THEORIE DES NOMBRES

BESANCON

Année 1978 - 1979

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

Colette PARIS

Bases sur $\mathbb{Z}$ des idéaux primaires canoniques d'un corps K, extension de $\mathbb{Q}$, cyclique, de degré premier impair ℓ 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 ℓ ($\ell \geq 5$) 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 ℓ. Notons D_K son discriminant. Si θ est un entier de trace 0 ou 1, suivant que ℓ divise ou ne divise pas D_K, on note f le polynome minimal de θ 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.
- $pE_K = \mathfrak{P}_1 \times \mathfrak{P}_2 \times \ldots \times \mathfrak{P}_\ell \Leftrightarrow f$ 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 polynome fondamental f de K .

Désignons par $D(\theta)$ *le discriminant du polynome* 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 , ℓ 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 ℓ 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 pE_K se factorise dans K.

I.1.- Notations et rappels .

1) Notations .

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

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

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

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

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

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

E_K : anneau des entiers de K .

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

2) Rappels ([16]).

- Résolvante de Lagrange d'un élément θ_u .

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

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

$$\chi_o(\sigma^h) = 1 \ , \ \chi_k(\sigma^h) = \varepsilon^{hk} \ , \ 1 \leq k \leq \ell-1 \ , \ h \in \mathbb{Z} \ , \ h \bmod. \ \ell \ .$$

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

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

- <u>Choix d'un polynome fondamental et d'une base de</u> E_K .

Les corps cycliques K , de degré premier impair ℓ , 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 θ de K .

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

$$\mathfrak{M} = (\langle \theta, \chi_k \rangle^{\ell}) \ , \ 1 \leq k \leq \ell-1 \ \Leftrightarrow \ \mathfrak{M} = \mathfrak{N}^{\ell} \prod_{j=1}^{j=\ell-1} \mathfrak{U}_j^{j^*}$$

où : j^* est un entier déterminé par : $1 \leq j^* \leq \ell-1$ et $jj^* \equiv 1 \ (\bmod. \ \ell)$,

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

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

En désignant par λ une base de l'idéal principal $\mathfrak{N}$, par μ une base de l'idéal $\prod_{j=1}^{\ell-1} \mathfrak{U}_j^{j^*}$, nous avons : $\mathfrak{M} = (\lambda^{\ell} \mu)$.

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

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

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

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

- Calcul de D_K .

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

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

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

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

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

où D_ℓ est le déterminant de Vandermonde d'ordre ℓ :

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

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 θ " .

Nous avons donc : $|D(\theta)| = I^2(\theta) \times D_K$ (I-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 :

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

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 θ_u^j dans la base $\{ 1, \theta_u, \ldots, \theta_{u+\ell-2} \}$ et on considère les $\ell-2$ égalités obtenues comme un système de $\ell-2$ équations à $\ell-2$ inconnues : θ_{u+1}, θ_{u+2}, ..., $\theta_{u+\ell-2}$. Ce système est un système de Cramer , car son déterminant Δ 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 θ_u , à coefficients entiers rationnels , de degré inférieur ou égal à $\ell-1$. Les formules (I-3) pour $h = 1, \ldots, \ell-2$ 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 : $\theta_{u+\ell-1} = s - \theta_u - \sum_{h=1}^{\ell-2} \theta_{u+h}$.

I.2.- Idéaux primaires canoniques de K .

Soit $\mathfrak{J}$ un idéal de K . On notera $\mathfrak{J}_u$, u mod. ℓ , 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 ℓ ; 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 $f(x) \equiv \prod_{u \bmod. \ell} (x-c_u) \pmod{p}$ 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 I.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 divise D_K .

Proposition I.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) $f(c_j) \equiv 0 \pmod{q}$, $1 \le j \le \ell$, et $\sum_{j=1}^{j=\ell} c_j \equiv s \pmod{q}$

(ii) $\{ q, \theta_i - c_i, 1 \le i \le \ell-1 \}$ 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 $\{ q, \theta_i - c_i, 1 \le i \le \ell-1 \}$ sera noté $\mathfrak{J} = (q, \theta_i - c_i, 1 \le i \le \ell-1)$.

3°) On obtient encore une base sur $\mathbb{Z}$ de $\mathfrak{J}$, en remplaçant dans la base précédente l'un quelconque des $\theta_i - c_i$, $1 \le i \le \ell-1$, par $\theta_\ell - c_\ell$.

4°) $\theta_i \equiv c_i \pmod{\mathfrak{J}} \Rightarrow \sigma^h(\theta_i) = \theta_{i+h} \equiv c_i \pmod{\sigma^h(\mathfrak{J}) = \mathfrak{J}_h}$.
$(i+h \bmod \ell)$

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

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, $1 \le j \le \ell$, 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 $\{ p^k, \theta_i - a_{i,k}, 1 \le i \le \ell-1 \}$ 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 , $1 \leq i \leq \ell$, θ_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 mod. ℓ) , 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 $\lambda \equiv x$ (mod. $\mathfrak{P}^2$) . Or $p \in \mathfrak{P}^2$, on aurait alors : $\lambda \equiv r$ (mod. $\mathfrak{P}^2$) avec $0 \leq r < p$, d'où card. $E_K/\mathfrak{P}^2 = p$, ce qui est impossible , car card. $E_K/\mathfrak{P}^2 = N(\mathfrak{P}^2) = p^2$.

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

On déduit de cette proposition le :

Théorème I.1 :

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

I.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 ℓ 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 : $\theta_i \equiv a_{i,k}$ (mod. $\mathfrak{P}^k$) , $1 \leq i \leq \ell$, et $\mathfrak{P}^k = (p^k , \theta_i - a_{i,k} , 1 \leq i \leq \ell-1)$ avec $a_{i,k} \in \mathbb{Z}$, $f(a_{i,k}) \equiv 0$ (mod. p^k) et $\sum_{i=1}^{i=\ell} a_{i,k} \equiv s$ (mod. p^k) , (corollaire I.1) . D'autre part , entre les θ_u , nous avons les relations :

(I-3) $\qquad d_h \theta_{u+h} = g_h(\theta_u)$, $1 \leq h \leq \ell-1$, $1 \leq u \leq \ell$, u+h mod. ℓ ,

où d_h divise $I(\theta)$. 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 I.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 ℓ 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 :

$$d_h a_{h+1,k} \equiv g_h(a_{1,k}) \pmod{p^k} \text{ , } \sum_{h=1}^{h=\ell} a_{h,k} \equiv s \pmod{p^k} .$$
$$1 \leq h \leq \ell-2$$

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 ℓ 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 Θ_i , $1 \leq i \leq \ell$, les racines dans $\mathbb{Q}_p$ du polynome f et on les associe aux racines réelles de f de la façon suivante :

on choisit arbitrairement Θ_1 associée à θ_1 , alors les racines Θ_{h+1} associées à θ_{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 Θ_i , et le nombre rationnel $a_{i,k}$ sera appelé " approximation p-adique modulo p^k de Θ_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 $\lambda - \mu = p^n \eta$, η 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 I.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 ℓ racines dans $\mathbb{Z}_p$ et la distance p-adique de deux quelconques des racines est 1 .

Théorème I.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 ℓ idéaux primaires canoniques conjugués :

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

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

$i+h \bmod. \ell$ $\qquad$ $i+\ell-h \bmod. \ell$

$\{ p^k , \theta_{i+h} - a_{i,k} , 1 \leq i \leq \ell-1 \}$ 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 Θ_1 , $a_{i,k}$, $2 \leq i \leq \ell$, est l'approximation p-adique modulo p^k de Θ_i .

Remarque :

La construction des $\mathbb{Z}$-bases des idéaux primaires canoniques de K , qui résulte de la proposition I.4 et du théorème I.3 , est théorique . Cette construction ne devient effective que lorsqu'on connait explicitement un polynome fondamental de K et lorsqu'on sait écrire les polynomes 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 :

$I(\theta)$ et $\sqrt{D_K}$ sont premiers entre eux .

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 $\mathfrak{Q}$ l'idéal premier , de degré un, tel que $\ell E_K = \mathfrak{Q}^\ell$. Alors $\mathfrak{Q}^2 = (\ell, \ell\theta_1, \theta_i - \theta_1, 2 \le i \le \ell-1)$.

Démonstration :

K étant non unitaire , $s = 0$ et $\sqrt{D_K} = \left(\ell^2 m\right)^{\frac{\ell-1}{2}}$, 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 , $j \neq i$, $\theta_j - \theta_i \in \mathfrak{Q}$;

posons alors pour tout couple (i,j) , $1 \le i < j \le \ell$, $(\theta_j - \theta_i)E_K = \mathfrak{Q} \times \mathfrak{I}_{j,i}$.

Le produit $\prod_{1 \le i < j \le \ell} (\theta_j - \theta_i)$ comportant $\frac{\ell(\ell-1)}{2}$ facteurs $\theta_j - \theta_i$,

nous aurons :

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

il en résulte : $\prod_{1 \le i < j \le \ell} \mathfrak{I}_{j,i} \equiv 0 \pmod{\mathfrak{Q}^{\frac{\ell(\ell-1)}{2}}}$.

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

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

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

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

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

Démontrons que $\mathfrak{P}^2 \subseteq \mathfrak{J}$.

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 $\alpha \in \mathfrak{P}^2$, dans la base précédente , $\alpha = x_o + x_1(\theta_1 - c) + \sum_{i=2}^{\ell-1} x_i(\theta_i - \theta_1)$, $x_i \in \mathbb{Z}$, $0 \leq i \leq \ell-1$.

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

D'autre part , α, ℓ , $\theta_i - \theta_1$, $2 \leq i \leq \ell-1$, étant dans $\mathfrak{P}^2$, $x_1(\theta_1 - c)$ est dans $\mathfrak{P}^2$. Nous avons donc : $\ell(\theta_1 - c) \in \mathfrak{P}^2$, $x_1(\theta_1 - c) \in \mathfrak{P}^2$, $\theta_1 - c \notin \mathfrak{P}^2$ (proposition I.3) . Il en résulte : $x_1 \equiv 0 \pmod{\ell}$.

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

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

De plus , d'après la démonstration précédente , tout élément de $\mathfrak{P}^2$ 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 : ℓ , $\ell(\theta_1 - c)$, $\theta_i - \theta_1$, $2 \leq i \leq \ell-1$. Il en résulte que ces éléments forment une $\mathbb{Z}$-base de $\mathfrak{A}^2$, ce qui démontre que :

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

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 $\sqrt{D_K} = \left[\ell^{2(1-s)} p_1 \times p_2 \times \ldots \times p_n \right]^{\frac{\ell-1}{2}}$ 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 I.2 , et en posant , pour tout couple (i,j) $1 \leq i < j \leq \ell$, $(\theta_j - \theta_i)E_K = \mathfrak{P} \times \mathfrak{I}_{j,i}$, nous avons :

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

d'où $\prod_{1 \leq i < j \leq \ell} \mathfrak{I}_{j,i} \equiv 0 \pmod{\mathfrak{P}^\ell}$. Par le raisonnement utilisé dans la démonstration du lemme II.1, on en déduit : $\theta_1 \equiv \ldots \equiv \theta_i \equiv \ldots \equiv \theta_\ell \pmod{\mathfrak{P}^2}$.

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 ℓ 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 I.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 $\mathfrak{A}$ l'idéal premier tel que $\ell E_K = \mathfrak{A}^\ell$, alors $\ell^\ell E_K = \mathfrak{A}^{\ell^2}$. Compte-tenu du lemme II.1 , et en posant , pour tout couple (i,j) , $1 \leq i < j \leq \ell$,

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

$$\prod_{1 \le i < j \le \ell} (\theta_j - \theta_i)E_K = \mathfrak{P}^{\ell(\ell-1)} \prod_{1 \le i < j \le \ell} \mathfrak{I}_{j,i} \equiv 0 \left(\text{mod. } \mathfrak{P}^{\ell^2}\right),$$

d'où $\prod_{1 \le i < j \le \ell} \mathfrak{I}_{j,i} \equiv 0 \ (\text{mod. } \mathfrak{P}^{\ell})$. On en déduit encore :

$\theta_1 \equiv \ldots \equiv \theta_i \equiv \ldots \equiv \theta_\ell \ (\text{mod. } \mathfrak{P}^2)$. On aurait : $\ell \in \mathfrak{P}^3$, d'où $\ell\theta_1 \in \mathfrak{P}^3$, et $\theta_i - \theta_1 \in \mathfrak{P}^3$, $2 \le i \le \ell-1$, ce qui montre que $\mathfrak{P}^2 \subseteq \mathfrak{P}^3$, d'où $\mathfrak{P}^2 = \mathfrak{P}^3$, ce qui est impossible .

