irréductible dans  $\mathbb{Z}/p\mathbb{Z}$ , pour tout entier  $k \geq 1$ , l'idéal  $p^k E_K$  se décompose en un produit de  $\ell$  idéaux primaires canoniques conjugués :

$$p^k E_K = \prod_{h=1}^{\ell} \sigma^h(\mathfrak{P}^k) \text{ avec, pour tout } h, 1 \leq h \leq \ell,$$

$$\sigma^h(\mathfrak{P}^k) = \mathfrak{P}_h^k = (p^k, \theta_{i+h} - a_{i,k}, 1 \leq i \leq \ell-1) = (p^k, \theta_i - a_{i+\ell-h,k}, 1 \leq i \leq \ell-1).$$

$i+h \pmod{\ell} \qquad \qquad \qquad i+\ell-h \pmod{\ell}$

$\{p^k, \theta_{i+h} - a_{i,k}, 1 \leq i \leq \ell-1\}$  et  $\{p^k, \theta_i - a_{i+\ell-h,k}, 1 \leq i \leq \ell-1\}$  sont deux  $\mathbb{Z}$ -bases (identiques si  $h = \ell$ ) de l'idéal  $\mathfrak{P}_h^k$  et si  $a_{1,k}$  est l'approximation p-adique modulo  $p^k$  de  $\theta_1$ ,  $a_{i,k}$ ,  $2 \leq i \leq \ell$ , est l'approximation p-adique modulo  $p^k$  de  $\theta_i$ .

Remarque :

La construction des  $\mathbb{Z}$ -bases des idéaux primaires canoniques de  $K$ , qui résulte de la proposition 1.4 et du théorème 1.3, est théorique. Cette construction ne devient effective que lorsqu'on connaît explicitement un polynôme fondamental de  $K$  et lorsqu'on sait écrire les polynômes  $g_h$ ; c'est ce qui a lieu dans le cas particulier des corps cycliques de degré 5.

Les résultats de cette première partie sont la généralisation immédiate des résultats obtenus dans le cas des corps cubiques cycliques pour les diviseurs premiers  $p$  de  $D_K$  et pour les nombres premiers  $p$  ne divisant pas  $D(\theta)$ .

PARTIE II

Représentation des idéaux  $\mathfrak{P}^k$  par des bases sur  $\mathbb{Z}$  lorsque  $p = N(\mathfrak{P})$  divise  $D(\theta)$  sans diviser  $D_K$ .

II.1.- Propriétés des diviseurs de  $I(\theta)$ .

Proposition II.1 :

$$\left| \begin{array}{l} I(\theta) \text{ et } \sqrt{D_K} \text{ sont premiers entre eux.} \end{array} \right.$$

Les nombres premiers qui divisent  $D(\theta)$  sans diviser  $D_K$  sont alors les diviseurs premiers de  $I(\theta)$ .

Pour démontrer de façon élémentaire ce résultat, nous avons besoin du

Lemme II.1 :

Soient  $K$  un corps non unitaire et  $\mathfrak{S}$  l'idéal premier, de degré un, tel que  $\ell E_K = \mathfrak{S}^\ell$ . Alors  $\mathfrak{S}^2 = (\ell, \ell\theta_1, \theta_i - \theta_1, 2 \leq i \leq \ell-1)$ .

Démonstration :

$K$  étant non unitaire,  $s = 0$  et  $\sqrt{D_K} = (\ell^{2m})^{\frac{\ell-1}{2}}$ , par suite  $\sqrt{D_K} \equiv 0 \pmod{\ell^{\ell-1}}$  et  $\sqrt{|D(\theta)|} = I(\theta) \times \sqrt{D_K} \equiv 0 \pmod{\ell^{\ell-1}}$ . D'après la proposition I.2, pour tout  $i$  et tout  $j$ ,  $j \neq i$ ,  $\theta_j - \theta_i \in \mathfrak{S}$ ; posons alors pour tout couple  $(i, j)$ ,  $1 \leq i < j \leq \ell$ ,  $(\theta_j - \theta_i)E_K = \mathfrak{S} \times \mathfrak{S}_{j,i}$ . Le produit  $\prod_{1 \leq i < j \leq \ell} (\theta_j - \theta_i)$  comportant  $\frac{\ell(\ell-1)}{2}$  facteurs  $\theta_j - \theta_i$ ,

nous aurons :

$$\left( \sqrt{|D(\theta)|} \right) E_K = \prod_{1 \leq i < j \leq \ell} (\theta_j - \theta_i) E_K = \mathfrak{S}^{\frac{\ell(\ell-1)}{2}} \prod_{1 \leq i < j \leq \ell} \mathfrak{S}_{j,i} \equiv 0 \pmod{\mathfrak{S}^{\ell(\ell-1)}},$$

il en résulte :

$$\prod_{1 \leq i < j \leq \ell} \mathfrak{S}_{j,i} \equiv 0 \pmod{\mathfrak{S}^{\frac{\ell(\ell-1)}{2}}}.$$



L'idéal premier  $\mathfrak{A}$  divisant le produit  $\prod \mathfrak{F}_{j,i}$ , il existe au moins un couple  $(i,j)$ ,  $1 \leq i < j \leq \ell$ , tel que  $\mathfrak{F}_{j,i} \equiv 0 \pmod{\mathfrak{A}}$ . Pour ces entiers  $i, j$ , on a  $\theta_j - \theta_i \equiv 0 \pmod{\mathfrak{A}^2}$ , ou encore  $\sigma^j(\theta) - \sigma^i(\theta) \equiv 0 \pmod{\mathfrak{A}^2}$ . Mais  $i \neq \ell$ ,  $\sigma^i$  admet un inverse  $\sigma^{-i}$  ( $\neq \sigma^i$ ) et  $\mathfrak{A}$  est invariant par tous les éléments du groupe  $G = \langle \sigma \rangle$ , par suite en posant  $\varphi = \sigma^{j-i}$ , on a :  $\theta \equiv \varphi(\theta) \pmod{\mathfrak{A}^2}$ , d'où  $\theta \equiv \varphi^k(\theta) \pmod{\mathfrak{A}^2}$ ,  $1 \leq k \leq \ell$ . Comme on a  $1 \leq j-i \leq \ell-1$ ,  $\varphi$  engendre  $G$  et  $\theta$  est congru à tous ses conjugués modulo  $\mathfrak{A}^2$ , ce qui s'écrit aussi :  $\theta_1 \equiv \theta_2 \equiv \dots \equiv \theta_i \equiv \dots \equiv \theta_\ell \pmod{\mathfrak{A}^2}$ .

Nous pouvons alors construire une base sur  $\mathbb{Z}$  de l'idéal  $\mathfrak{A}^2$ .

Nous avons :  $\ell \in \mathfrak{A}^2$ ,  $\ell(\theta_1 - c) \in \mathfrak{A}^2$ ,  $\theta_i - \theta_1 \in \mathfrak{A}^2$ ,  $2 \leq i \leq \ell-1$ .

Considérons alors l'idéal entier  $\mathfrak{F} = \ell\lambda_0 + \ell(\theta_1 - c)\lambda_1 + \sum_{i=2}^{\ell-1} \lambda_i(\theta_i - \theta_1)$ ,

avec  $\lambda_i \in E_K$ ,  $0 \leq i \leq \ell-1$ . Il est clair que  $\mathfrak{F} \subseteq \mathfrak{A}^2$ .

Démontrons que  $\mathfrak{A}^2 \subseteq \mathfrak{F}$ .

Or  $\{1, \theta_i, 1 \leq i \leq \ell-1\}$  est une base de  $E_K$ , et il en est de même de  $\{1, \theta_1 - c, \theta_i - \theta_1, 2 \leq i \leq \ell-1\}$ . Soit  $\alpha \in \mathfrak{A}^2$ , dans la base précédente,

$\alpha = x_0 + x_1(\theta_1 - c) + \sum_{i=2}^{\ell-1} x_i(\theta_i - \theta_1)$ ,  $x_i \in \mathbb{Z}$ ,  $0 \leq i \leq \ell-1$ .

Remarquons d'abord que :  $\alpha, \theta_1 - c, \theta_i - \theta_1, 2 \leq i \leq \ell-1$ , étant dans  $\mathfrak{A}$ ,  $x_0$  appartient à  $\mathfrak{A} \cap \mathbb{Z}$ , d'où :  $x_0 \equiv 0 \pmod{\ell}$ .

D'autre part,  $\alpha, \ell, \theta_i - \theta_1, 2 \leq i \leq \ell-1$ , étant dans  $\mathfrak{A}^2$ ,  $x_1(\theta_1 - c)$  est dans  $\mathfrak{A}^2$ . Nous avons donc :  $\ell(\theta_1 - c) \in \mathfrak{A}^2$ ,  $x_1(\theta_1 - c) \in \mathfrak{A}^2$ ,  $\theta_1 - c \notin \mathfrak{A}^2$  (proposition 1.3). Il en résulte :  $x_1 \equiv 0 \pmod{\ell}$ .

Alors :  $\alpha = x_0\ell + x_1\ell(\theta_1 - c) + \sum_{i=2}^{\ell-1} x_i(\theta_i - \theta_1) \in \mathfrak{F}$  ;

nous avons donc montré que  $\mathfrak{A}^2 \subseteq \mathfrak{F}$ , par suite  $\mathfrak{A}^2 = \mathfrak{F}$ .