Proposition II.2 :

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

Démonstration :

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

Raisonnons par l'absurde : si l'idéal pE_K est inerte , il existe i et j tels que $\theta_j - \theta_i \equiv 0 \ (\text{mod. } pE_K)$ et comme pE_K est invariant par les éléments de G , on en déduit encore : $\theta_1 \equiv \ldots \equiv \theta_i \equiv \ldots \equiv \theta_\ell \ (\text{mod. } pE_K)$ et $s = \sum_{j=1}^{\ell} \theta_j \equiv \ell\theta_u \ (\text{mod. } pE_K)$, $1 \le u \le \ell$. Si K est unitaire , $s = 1$, donc $\ell\theta_u \equiv s \ (\text{mod. } pE_K) \Rightarrow p \neq \ell$. Si K est non unitaire , $s = 0$ et ℓ divise D_K , mais comme $I(\theta)$ est premier à $\sqrt{D_K}$, ℓ ne divise pas $I(\theta)$, on a donc encore $p \neq \ell$.

Soit alors λ un entier quelconque de K .

Dans la base $\{ 1, \theta_i , 1 \le i \le \ell-1 \}$ de E_K , $\lambda = x_o + \sum_{i=1}^{\ell-1} x_i \theta_i$, $x_i \in \mathbb{Z}$, $0 \le i \le \ell-1$, d'où : $\ell\lambda = \ell x_o + \sum_{i=1}^{\ell-1} x_i(\ell\theta_i) \equiv \ell x_o + s \sum_{i=1}^{\ell-1} x_i \ (\text{mod. } pE_K)$.

Puisque p est premier à ℓ , il existe $r \in \mathbb{Z}$ tel que $\lambda \equiv r \ (\text{mod. } pE_K)$, 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 ℓ 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 $\mathfrak{P}^k \cap \mathbb{Z} = p^k \mathbb{Z}$.

2°) f se factorise dans $\mathbb{Z}/p\mathbb{Z}$ et dans $\mathbb{Q}_p$ (§ I.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 , Θ_u , $1 \leq u \leq \ell$, étant les racines p-adiques de f , associées aux racines réelles θ_u de f et d étant la distance p-adique définie au paragraphe I.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 Θ_j et Θ_i associées à θ_j et θ_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 ν, c'est-à-dire :

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

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 $g(x) \equiv 0$ (mod. p) si et seulement si :

(1) $\dfrac{g^{(k)}(a)}{k!} \equiv 0$ (mod. p) , $0 \leq k \leq t-1$;

(2) $\dfrac{g^{(t)}(a)}{t!} \not\equiv 0$ (mod. 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: $g(x) \equiv (x-a)^t \varphi(x)$ (mod. p) , $\varphi \in \mathbb{Z}[X]$, $\varphi(a) \not\equiv 0$ (mod. p) et en sachant que , puisque $\varphi \in \mathbb{Z}[X]$, il en est de même de $\dfrac{\varphi(q)}{q!}$, 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 $g(x) \equiv 0$ (mod. 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 $D_K \equiv 0$ (mod. p) , la congruence fondamentale mod. p admet une racine d'ordre ℓ . 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 pE_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 :

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

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 θ) 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 ≥ 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 : $1 \leq t_k \leq \ldots \leq t_j \leq \ldots \leq t_1$.

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 $I(\theta)$.

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 ℓ 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 $u \notin \mathcal{S}_1$, en posant $\mathcal{S}_1 = \{i_h\}_{1 \leq h \leq t}$. Avec les notations de la proposition I.1 , nous avons : $c_j \equiv a \pmod{p}$ si $j \in \mathcal{S}_1$ et $c_j \not\equiv a \pmod{p}$ si $j \notin \mathcal{S}_1$. Il en résulte :

$f(x) \equiv (x - a)^t g(x) \pmod{p}$ avec $g(x) = \prod_{j \notin \mathcal{S}_1} (x - c_j)$.

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 divise 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 ε , dont le polynome 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 $1 \leq t_h \leq \ldots \leq t_j \leq \ldots \leq t_1$. 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) $\dfrac{f^{(k)}(a_h)}{k!} \equiv 0 \left(\text{mod. } p^{T_h - hk}\right)$ si $0 \le k \le e$

(ii) $\dfrac{f^{(t_h)}(a_h)}{t_h!} \not\equiv 0 \left(\text{mod. } p^{T_h - h t_h + 1}\right)$.

Remarques :

1°) $t_h - 1 \le e \le t_1 - 1$.

En effet, soit $e = \left[\frac{1}{h}(T_h - 1)\right]$ ($[x]$ désignant la partie entière de x). Comme $1 \le t_h \le \ldots \le t_j \le \ldots \le t_1$, $T_h = \sum_{j=1}^{j=h} t_j \le h t_1$, d'où

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

De même : $h t_h \le T_h$, donc $h t_h - h \le T_h - h \le T_h - 1$, d'où $t_h - 1 \le \frac{1}{h}(T_h - 1)$ et $t_h - 1 \le e$.

2°) Si $h t_h < T_h$, alors $h t_h \le T_h - 1$, d'où $t_h \le \frac{1}{h}(T_h - 1)$ et $t_h \le e$; 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 ℓ ; pour tout entier k , $1 \le k \le \ell$, $\dfrac{f^{(k)}}{k!}$ 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 $C_\ell^k \left(= C_\ell^{\ell-k}\right)$ est le coefficient du binôme et chaque polynome $P_{i',k}$, $1 \le i' \le C_\ell^k$, est le produit des éléments d'une combinaison $\ell - k$ à $\ell - k$ des ℓ facteurs $X - \theta_u$, $1 \le u \le \ell$.

Ce résultat se démontre élémentairement, par récurrence,

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

$P_{i',k}$, $1 \le i' \le C_\ell^k$, désignent les polynomes obtenus de la façon suivante: à partir des ℓ facteurs $X - \theta_u$, $1 \le u \le \ell$, du polynome f , on forme toutes les combinaisons ℓ-k à ℓ-k ($1 \le k \le \ell-1$) de ces ℓ facteurs ; à chacune de ces combinaisons on associe le produit de tous ses éléments. On obtient ainsi des polynomes de degré ℓ-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 , $1 \le j \le h$, on introduit les ensembles d'entiers $\mathcal{E}_j = \{ u , 1 \le u \le \ell , \text{ tel que } \theta_u \equiv a_h \ (\text{mod. } \mathfrak{P}^j) \}$.

Par définition d'une racine d'ordre t_j d'un idéal , card. $\mathcal{E}_j = t_j$ et les ensembles $\mathcal{E}_j$ forment une suite décroissante pour l'inclusion : $\mathcal{E}_{j+1} \subseteq \mathcal{E}_j$, $1 \le j \le h-1$.

On pose :

- $\mathcal{E}'_h = \mathcal{E}_h$ et pour tout j , $1 \le j \le h-1$, $\mathcal{E}'_j = \mathcal{E}_j - \mathcal{E}_{j+1}$, ($\mathcal{E}'_j = \phi \Leftrightarrow \mathcal{E}_j = \mathcal{E}_{j+1}$) .

- Pour tout j , $1 \le j \le h$, $t'_j = \text{card. } \mathcal{E}'_j$. On a donc : $t'_h = t_h$ (≥ 1) et pour j , $1 \le j \le h-1$, $t'_j = t_j - t_{j+1}$ ($t'_j = 0 \Leftrightarrow \mathcal{E}'_j = \phi$) .

- $\mathcal{H} = \{ j , 1 \le j \le h , \text{ tel que } \mathcal{E}'_j \neq \phi \}$ (l'ensemble $\mathcal{H}$ est non vide car $\mathcal{E}'_h = \mathcal{E}_h \neq \phi \Rightarrow h \in \mathcal{H}$) .

Démontrons (i) .

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

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

guer deux cas :

α) $h = 1$ <u>ou</u> $h \geq 2$ <u>et pour tout</u> j , $1 \leq j \leq h-1$, $\mathcal{S}'_j = \phi$

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

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

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

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

β) $h \geq 2$ <u>et il existe</u> j , $1 \leq j \leq h-1$, <u>tel que</u> $\mathcal{S}'_j \neq \phi$.

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

deux à deux disjoints) , nous avons :

$$\prod_{i \in \mathcal{S}_1} (a_h - \theta_i) = \prod_{j \in \mathcal{H}} \Big(\prod_{i \in \mathcal{S}'_j} (a_h - \theta_i) \Big) .$$

Pour tout $i \in \mathcal{S}'_j \neq \phi$, $a_h - \theta_i \in \mathfrak{P}^j$ et card. $\mathcal{S}'_j = t'_j > 0$,

par suite :

$\prod_{i \in \mathcal{S}'_j} (a_h - \theta_i) \in \mathfrak{P}^{j t'_j}$ et $\prod_{j \in \mathcal{H}} \Big(\prod_{i \in \mathcal{S}'_j} (a_h - \theta_i) \Big) \in \prod_{j \in \mathcal{H}} \mathfrak{P}^{j t'_j} = \mathfrak{P}^{\sum_{j \in \mathcal{H}} j t'_j}$.

Or $\mathcal{S}'_j = \phi \Leftrightarrow t'_j = 0$, alors $\sum_{j \in \mathcal{H}} j t'_j = \sum_{j=1}^{j=h} j t'_j = \sum_{j=1}^{j=h-1} j t'_j + h t_h$ 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 $\prod_{i \in \mathcal{S}_1} (a_h - \theta_i) \in \mathfrak{P}^{T_h}$.

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

blit (i) pour $k = 0$.

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

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

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

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

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 $i \in \mathcal{E}'_j \neq \emptyset$ tels que $X - \theta_i$ divise $P_{i',k}$. Par convention , si $\mathcal{E}'_j = \emptyset$, on posera $t'_j - s_{j,i'} = 0$.

On considère à nouveau les deux cas :

α) $h = 1$ $\underline{\text{ou}}$ $h \geq 2$ $\underline{\text{et pour tout}}$ j , $1 \leq j \leq h-1$, $\mathcal{E}'_j = \emptyset$.

Alors $\mathcal{E}'_h = \mathcal{E}_h = \mathcal{E}_1$ et $T_h = h t_h$. Le nombre d'entiers $i \in \mathcal{E}_h$ 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 $\prod_{i \in \mathcal{E}_1} (a_h - \theta_i) = \prod_{i \in \mathcal{E}_h} (a_h - \theta_i) \in \mathfrak{P}^{h(t_h - s_{h,i'})}$ mais $h t_h - h s_{h,i'} = T_h - h s_{h,i'} \geq T_h - hk$, par suite

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

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

Comme $\mathcal{E}_1 = \bigcup_{j \in \mathcal{H}} \mathcal{E}'_j$, le nombre des entiers $i \in \mathcal{E}_1$ tels que $X - \theta_i$ divise $P_{i',k}$ est : $\sum_{j \in \mathcal{H}} (t'_j - s_{j,i'}) \geq t_1 - k$.

Mais $t'_j - s_{j,i'} = 0$ si $\mathcal{E}'_j = \emptyset$; on a alors :

$$\sum_{j \in \mathcal{H}} (t'_j - s_{j,i'}) = \sum_{j=1}^{j=h} (t'_j - s_{j,i'}) = t_h - s_{h,i'} + \sum_{j=1}^{j=h-1} (t_j - t_{j+1} - s_{j,i'})$$

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

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 : $\prod_{i \in \mathcal{E}_1} (a_h - \theta_i) = \prod_{j \in \mathcal{H}} \left(\prod_{i \in \mathcal{E}'_j} (a_h - \theta_i) \right)$,

en convenant de poser $\prod_{i \in \mathcal{E}'_j} (a_h - \theta_i) = 1$, si , pour tout $i \in \mathcal{E}'_j$, $X - \theta_i$ 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 $j \in \mathcal{H}$, $\prod_{i \in \mathcal{E}'_j} (a_h - \theta_i) \in \mathfrak{P}^{j(t'_j - s_{j,i'})}$ et

$\prod_{j \in \mathcal{H}} \left(\prod_{i \in \mathcal{E}'_j} (a_h - \theta_i) \right) \in \mathfrak{P}^{w_i}$ avec $w_i = \sum_{j \in \mathcal{H}} j(t'_j - s_{j,i'})$.