De plus, d'après la démonstration précédente, tout élément de  $\mathfrak{A}^2$  s'écrit, de façon unique, (à cause de l'indépendance linéaire sur  $\mathbb{Z}$  de :  $1, \theta_1 - c, \theta_i - \theta_1, 2 \leq i \leq \ell-1$ ) comme combinaison

linéaire, à coefficients dans  $\mathbb{Z}$ , des éléments :  $\ell$ ,  $\ell(\theta_1 - c)$ ,  $\theta_i - \theta_1$ ,  $2 \leq i \leq \ell-1$ . Il en résulte que ces éléments forment une  $\mathbb{Z}$ -base de  $\mathfrak{S}^2$ , ce qui démontre que :

$$\mathfrak{S}^2 = (\ell, \ell(\theta_1 - c), \theta_i - \theta_1, 2 \leq i \leq \ell-1) = (\ell, \ell\theta_1, \theta_i - \theta_1, 2 \leq i \leq \ell-1).$$

Démonstration de la proposition II.1 : Nous raisonnons par l'absurde.

Soit  $p$  un nombre premier tel que  $I(\theta) \equiv 0 \equiv \sqrt{D_K} \pmod{p}$ .

Nous avons  $\sqrt{D_K} = \left[ \ell^{2(1-s)} p_1 \times p_2 \times \dots \times p_n \right]^{\frac{\ell-1}{2}}$  avec  $s = 1$  pour un corps unitaire,  $s = 0$  sinon. Il faut donc considérer deux cas :

1°)  $p \neq \ell$ . Alors  $p \in \{p_i\}_{1 \leq i \leq n}$  et  $p \equiv 1 \pmod{\ell}$ .

Par hypothèse nous avons :

$$\sqrt{|D(\theta)|} = I(\theta) \times \sqrt{D_K} \equiv 0 \equiv \prod_{1 \leq i < j \leq \ell} (\theta_j - \theta_i) \pmod{p^{\frac{\ell+1}{2}}}.$$

Or  $D_K \equiv 0 \pmod{p} \Leftrightarrow pE_K = \mathfrak{P}^\ell$ , d'où :  $p^{\frac{\ell+1}{2}} E_K = \mathfrak{P}^{\frac{\ell(\ell+1)}{2}}$ .

Compte-tenu de la proposition 1.2, et en posant, pour tout couple  $(i, j)$

$1 \leq i < j \leq \ell$ ,  $(\theta_j - \theta_i)E_K = \mathfrak{P} \times \mathfrak{S}_{j,i}$ , nous avons :

$$\prod_{1 \leq i < j \leq \ell} (\theta_j - \theta_i)E_K = \mathfrak{P}^{\frac{\ell(\ell-1)}{2}} \prod_{1 \leq i < j \leq \ell} \mathfrak{S}_{j,i} \equiv 0 \pmod{\mathfrak{P}^{\frac{\ell(\ell+1)}{2}}}$$

d'où  $\prod_{1 \leq i < j \leq \ell} \mathfrak{S}_{j,i} \equiv 0 \pmod{\mathfrak{P}^\ell}$ . Par le raisonnement utilisé dans la

démonstration du lemme II.1, on en déduit :  $\theta_1 \equiv \dots \equiv \theta_i \equiv \dots \equiv \theta_\ell \pmod{\mathfrak{P}^2}$ .

Par suite  $s = \sum_{j=1}^{\ell} \theta_j \equiv \ell \theta_u \pmod{\mathfrak{P}^2}$ ,  $1 \leq u \leq \ell$ . Mais,  $p$  est premier

avec  $\ell$  et  $p \in \mathfrak{P}^2$ , il existe alors  $r \in \mathbb{Z}$  tel que  $\theta_u \equiv r \pmod{\mathfrak{P}^2}$ , ce qui est impossible (proposition 1.3).

2°)  $p = \ell$ . Puisque  $\sqrt{D_K} \equiv 0 \pmod{\ell}$ ,  $s = 0$  et  $\sqrt{D_K} \equiv 0 \pmod{\ell^{\ell-1}}$ , par suite  $\sqrt{|D(\theta)|} = I(\theta) \times \sqrt{D_K} \equiv 0 \pmod{\ell^\ell}$ . Soit  $\mathfrak{S}$  l'idéal premier tel que  $\ell E_K = \mathfrak{S}^\ell$ , alors  $\ell^\ell E_K = \mathfrak{S}^{\ell^2}$ . Compte-tenu du lemme II.1, et en posant, pour tout couple  $(i, j)$ ,  $1 \leq i < j \leq \ell$ ,

$$(\theta_j - \theta_i)E_K = \mathfrak{g}^2 \times \mathfrak{S}_{j,i} :$$

$$\prod_{1 \leq i < j \leq \ell} (\theta_j - \theta_i)E_K = \mathfrak{g}^{\ell(\ell-1)} \prod_{1 \leq i < j \leq \ell} \mathfrak{S}_{j,i} \equiv 0 \pmod{\mathfrak{g}^{\ell^2}},$$

d'où  $\prod_{1 \leq i < j \leq \ell} \mathfrak{S}_{j,i} \equiv 0 \pmod{\mathfrak{g}^{\ell}}$ . On en déduit encore :

$\theta_1 \equiv \dots \equiv \theta_i \equiv \dots \equiv \theta_{\ell} \pmod{\mathfrak{g}^2}$ . On aurait :  $\ell \in \mathfrak{g}^3$ , d'où  $\ell \theta_1 \in \mathfrak{g}^3$ , et  $\theta_i - \theta_1 \in \mathfrak{g}^3$ ,  $2 \leq i \leq \ell-1$ , ce qui montre que  $\mathfrak{g}^2 \subseteq \mathfrak{g}^3$ , d'où  $\mathfrak{g}^2 = \mathfrak{g}^3$ , ce qui est impossible.

Proposition II.2 :

| Si  $I(\theta) \equiv 0 \pmod{p}$ , l'idéal  $pE_K$  se décompose dans  $K$ .

Démonstration :

$$I(\theta) \equiv 0 \pmod{p} \Rightarrow \sqrt{|D(\theta)|} \equiv 0 \equiv \prod_{1 \leq i < j \leq \ell} (\theta_j - \theta_i) \pmod{p}.$$

Raisonnons par l'absurde : si l'idéal  $pE_K$  est inerte, il existe  $i$  et  $j$  tels que  $\theta_j - \theta_i \equiv 0 \pmod{pE_K}$  et comme  $pE_K$  est invariant par les éléments de  $G$ , on en déduit encore :  $\theta_1 \equiv \dots \equiv \theta_i \equiv \dots \equiv \theta_{\ell} \pmod{pE_K}$

et  $s = \sum_{j=1}^{\ell} \theta_j \equiv \ell \theta_u \pmod{pE_K}$ ,  $1 \leq u \leq \ell$ . Si  $K$  est unitaire,  $s = 1$ ,

donc  $\ell \theta_u \equiv s \pmod{pE_K} \Rightarrow p \neq \ell$ . Si  $K$  est non unitaire,  $s = 0$  et  $\ell$  divise  $D_K$ , mais comme  $I(\theta)$  est premier à  $\sqrt{D_K}$ ,  $\ell$  ne divise pas  $I(\theta)$ , on a donc encore  $p \neq \ell$ .

Soit alors  $\lambda$  un entier quelconque de  $K$ .

Dans la base  $\{ 1, \theta_i, 1 \leq i \leq \ell-1 \}$  de  $E_K$ ,  $\lambda = x_0 + \sum_{i=1}^{\ell-1} x_i \theta_i$ ,  $x_i \in \mathbb{Z}$ ,

$$0 \leq i \leq \ell-1, \text{ d'où : } \ell \lambda = \ell x_0 + \sum_{i=1}^{\ell-1} x_i (\ell \theta_i) \equiv \ell x_0 + s \sum_{i=1}^{\ell-1} x_i \pmod{pE_K}.$$

Puisque  $p$  est premier à  $\ell$ , il existe  $r \in \mathbb{Z}$  tel que  $\lambda \equiv r \pmod{pE_K}$ , par suite  $\text{card. } E_K/pE_K = p = N(pE_K)$ , ce qui contredit l'hypothèse  $pE_K$  inerte.

Conséquences :

1°) Pour tout diviseur premier  $p$  de  $I(\theta)$ , l'idéal  $pE_K$  est décomposé et comme  $I(\theta)$  est premier à  $\sqrt{D_K}$ ,  $p$  ne divise pas  $D_K$ . Par suite  $pE_K$  se décompose en un produit de  $\ell$  idéaux premiers de degré un, deux à deux distincts et conjugués, et si  $\mathfrak{P}$  est l'un quelconque de ces idéaux premiers, pour tout entier  $k$ ,  $\mathfrak{P}^k$  est un idéal primaire canonique et  $\mathfrak{P}^k \cap Z = p^k Z$ .

2°)  $f$  se factorise dans  $Z/pZ$  et dans  $\mathbb{Q}_p$  (§ 1.2).

Soit  $r$  l'entier,  $r \geq 1$ , tel que  $I(\theta) \equiv 0 \pmod{p^r}$  et  $I(\theta) \not\equiv 0 \pmod{p^{r+1}}$ . Alors  $\sqrt{|D(\theta)|} = |D_\ell| = I(\theta) \times \sqrt{D_K} \equiv 0 \pmod{p^r}$  et  $\sqrt{|D(\theta)|} \not\equiv 0 \pmod{p^{r+1}}$ , d'où  $D_\ell = \prod_{1 \leq i < j \leq \ell} (\theta_j - \theta_i)$

$\in \mathfrak{P}^r$ ,  $D_\ell \notin \mathfrak{P}^{r+1}$  pour tout idéal premier  $\mathfrak{P}$  de norme  $p$ . Considérons un couple  $(i, j)$ ,  $1 \leq i < j \leq \ell$  : ou bien  $\theta_j - \theta_i \notin \mathfrak{P}$ , ou bien  $\theta_j - \theta_i \in \mathfrak{P}$ ; dans ce dernier cas, comme  $\theta_j - \theta_i \notin \mathfrak{P}^{r+1}$ , il existe un entier  $r_{i,j}$ ,  $1 \leq r_{i,j} \leq r$ , tel que  $\theta_j - \theta_i \in \mathfrak{P}^{r_{i,j}}$  et  $\theta_j - \theta_i \notin \mathfrak{P}^{r_{i,j}+1}$ . En convenant que  $\mathfrak{P}^0 = E_K$ , on posera  $r_{i,j} = 0$  si  $\theta_j - \theta_i \notin \mathfrak{P}$ . Dans ces conditions, pour tout couple  $(i, j)$ ,  $1 \leq i < j \leq \ell$ , il existe un entier  $r_{i,j}$ ,  $0 \leq r_{i,j} \leq r$ , tel que  $\theta_j - \theta_i \in \mathfrak{P}^{r_{i,j}}$  et  $\theta_j - \theta_i \notin \mathfrak{P}^{r_{i,j}+1}$ ; il en résulte :

$$D_\ell = \prod_{1 \leq i < j \leq \ell} (\theta_j - \theta_i) \in \mathfrak{P}^{\left(\sum_{1 \leq i < j \leq \ell} r_{i,j}\right)} \text{ et } D_\ell \notin \mathfrak{P}^{\left(\sum_{1 \leq i < j \leq \ell} r_{i,j}+1\right)},$$

ce qui montre que  $r = \sum_{1 \leq i < j \leq \ell} r_{i,j}$  (en particulier, au moins un des

$r_{i,j}$  est non nul). De plus,  $\theta_u$ ,  $1 \leq u \leq \ell$ , étant les racines  $p$ -adiques de  $f$ , associées aux racines réelles  $\theta_u$  de  $f$  et  $d$  étant la distance

$p$ -adique définie au paragraphe 1.4, nous avons :  $d(\theta_j, \theta_i) = \left(\frac{1}{p}\right)^{r_{i,j}}$

et  $\prod_{1 \leq i < j \leq \ell} d(\theta_j, \theta_i) = \left(\frac{1}{p}\right)^r$ .

Nous pouvons donc énoncer :

Proposition II.3 :

Si  $I(\theta) \equiv 0 \pmod{p^r}$  et  $I(\theta) \not\equiv 0 \pmod{p^{r+1}}$  ( $r \geq 1$ ), pour tout idéal premier  $\mathfrak{P}$  de norme  $p$  et pour tout couple  $(i, j)$ ,  $1 \leq i < j \leq \ell$ , il existe un entier  $r_{i,j}$ ,  $0 \leq r_{i,j} \leq r$ , tel que  $\theta_j - \theta_i \in \mathfrak{P}^{r_{i,j}}$  et  $\theta_j - \theta_i \notin \mathfrak{P}^{r_{i,j}+1}$  et on a :  $r = \sum_{1 \leq i < j \leq \ell} r_{i,j}$ . Ces entiers  $r_{i,j}$  mesurent la distance  $p$ -adique des racines  $\theta_j$  et  $\theta_i$  associées à  $\theta_j$  et  $\theta_i$  et

$$\prod_{1 \leq i < j \leq \ell} d(\theta_j, \theta_i) = \left(\frac{1}{p}\right)^r .$$

Pour construire des  $\mathbb{Z}$ -bases des idéaux  $\mathfrak{P}^k$  lorsque  $p = N(\mathfrak{P})$  divise  $I(\theta)$ , nous avons besoin des notions de racine multiple d'une congruence algébrique et de racine d'un idéal .

II.2.- Racines multiples d'une congruence algébrique .

Soit  $p$  un nombre premier ,  $k$  un entier naturel et  $g$  un polynome primitif de  $\mathbb{Z}[X]$  , de degré  $\nu$  , c'est-à-dire :

$$g = a_0 X^\nu + a_1 X^{\nu-1} + \dots + a_p X^{\nu-p} + \dots + a_{\nu-1} X + a_\nu ,$$

les  $a_i$  ,  $0 \leq i \leq \nu$  , étant des entiers rationnels , premiers entre eux dans leur ensemble . Nous définissons l'ordre de multiplicité d'une racine d'une congruence algébrique suivant le module primaire  $p^k$  par analogie avec la définition d'une racine multiple d'un polynome dans un corps commutatif de la façon suivante :

Définition II.1 :

On appelle ordre de multiplicité d'une racine  $a$  de la congruence  $g(x) \equiv 0 \pmod{p^k}$  le plus grand entier  $t$  tel que  $g$  soit divisible par  $(X-a)^t$  modulo  $p^k$  .

- Si  $t = 1$  , on dit que  $a$  est racine simple ou racine d'ordre 1 de la congruence mod.  $p^k$  .
- Si  $t > 1$  , on dit que  $a$  est racine multiple d'ordre  $t$  de la congruence .

Pour tout polynome  $g$ , on pose  $g^{(0)} = g$  et  $g^{(k)}$ ,  $k \geq 1$ , désigne le polynome dérivé d'ordre  $k$  de  $g$ . Une racine d'ordre  $t$  d'une congruence algébrique suivant un module premier  $p$  est alors caractérisée par la propriété :

Proposition II.4 :

Soient  $p$  un nombre premier et  $g$  un polynome primitif de  $\mathbb{Z}[X]$ . Alors  $a \in \mathbb{Z}$  est racine d'ordre  $t$  ( $t \geq 1$ ) de la congruence  $g(x) \equiv 0 \pmod{p}$  si et seulement si :

- (1)  $\frac{g^{(k)}(a)}{k!} \equiv 0 \pmod{p}$ ,  $0 \leq k \leq t-1$  ;
- (2)  $\frac{g^{(t)}(a)}{t!} \not\equiv 0 \pmod{p}$ .

Le résultat est connu pour  $t = 1$  ([11]). La condition suffisante résulte immédiatement de la formule de Taylor. La condition nécessaire est obtenue en calculant, par la formule de Leibnitz, les dérivées successives, mod.  $p$ , de  $g$ , qui, par définition, s'écrit :  $g(x) \equiv (x-a)^t \varphi(x) \pmod{p}$ ,  $\varphi \in \mathbb{Z}[X]$ ,  $\varphi(a) \not\equiv 0 \pmod{p}$  et en sachant que, puisque  $\varphi \in \mathbb{Z}[X]$ , il en est de même de  $\frac{\varphi(q)}{q!}$ , pour tout entier  $q$  ([11]).

Nous connaissons le résultat suivant ([11]) :

Soit  $g$  un polynome primitif de  $\mathbb{Z}[X]$ , de discriminant  $D$  non nul. Alors, si la congruence  $g(x) \equiv 0 \pmod{p}$  a une racine multiple,  $D$  est divisible par  $p$ .

La réciproque est vraie lorsque  $g$  est un polynome fondamental d'un corps cyclique  $K$  de degré premier impair. En effet : nous savons déjà que si  $D_K \equiv 0 \pmod{p}$ , la congruence fondamentale mod.  $p$  admet une racine d'ordre  $\ell$ . Il reste à démontrer la :

Proposition II.5 :

Si  $p$  est un diviseur premier de  $I(\theta)$ , la congruence fondamentale  $f(x) \equiv 0 \pmod{p}$  admet une racine multiple.

Démonstration :

On suppose  $I(\theta) \equiv 0 \pmod{p}$ . Soit  $\mathfrak{P}$  l'un quelconque des idéaux premiers divisant  $p \in E_K$ . Il existe au moins un couple  $(i, j)$ ,  $1 \leq i < j \leq \ell$ , tel que  $\theta_j - \theta_i \in \mathfrak{P}$  (proposition II.3). Mais, d'après la proposition I.1, nous avons :  $\theta_j \equiv c_j$ ,  $\theta_i \equiv c_i \pmod{\mathfrak{P}}$ , d'où  $\theta_j - \theta_i \equiv c_j - c_i \pmod{\mathfrak{P}}$  et  $c_j - c_i \in \mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$ , par suite  $c_j \equiv c_i \equiv a \pmod{p}$ . De  $f(x) = \prod_{u=1}^{u=\ell} (x - \theta_u)$  avec  $\theta_u \equiv c_u \pmod{\mathfrak{P}}$ ,  $1 \leq u \leq \ell$ , on déduit :

$$f(x) \equiv \prod_{u=1}^{u=\ell} (x - c_u) \pmod{\mathfrak{P}}, \text{ puis } f(x) \equiv \prod_{u=1}^{u=\ell} (x - c_u) \pmod{p}.$$

$$\text{On a donc } f(x) \equiv (x - c_j)(x - c_i) \prod_{\substack{1 \leq u \leq \ell \\ u \neq i, j}} (x - c_u) \pmod{p},$$

ou encore  $f(x) \equiv (x - a)^2 \varphi(x) \pmod{p}$ , en posant

$$\varphi(x) = \prod_{\substack{1 \leq u \leq \ell \\ u \neq i, j}} (x - c_u)$$

ce qui montre que  $a$  est racine multiple d'ordre  $t \geq 2$  de la congruence  $f(x) \equiv 0 \pmod{p}$ . Et puisque  $D_K \not\equiv 0 \pmod{p}$ , on a  $t \leq \ell - 1$ .

Racine d'ordre  $t$  d'un idéal.