Comme $\mathcal{E}'_j = \emptyset \Rightarrow t'_j - s_{j,i'} = 0$, 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 $w_i \geq T_h - hk > 0$ $\left(\text{car } k \leq e = \left[\frac{1}{h}(T_h - 1) \right] \leq \frac{1}{h}(T_h - 1) < \frac{T_h}{h} \right)$.

Par suite , comme dans le cas $\alpha)$, $\prod_{i \in \mathcal{E}_1} (a_h - \theta_i) \in \mathfrak{P}^{T_h - hk}$.

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

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

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

Démontrons (ii) .

Remarquons que , puisque : $h t_h \le T_h$ (p. 26) , $T_h - h t_h + 1 \ge 1$.

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

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

Or card. $\mathcal{E}_h = t_h$, donc , il existe un entier unique i'_1 , $1 \le i'_1 \le C_\ell^{t_h}$ tel que , pour tout $i \in \mathcal{E}_h$, $X - \theta_i$ 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 :

$\alpha)$ $h = 1$ <u>ou</u> $h \ge 2$ <u>et pour tout</u> j, $1 \le j \le h-1$, $\mathcal{E}'_j = \phi$.

Alors $\mathcal{E}_h = \mathcal{E}_1$, $T_h = h t_h$ et $P_{i'_1,t_h}(a_h) = \prod_{i \notin \mathcal{E}_1} (a_h - \theta_i)$ (ce produit comprenant $\ell - t_1$ termes). Comme, par définition de $\mathcal{E}_1$, pour tout $i \notin \mathcal{E}_1$, $a_h - \theta_i \notin \mathfrak{P}$, d'où $P_{i'_1,t_h}(a_h) \notin \mathfrak{P}$. C'est le résultat annoncé , car dans ce cas : $1 = T_h - h t_h + 1$.

$\beta)$ $h \ge 2$ <u>et il existe</u> j, $1 \le j \le h-1$, <u>tel que</u> $\mathcal{E}'_j \ne \phi$.

Il en résulte en particulier $t_h < t_1$ et $\mathcal{E}_1 - \mathcal{E}_h \ne \phi$.

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

$i \in \mathcal{E}_1 - \mathcal{E}_h$. Comme $\mathcal{E}_1 - \mathcal{E}_h = \bigcup_{j \in \mathcal{H} \setminus \{h\}} \mathcal{E}'_j$, nous décomposons $P_{i'_1, t_h}(a_h)$

sous la forme : $P_{i'_1, t_h}(a_h) = \underbrace{\prod_{j \in \mathcal{H} \setminus \{h\}} \Big(\prod_{i \in \mathcal{E}'_j} (a_h - \theta_i) \Big)}_{t_1 - t_h \text{ facteurs}} \times \underbrace{\prod_{i \notin \mathcal{E}_1} (a_h - \theta_i)}_{\ell - t_1 \text{ facteurs}}$.

Considérons l'idéal $\Big(P_{i'_1, t_h}(a_h)\Big) E_K$ engendré par $P_{i'_1, t_h}(a_h)$ dans K :

$$\Big(P_{i'_1, t_h}(a_h)\Big) E_K = \prod_{j \in \mathcal{H} \setminus \{h\}} \Big(\prod_{i \in \mathcal{E}'_j} (a_h - \theta_i) E_K \Big) \times \prod_{i \notin \mathcal{E}_1} (a_h - \theta_i) E_K .$$

Pour tout $i \notin \mathcal{E}_1$, l'idéal $(a_h - \theta_i) E_K$ est premier avec $\mathfrak{P}$.

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

De plus, les ensembles $\mathcal{E}'_j$ 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 $(\mathfrak{A}_i , \mathfrak{P}) = E_K$, $\big((\mathfrak{A}_i , \mathfrak{P})$ désignant le p.g.c.d. des idéaux $\mathfrak{A}_i$ et $\mathfrak{P} \big)$.

Nous avons alors :

$$\prod_{i \in \mathcal{E}'_j} (a_h - \theta_i) E_K = \mathfrak{P}^{j t'_j} \times \prod_{i \in \mathcal{E}'_j} \mathfrak{A}_i \quad \text{et}$$

$$\prod_{j \in \mathcal{H} \setminus \{h\}} \Big(\prod_{i \in \mathcal{E}'_j} (a_h - \theta_i) E_K \Big) = \mathfrak{P}^{\left(\sum_{j \in \mathcal{H} \setminus \{h\}} j t'_j \right)} \times \mathfrak{A} \quad \text{en posant :}$$

$\mathfrak{A} = \prod_{j \in \mathcal{H} \setminus \{h\}} \Big(\prod_{i \in \mathcal{E}'_j} \mathfrak{A}_i \Big)$. Compte-tenu de $\mathcal{E}'_j = \emptyset \Leftrightarrow t_j - t_{j+1} = 0$,

$$\sum_{j \in \mathcal{H} \setminus \{h\}} j t'_j = \sum_{j=1}^{h-1} j t'_j = T_h - h t_h \quad \text{(p. 28)} .$$

D'où :

$$\Big(P_{i'_1, t_h}(a_h)\Big) E_K = \mathfrak{P}^{T_h - hk} \times \mathfrak{B} \text{ , avec } \mathfrak{B} = \mathfrak{A} \times \prod_{i \notin \mathcal{E}_1} (a_h - \theta_i) E_K .$$

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

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 $i \in \mathcal{E}_h$, alors le nombre des $i \in \mathcal{E}_h$ tels que $X - \theta_i$ divise $P_{i', t_h}(X)$ est $t_h - s_{h, i'} \geq 1$.

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

β) <u>Si</u> $h \geq 2$ <u>et s'il existe</u> j , $1 \leq j \leq h-1$, <u>tel que</u> $\mathcal{E}'_j \neq \emptyset$, 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 :

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

Nous avons donc :

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

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

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

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) $\dfrac{f^{(k)}(a)}{k\,!} \equiv 0 \pmod{p^{t-k}}$ si $0 \leq k \leq t-1$;

(ii) $\dfrac{f^{(t)}(a)}{t\,!} \not\equiv 0 \pmod{p}$.

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 $\mathfrak{P}^h$.

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

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

Démonstration :

a_h ($\equiv a \pmod{p}$) 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 : $$f(x) = \sum_{k=0}^{k=\ell} p^{hk} \frac{f^{(k)}(a_h)}{k\,!} x_h^k = \sum_{k=0}^{k=\ell} b_k x_h^k .$$

Pour tout k, $0 \leq k \leq \ell$, $b_k = p^{hk} \dfrac{f^{(k)}(a_h)}{k!} \equiv 0 \left(\text{mod.}\, p^{T_h}\right)$,

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 $b_k \equiv 0 \left(\text{mod.}\, p^{T_h}\right)$ en résulte immédiatement .

De plus, d'après (ii) de la proposition II.7, $b_{t_h} \not\equiv 0 \left(\text{mod.}\, p^{T_h+1}\right)$. 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 ℓ .

Remarque :

Si $k \geq t_1 + 1$, $hk \geq ht_1 + h \geq ht_1 + 1 \geq T_h + 1$ (p. 26), alors $b_k \equiv 0 \left(\text{mod.}\, p^{T_h+1}\right)$ 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 $f_h(x_h) \equiv \varphi_h(x_h)$ (mod. p), φ_h étant un polynome de $\mathbb{Z}[X]$, de degré ν, 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 $f_h(x_h) \equiv 0 \,(\text{mod.}\, p^{h'})$ ($h' \geq 1$) 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 $f(x) \equiv 0$ (mod. p), $h \in \mathbb{N}^*$ et $a_h \equiv a$ (mod. 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 $\alpha_{h,1} = \dfrac{a_{h+1} - a_h}{p^h}$ 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 :

pour tout k , $1 \leq k \leq \ell$, $f^{(k)}(x) = A_h\, p^{(T_h - hk)}\, f_h^{(k)}(x_h)$ (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 $\mathfrak{P}^{h+1}$:

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

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

$f(a_{h+1}) \equiv 0 \left(\text{mod. } p^{T_h+1} \right)$ et $\left(f(a_{h+1})\right)E_K = \mathfrak{P}^{T_h+1} \times \mathfrak{Q}$.

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

Comme $a_{h+1} \equiv a_h \ (\text{mod. } p^h)$, a_{h+1} est racine d'ordre t_j des idéaux $\mathfrak{P}^j$, $1 \le j \le h$, avec : $1 < t_h \le \ldots \le t_j \le \ldots \le t_1$.

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

- Pour tout j , $1 \le j \le h$,

  $\mathcal{E}_j = \{ u \ , \ 1 \le u \le \ell \ , \text{ tel que } \theta_u \equiv a_{h+1} \ (\text{mod. } \mathfrak{P}^j) \}$
- $\mathcal{E}'_h = \mathcal{E}_h$, et pour tout j , $1 \le j \le h-1$, $\mathcal{E}'_j = \mathcal{E}_j - \mathcal{E}_{j+1}$
- $\mathcal{H} = \{ j \ , \ 1 \le j \le h \ , \text{ tel que } \mathcal{E}'_j \neq \emptyset \}$.

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

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

Nous avons :

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

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

avec $\mathfrak{A}_h = \prod_{i \in \mathcal{E}_h} \mathfrak{A}_{i,h}$.

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

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

Si $i \notin \mathcal{S}_1$, $a_{h+1} \not\equiv \theta_i \pmod{\mathfrak{P}}$ et $\left(\prod_{i \notin \mathcal{S}_1} (a_{h+1} - \theta_i) E_K , \mathfrak{P} \right) = E_K$.

En écrivant $\prod_{j \in \mathcal{H}} \left(\prod_{i \in \mathcal{S}'_j} (a_{h+1} - \theta_i) E_K \right)$ sous la forme :

$$\prod_{i \in \mathcal{S}_h} (a_{h+1} - \theta_i) \times \prod_{j \in \mathcal{H} \setminus \{h\}} \left(\prod_{i \in \mathcal{S}'_j} (a_{h+1} - \theta_i) E_K \right)$$

et compte-tenu de : $\sum_{j \in \mathcal{H} \setminus \{h\}} j t'_j = \sum_{j=1}^{j=h-1} j t'_j = T_h - h t_h$, on obtient

finalement $\left(f(a_{h+1}) \right) E_K = \mathfrak{P}^{T_h} \times \mathfrak{A}_h \times \mathfrak{B} = \mathfrak{P}^{T_h + 1} \times \mathfrak{Q}$ où $(\mathfrak{B}, \mathfrak{P}) = E_K$.

Alors $\mathfrak{A}_h = \prod_{i \in \mathcal{S}_h} \mathfrak{A}_{i,h} \equiv 0 \pmod{\mathfrak{P}}$, et il existe au moins un entier i' , $i' \in \mathcal{S}_h$, tel que $\mathfrak{A}_{i',h} \equiv 0 \pmod{\mathfrak{P}}$; il en résulte : $(a_{h+1} - \theta_{i'}) E_K = \mathfrak{P}^h \mathfrak{A}_{i',h} \equiv 0 \pmod{\mathfrak{P}^{h+1}}$, ce qui montre que $a_{h+1} = a_h + p^h \alpha_{h,1}$ est racine de l'idéal $\mathfrak{P}^{h+1}$ (relativement à $\theta_{i'}$) . Soit alors t' ($t' \geq 1$) l'ordre de cette racine . D'après la condition nécessaire $t' = t_{h+1}$.

Conséquences :

1°) Le nombre des racines , non congrues mod. p , de la congruence $f_h(x_h) \equiv 0 \pmod{p}$ est égal au nombre des racines de l'idéal $\mathfrak{P}^{h+1}$, non congrues mod. p^{h+1} , et qui sont congrues à a_h mod. p^h . En fait , il y a bijection entre les racines de l'idéal $\mathfrak{P}^{h+1}$, congrues à a_h , mod. p^h , et les racines de la congruence $f_h(x_h) \equiv 0 \pmod{p}$ avec conservation des ordres de multiplicité .

2°) Soient β_i , $1 \leq i \leq q$, les racines incongrues mod. p de la congruence $f_h(x_h) \equiv 0 \pmod{p}$ et s_i l'ordre de multiplicité de chacune de ces racines ($1 \leq s_i \leq t_h$ pour tout $i \in \{1, 2, \ldots, q\}$) .