En 1971, au cours d'un exposé, J.J. PAYAN a donné la définition suivante : Soit  $\mathfrak{A}$  un idéal entier de  $K$ . On dit que  $a$  ( $a \in \mathbb{Z}$ ) est racine de l'idéal  $\mathfrak{A}$  (relativement à  $\theta$ ) si  $\theta - a \in \mathfrak{A}$ .

Nous allons préciser cette notion en définissant l'ordre d'une racine d'un idéal.

Définition II.2 :

Soit  $\mathfrak{P}^k$  ( $k \in \mathbb{N}^*$ ) un idéal primaire canonique . On dit que  $a$  ( $a \in \mathbb{Z}$ ) est racine d'ordre  $t$  ( $t$  entier  $\geq 1$ ) de l'idéal  $\mathfrak{P}^k$ , s'il existe  $t$  entiers  $i_h$  tels que  $\theta_{i_h} - a \in \mathfrak{P}^k$  pour  $1 \leq h \leq t$ , et  $\theta_u - a \notin \mathfrak{P}^k$  si  $u \notin \{i_h\}_{1 \leq h \leq t}$ .

Conséquence :

Soit  $k$  un entier,  $k \geq 2$ , et soit  $a$  une racine d'ordre  $t_k$  de l'idéal  $\mathfrak{P}^k$ ; comme  $\mathfrak{P}^k \subset \mathfrak{P}^{k-1}$ ,  $\theta_{i_h} - a \in \mathfrak{P}^{k-1}$  pour  $1 \leq h \leq t_k$ , donc  $a$  est racine d'ordre  $t_{k-1} \geq t_k$  de  $\mathfrak{P}^{k-1}$ . Par suite, une racine  $a$  d'ordre  $t_k$  de l'idéal  $\mathfrak{P}^k$  est racine d'ordre  $t_j$  de tout idéal  $\mathfrak{P}^j$  pour  $1 \leq j \leq k$  et on a :  $1 \leq t_k \leq \dots \leq t_j \leq \dots \leq t_1$ .

Relation entre les racines de la congruence  $f(x) \equiv 0 \pmod{p}$  et les racines d'un idéal premier  $\mathfrak{P}$  de norme  $p$ .

Proposition II.6 :

Soit  $p$  un diviseur premier de  $l(\theta)$ . Alors  $a$  ( $a \in \mathbb{Z}$ ) est racine d'ordre  $t$  ( $1 \leq t \leq \ell$ ) de la congruence fondamentale mod.  $p$  si et seulement si  $a$  est racine d'ordre  $t$  de l'un quelconque de  $\ell$  idéaux premiers de norme  $p$ .

Démonstration :

La condition est suffisante .

Soit  $a$  une racine d'ordre  $t$  de l'un quelconque des idéaux premiers  $\mathfrak{P}$  divisant  $pE_K$ . Il existe donc  $t$  entiers  $i_h$  tels que  $\theta_{i_h} \equiv a \pmod{\mathfrak{P}}$ ,  $1 \leq h \leq t$ , et  $\theta_u \not\equiv a \pmod{\mathfrak{P}}$  si  $u \notin \mathcal{O}_1$ , en posant  $\mathcal{O}_1 = \{i_h\}_{1 \leq h \leq t}$ . Avec les notations de la proposition I.1, nous avons :  $c_j \equiv a \pmod{p}$  si  $j \in \mathcal{O}_1$  et  $c_j \not\equiv a \pmod{p}$  si  $j \notin \mathcal{O}_1$ . Il en résulte :  $f(x) \equiv (x - a)^t g(x) \pmod{p}$  avec  $g(x) = \prod_{j \notin \mathcal{O}_1} (x - c_j)$ .



Comme  $a - c_j \not\equiv 0 \pmod{p}$  pour tout  $j \notin \mathcal{S}_1$ ,  $g(a) \not\equiv 0 \pmod{p}$ , ce qui montre que  $a$  est racine d'ordre  $t$  de la congruence  $f(x) \equiv 0 \pmod{p}$ .

La condition est nécessaire .

Soient  $a$  une racine d'ordre  $t$  ( $t \geq 1$ ) de la congruence  $f(x) \equiv 0 \pmod{p}$  et  $\mathfrak{P}$  un idéal premier de norme  $p$ . Nous avons  $\theta_j \equiv c_j \pmod{\mathfrak{P}}$ ,

$1 \leq j \leq \ell$ ,  $c_j \in \mathbb{Z}$ . Comme  $f(x) \equiv \prod_{u=1}^{u=\ell} (x - c_u) \pmod{p}$ ,  $f(a) \equiv 0$

$\pmod{p} \Leftrightarrow \prod_{u=1}^{u=\ell} (a - c_u) \equiv 0 \pmod{p}$  et le nombre premier  $p$  divi-

se au moins un des facteurs  $a - c_u$ . Appelons  $t'$  le nombre d'entiers  $i$ ,  $1 \leq i \leq \ell$ , tels que  $c_i \equiv a \pmod{p}$ , ( $1 \leq t' < \ell$ ) et désignons par  $i_h$ ,  $1 \leq h \leq t'$ , ces  $t'$  entiers. Nous avons :

$a \equiv c_{i_h} \equiv \theta_{i_h} \pmod{\mathfrak{P}}$ ,  $1 \leq h \leq t'$ ,  $a \not\equiv \theta_u \pmod{\mathfrak{P}}$  si  $u \neq i_h$ ,  $1 \leq h \leq t'$ .

$a$  est donc racine d'ordre  $t'$  de l'idéal  $\mathfrak{P}$ , et d'après la condition suffisante  $t' = t$ .

Remarque :

La proposition II.6 n'est valable que pour un nombre premier  $p$  et les idéaux premiers  $\mathfrak{P}$  de norme  $p$ . Si  $k > 1$ , il n'y a plus coïncidence entre la notion de racine d'ordre  $t$  de la congruence  $f(x) \equiv 0 \pmod{p}$  et celle de racine d'ordre  $t$  des idéaux primaires canoniques  $\mathfrak{P}^k$  : pour  $k > 1$ , si  $a$  est racine d'ordre  $t$  de l'idéal primaire canonique  $\mathfrak{P}^k$ ,  $a$  est racine d'ordre  $\tau \geq t$  de la congruence  $f(x) \equiv 0 \pmod{p^k}$  et il existe des exemples numériques montrant qu'on peut avoir  $\tau > t$ .

Puisque, pour les diviseurs premiers  $p$  de  $I(\theta)$ , la congruence fondamentale mod.  $p$  admet une racine multiple, il faut savoir s'il est possible que toutes ses racines soient multiples. Dans la troisième partie, nous montrons que, dans le cas des corps de degré 5, nous sommes assurés de l'existence, au moins, d'une racine simple.

Par contre, pour les degrés  $\ell > 5$ , on peut trouver des corps  $K$  et des nombres premiers  $p$  tels que la congruence  $f(x) \equiv 0 \pmod{p}$  n'admette que des racines multiples. Un exemple simple est celui du corps  $K$ , primaire, non unitaire, de degré 11, de discriminant  $11^{20}$ , construit à partir d'une racine primitive  $11^{\text{ième}}$  de l'unité  $\epsilon$ , dont le polynôme fondamental  $f$  se réduit mod. 3 à :  $f(x) \equiv x^3 (x+1)^4 (x-1)^4 \pmod{3}$  ([16]).

Comme il y a des cas où la congruence fondamentale mod.  $p$  n'admet que des racines multiples, il faut trouver une méthode, qui permette, à partir de l'une quelconque de ces racines multiples, de construire les approximations  $p$ -adiques mod.  $p^k$ , pour tout entier  $k$ , des racines de  $f$  dans  $\mathbb{Q}_p$ . Cette méthode, qui présente des analogies avec la méthode de Newton-Puiseux concernant les points critiques des fonctions algébriques d'une variable ([1]) (bien qu'elle ait été obtenue indépendamment de cette dernière) nous est suggérée par l'étude des propriétés des racines suivant les puissances successives d'un idéal premier  $\mathfrak{P}$ .

### II.3.- Racines suivant les puissances successives d'un idéal premier.

#### Proposition II.7 :

Soient  $p$  un nombre premier divisant  $I(\theta)$  et  $\mathfrak{P}$  l'un quelconque des idéaux premiers de norme  $p$ . On suppose que  $a \in \mathbb{Z}$  est racine multiple d'ordre  $t_1$  ( $1 < t_1 \leq \ell - 1$ ) de la congruence  $f(x) \equiv 0 \pmod{p}$ . Soit  $h \in \mathbb{N}^*$  et soit  $a_h \in \mathbb{Z}$ ,  $a_h \equiv a \pmod{p}$  une racine d'ordre  $t_h$  de l'idéal  $\mathfrak{P}^h$  ( $t_h \geq 1$  si  $h > 1$ );  $a_h$  est donc racine d'ordre  $t_j$  des idéaux  $\mathfrak{P}^j$  pour  $1 \leq j \leq h$ , avec  $1 \leq t_h \leq \dots \leq t_j \leq \dots \leq t_1$ . Posons  $T_h = \sum_{j=1}^{j=h} t_j$ , et soit  $e$  la partie entière du nombre rationnel  $\frac{1}{h}(T_h - 1) > 0$ .

Dans ces conditions :

$$(i) \quad \frac{f^{(k)}(a_h)}{k!} \equiv 0 \pmod{p^{T_h - hk}} \quad \text{si } 0 \leq k \leq e$$

$$(ii) \quad \frac{f^{(t_h)}(a_h)}{t_h!} \not\equiv 0 \pmod{p^{T_h - ht_h + 1}} .$$

Remarques :

1°)  $t_h - 1 \leq e \leq t_1 - 1$  .

En effet, soit  $e = \left[ \frac{1}{h}(T_h - 1) \right]$  (  $[x]$  désignant la partie entière de  $x$  ).

Comme  $1 \leq t_h \leq \dots \leq t_j \leq \dots \leq t_1$  ,  $T_h = \sum_{j=1}^{j=h} t_j \leq ht_1$  , d'où

$$\frac{1}{h}(T_h - 1) \leq t_1 - \frac{1}{h} , \quad \text{et } e \leq \left[ t_1 - \frac{1}{h} \right] = t_1 - 1 .$$

De même :  $ht_h \leq T_h$  , donc  $ht_h - h \leq T_h - h \leq T_h - 1$  , d'où

$$t_h - 1 \leq \frac{1}{h}(T_h - 1) \quad \text{et} \quad t_h - 1 \leq e .$$

2°) Si  $ht_h < T_h$  , alors  $ht_h \leq T_h - 1$  , d'où  $t_h \leq \frac{1}{h}(T_h - 1)$  et  $t_h \leq e$  ; la propriété (i) sera encore valable pour  $k = t_h$  .

Pour démontrer cette proposition , nous avons besoin du :

Lemme II.2 :

Soit  $f$  un polynome fondamental d'un corps  $K$  , cyclique , de degré premier impair  $\ell$  ; pour tout entier  $k$  ,  $1 \leq k \leq \ell$  ,  $\frac{f^{(k)}}{k!}$  est un polynome de  $\mathbb{Z}[X]$  , de degré  $\ell - k$  ( [11] ) , qui s'écrit sous la forme :

$$\frac{f^{(k)}(X)}{k!} = \sum_{i'=1}^{i'=C_\ell^k} P_{i',k}(X) ,$$

où  $C_\ell^k (= C_\ell^{\ell-k})$  est le coefficient du binôme et chaque polynome  $P_{i',k}$  ,  $1 \leq i' \leq C_\ell^k$  , est le produit des éléments d'une combinaison  $\ell - k$  à  $\ell - k$  des  $\ell$  facteurs  $X - \theta_u$  ,  $1 \leq u \leq \ell$  .

Ce résultat se démontre élémentairement, par récurrence,

à partir de :  $f'(X) = \sum_{i'=1}^{i'=\ell} \left( \prod_{\substack{1 \leq i \leq \ell \\ i \neq i'}} (X - \theta_i) \right) \quad ([10]) .$

$P_{i',k}$ ,  $1 \leq i' \leq C_\ell^k$ , désignent les polynomes obtenus de la façon suivante: à partir des  $\ell$  facteurs  $X - \theta_u$ ,  $1 \leq u \leq \ell$ , du polynome  $f$ , on forme toutes les combinaisons  $\ell-k$  à  $\ell-k$  ( $1 \leq k \leq \ell-1$ ) de ces  $\ell$  facteurs ; à chacune de ces combinaisons on associe le produit de tous ses éléments. On obtient ainsi des polynomes de degré  $\ell-k$ , tous distincts, en nombre  $C_\ell^{\ell-k}$ , qu'on numérote de façon arbitraire et qu'on note avec deux indices : un indice variable  $i'$ , qui est le numéro du polynome, et un indice  $k$ , qui est l'ordre du polynome dérivé  $\frac{f^{(k)}}{k!}$  considéré.

Si  $k = \ell$ , on sait que  $\frac{f^{(\ell)}(X)}{\ell!} = 1$ .

Démonstration de la proposition II.7 :

Les notations utilisées sont les suivantes :

- Pour tout  $j$ ,  $1 \leq j \leq h$ , on introduit les ensembles d'entiers  $\delta_j = \{u, 1 \leq u \leq \ell, \text{ tel que } \theta_u \equiv a_h \pmod{\mathfrak{P}^j}\}$ .

Par définition d'une racine d'ordre  $t_j$  d'un idéal,  $\text{card. } \delta_j = t_j$  et les ensembles  $\delta_j$  forment une suite décroissante pour l'inclusion :

$\delta_{j+1} \subseteq \delta_j$ ,  $1 \leq j \leq h-1$ .

On pose :

-  $\delta_h^1 = \delta_h$  et pour tout  $j$ ,  $1 \leq j \leq h-1$ ,  $\delta_j^1 = \delta_j - \delta_{j+1}$ ,  
 ( $\delta_j^1 = \emptyset \Leftrightarrow \delta_j = \delta_{j+1}$ ).

- Pour tout  $j$ ,  $1 \leq j \leq h$ ,  $t_j^1 = \text{card. } \delta_j^1$ . On a donc :  
 $t_h^1 = t_h (\geq 1)$  et pour  $j$ ,  $1 \leq j \leq h-1$ ,  $t_j^1 = t_j - t_{j+1}$  ( $t_j^1 = 0 \Leftrightarrow \delta_j^1 = \emptyset$ ).

-  $\mathfrak{H} = \{j, 1 \leq j \leq h, \text{ tel que } \delta_j^1 \neq \emptyset\}$  (l'ensemble  $\mathfrak{H}$  est non vide car  $\delta_h^1 = \delta_h \neq \emptyset \Rightarrow h \in \mathfrak{H}$ ).

Démontrons (i) .

$$1^{\circ) \text{ } \underline{k=0} . \text{ Considérons } f(a_h) = \prod_{i \in \mathcal{G}_1} (a_h - \theta_i) \times \prod_{i \notin \mathcal{G}_1} (a_h - \theta_i)$$

et montrons que  $\prod_{i \in \mathcal{G}_1} (a_h - \theta_i) \in \mathbb{P}^{T_h}$  . Pour ce faire , il faut distin -

guer deux cas :

$$\alpha) h = 1 \text{ ou } h \geq 2 \text{ et pour tout } j, 1 \leq j \leq h-1, \mathcal{G}_j' = \emptyset$$

ce qui est équivalent à :  $h \geq 2$  et  $\mathcal{G}_j = \mathcal{G}_1, t_j = t_1, 2 \leq j \leq h$  .

$$\text{On a donc dans ces deux cas : } \mathcal{G}_1 = \mathcal{G}_h \text{ et } T_h = h t_h .$$

Pour tout  $i \in \mathcal{G}_h, a_h - \theta_i \in \mathbb{P}^h$  ; comme  $\text{card. } \mathcal{G}_h = t_h$  ,

$$\text{nous avons : } \prod_{i \in \mathcal{G}_1} (a_h - \theta_i) = \prod_{i \in \mathcal{G}_h} (a_h - \theta_i) \in \mathbb{P}^{h t_h} = \mathbb{P}^{T_h} .$$

$$\beta) h \geq 2 \text{ et il existe } j, 1 \leq j \leq h-1, \text{ tel que } \mathcal{G}_j' \neq \emptyset .$$

Dans ce cas , en remarquant que  $\mathcal{G}_1 = \bigcup_{j \in \mathfrak{H}} \mathcal{G}_j'$  (réunion d'ensembles

deux à deux disjoints) , nous avons :

$$\prod_{i \in \mathcal{G}_1} (a_h - \theta_i) = \prod_{j \in \mathfrak{H}} \left( \prod_{i \in \mathcal{G}_j'} (a_h - \theta_i) \right) .$$

Pour tout  $i \in \mathcal{G}_j' \neq \emptyset, a_h - \theta_i \in \mathbb{P}^j$  et  $\text{card. } \mathcal{G}_j' = t_j' > 0$  ,

par suite :

$$\prod_{i \in \mathcal{G}_j'} (a_h - \theta_i) \in \mathbb{P}^{j t_j'} \text{ et } \prod_{j \in \mathfrak{H}} \left( \prod_{i \in \mathcal{G}_j'} (a_h - \theta_i) \right) \in \prod_{j \in \mathfrak{H}} \mathbb{P}^{j t_j'} = \mathbb{P}^{\sum_{j \in \mathfrak{H}} j t_j'} .$$

Or  $\mathcal{G}_j' = \emptyset \Leftrightarrow t_j' = 0$  , alors  $\sum_{j \in \mathfrak{H}} j t_j' = \sum_{j=1}^{j=h} j t_j' = \sum_{j=1}^{j=h-1} j t_j' + h t_h$  et on

établit facilement par récurrence que  $\sum_{j=1}^{h-1} j t_j' = T_h - h t_h$  .

Par suite :  $\sum_{j=1}^{j=h} j t_j' = T_h$  et on a bien  $\prod_{i \in \mathcal{G}_1} (a_h - \theta_i) \in \mathbb{P}^{T_h}$  .

Dans les deux cas :  $f(a_h) \in \mathbb{P}^{T_h} \cap \mathbb{Z} = \mathbb{P}^{T_h} \mathbb{Z}$  , ce qui éta -

blit (i) pour  $k = 0$  .

2°)  $1 \leq k \leq e$ . Considérons, pour chaque  $i'$ ,  $1 \leq i' \leq C_\ell^k$ ,  $P_{i',k}(X) = \prod_i (X - \theta_i)$ ,  $i$  prenant  $\ell - k$  valeurs entières distinctes dans l'ensemble  $\{1, 2, \dots, \ell\}$ . Or, parmi les  $\ell$  facteurs  $X - \theta_u$ ,  $1 \leq u \leq \ell$ , il y a  $t_1$  facteurs  $X - \theta_u$  pour lesquels  $u \in \mathcal{S}_1$ ; donc, parmi les  $\ell - k$  facteurs  $X - \theta_i$  de  $P_{i',k}$ , il y a au moins  $t_1 - k$  facteurs pour lesquels  $i \in \mathcal{S}_1$  et au plus  $\ell - t_1$  facteurs pour lesquels  $i \notin \mathcal{S}_1$ . Remarquons que :  $1 \leq k \leq e (\leq t_1 - 1) \Rightarrow t_1 - k \geq t_1 - e \geq 1$ .