Montrons que $\sum_{i=1}^{i=q} s_i = t_h$. Pour cela , considérons les ensembles :

$$\mathcal{S}_{i,h+1} = \left\{ u \in \mathcal{S}_h \text{ tel que } \theta_u \equiv a_h + p^h \beta_i \pmod{\mathfrak{P}^{h+1}} \right\} , \quad 1 \leq i \leq q ;$$

nous avons card. $\mathcal{S}_{i,h+1} = s_i$. Il est immédiat que $\mathcal{S}_h = \bigcup_{1 \leq i \leq q} \mathcal{S}_{i,h+1}$

avec $\mathcal{E}_{i,h+1} \cap \mathcal{E}_{j,h+1} = \phi$ si $i \neq j$.

Par suite : card. $\mathcal{E}_h = t_h = \sum_{i=1}^{i=q}$ card. $\mathcal{E}_{i,h+1} = \sum_{i=1}^{i=q} s_i$.

Théorème II.2 :

Les hypothèses sont les mêmes que celles du théorème II.1. On suppose de plus que : $a_{h+1} \equiv a_h \pmod{p^h}$ est racine d'ordre 1 de l'idéal $\mathfrak{P}^{h+1}$ .Soit h' un entier ≥ 2 ; $a_{h+h'} \equiv a_{h+1} \pmod{p^{h+1}}$ est racine de l'idéal $\mathfrak{P}^{h+h'}$ si et seulement si $\alpha_{h,h'} = \frac{a_{h+h'} - a_h}{p^h}$ est une racine de la congruence $f_h(x_h) \equiv 0 \pmod{p^{h'}}$, qui est racine simple de cette congruence modulo p .

La démonstration de ce théorème est analogue à celle du théorème II.1 .

Condition nécessaire .

Soit $a_{h+h'} \equiv a_{h+1} \pmod{p^{h+1}} \equiv a_h \pmod{p^h}$ une racine de l'idéal $\mathfrak{P}^{h+h'}$. Alors $a_{h+h'}$ est racine d'ordre t_h de $\mathfrak{P}^h$, racine d'ordre 1 de $\mathfrak{P}^{h+1}$, et par suite , racine d'ordre 1 de tous les idéaux $\mathfrak{P}^{h+u}$, $1 \leq u \leq h'$. On a donc : $1 = \underset{1 \leq u \leq h'}{t_{h+u}} < t_h \leq \ldots \; t_j \leq \ldots t_1$, et $T_{h+h'} = \sum_{j=1}^{j=h+h'} t_j = T_h + h'$. Comme $a_{h+h'} \equiv a_h \pmod{p^h}$, posons $a_{h+h'} = a_h + p^h \alpha_{h,h'}$. Puisque $(A_h, p) = 1$, il résulte de la formule (II-1) : $f_h(\alpha_{h,h'}) \equiv 0 \pmod{p^{h'}}$.

De plus , $a_{h+h'}$ étant racine d'ordre 1 de $\mathfrak{P}^{h+1}$, le théorème II.1 montre que $\alpha_{h,h'}$ est racine simple de la congruence $f_h(x_h) \equiv 0 \pmod{p}$.

Condition suffisante .

Soit $\alpha_{h,h'}$ une racine de la congruence $f_h(x_h) \equiv 0 \pmod{p^{h'}}$ ($h' \geq 2$) qui soit racine simple de cette congruence mod. p . Posons $a_{h+h'} = a_h + p^h \alpha_{h,h'}$. Alors $f(a_{h+h'}) \equiv 0 \left(\text{mod. } p^{T_h + h'}\right)$, par suite $\left(f(a_{h+h'})\right) E_K = \mathfrak{P}^{T_h + h'} \times \mathfrak{Q}$.

Cherchons, à nouveau, une autre expression de l'idéal $\left(f(a_{h+h'})\right)E_K$. D'après le théorème II.1 , $a_{h+h'}$ est racine d'ordre 1 de l'idéal $\mathfrak{P}^{h+1}$; par conséquent , il existe un entier unique $i' \in \mathcal{S}_h$ tel que $a_{h+h'} \equiv \theta_{i'}$ (mod. $\mathfrak{P}^{h+1}$) et pour tout $i \in \mathcal{S}_h$, $i \neq i'$, $\theta_i \equiv a_{h+h'}$ (mod. $\mathfrak{P}^h$) et $\theta_i \not\equiv a_{h+h'}$ (mod. $\mathfrak{P}^{h+1}$) . Alors : $(a_{h+h'} - \theta_{i'})E_K = \mathfrak{P}^{h+1}\,\mathfrak{A}_{i',h}$, et $(a_{h+h'} - \theta_i)E_K = \mathfrak{P}^h\,\mathfrak{A}_{i,h}$, si $i \in \mathcal{S}_h$, $i \neq i'$, avec $(\mathfrak{A}_{i,h}, \mathfrak{P}) = E_K$. Il en résulte :

$$\prod_{i \in \mathcal{S}_h} (a_{h+h'} - \theta_i)E_K = (a_{h+h'} - \theta_{i'})E_K \times \prod_{\substack{i \in \mathcal{S}_h \\ i \neq i'}} (a_{h+h'} - \theta_i)E_K$$

$$= \mathfrak{P}^{h+1}\,\mathfrak{A}_{i',h} \times \mathfrak{P}^{h(t_h-1)} \times \prod_{\substack{i \in \mathcal{S}_h \\ i \neq i'}} \mathfrak{A}_{i,h}$$

$$= \mathfrak{P}^{h t_h + 1} \times \mathfrak{A}_{i',h} \times \mathfrak{A}_h$$

en posant $\mathfrak{A}_h = \prod_{\substack{i \in \mathcal{S}_h \\ i \neq i'}} \mathfrak{A}_{i,h}$; et puisque $(\mathfrak{A}_{i,h}, \mathfrak{P}) = E_K$,

si $i \in \mathcal{S}_h$, $i \neq i'$, on a : $\mathfrak{A}_h \not\equiv 0$ (mod. $\mathfrak{P}$) .

En reprenant le raisonnement utilisé dans la démonstration du théorème II.1 , nous obtenons finalement :

$$\left(f(a_{h+h'})\right)E_K = \mathfrak{P}^{T_h+1} \times \mathfrak{A}_{i',h} \times \mathfrak{B} = \mathfrak{P}^{T_h+h'} \times \mathfrak{Q} ,$$

avec $(\mathfrak{B}, \mathfrak{P}) = E_K$; par suite $\mathfrak{A}_{i',h} \equiv 0$ (mod. $\mathfrak{P}^{h'-1}$) , et $(a_{h+h'} - \theta_{i'})E_K \equiv 0$ (mod. $\mathfrak{P}^{h+h'}$) , ce qui montre que $a_{h+h'}$ est racine de l'idéal $\mathfrak{P}^{h+h'}$ (relativement à $\theta_{i'}$) et l'ordre de cette racine est 1 (puisque $a_{h+h'}$ est déjà racine d'ordre 1 de $\mathfrak{P}^{h+1}$) .

Il résulte immédiatement des théorèmes II.1 et II.2 le :

Corollaire II.3 :

Soit a une racine multiple de la congruence $f(x) \equiv 0$ (mod. p) et soit $a_h \equiv a$ (mod. p) une racine d'ordre t_h de l'idéal $\mathfrak{P}^h$ ($h \geq 1$, $t_h > 1$) . f_h étant le polynome déduit de f par le changement de variable $x = a_h + p^h x_h$, on suppose que la congruence $f_h(x_h) \equiv 0$ (mod. p) admet au moins une racine simple $\alpha_{h,1}$. Pour tout entier h', $h' \geq 2$, soit $\alpha_{h,h'} \equiv \alpha_{h,1}$ (mod. p) la racine unique , au module $p^{h'}$ près (lemme de Hensel) de la congruence $f_h(x_h) \equiv 0$ (mod. $p^{h'}$) . Alors , la suite des entiers $a_{h+h'}$, définis par :

$$a_{h+h'} = a_h + p^h \alpha_{h,h'} , \quad h' \geq 1$$

converge p-adiquement vers une racine de f dans $\mathbb{Z}_p$.

Remarque :

Comme $a_{h+h'} \equiv a_h$ (mod. p^h) $\equiv a$ (mod. p) , nous avons obtenu une suite p-adique , de premier terme a , racine multiple de la congruence fondamentale mod. p et qui converge vers une racine p-adique de f .

II.4.- Application à la construction des approximations p-adiques d'une racine du polynome f dans $\mathbb{Q}_p$ à partir d'une racine multiple de la congruence fondamentale modulo p .

Soit r l'entier ($r \geq 1$) tel que $I(\theta) \equiv 0$ (mod. p^r) et $I(\theta) \not\equiv 0$ (mod. p^{r+1}) . On suppose que la congruence $f(x) \equiv 0$ (mod.p) n'admet que des racines multiples . On choisit parmi celles-ci une racine a , d'ordre t_1 le plus petit possible .

Soit $\mathfrak{P}$ un idéal premier divisant pE_K , a est racine d'ordre t_1 de $\mathfrak{P}$ (prop.II.6) et on pose $\mathcal{S}_1 = \{u,\ 1 \leq u \leq \ell$, tel que $\theta_u \equiv a$ (mod.$\mathfrak{P}$)$\}$.

Par le changement de variable : $x = a + px_1$, on obtient

$$f(x) = A_1 p^{t_1} f_1(x_1) .$$

Il y a deux cas possibles :

- la congruence $f_1(x_1) \equiv 0 \pmod{p}$ admet au moins une racine simple, auquel cas, d'après le corollaire II.3, on sait construire une suite p-adique, de premier terme a, convergeant vers une racine p-adique de f.

- la congruence $f_1(x_1) \equiv 0 \pmod{p}$ n'admet que des racines multiples. On choisit alors, parmi celles-ci, une racine $\alpha_{1,1}$, d'ordre t_2 le plus petit possible ($2 \leq t_2 \leq t_1$). D'après le théorème II.1, $a_2 = a + p\,\alpha_{1,1}$ est racine d'ordre t_2 de l'idéal $\mathfrak{P}^2$ (pour des θ_u tels que $u \in \mathcal{S}_1$).

On pose $x = a_2 + p^2 x_2 = a + p\,\alpha_{1,1} + p^2 x_2$ et on a : $f(x) = A_2\, p^{t_1+t_2} f_2(x_2)$. (Remarquons que ce deuxième changement de variable $x = a + p(\alpha_{1,1} + p x_2)$ revient à faire dans $f_1(x_1)$ le changement de variable $x_1 = \alpha_{1,1} + p x_2$)

Aux racines de la congruence $f_2(x_2) \equiv 0 \pmod{p}$ sont associées des racines de l'idéal $\mathfrak{P}^3$ (relativement à des θ_u, pour $u \in \mathcal{S}_1$) avec le même ordre de multiplicité.

Si la congruence $f_2(x_2) \equiv 0 \pmod{p}$ n'a pas de racine simple, on continue le procédé. On construira ainsi, de proche en proche une suite (f_k) de polynomes de la variable x_k, jusqu'à l'obtention d'un polynome f_h tel que la congruence $f_h(x_h) \equiv 0 \pmod{p}$ admette une racine simple. Un tel polynome existe d'après la proposition suivante :

Proposition II.8 :

Soient $r_{i,j}$ les entiers définis dans la proposition II.3. Soit $\rho = \sup r_{i,j}$, pour les couples $(i,j) \in \mathcal{S}_1 \times \mathcal{S}_1$ avec $i < j$. Alors on a : $1 \leq \rho \leq r$, et il existe un entier h, $h \leq \rho$, tel que la congruence $f_h(x_h) \equiv 0 \pmod{p}$ admette une racine simple.

Démonstration :

Considérons les couples $(i, j) \in \mathcal{S}_1^2$ avec $i < j$.

D'après la définition de $\mathcal{S}_1$, pour tous ces couples , $\theta_j - \theta_i \in \mathfrak{P}$.

D'autre part (proposition II.3) , à chacun de ces couples est associé un entier $r_{i,j}$ tel que $\theta_j - \theta_i \in \mathfrak{P}^{r_{i,j}}$ et $\theta_j - \theta_i \notin \mathfrak{P}^{r_{i,j}+1}$.

Nous avons donc : $1 \leq r_{i,j} \leq r$, $\forall (i, j) \in \mathcal{S}_1^2$, d'où :
$i<j$

$1 \leq \rho = \sup r_{i,j} \leq r$. Alors , $\forall (i, j) \in \mathcal{S}_1^2$, $i \neq j$, $\theta_j - \theta_i \notin \mathfrak{P}^{\rho+1}$.

– Ou bien nous avons obtenu un entier h , $1 \leq h \leq \rho-1$, tel que la congruence $f_h(x_h) \equiv 0$ (mod. p) admette une racine simple et la proposition est démontrée .

– Ou bien nous avons construit les polynomes f_k , $1 \leq k \leq \rho-1$ et les congruences $f_k(x_k) \equiv 0$ (mod. p) n'admettent que des racines multiples . Soit $\alpha_{\rho-1,1}$ une racine d'ordre t_ρ ($t_\rho \geq 2$) de la congruence $f_{\rho-1}(x_{\rho-1}) \equiv 0$ (mod. p) . Il lui correspond une racine a_ρ d'ordre t_ρ de l'idéal $\mathfrak{P}^\rho$ et le changement de variable $x = a_\rho + p^\rho x_\rho$ conduit au polynome f_ρ tel que

$$f(x) = A_\rho p^{T_\rho} f_\rho(x_\rho) .$$

Or les racines de la congruence $f_\rho(x_\rho) \equiv 0$ (mod. p) sont associées aux racines de l'idéal $\mathfrak{P}^{\rho+1}$ (relativement à des θ_u , pour $u \in \mathcal{S}_1$) avec le même ordre de multiplicité et l'idéal $\mathfrak{P}^{\rho+1}$ n'admet que des racines d'ordre 1 relativement aux θ_u pour $u \in \mathcal{S}_1$. Il en résulte donc que toutes les racines de la congruence $f_\rho(x_\rho) \equiv 0$ (mod. p) sont simples.

II.5.- Construction des approximations p-adiques de toutes les racines de f dans $\mathbb{Q}_p$ et bases sur $\mathbb{Z}$ des idéaux $\mathfrak{P}^k$, lorsque $p = N(\mathfrak{P})$ divise $I(\theta)$.

Soit p un diviseur premier de $I(\theta)$ et soit a une racine (simple s'il en existe une , multiple sinon) de la congruence $f(x) \equiv 0$ (mod.p). Il existe un idéal premier $\mathfrak{P}$ divisant pE_K tel que $\theta_1 \equiv a$ (mod.$\mathfrak{P}$).

Nous savons construire (par application du lemme de Hensel dans le cas d'une racine simple , par la méthode du § II.4 pour une racine multiple) une suite d'entiers $a_{1,k}$, de premier terme $a_{1,1} \equiv a$ (mod. p) et tels que : $f(a_{1,k}) \equiv 0$ (mod. p^k) pour tout $k \in \mathbb{N}^*$, et $a_{1,k} \equiv a_{1,j}$ (mod. p^j) pour tout $k \in \mathbb{N}^*$ et tout j , $1 \leq j \leq k-1$.

Cette suite converge donc , lorsque $k \to \infty$, vers la racine p-adique Θ_1 de f , associée à la racine réelle θ_1 (p. 13) . A partir de cette suite p-adique , nous construisons les $\ell-1$ autres suites p-adiques convergeant vers les $\ell-1$ racines Θ_ν , $2 \leq \nu \leq \ell$, de f dans $\mathbb{Q}_p$, de la façon suivante :

Considérons les expressions des racines réelles de f en fonction de la racine θ_1 : $d_h\, \theta_{h+1} = g_h(\theta_1)$, $1 \leq h \leq \ell-1$ (I-3)

Pour tout h , $1 \leq h \leq \ell-1$, les entiers d_h divisent $I(\theta)$ avec l'hypothèse : $I(\theta) \equiv 0$ (mod. p^r) et $I(\theta) \not\equiv 0$ (mod. p^{r+1}) ($r \geq 1$). Alors , ou bien $d_h \not\equiv 0$ (mod. p) , ou bien $d_h \equiv 0$ (mod. p) et comme $d_h \not\equiv 0$ (mod. p^{r+1}) , il existe un entier r_h , $1 \leq r_h \leq r$, tel que $d_h \equiv 0$ (mod. p^{r_h}) et $d_h \not\equiv 0$ (mod. p^{r_h+1}) . Si $d_h \not\equiv 0$ (mod. p) , on posera $r_h = 0$.

Supposons que nous ayons construit la suite ($a_{1,k}$) des approximations p-adiques , modulo p^k , de la racine Θ_1 de f . Il existe un idéal premier $\mathfrak{P}$, de norme p , tel que $\theta_1 \equiv a_{1,k}$ (mod. $\mathfrak{P}^k$) , pour tout $k \in \mathbb{N}^*$.

Pour tout i , $2 \leq i \leq \ell$, désignons par $a_{i,k}$ l'entier rationnel , unique au module p^k près , tel que $\theta_i \equiv a_{i,k}$ (mod. $\mathfrak{P}^k$) (corollaire I.1) . Nous avons donc : $f(a_{i,k}) \equiv 0$ (mod. p^k) , $1 \leq i \leq \ell$, et $\sum_{i=1}^{i=\ell} a_{i,k} \equiv s$ (mod. p^k) ce qui détermine $a_{\ell,k}$, si les $a_{i,k}$, $1 \leq k \leq \ell-1$, sont connus . $a_{1,k}$ étant connu , il suffit donc de calculer $a_{i+1,k}$ pour $1 \leq i \leq \ell-2$.

Pour tout i, $1 \le i \le \ell-2$, $d_i(\theta_{i+1} - a_{i+1,k}) = g_i(\theta_1) - d_i a_{i+1,k} \in \mathfrak{P}^{k+r_i}$ ($r_i \ge 0$) et comme $\theta_1 \equiv a_{1,k+r_i} \pmod{\mathfrak{P}^{k+r_i}}$, nous avons : $g_i(a_{1,k+r_i}) - d_i a_{i+1,k} \in \mathfrak{P}^{k+r_i} \cap \mathbb{Z} = p^{k+r_i}\mathbb{Z}$, d'où :

$$(\mathcal{C}) \quad d_i a_{i+1,k} \equiv g_i(a_{1,k+r_i}) \pmod{p^{k+r_i}}, \quad 1 \le i \le \ell-2 .$$

Or : ou bien, $r_i = 0 \Leftrightarrow d_i \not\equiv 0 \pmod{p}$ et la congruence $(\mathcal{C})$ se réduit à : $d_i a_{i+1,k} \equiv g_i(a_{1,k}) \pmod{p^k}$ avec $(d_i, p) = 1$

ou bien, $r_i \ge 1$ et $d_i = p^{r_i} d_i'$ avec $(d_i', p) = 1$.

La congruence $(\mathcal{C})$ montre alors que, nécessairement,

$$g_i(a_{1,k+r_i}) \equiv 0 \pmod{p^{r_i}}, \quad \text{d'où } g_i(a_{1,k+r_i}) = p^{r_i} G_i$$

et la congruence $(\mathcal{C})$ se réduit à : $d_i' a_{i+1,k} \equiv G_i \pmod{p^k}$.

Dans les deux cas, $(\mathcal{C})$ détermine $a_{i+1,k}$, $1 \le i \le \ell-2$, de façon unique mod. p^k .

Nous savons de plus, (proposition II.3), que, pour tout couple (i, j), $1 \le i < j \le \ell$, il existe un entier $r_{i,j}$, $0 \le r_{i,j} \le r$, 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, pour ceux des couples (i,j) pour lesquels $r_{i,j} \neq 0$:

$$a_{j,k} \equiv a_{i,k} \pmod{p^k} \text{ si } 1 \le k \le r_{i,j},$$

$$a_{j,k} \not\equiv a_{i,k} \pmod{p^k} \text{ si } k \ge r_{i,j}+1 .$$

Soit $\rho' = \sup_{1 \le i < j \le \ell} r_{i,j}$, alors pour tout (i, j), $1 \le i < j \le \ell$, $\theta_j - \theta_i \in \mathfrak{P}^{\rho'+1}$. Par suite, pour tout i, tout $j \neq i$, $a_{j,k} \not\equiv a_{i,k} \pmod{p^k}$ si $k \ge \rho'+1$.

En résumé, nous avons :

Proposition II.9 :

Soit p un nombre premier tel que $l(\theta) \equiv 0 \pmod{p^r}$ et $l(\theta) \not\equiv 0 \pmod{p^{r+1}}$ $(r \geq 1)$. Pour tout $k \in \mathbb{N}^*$, il existe ℓ entiers rationnels $a_{i,k}$, $1 \leq i \leq \ell$, tels que :

$$\begin{cases} f(a_{i,k}) \equiv 0 \pmod{p^k} & 1 \leq i \leq \ell \\ d_i\, a_{i+1,k} \equiv g_i(a_{1,k+r_i}) \pmod{p^{k+r_i}} & 1 \leq i \leq \ell-2 \\ a_{\ell,k} \equiv s - \sum_{i=1}^{\ell-1} a_{i,k} \pmod{p^k} \end{cases}$$

De plus : $a_{j,k} \equiv a_{i,k} \pmod{p^k}$ si $0 \leq k \leq r_{i,j}$; $a_{j,k} \not\equiv a_{i,k} \pmod{p^k}$ si $k \geq r_{i,j} + 1$, et $a_{j,k} \not\equiv a_{i,k} \pmod{p^k}$ pour tout (i,j), $1 \leq i < j \leq \ell$ et pour tout $k \geq \rho' + 1$ où $\rho' = \sup_{1 \leq i < j \leq \ell} r_{i,j}$.

Les $a_{i,k}$, $1 \leq i \leq \ell$, sont les approximations p-adiques modulo p^k des ℓ racines Θ_i de f dans $\mathbb{Z}_p$ et on a :

$$\prod_{1 \leq i < j \leq \ell} d(\Theta_j, \Theta_i) = \left(\frac{1}{p}\right)^r \qquad \text{(p. 19)}$$

Nous avons alors les deux théorèmes suivants, analogues aux théorèmes I.2 et I.3 :

Théorème II.3 :

Soit p un nombre premier tel que $l(\theta) \equiv 0 \pmod{p^r}$ et $l(\theta) \not\equiv 0 \pmod{p^{r+1}}$ $(r \geq 1)$. Alors l'équation $f(x) = 0$ admet ℓ racines Θ_i dans $\mathbb{Z}_p$ et le produit des distances mutuelles des racines est :

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

Théorème II.4 :

Soit p un nombre premier tel que $I(\theta) \equiv 0 \pmod{p^r}$ et $I(\theta) \not\equiv 0 \pmod{p^{r+1}}$ $(r \geq 1)$. Pour tout entier k, $k \geq 1$, l'idéal $p^k E_K$ se décompose en un produit de ℓ idéaux primaires canoniques conjugués :

$$p^k E_K = \prod_{h=1}^{h=\ell} \sigma^h(\mathfrak{P}^k)$$

avec pour tout h, $1 \leq h \leq \ell$,

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

$h+i \bmod. \ell$ $\qquad$ $i+\ell-h \bmod. \ell$

$\{ p^k,\ \theta_{h+i} - a_{i,k},\ 1 \leq i \leq \ell-1 \}$ 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 les $a_{i,k}$, $1 \leq i \leq \ell$, sont les approximations p-adiques, modulo p^k, des racines Θ_i de f dans $\mathbb{Q}_p$, que l'on calcule à l'aide de la proposition II.9.

PARTIE III

Cas particulier des corps cycliques de degré 5 .

III.1.- Rappels .

Les notations sont les mêmes que celles utilisées dans le cas général ; nous précisons certaines d'entre elles dans ce cas particulier .

Nous choisissons r = 2 comme générateur du groupe multiplicatif $(\mathbb{Z}/5\mathbb{Z})^*$. Nous avons alors : $Gal(\mathbb{Q}'/\mathbb{Q}) = \langle \tau \rangle$, les automorphismes τ^i , $1 \le i \le 4$, étant définis par : $\tau^i(\varepsilon^k) = \varepsilon^{2^i k}$, $2^i k$ modulo 5 .