Par contre le nombre des facteurs  $X - \theta_i$  de  $P_{i',k}$  pour lesquels  $i \notin \mathcal{S}_1$  peut être nul. Nous écrirons :

$$P_{i',k}(X) = \prod_{i \in \mathcal{S}_1} (X - \theta_i) \times \prod_{i \notin \mathcal{S}_1} (X - \theta_i),$$

en convenant de poser  $\prod_{i \notin \mathcal{S}_1} (X - \theta_i) = 1$ , si le nombre de facteurs

$X - \theta_i$ ,  $i \notin \mathcal{S}_1$ , est nul.

Nous démontrons que, pour tout  $i'$ ,  $1 \leq i' \leq C_\ell^k$ ,  $P_{i',k}(a_h) \in \mathbb{P}^{T_h - hk}$ , en montrant que  $\prod_{i \in \mathcal{S}_1} (a_h - \theta_i) \in \mathbb{P}^{T_h - hk}$ .

Pour tout  $j$ ,  $1 \leq j \leq h$ , désignons par  $t_j^! - s_{j,i'}$ ,  $0 \leq t_j^! - s_{j,i'} \leq t_j^!$ , le nombre des entiers  $i \in \mathcal{S}_j^! \neq \emptyset$  tels que  $X - \theta_i$  divise  $P_{i',k}$ . Par convention, si  $\mathcal{S}_j^! = \emptyset$ , on posera  $t_j^! - s_{j,i'} = 0$ .

On considère à nouveau les deux cas :

$\alpha)$   $h = 1$  ou  $h \geq 2$  et pour tout  $j$ ,  $1 \leq j \leq h-1$ ,  $\mathcal{S}_j^! = \emptyset$ .

Alors  $\mathcal{S}_h^! = \mathcal{S}_h = \mathcal{S}_1$  et  $T_h = ht_h$ . Le nombre d'entiers  $i \in \mathcal{S}_h$  tels que  $X - \theta_i$  divise  $P_{i',k}$  est  $t_h - s_{h,i'} = t_1 - s_{h,i'} \geq t_1 - k$ . On en déduit :

$s_{h,i'} \leq k$  et  $\prod_{i \in \mathcal{S}_1} (a_h - \theta_i) = \prod_{i \in \mathcal{S}_h} (a_h - \theta_i) \in \mathbb{P}^{h(t_h - s_{h,i'})}$  mais

$ht_h - hs_{h,i'} = T_h - hs_{h,i'} \geq T_h - hk$ , par suite

$$\prod_{i \in \mathcal{S}_1} (a_h - \theta_i) \in \mathbb{P}^{T_h - hk} \quad \left( \text{puisque } \mathbb{P}^{h(t_h - s_{h,i'})} \subseteq \mathbb{P}^{T_h - hk} \right).$$

$\beta) h \geq 2$  et il existe  $j, 1 \leq j \leq h-1$  tel que  $\mathcal{G}_j^! \neq \emptyset$ .

Comme  $\mathcal{G}_1 = \bigcup_{j \in \mathfrak{H}} \mathcal{G}_j^!$ , le nombre des entiers  $i \in \mathcal{G}_1$  tels que  $X - \theta_i$  di-

visé  $P_{i',k}$  est :  $\sum_{j \in \mathfrak{H}} (t_j^! - s_{j,i'}) \geq t_1 - k$ .

Mais  $t_j^! - s_{j,i'} = 0$  si  $\mathcal{G}_j^! = \emptyset$ ; on a alors :

$$\begin{aligned} \sum_{j \in \mathfrak{H}} (t_j^! - s_{j,i'}) &= \sum_{j=1}^{j=h} (t_j^! - s_{j,i'}) = t_h - s_{h,i'} + \sum_{j=1}^{j=h-1} (t_j - t_{j+1} - s_{j,i'}) \\ &= t_h + \sum_{j=1}^{h-1} (t_j - t_{j+1}) - \sum_{j=1}^{j=h} s_{j,i'}. \end{aligned}$$

D'où :  $0 \leq \sum_{j=1}^{j=h} s_{j,i'} \leq k$ .

Dans ce qui suit, les produits portant sur  $a_h - \theta_i$  seront effectués pour les  $i$  tels que  $X - \theta_i$  divise  $P_{i',k}$ , nous ne le répèterons pas chaque fois.

Considérons :  $\prod_{i \in \mathcal{G}_1} (a_h - \theta_i) = \prod_{j \in \mathfrak{H}} \left( \prod_{i \in \mathcal{G}_j^!} (a_h - \theta_i) \right)$ ,

en convenant de poser  $\prod_{i \in \mathcal{G}_j^!} (a_h - \theta_i) = 1$ , si, pour tout  $i \in \mathcal{G}_j^!$ ,  $X - \theta_i$

ne divise pas  $P_{i',k}$ , donc si  $t_j^! - s_{j,i'} = 0$ . Compte-tenu de  $\mathfrak{P}^\circ = E_K$ ,

nous avons, pour tout  $j \in \mathfrak{H}$ ,  $\prod_{i \in \mathcal{G}_j^!} (a_h - \theta_i) \in \mathfrak{P}^{j(t_j^! - s_{j,i'})}$  et

$$\prod_{j \in \mathfrak{H}} \left( \prod_{i \in \mathcal{G}_j^!} (a_h - \theta_i) \right) \in \mathfrak{P}^{w_i} \text{ avec } w_i = \sum_{j \in \mathfrak{H}} j(t_j^! - s_{j,i'}).$$

Comme  $\mathcal{G}_j^! = \emptyset \Rightarrow t_j^! - s_{j,i'} = 0$ , on a aussi :

$$w_i = \sum_{j=1}^{j=h} j(t_j^! - s_{j,i'}) = \sum_{j=1}^{j=h} j t_j^! - \sum_{j=1}^{j=h} j s_{j,i'}.$$

Or  $\sum_{j=1}^{j=h} j t_j^! = T_h$  (p. 28) et  $\sum_{j=1}^{j=h} j s_{j,i'} \leq h \sum_{j=1}^{j=h} s_{j,i'} \leq hk$ ,

d'où  $w_i \geq T_h - hk > 0$  (car  $k \leq e = \left[ \frac{1}{h}(T_h - 1) \right] \leq \frac{1}{h}(T_h - 1) < \frac{T_h}{h}$ ).

Par suite , comme dans le cas  $\alpha$  ) ,  $\prod_{i \in \delta_1} (a_h - \theta_i) \in \mathfrak{P}^{T_h - hk}$  .

Puisque  $P_{i',k}(a_h) \in \mathfrak{P}^{T_h - hk}$  pour tout  $i'$  ,  $1 \leq i' \leq C_\ell^k$  ,

$$\frac{f^{(k)}(a_h)}{k!} = \sum_{i'=1}^{C_\ell^k} P_{i',k}(a_h) \in \mathfrak{P}^{T_h - hk} \cap \mathbb{Z} = \mathfrak{p}^{T_h - hk} \mathbb{Z}$$

ce qui établit (i) pour  $1 \leq k \leq e$  .

Démontrons (ii) .

Remarquons que , puisque :  $ht_h \leq T_h$  ( p. 26 ) ,

$$T_h - ht_h + 1 \geq 1 .$$

$$\text{Nous avons } \frac{f^{(t_h)}(X)}{t!} = \sum_{i'=1}^{C_\ell^{t_h}} P_{i',t_h}(X) .$$

Pour chaque  $i'$  ,  $P_{i',t_h}(X)$  est le produit des éléments d'une combinaison  $\ell - t_h$  à  $\ell - t_h$  des  $\ell$  facteurs  $X - \theta_u$  .

Or  $\text{card. } \delta_h = t_h$  , donc , il existe un entier unique  $i'_1$  ,  $1 \leq i'_1 \leq C_\ell^{t_h}$  tel que , pour tout  $i \in \delta_h$  ,  $X - \theta_i$  ne divise pas  $P_{i'_1,t_h}(X)$  .

- Nous démontrons d'abord que  $P_{i'_1,t_h}(a_h) \notin \mathfrak{P}^{T_h - hk + 1}$  .

Pour cela , nous distinguons encore les deux cas :

$\alpha$ )  $h = 1$  ou  $h \geq 2$  et pour tout  $j$  ,  $1 \leq j \leq h-1$  ,  $\delta_j^! = \emptyset$  .

Alors  $\delta_h = \delta_1$  ,  $T_h = ht_h$  et  $P_{i'_1,t_h}(a_h) = \prod_{i \in \delta_1} (a_h - \theta_i)$  ( ce produit comprenant  $\ell - t_1$  termes ) . Comme , par définition de  $\delta_1$  , pour tout

$i \in \delta_1$  ,  $a_h - \theta_i \notin \mathfrak{P}$  , d'où  $P_{i'_1,t_h}(a_h) \notin \mathfrak{P}$  . C'est le résultat annoncé ,

car dans ce cas :  $1 = T_h - ht_h + 1$  .

$\beta$ )  $h \geq 2$  et il existe  $j$  ,  $1 \leq j \leq h-1$  , tel que  $\delta_j^! \neq \emptyset$  .

Il en résulte en particulier  $t_h < t_1$  et  $\delta_1 - \delta_h \neq \emptyset$  .