Pour tout $\alpha \in \mathbb{Q}'$, le conjugué $\tau^i(\alpha)$ étant noté α_j , $1 \le j \le 4$, $j \equiv 2^i \pmod 5$ nous avons : $\tau(\alpha) = \alpha_2$, $\tau^2(\alpha) = \alpha_4$, $\tau^3(\alpha) = \alpha_3$, $\tau^4(\alpha) = \alpha_1 = \alpha$; il en résulte , pour tout j , $1 \le j \le 4$, $\tau(\alpha_j) = \alpha_{2j}$, $\tau^2(\alpha_j) = \alpha_{4j}$, $\tau^3(\alpha_j) = \alpha_{3j}$, $\tau^4(\alpha_j) = \alpha_j$ (avec pour tout $(i,j) \in \{1,2,3,4\}^2$, $ij \bmod 5 \in \{1,2,3,4\}$) .

Les résolvantes de Lagrange :

$\langle \theta_u, \chi_k \rangle = \sum_{\varphi \in G} \chi_k(\varphi^{-1})\, \varphi(\theta_u)$, $0 \le k \le 4$, seront notées :

$$\overline{\theta_{u,j}} = \langle \theta_u, \chi_{5-j} \rangle = \sum_{h=1}^{h=5} \varepsilon^{jh}\, \theta_{u+h} \quad , \quad 1 \le u \le 5 \ , \ 1 \le j = 5-k \le 5 \quad , \text{ et}$$

plus simplement , pour u = 1 ,

$$\overline{\theta}_j = \overline{\theta_{1,j}} = \langle \theta_1, \chi_{5-j} \rangle = \sum_{h=1}^{h=5} \varepsilon^{jh}\, \theta_{h+1} \quad , \quad 1 \le j \le 5 \ .$$

Le corps $\mathbb{Q}'$ est principal et nous savons que : ([16])

$$\overline{\theta_{u,j}}^{\,5} = \lambda_j^5\, \alpha_j\, \alpha_{2j}^3\, \alpha_{3j}^2\, \alpha_{4j}^4 = \lambda_j^5 \prod_{\substack{i=1 \\ ij \bmod 5}}^{i=4} \alpha_{ij}^{i^*} \quad ,$$

$1 \le j \le 4$

avec : $1 \le i^* \le 4$, $ii^* \equiv 1 \pmod 5$,

$\lambda_j \in \mathbb{Q}'$,

α_1 , α_2 , α_3 , α_4 entiers conjugués de $\mathbb{Q}'$ tels que $m = N(\alpha_i) = p_1 \times p_2 \times \dots \times p_n$, les p_i étant des nombres premiers tous distincts et $p_i \equiv 1 \pmod 5$ pour tout i .

Polynome fondamental f de K et base de E_K .

Nous choisissons pour polynome fondamental de K (polynome dont quatre parmi les cinq racines forment avec 1 une base de E_K) le polynome f défini par la formule (III-1) :

$$5^5 f(X) = (5X-s)^5 - 10\, m \times 5^{2(1-s)}(5X-s)^3 - 5m \times 5^{3(1-s)} \sum_{i=1}^{i=4} \alpha_{2i}\alpha_{4i}(5X-s)^2$$

$$+ 5m \times 5^{4(1-s)} \left[m - \sum_{i=1}^{i=4} \alpha_i \alpha_{2i}^2 \alpha_{4i} \right] (5X-s) - 5^{5(1-s)}\, m \sum_{i=1}^{i=4} \alpha_{2i}^2 \alpha_{3i} \alpha_{4i}^3$$

avec s = 1 pour un corps unitaire , s = 0 sinon .

Nous choisissons pour base de E_K : $\{ 1, \theta_1, \theta_2, \theta_3, \theta_4 \}$.

Etude du discriminant $D(\theta)$ du polynome f et de l'indice $I(\theta)$.

Nous avons $D(\theta) = D_5^2$ (p. 6)

où $$D_5 = \left| \theta_j^{i-1} \right|_{\substack{1 \le i \le 5 \\ 1 \le j \le 5}} = \prod_{1 \le i < j \le 5} (\theta_j - \theta_i) .$$

D_5 comporte 10 facteurs $\theta_j - \theta_i$ et peut être mis sous la forme de deux produits de chacun cinq termes :

$$D_5 = - \prod_{\substack{i=1 \\ (i+1 \bmod 5)}}^{i=5} (\theta_{i+1} - \theta_i) \times \prod_{\substack{i=1 \\ (i+2 \bmod 5)}}^{i=5} (\theta_{i+2} - \theta_i) = - M_1 \times M_2$$

en posant :

$$M_1 = \prod_{i=1}^{i=5} (\theta_{i+1} - \theta_i) = N(\theta_2 - \theta_1) = N\left(\sigma(\theta) - \theta\right)$$

$$M_2 = \prod_{i=1}^{i=5} (\theta_{i+2} - \theta_i) = N(\theta_3 - \theta_1) = N\left(\sigma^2(\theta) - \theta\right) .$$

Ces entiers rationnels M_1 et M_2 ont la propriété suivante :

Lemme III.1 :

M_1 et M_2 sont divisibles par $M = \sqrt[4]{D_K} = 5^{2(1-s)}\, m$ (p. 6)

Démonstration :

Soit p un diviseur premier de M ; deux cas sont à considérer :

1°) p divise m (donc $p \neq 5$) . Soit $\mathfrak{P}$ l'idéal premier tel que $\mathfrak{P}^5 = pE_K$. Pour tout couple (i, j) , $i \neq j$, $\theta_i \equiv \theta_j$ (mod. $\mathfrak{P}$) (proposition I.2) , donc en particulier $\theta_1 \equiv \theta_2 \equiv \theta_3$ (mod. $\mathfrak{P}$) , il en résulte:

pour $1 \leq j \leq 2$, $M_j \in \mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$, d'où $M_j \equiv 0$ (mod. p) .

Puisque $m = p_1 \times p_2 \times \ldots \times p_n$, les p_i étant des nombres premiers tous différents , congrus à 1 mod. 5 , M_j , $1 \leq j \leq 2$, est divisible par m . Comme pour $s = 1$, $M = m$, le lemme est démontré dans ce cas.

2°) $p = 5$, alors $s = 0$. Soit $\mathfrak{Q}$ l'idéal premier tel que $\mathfrak{Q}^5 = 5E_K$, nous avons : $\theta_j \equiv \theta_i$ (mod. $\mathfrak{Q}^2$) pour tout i et tout $j \neq i$ (lemme II.1); il en résulte , si $1 \leq i \leq 5$, $\theta_{i+1} - \theta_i \in \mathfrak{Q}^2$ et $\theta_{i+2} - \theta_i \in \mathfrak{Q}^2$, d'où ,

pour $1 \leq j \leq 2$, $M_j \in (\mathfrak{Q}^2)^5 \cap \mathbb{Z} = 5^2\mathbb{Z}$, et $M_j \equiv 0$ (mod. 5^2) ,

ce qui , puisque $(5, m) = 1$, démontre le lemme dans le cas $s = 0$.

Conséquence :

Pour $j = 1, 2$, posons $|M_j| = Mm_j$, alors :

$\sqrt{D(\theta)} = |D_5| = |M_1 M_2| = M^2 m_1 m_2 = I(\theta) \times \sqrt{D_K}$ (p.6, 7) ,

par suite : $I(\theta) = m_1 \times m_2$ (III-2)

Remarques :

1°) Le résultat précédent se généralise sans difficulté dans le cas des corps cycliques de degré premier impair quelconque $\ell > 5$.

2°) M_1 et M_2 se calculent à l'aide des résolvantes de Lagrange , et on en déduit une expression de m_1 et m_2 ne portant que sur les ε^h , $1 \leq h \leq 4$ et le quadruplet $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$:

$$5^{1+3s} m_1 = |(\varepsilon^4-2\varepsilon^3+2\varepsilon^2-\varepsilon)(\alpha_2^2\alpha_3\alpha_4^3-\alpha_1^3\alpha_2\alpha_3^2)+(2\varepsilon^4+\varepsilon^3-\varepsilon^2-2\varepsilon)(\alpha_1\alpha_3^3\alpha_4^2-\alpha_1^2\alpha_2^3\alpha_4)|$$

$$+|5m(\varepsilon^3-\varepsilon^2)(\alpha_2\alpha_4-\alpha_1\alpha_3)+5m(\varepsilon^4-\varepsilon)(\alpha_1\alpha_2-\alpha_3\alpha_4)|$$

$$5^{1+3s} m_2 = |(\varepsilon^4-2\varepsilon^3+2\varepsilon^2-\varepsilon)(\alpha_1^2\alpha_2^3\alpha_4-\alpha_1\alpha_3^3\alpha_4^2)+(2\varepsilon^4+\varepsilon^3-\varepsilon^2-2\varepsilon)(\alpha_2^2\alpha_3\alpha_4^3-\alpha_1^3\alpha_2\alpha_3^2)|$$

$$+|5m(\varepsilon^3-\varepsilon^2)(\alpha_1\alpha_2-\alpha_3\alpha_4)+5m(\varepsilon^4-\varepsilon)(\alpha_1\alpha_3-\alpha_2\alpha_4)| \quad \text{(avec s = 0 ou 1)}$$

3°) Si nous gardons θ_1 et échangeons les autres θ de la façon suivante : nous remplaçons θ_2 par θ_3 , θ_3 par θ_5 , θ_4 par θ_2 , θ_5 par θ_4 , alors M_1 devient M_2,et m_1 devient m_2 , ce qui revient à remplacer, dans l'expression de m_1 , α_i par $\tau^3(\alpha_i)$.

III.2.- Etude des racines multiples de la congruence $f(x) \equiv 0 \pmod{p}$ pour les diviseurs premiers p de $I(\theta)$.

(Rappelons que le polynome fondamental f étudié dans la suite est le polynome donné par la formule (III-1)) .

Proposition III.1 :

La congruence fondamentale $f(x) \equiv 0 \pmod{p}$ n'admet pas de racine multiple d'ordre 3 , pour tout diviseur premier p de $I(\theta)$.

Démonstration :

Supposons que la congruence $f(x) \equiv 0 \pmod{p}$ admette une racine triple a, alors : $f(x) \equiv (x-a)^3 (x-b)(x-c) \pmod{p}$ (p.19), ($b \not\equiv a \not\equiv c \pmod{p}$ et $b \not\equiv c \pmod{p}$ ou $b \equiv c \pmod{p}$) .
Soit $\mathfrak{P}$ l'un quelconque des idéaux premiers , de norme p ; a est racine d'ordre 3 de $\mathfrak{P}$ (proposition II.6) , et en remplaçant éventuellement $\mathfrak{P}$ par l'un de ses conjugués , on peut supposer :

$$\theta_1 \equiv \theta_i \equiv \theta_j \equiv a \ , \quad \theta_h \equiv b \ , \quad \theta_k \equiv c \pmod{\mathfrak{P}}$$
$$2 \le i < j \le 5 \qquad 2 \le h < k \le 5 \ , \ h \overset{i}{\underset{j}{\neq}} k \ .$$

(Remarquons que $\{ \theta_1 , \theta_i , \theta_j , \theta_h , \theta_k \} = \{ \theta_1 , \theta_2 , \theta_3 , \theta_4 , \theta_5 \}$ à l'ordre près) .

Soient : $E_{\mathbb{Q}'}$ l'anneau des entiers du corps $\mathbb{Q}'$

$E_{K\mathbb{Q}'}$ l'anneau des entiers du corps $K\mathbb{Q}'$ (composé de K et $\mathbb{Q}'$)

On désigne par : $\mathfrak{P}_{K\mathbb{Q}'}$ l'idéal engendré par $\mathfrak{P}$ dans $K\mathbb{Q}'$, c'est-à-dire ,

$$\mathfrak{P}_{K\mathbb{Q}'} = \mathfrak{P}E_{K\mathbb{Q}'} = \left\{ \sum_j u_j \xi_j \, , \; u_j \in \mathfrak{P} \, , \; \xi_j \in E_{K\mathbb{Q}'} \right\} \text{ (j en nombre fini),}$$

et on désigne par : $\mathfrak{P}_{\mathbb{Q}'}$ le sous-anneau de $E_{K\mathbb{Q}'}$ constitué par l'ensemble des sommes finies $\sum_j u_j \delta_j$, où $u_j \in \mathfrak{P}$ et $\delta_j \in E_{\mathbb{Q}'}$, donc :

$$\mathfrak{P}_{\mathbb{Q}'} = \left\{ \sum_j u_j \delta_j \, , \; u_j \in \mathfrak{P} \, , \; \delta_j \in E_{\mathbb{Q}'} \right\} \subseteq \mathfrak{P}_{K\mathbb{Q}'} \, .$$

j en nombre fini

Remarquons qu'en général $\mathfrak{P}_{\mathbb{Q}'}$ n'est pas un idéal de $E_{K\mathbb{Q}'}$, car le produit d'un élément de $\mathfrak{P}_{\mathbb{Q}'}$ par un entier de $K\mathbb{Q}'$ n'appartient pas nécessairement à $\mathfrak{P}_{\mathbb{Q}'}$. Mais on démontre que :

- (1) $\mathfrak{P}_{\mathbb{Q}'}$ est un module sur $E_{\mathbb{Q}'}$ et $\mathfrak{P}_{\mathbb{Q}'} \cap E_{\mathbb{Q}'} = pE_{\mathbb{Q}'}$
- (2) si $(D_K , D_{\mathbb{Q}'}) = 1$, $\mathfrak{P}_{\mathbb{Q}'} = \mathfrak{P}_{K\mathbb{Q}'}$

(D_K , $D_{\mathbb{Q}'}$ désignant respectivement les discriminants des corps K et $\mathbb{Q}'$).

Pour démontrer que $\mathfrak{P}_{\mathbb{Q}'} \cap E_{\mathbb{Q}'} = pE_{\mathbb{Q}'}$, on utilise la propriété des degrés :

$$[K\mathbb{Q}' : \mathbb{Q}] = \ell(\ell-1) = [K : \mathbb{Q}] \times [\mathbb{Q}' : \mathbb{Q}] \quad ([2]) \, ,$$

d'où il résulte ([4]) que les extensions K et $\mathbb{Q}'$ de $\mathbb{Q}$ sont linéairement disjointes sur $\mathbb{Q}$; on montre alors que tout $\lambda' \in \mathfrak{P}_{\mathbb{Q}'} \cap E_{\mathbb{Q}'}$ est de la forme : $\lambda' = p\,\delta'$, $\delta' \in E_{\mathbb{Q}'}$; le résultat s'en déduit immédiatement.
Pour démontrer (2) , en invoquant le théorème sur la composition des corps de nombres dont les discriminants sont premiers entre eux ([8] et [9] ou [5]) on montre d'abord que tout élément ξ de $E_{K\mathbb{Q}'}$ s'écrit :

$\xi = \sum_{k=0}^{\ell-2} \alpha_k \varepsilon^k$, $\alpha_k \in E_K$ pour tout k (E_K désignant toujours l'anneau des entiers de K) , puis on montre que $\mathfrak{P}_{K\mathbb{Q}'} \subseteq \mathfrak{P}_{\mathbb{Q}'}$, d'où le résultat.

Considérons les résolvantes de Lagrange :

$$\overline{\theta}_\nu = \sum_{w=1}^{w=5} \varepsilon^{\nu w}\, \theta_{w+1} = \sum_{w=1}^{w=5} \varepsilon^{\nu(w-1)}\, \theta_w$$

$1 \le \nu \le 4$ $\qquad$ $(w+1 \bmod. 5)$

Posons : $\theta_u = a + \alpha_u$ si $u \in \{1, i, j\}$, $\theta_h = b + \alpha_h$, $\theta_k = c + \alpha_k$, avec α_u, α_h, α_k dans $\mathfrak{P}$. Alors $\overline{\theta}_\nu = \omega_\nu + \rho_\nu$, $1 \le \nu \le 4$, où :

$$\omega_\nu = a(1 + \varepsilon^{\nu(i-1)} + \varepsilon^{\nu(j-1)}) + b\,\varepsilon^{\nu(h-1)} + c\,\varepsilon^{\nu(k-1)} \in E_{\mathbb{Q}'}$$

$$\rho_\nu = \alpha_1 + \alpha_i\,\varepsilon^{\nu(i-1)} + \alpha_j\,\varepsilon^{\nu(j-1)} + \alpha_h\,\varepsilon^{\nu(h-1)} + \alpha_k\,\varepsilon^{\nu(k-1)} \in \mathfrak{P}_{\mathbb{Q}'}$$

Les quatre entiers $\nu(i-1)$, $\nu(j-1)$, $\nu(h-1)$, $\nu(k-1)$ sont deux à deux distincts et appartiennent mod. 5 à $\{1, 2, 3, 4\}$, donc :
$1 + \varepsilon^{\nu(i-1)} + \varepsilon^{\nu(j-1)} + \varepsilon^{\nu(h-1)} + \varepsilon^{\nu(k-1)} = \varepsilon^4 + \varepsilon^3 + \varepsilon^2 + \varepsilon + 1 = 0$.
Par suite : $\omega_\nu = (b-a)\,\varepsilon^{\nu(h-1)} + (c-a)\,\varepsilon^{\nu(k-1)}$.

Nous savons que ([16]) :

$\overline{\theta}_1\,\overline{\theta}_4 = \overline{\theta}_2\,\overline{\theta}_3 = 5^{2(1-s)}\, m = \overline{\theta}_\nu\,\overline{\theta}_{\ell-\nu}$, $1 \le \nu \le 2$, (avec $s = 1$ pour un corps unitaire, $s = 0$ sinon).

On a :

$$\overline{\theta}_\nu\,\overline{\theta}_{\ell-\nu} = (\omega_\nu + \rho_\nu)(\omega_{\ell-\nu} + \rho_{\ell-\nu}) = \omega_\nu\,\omega_{\ell-\nu} + (\rho_\nu\,\omega_{\ell-\nu} + \omega_\nu\,\rho_{\ell-\nu} + \rho_\nu\rho_{\ell-\nu})$$

$$= \omega_\nu\,\omega_{\ell-\nu} + \nu_\nu$$

avec $\omega_\nu\,\omega_{\ell-\nu} \in E_{\mathbb{Q}'}$, $\nu_\nu \in \mathfrak{P}_{\mathbb{Q}'}$ (car $\mathfrak{P}_{\mathbb{Q}'}$ est un module sur $E_{\mathbb{Q}'}$).

Alors $\overline{\theta}_1\,\overline{\theta}_4 = \overline{\theta}_2\,\overline{\theta}_3 \Rightarrow \omega_1\,\omega_4 - \omega_2\,\omega_3 = \nu_2 - \nu_1$,

ce qui montre que $\omega_1\,\omega_4 - \omega_2\,\omega_3 \in \mathfrak{P}_{\mathbb{Q}'} \cap E_{\mathbb{Q}'} = pE_{\mathbb{Q}'}$; d'où la congruence dans $E_{\mathbb{Q}'}$: $\omega_1\,\omega_4 - \omega_2\,\omega_3 \equiv 0 \pmod{p}$.

Nous avons :

$$\omega_1\,\omega_4 - \omega_2\,\omega_3 = (b-a)(c-a)\,[\varepsilon^{4h+k} + \varepsilon^{h+4k} - \varepsilon^{2h+3k} - \varepsilon^{3h+2k}]\,.$$

Posons $y = 4h + k \equiv k - h \pmod{5}$, alors $3h + 2k \equiv 2y \pmod{5}$, $2h + 3k \equiv 3y \pmod{5}$, $h + 4k \equiv 4y \pmod{5}$; comme $2 \le h < k \le 5$,

nous avons $1 \leq k-h \leq 3$ et $y \equiv 1$, 2 ou 3 (mod. 5) , il en résulte :

$\varepsilon^y + \varepsilon^{4y} - \varepsilon^{3y} - \varepsilon^{2y} = \pm [\varepsilon^4 - \varepsilon^3 - \varepsilon^2 + \varepsilon]$ (suivant que $y \equiv 1$ (mod. 5) ou $y \equiv 2$ ou 3 (mod. 5)) .

Par suite :

$\omega_1 \omega_4 - \omega_2 \omega_3 \equiv 0$ (mod. p) $\Rightarrow$ (b-a) (c-a) $[\varepsilon - \varepsilon^3 - \varepsilon^2 + \varepsilon] \equiv 0$ (mod.p).

Mais (ε^4 , ε^3 , ε^2 , ε) étant une base sur $\mathbb{Z}$ de $E_{\mathbb{Q}'}$, ces quatre éléments sont linéairement indépendants sur $\mathbb{Z}$, et par conséquent

(b-a) (c-a) $\equiv 0$ (mod. p) .

Or cette dernière congruence est impossible par hypothèse , par suite la congruence fondamentale n'admet pas de racine triple .

Remarque :

La proposition précédente se généralise très simplement dans le cas des corps cycliques de degré premier impair ℓ quelconque sous la forme suivante :

Si p est un diviseur premier de $I(\theta)$, la congruence fondamentale mod. p n'admet pas de racine multiple d'ordre $\ell-2$.

Conséquence de la proposition III.1 :

Si $I(\theta) \equiv 0$ (mod. p) , puisque la somme des ordres de multiplicité des racines de la congruence fondamentale (mod. p) est 5 et que cette congruence n'admet pas de racine triple , alors :

1°) il existe toujours au moins une racine simple

2°) les seuls cas possibles sont :

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

Nous étudions chacun de ces différents cas .

Existence d'une racine double et de trois racines simples pour la congruence fondamentale mod. p .

Proposition III.2 :

Soit p un diviseur premier de $I(\theta) = m_1 \times m_2$.
La congruence fondamentale $f(x) \equiv 0$ (mod. p) admet une racine double et trois racines simples si et seulement si $p \geq 5$ et un seul des deux nombres m_1 , m_2 est divisible par p .

Démonstration :

Condition nécessaire .

Soit p un diviseur premier de $I(\theta)$, on suppose que $f(x) \equiv (x-a)^2 (x-b)(x-c)(x-d)$ (mod. p) , avec , a, b, c, d entiers rationnels deux à deux incongrus mod. p , ce qui entraîne $p \geq 5$.
D'après la proposition II.6, a est racine d'ordre 2 , et b, c, d sont racines d'ordre 1 de l'un quelconque des idéaux premiers $\mathfrak{P}$ de norme p . b, c, d jouant le même rôle et en remplaçant éventuellement l'idéal $\mathfrak{P}$ par un de ses conjugués , nous avons deux cas à considérer :

- $\theta_1 \equiv \theta_2 \equiv a$, $\theta_3 \equiv b$, $\theta_4 \equiv c$, $\theta_5 \equiv d$ (mod. $\mathfrak{P}$)
- $\theta_1 \equiv \theta_3 \equiv a$, $\theta_2 \equiv c$, $\theta_4 \equiv d$, $\theta_5 \equiv b$ (mod. $\mathfrak{P}$) .

Le deuxième cas se déduit du premier en conservant θ_1 et remplaçant θ_2 par θ_3 , θ_3 par θ_5 , θ_4 par θ_2 et θ_5 par θ_4 , ce qui transforme m_1 en m_2 et revient à remplacer α_i par $\tau^3(\alpha_i)$ (p. 51) .

Nous étudions alors uniquement le premier cas :

$$\theta_1 \equiv \theta_2 \text{ (mod. } \mathfrak{P}) \Rightarrow M_1 = \prod_{i=1}^{i=5} (\theta_{i+1} - \theta_i) \in \mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z} ,$$

d'où : $|M_1| = Mm_1 \equiv 0$ (mod. p) et comme $M = \sqrt[4]{D_K} \not\equiv 0$ (mod. p) (proposition II.1) , $m_1 \equiv 0$ (mod. p) .

De plus , les quatre entiers a, b, c, d, étant deux à deux incongrus mod. p , $\theta_{i+2} - \theta_i \notin \mathfrak{P}$ pour tout i , $1 \leq i \leq 5$. Il en résulte :

$M_2 = \prod_{i=1}^{5} (\theta_{i+2} - \theta_i) \notin \mathfrak{P}$, donc $|M_2| = M m_2 \not\equiv 0 \pmod{p}$ et $m_2 \not\equiv 0 \pmod{p}$.

Condition suffisante .

p étant un nombre premier , $p \geq 5$, on suppose $m_1 \equiv 0$ (mod. p) et $m_2 \not\equiv 0$ (mod. p) . Alors $M_1 \equiv 0$ (mod. p) et aussi $M_1 \equiv 0$ (mod. $\mathfrak{P}$) , où $\mathfrak{P}$ est l'un quelconque des idéaux premiers de norme p . L'idéal premier $\mathfrak{P}$ contenant le produit $\prod_{i=1}^{i=5} (\theta_{i+1} - \theta_i)$ contient au moins une des différences $\theta_{i+1} - \theta_i$, et en remplaçant éventuellement $\mathfrak{P}$ par un de ses conjugués , on peut supposer que $\theta_2 - \theta_1 \in \mathfrak{P}$.