D'après la définition de  $i'_1$  ,  $P_{i'_1,t_h}(X)$  ne contient aucun facteur  $X - \theta_i$  , pour  $i \in \delta_h$  et contient tous les facteurs  $X - \theta_i$  pour



$i \in \delta_1 - \delta_h$ . Comme  $\delta_1 - \delta_h = \bigcup_{j \in \mathbb{H} \setminus \{h\}} \delta_j'$ , nous décomposons  $P_{i_1', t_h}(a_h)$

$$\text{sous la forme : } P_{i_1', t_h}(a_h) = \underbrace{\prod_{j \in \mathbb{H} \setminus \{h\}} \left( \prod_{i \in \delta_j'} (a_h - \theta_i) \right)}_{t_1 - t_h \text{ facteurs}} \times \underbrace{\prod_{i \notin \delta_1} (a_h - \theta_i)}_{\ell - t_1 \text{ facteurs}}.$$

Considérons l'idéal  $(P_{i_1', t_h}(a_h)) E_K$  engendré par  $P_{i_1', t_h}(a_h)$  dans  $K$ :

$$(P_{i_1', t_h}(a_h)) E_K = \prod_{j \in \mathbb{H} \setminus \{h\}} \left( \prod_{i \in \delta_j'} (a_h - \theta_i) E_K \right) \times \prod_{i \notin \delta_1} (a_h - \theta_i) E_K.$$

Pour tout  $i \notin \delta_1$ , l'idéal  $(a_h - \theta_i) E_K$  est premier avec  $\mathfrak{P}$ .

Pour tout  $j \in \mathbb{H} \setminus \{h\}$ , et pour tout  $i \in \delta_j'$ ,  $a_h - \theta_i \in \mathfrak{P}^j$  et  $a_h - \theta_i \notin \mathfrak{P}^{j+1}$ .

De plus, les ensembles  $\delta_j'$  étant deux à deux disjoints, l'idéal  $(a_h - \theta_i) E_K$  ne dépend pas de  $j$ ; on peut donc poser  $(a_h - \theta_i) E_K = \mathfrak{P}^j \times \mathfrak{A}_i$ , avec  $(\mathfrak{A}_i, \mathfrak{P}) = E_K$ , ( $(\mathfrak{A}_i, \mathfrak{P})$  désignant le p.g.c.d. des idéaux  $\mathfrak{A}_i$  et  $\mathfrak{P}$ ).

Nous avons alors :

$$\prod_{i \in \delta_j'} (a_h - \theta_i) E_K = \mathfrak{P}^{j t_j'} \times \prod_{i \in \delta_j'} \mathfrak{A}_i \quad \text{et}$$

$$\prod_{j \in \mathbb{H} \setminus \{h\}} \left( \prod_{i \in \delta_j'} (a_h - \theta_i) E_K \right) = \mathfrak{P}^{\left( \sum_{j \in \mathbb{H} \setminus \{h\}} j t_j' \right)} \times \mathfrak{A} \quad \text{en posant :}$$

$$\mathfrak{A} = \prod_{j \in \mathbb{H} \setminus \{h\}} \left( \prod_{i \in \delta_j'} \mathfrak{A}_i \right). \quad \text{Compte-tenu de } \delta_j' = \emptyset \Leftrightarrow t_j - t_{j+1} = 0,$$

$$\sum_{j \in \mathbb{H} \setminus \{h\}} j t_j' = \sum_{j=1}^{h-1} j t_j' = T_h - h t_h \quad (\text{p. 28}).$$

D'où :

$$(P_{i_1', t_h}(a_h)) E_K = \mathfrak{P}^{T_h - h t_h} \times \mathfrak{B}, \quad \text{avec } \mathfrak{B} = \mathfrak{A} \times \prod_{i \notin \delta_1} (a_h - \theta_i) E_K.$$

On a  $(\mathfrak{B}, \mathfrak{P}) = E_K$ , car  $\mathfrak{B}$  est un produit d'idéaux tous premiers avec  $\mathfrak{P}$ , d'où le résultat.

- Nous démontrons maintenant que, pour tout  $i'$ ,  $1 \leq i' \neq i_1' \leq C_\ell^{t_h}$ ,

$$P_{i_1', t_h}(a_h) \in \mathfrak{P}^{T_h - h k + 1}.$$

Ce résultat se démontre de la même façon que (i) pour  $1 \leq k \leq e$ . Avec les mêmes notations, si  $1 \leq i' \neq i'_1 \leq C_\ell^{t_h}$ ,  $P_{i', t_h}(X)$  contient au moins un facteur  $X - \theta_i$  pour  $i \in \mathcal{G}_h$ , alors le nombre des  $i \in \mathcal{G}_h$  tels que  $X - \theta_i$  divise  $P_{i', t_h}(X)$  est  $t_h - s_{h, i'} \geq 1$ .

$\alpha)$  Si  $h = 1$  ou  $h \geq 2$  et pour tout  $j$ ,  $1 \leq j \leq h-1$ ,  $\mathcal{G}_j^! = \emptyset$ , on montre que  $P_{i', t_h}(a_h) \in \mathfrak{P}^{h(t_h - s_{h, i'})} \subseteq \mathfrak{P} = \mathfrak{P}^{T_h - ht_h + 1}$ , car  $h(t_h - s_{h, i'}) \geq h \geq 1$  et  $T_h - ht_h + 1 = 1$ .

$\beta)$  Si  $h \geq 2$  et s'il existe  $j$ ,  $1 \leq j \leq h-1$ , tel que  $\mathcal{G}_j^! \neq \emptyset$ , on montre que :

- $0 \leq \sum_{j=1}^{j=h} s_{j, i'} \leq t_h$
- $P_{i', t_h}(a_h) \in \mathfrak{P}^{w_i}$ , avec  $w_i = \sum_{j=1}^{j=h} j t_j^! - \sum_{j=1}^{j=h} j s_{j, i'}$ .

Minorons  $w_i = T_h - \sum_{j=1}^{j=h} j s_{j, i'} = \sum_{j=1}^{h-1} t_j - \sum_{j=1}^{h-1} j s_{j, i'} + t_h - s_{h, i'} - (h-1) s_{h, i'}$

$$= \sum_{j=1}^{h-1} t_j + (t_h - s_{h, i'}) - \left[ \sum_{j=1}^{h-1} j s_{j, i'} + (h-1) s_{h, i'} \right].$$

Or :  $\sum_{j=1}^{h-1} j s_{j, i'} + (h-1) s_{h, i'} \leq (h-1) \left[ \sum_{j=1}^{h-1} s_{j, i'} + s_{h, i'} \right]$

$$= (h-1) \sum_{j=1}^h s_{j, i'}.$$

Par suite, compte-tenu de  $\sum_{j=1}^h s_{j, i'} \leq t_h$  et  $t_h - s_{h, i'} \geq 1$ , on a :

$$w_i \geq \sum_{j=1}^{h-1} t_{j+1} - (h-1) t_h = T_h - ht_h + 1.$$

Nous avons donc :

$$P_{i', t_h}(a_h) \in \mathfrak{P}^{T_h - ht_h + 1} \quad 1 \leq i' \neq i'_1 \leq C_\ell^{t_h}$$

$$P_{i'_1, t_h}(a_h) \notin \mathfrak{P}^{T_h - ht_h + 1}.$$

Il en résulte 
$$\frac{f^{(t_h)}(a_h)}{t_h!} = \sum_{i'=1}^{t_h} C_{i'}^{t_h} P_{i', t_h}(a_h) \notin \mathfrak{P}^{T_h - h t_h + 1} \cap \mathbb{Z},$$

ce qui établit (ii) .

Dans le cas particulier , où  $h = 1$  ,  $t_1 = t$  ,  $a_1 = a$  , compte-tenu de la proposition II.6 , nous obtenons le :

Corollaire II.1 :

Soit  $p$  un diviseur premier de  $I(\theta)$  . On suppose que  $a \in \mathbb{Z}$  est racine multiple d'ordre  $t$  ( $t > 1$ ) de la congruence fondamentale  $f(x) \equiv 0 \pmod{p}$  , alors :

- (i)  $\frac{f^{(k)}(a)}{k!} \equiv 0 \pmod{p^{t-k}}$  si  $0 \leq k \leq t-1$  ;
- (ii)  $\frac{f^{(t)}(a)}{t!} \not\equiv 0 \pmod{p}$  .

Application de la proposition II.7 à la transformation du polynome  $f$  .

Corollaire II.2 :

Soient :  $p$  un diviseur premier de  $I(\theta)$  ,  $a$  une racine multiple d'ordre  $t_1$  ( $t_1 > 1$ ) de la congruence  $f(x) \equiv 0 \pmod{p}$  ,  $h \in \mathbb{N}^*$  et  $a_h \equiv a \pmod{p}$  une racine d'ordre  $t_h$  ( $t_h > 1$ ) de l'idéal  $\mathfrak{P}^h$  .

Alors :  $f(x) = A_h p^{T_h} f_h(x_h)$  (II-1)

où  $A_h$  est un entier rationnel premier à  $p$  et  $x_h = \frac{x - a_h}{p^h}$  .

Démonstration :

$a_h \left( \equiv a \pmod{p} \right)$  étant une racine d'ordre  $t_h$  ( $t_h > 1$ ) de l'idéal  $\mathfrak{P}^h$  , posons :  $x = a_h + p^h x_h$  . Par la formule de Taylor, nous

avons : 
$$f(x) = \sum_{k=0}^{k=t_h} p^{hk} \frac{f^{(k)}(a_h)}{k!} x_h^k = \sum_{k=0}^{k=t_h} b_k x_h^k .$$

$$\text{Pour tout } k, 0 \leq k \leq \ell, b_k = p^{hk} \frac{f^{(k)}(a_h)}{k!} \equiv 0 \pmod{p^{T_h}},$$

car : - si  $0 \leq k \leq e$ , cela résulte du (i) de la proposition II.7

- si  $e+1 \leq k \leq \ell$ , comme  $k \geq \left[ \frac{1}{h}(T_h - 1) \right] + 1 > \frac{1}{h}(T_h - 1)$ ,

on a  $hk > T_h - 1$ , et les deux membres étant entiers :  $hk \geq T_h$  ;

la congruence  $b_k \equiv 0 \pmod{p^{T_h}}$  en résulte immédiatement.

De plus, d'après (ii) de la proposition II.7,  $b_{t_h} \not\equiv 0 \pmod{p^{T_h+1}}$ . Par suite, le p.g.c.d. des coefficients  $b_k, 0 \leq k \leq \ell$ , est de la forme  $A_h p^{T_h}$ , où  $A_h$  est un entier rationnel premier avec  $p$ .

On peut donc écrire :  $f(x) = A_h p^{T_h} f_h(x_h)$  (II-1)

où  $f_h$  est un polynome primitif de  $\mathbb{Z}[X]$  de degré  $\ell$ .

Remarque :

Si  $k \geq t_1 + 1$ ,  $hk \geq ht_1 + h \geq ht_1 + 1 \geq T_h + 1$  (p. 26), alors  $b_k \equiv 0 \pmod{p^{T_h+1}}$  et le coefficient de  $x_h^k$  dans le polynome  $f_h$  est divisible par  $p$ . Par contre, le coefficient de  $x_h^{t_h}$  n'est pas divisible par  $p$ . On a alors  $f_h(x_h) \equiv \varphi_h(x_h) \pmod{p}$ ,  $\varphi_h$  étant un polynome de  $\mathbb{Z}[X]$ , de degré  $\nu$ , et on a :  $t_h \leq \nu \leq t_1$ .

Le polynome  $f_h$  va nous permettre de construire les suites d'approximations des racines de  $f$  dans  $\mathbb{Q}_p$  ayant pour premier terme une racine multiple de la congruence fondamentale modulo  $p$ .

Relation entre les racines de la congruence  $f_h(x_h) \equiv 0 \pmod{p^{h'}}$  ( $h' \geq 1$ ) et les racines des idéaux  $\mathfrak{P}^{h+h'}$ .

Théorème II.1 :

Soient :  $p$  un diviseur premier de  $I(\theta)$ ,  $\mathfrak{P}$  l'un quelconque des idéaux premiers divisant  $pE_K$ ,  $a$  une racine multiple d'ordre  $t_1$  de la congruence  $f(x) \equiv 0 \pmod{p}$ ,  $h \in \mathbb{N}^*$  et  $a_h \equiv a \pmod{p}$  une racine

d'ordre  $t_h$  de l'idéal  $\mathfrak{p}^h$  ( $t_h > 1$ ).

Soit alors  $f_h$  le polynome défini par la formule (II-1).

Dans ces conditions :  $a_{h+1} \equiv a_h \pmod{p^h}$  est racine d'ordre  $t_{h+1}$

( $1 \leq t_{h+1} \leq t_h$ ) de l'idéal  $\mathfrak{p}^{h+1}$  si et seulement si  $\alpha_{h,1} = \frac{a_{h+1} - a_h}{p^h}$  est

racine d'ordre  $t_{h+1}$  de la congruence  $f_h(x_h) \equiv 0 \pmod{p}$ .

Démonstration :

La condition nécessaire se démontre très facilement.

De la formule (II-1), on déduit, par récurrence, en dérivant par rapport à  $x_h$  :

$$\text{pour tout } k, 1 \leq k \leq \ell, f_h^{(k)}(x) = A_h p^{(T_h - hk)} f_h^{(k)}(x_h) \quad (\text{II-2})$$

Puisque  $a_{h+1} \equiv a_h \pmod{p^h}$ , on pose  $a_{h+1} = a_h + p^h \alpha_{h,1}$ .

Comme  $(A_h, p) = 1$ , il résulte des formules (II-1), (II-2) et de la proposition II.7 appliquée à la racine  $a_{h+1}$ , d'ordre  $t_{h+1}$ , de l'idéal  $\mathfrak{p}^{h+1}$  :

$$\frac{f_h^{(k)}(\alpha_{h,1})}{k!} \equiv 0 \pmod{p^{t_{h+1}-k}} \text{ si } 0 \leq k \leq t_{h+1}-1; \frac{f_h^{(t_{h+1})}(\alpha_{h,1})}{t_{h+1}!} \not\equiv 0 \pmod{p}$$

ce qui montre, compte-tenu de la proposition II.4, que  $\alpha_{h,1}$  est racine d'ordre  $t_{h+1}$  de la congruence  $f_h(x_h) \equiv 0 \pmod{p}$ .

Condition suffisante.

Soient  $a_h \equiv a \pmod{p}$  une racine d'ordre  $t_h$  ( $t_h > 1$ ) de l'idéal  $\mathfrak{p}^h$  ( $h \geq 1$ ) et  $f_h$  le polynome obtenu par le changement de variable  $x = a_h + p^h x_h$ , on suppose que  $\alpha_{h,1}$  est une racine, d'ordre  $t_{h+1} \geq 1$ , de la congruence  $f_h(x_h) \equiv 0 \pmod{p}$ .

On pose  $a_{h+1} = a_h + p^h \alpha_{h,1}$ , alors d'après (II-1) :

$$f(a_{h+1}) \equiv 0 \pmod{p^{T_{h+1}}} \quad \text{et} \quad (f(a_{h+1}))E_K = \mathbb{P}^{T_{h+1}} \times \mathcal{Q}.$$

Cherchons une autre expression de l'idéal  $(f(a_{h+1}))E_K$ .

Comme  $a_{h+1} \equiv a_h \pmod{p^h}$ ,  $a_{h+1}$  est racine d'ordre  $t_j$  des idéaux  $\mathbb{P}^j$ ,  $1 \leq j \leq h$ , avec :  $1 < t_h \leq \dots \leq t_j \leq \dots \leq t_1$ .

Nous reprenons les notations de la démonstration de la proposition II.7 :

- Pour tout  $j$ ,  $1 \leq j \leq h$ ,  
 $\mathcal{G}_j = \{u, 1 \leq u \leq \ell, \text{ tel que } \theta_u \equiv a_{h+1} \pmod{\mathbb{P}^j}\}$
- $\mathcal{G}'_h = \mathcal{G}_h$ , et pour tout  $j$ ,  $1 \leq j \leq h-1$ ,  $\mathcal{G}'_j = \mathcal{G}_j - \mathcal{G}_{j+1}$
- $\mathcal{H} = \{j, 1 \leq j \leq h, \text{ tel que } \mathcal{G}'_j \neq \emptyset\}$ .

Décomposons l'idéal  $(f(a_{h+1}))E_K = \prod_{i=1}^{i=\ell} (a_h - \theta_i)E_K$  sous la forme :

$$(f(a_{h+1}))E_K = \prod_{i \in \mathcal{G}_1} (a_h - \theta_i)E_K \times \prod_{i \notin \mathcal{G}_1} (a_{h+1} - \theta_i)E_K.$$

Nous avons :

$$\prod_{i \in \mathcal{G}_1} (a_{h+1} - \theta_i)E_K = \begin{cases} \prod_{i \in \mathcal{G}_h} (a_{h+1} - \theta_i)E_K, & \text{si } h = 1 \text{ ou } h \geq 2 \\ & \text{et } \mathcal{G}'_j = \emptyset \text{ pour tout } j, 1 \leq j \leq h-1 \\ \prod_{j \in \mathcal{H}} \left( \prod_{i \in \mathcal{G}'_j} (a_{h+1} - \theta_i)E_K \right), & \text{si } h \geq 2 \text{ et il} \\ & \text{existe } j, 1 \leq j \leq h-1, \text{ tel que } \mathcal{G}'_j \neq \emptyset. \end{cases}$$

Si  $i \in \mathcal{G}_h$ ,  $a_{h+1} \equiv \theta_i \pmod{\mathbb{P}^h}$ , d'où  $(a_{h+1} - \theta_i)E_K = \mathbb{P}^h \times \mathcal{U}_{i,h}$ , et comme  $\text{card. } \mathcal{G}_h = t_h$ ,  $\prod_{i \in \mathcal{G}_h} (a_{h+1} - \theta_i)E_K = \mathbb{P}^{h t_h} \times \mathcal{U}_h$ ,

avec  $\mathcal{U}_h = \prod_{i \in \mathcal{G}_h} \mathcal{U}_{i,h}$ .

Si  $j \in \mathcal{H} \setminus \{h\}$ , et  $i \in \mathcal{G}'_j$ ,  $a_{h+1} \equiv \theta_i \pmod{\mathbb{P}^j}$  et  $a_{h+1} \not\equiv \theta_i \pmod{\mathbb{P}^{j+1}}$ , d'où :  $(a_{h+1} - \theta_i)E_K = \mathbb{P}^j \mathcal{U}_{i,j}$  avec  $(\mathcal{U}_{i,j}, \mathbb{P}) = E_K$ , et comme  $\text{card. } \mathcal{G}'_j = t'_j > 0$ ,  $\prod_{i \in \mathcal{G}'_j} (a_{h+1} - \theta_i)E_K = \mathbb{P}^{j t'_j} \mathcal{U}_j$ ,

en posant  $\mathcal{U}_j = \prod_{i \in \mathcal{G}'_j} \mathcal{U}_{i,j}$ , et on a  $(\mathcal{U}_j, \mathbb{P}) = E_K$ .