Démontrons que , pour tout i , $2 \leq i \leq 5$, $\theta_{i+1} - \theta_i \notin \mathfrak{P}$.

α) $\theta_3 - \theta_2 \notin \mathfrak{P}$ (resp. $\theta_1 - \theta_5 \notin \mathfrak{P}$) sinon $\theta_3 - \theta_1 \in \mathfrak{P}$ (resp. $\theta_2 - \theta_5 \in \mathfrak{P}$) , ce qui n'est pas vérifié , car

$$m_2 \not\equiv 0 \text{ (mod. p)} \Rightarrow M_2 = \prod_{i=1}^{i=5} (\theta_{i+2} - \theta_i) \not\equiv 0 \text{ (mod. p)} \Rightarrow M_2 \not\equiv 0 \text{ (mod. } \mathfrak{P})$$

et $\theta_{i+2} - \theta_i \notin \mathfrak{P}$ pour tout i , $1 \leq i \leq 5$. Donc s'il existe i tel que $\theta_{i+1} - \theta_i \in \mathfrak{P}$, alors i = 3 ou i = 4 . De plus $\mathfrak{P}$ ne contient qu'une seule des deux différences $\theta_4 - \theta_3$ et $\theta_5 - \theta_4$, sinon on aurait $\theta_5 - \theta_3 \in \mathfrak{P}$.

β) $\theta_4 - \theta_3 \notin \mathfrak{P}$. Nous le démontrons par l'absurde : si $\theta_4 - \theta_3 \in \mathfrak{P}$, il existe $(a, b, d) \in \mathbb{Z}^3$ tels que $\theta_1 \equiv \theta_2 \equiv a$, $\theta_3 \equiv \theta_4 \equiv b$, $\theta_5 \equiv d$ (mod. $\mathfrak{P}$) (proposition I.2) et puisque $\theta_3 - \theta_1 \notin \mathfrak{P}$, $\theta_2 - \theta_5 \notin \mathfrak{P}$, $\theta_5 - \theta_3 \notin \mathfrak{P}$, on a , $a \not\equiv b \not\equiv d \not\equiv a$ (mod. p) . Comme dans la démonstration de la proposition III.1 , en posant : $\theta_i = a + \alpha_i$ si i = 1 , 2 , $\theta_i = b + \alpha_i$, si i = 3, 4 , $\theta_5 = d + \alpha_5$, $\alpha_i \in \mathfrak{P}$, $1 \leq i \leq 5$, nous obtenons $\overline{\theta}_\nu = \omega_\nu + \rho_\nu$, $1 \leq \nu \leq 4$, avec :

$$\omega_\nu = a(1+\epsilon^\nu) + b(\epsilon^{2\nu} + \epsilon^{3\nu}) + d\epsilon^{4\nu}$$
$$= (a-d)(1+\epsilon^\nu) + (b-d)(\epsilon^{2\nu} + \epsilon^{3\nu}) \in E_{\mathbb{Q}'}$$

$$\rho_\nu = \sum_{i=1}^{i=5} \epsilon^{\nu(i-1)} \alpha_i \in \mathfrak{P}_{\mathbb{Q}'} .$$

Alors $\overline{\theta}_1 \overline{\theta}_4 = \overline{\theta}_2 \overline{\theta}_3 \Rightarrow \omega_1 \omega_4 - \omega_2 \omega_3 \Rightarrow (a-b)^2 (\epsilon^4 - \epsilon^3 - \epsilon^2 + \epsilon) \equiv 0 \ (p)$

ce qui est impossible puisque $a \not\equiv b \ (\text{mod. } p)$.

Donc, si $\theta_2 - \theta_1 \in \mathfrak{P}$, alors $\theta_4 - \theta_3 \notin \mathfrak{P}$.

γ) $\theta_5 - \theta_4 \notin \mathfrak{P}$. En effet, si $\theta_2 - \theta_1 \in \mathfrak{P}$ et $\theta_5 - \theta_4 \in \mathfrak{P}$, par conjugaison, on aurait :

$\theta_4 - \theta_3 = \sigma^2 (\theta_2 - \theta_1) \in \sigma^2 (\mathfrak{P})$ et $\theta_2 - \theta_1 = \sigma^2 (\theta_5 - \theta_4) \in \sigma^2 (\mathfrak{P})$

ce qui est impossible d'après β), en remplaçant l'idéal $\mathfrak{P}$ par son conjugué $\sigma^2 (\mathfrak{P})$.

Nous avons donc montré que, si $p \geq 5$, $m_1 \equiv 0 \ (\text{mod. } p)$ et $m_2 \not\equiv 0 \ (\text{mod. } p)$, il existe un idéal premier $\mathfrak{P}$, de norme p, tel que:

$$\theta_2 - \theta_1 \in \mathfrak{P}, \ \theta_{i+1} - \theta_i \notin \mathfrak{P}, \ 2 \leq i \leq 5, \ \theta_{i+2} - \theta_i \notin \mathfrak{P}, \ 1 \leq i \leq 5 .$$

Toujours, compte-tenu de la proposition I.2, il existe des entiers rationnels a, b, c, d, deux à deux incongrus mod. p, tels que :

$$\theta_1 \equiv \theta_2 \equiv a, \ \theta_3 \equiv b, \ \theta_4 \equiv c, \ \theta_5 \equiv d \quad (\text{mod. } \mathfrak{P}) .$$

Il en résulte : $f(x) = \prod_{i=1}^{5} (x - \theta_i) \equiv (x-a)^2 (x-b) (x-c) (x-d) \ (\text{mod. } p)$,

ce qui montre que la congruence fondamentale admet une racine double a et trois racines simples.

Remarques :

1°) Il résulte de la démonstration précédente que :

$$\left.\begin{array}{l} \theta_2 \equiv \theta_1 \equiv a \text{ et } \theta_4 \equiv \theta_3 \equiv b \quad (\text{mod. } \mathfrak{P}) \\ \text{ou} \\ \theta_2 \equiv \theta_1 \equiv a \text{ et } \theta_5 \equiv \theta_4 \equiv b \quad (\text{mod. } \mathfrak{P}) \end{array}\right\} \Rightarrow a \equiv b \ (\text{mod. } p)$$

En conservant θ_1 et en remplaçant θ_2 par θ_3, θ_3 par θ_5, θ_4 par θ_2 et θ_5 par θ_4, on en déduit :

$$\left.\begin{array}{l} \theta_3 \equiv \theta_1 \equiv a \text{ et } \theta_2 \equiv \theta_5 \equiv b \quad (\text{mod. } \mathfrak{P}) \\ \text{ou} \\ \theta_3 \equiv \theta_1 \equiv a \text{ et } \theta_4 \equiv \theta_2 \equiv b \quad (\text{mod. } \mathfrak{P}) \end{array}\right\} \Rightarrow a \equiv b \ (\text{mod. } p)$$

2°) Relations vérifiées par les racines a, b, c, d .

On suppose $m_1 \equiv 0 \pmod{p}$ et $m_2 \not\equiv 0 \pmod{p}$.

Nous savons alors que : $f(x) \equiv (x-a)^2 (x-b)(x-c)(x-d) \pmod{p}$,

d'où : $2a + b + c + d \equiv s \pmod{p}$.

Considérons l'idéal premier $\mathfrak{P} = (p, \theta_1 - a, \theta_2 - a, \theta_3 - b, \theta_4 - c)$ $\left(\text{avec } \theta_5 \equiv d \pmod{\mathfrak{P}}\right)$. Nous posons $\theta_i = a + \alpha_i$, si $i = 1, 2$, $\theta_3 = b + \alpha_3$, $\theta_4 = c + \alpha_4$, $\theta_5 = d + \alpha_5$, $\alpha_i \in \mathfrak{P}$, $1 \leq i \leq 5$ et nous calculons (avec les notations de la démonstration de la proposition III.1) $\omega_1 \omega_4 - \omega_2 \omega_3$.

Nous obtenons alors que $\omega_1 \omega_4 - \omega_2 \omega_3 \equiv 0 \pmod{p}$, si et seulement si :

$$(b-a)(c-a) + (c-a)(d-a) - (b-a)(d-a) \equiv 0 \pmod{p} .$$

Existence de deux racines doubles et d'une racine simple pour la congruence fondamentale mod. p .

Proposition III.3 :

Soit p un diviseur premier de $I(\theta)$.

La congruence $f(x) \equiv 0 \pmod{p}$ admet deux racines doubles et une racine simple si et seulement si :

$$\begin{cases} p \neq 2 \text{ et } p \neq 5 \\ m_1 \equiv m_2 \equiv 0 \pmod{p} \\ \sum_{i=1}^{i=4} \alpha_{2i}^2 \, \alpha_{3i} \, \alpha_{4i}^3 \equiv 0 \pmod{p} \end{cases}$$

Démonstration :

Condition nécessaire .

Soit p un diviseur premier de $I(\theta)$.

On suppose que $f(x) \equiv (x-a)^2 (x-b)^2 (x-c) \pmod{p}$ avec :

$$a \not\equiv b \not\equiv c \not\equiv a \pmod{p} \text{ et } 2a + 2b + c \equiv s \pmod{p} .$$

(Remarquons que nécessairement $p \neq 2$) . D'après la proposition II.6 ,

a et b sont racines d'ordre 2 , c est racine d'ordre 1 de l'un quelconque des idéaux premiers divisant pE_K , et parmi ceux-ci, il existe au moins un idéal $\mathfrak{P}$ tel que l'on ait $\theta_1 \equiv a \pmod{\mathfrak{P}}$ et $\theta_i \equiv a$, b, ou c $\pmod{\mathfrak{P}}$ si $i \in \{2, 3, 4, 5\}$.

A priori , il y a 12 cas à envisager . Compte-tenu de la remarque 1°) p. 57 , 4 de ces cas sont impossibles . Par conjugaison, à partir de ces 4 cas , on élimine 4 autres cas . Il reste alors 4 possibilités qui se déduisent de l'une d'elles par conjugaison . Par suite , nous étudions le seul cas :

$$\theta_1 \equiv \theta_2 \equiv a \ , \ \theta_3 \equiv \theta_5 \equiv b \ , \ \theta_4 \equiv c \pmod{\mathfrak{P}} \ .$$

Nous savons que :

$$\theta_1 \equiv \theta_2 \pmod{\mathfrak{P}} \Rightarrow m_1 \equiv 0 \pmod{p} \quad \text{(p. 55)}$$

On montre de même que :

$$\theta_3 \equiv \theta_5 \pmod{\mathfrak{P}} \Rightarrow m_2 \equiv 0 \pmod{p} \ .$$

Posons $\theta_i = a + \alpha_i$ si i = 1 ou 2 , $\theta_i = b + \alpha_i$ si i = 3 ou 5 , $\theta_4 = c + \alpha_4$, $\alpha_i \in \mathfrak{P}$, $1 \leq i \leq 5$. Nous avons : $\overline{\theta}_\nu = \omega_\nu + \rho_\nu$, $1 \leq \nu \leq 4$, avec

$$\omega_\nu = a(1+\epsilon^\nu) + b(\epsilon^{2\nu} + \epsilon^{4\nu}) + c\epsilon^{3\nu}$$
$$= (a-c)(1+\epsilon^\nu) + (b-c)(\epsilon^{2\nu} + \epsilon^{4\nu}) \in E_{\mathbb{Q}'}$$

$$\rho_\nu = \sum_{i=1}^{i=5} \epsilon^{\nu(i-1)} \alpha_i \in \mathfrak{P}_{\mathbb{Q}'} \ .$$

Nous avons $\omega_1\omega_4 - \omega_2\omega_3 = (a-b)(a+b-2c)(\epsilon^4 - \epsilon^3 - \epsilon^2 + \epsilon)$.

Comme $a \not\equiv b \pmod{p}$, $\omega_1\omega_4 - \omega_2\omega_3 \equiv 0 \pmod{p}$ si et seulement si :

$$a + b - 2c \equiv 0 \pmod{p} \ .$$

Donc , si $f(x) \equiv (x-a)^2 (x-b)^2 (x-c) \pmod{p}$,

on a : $\begin{cases} a + b - 2c \equiv 0 \pmod{p} \\ 2a+2b + c \equiv s \pmod{p} \ . \end{cases}$

Il en résulte : $5c \equiv s \pmod{p}$, ce qui montre que $p \neq 5$

(car : si s = 0 , 5 divise D_K et p divise $I(\theta)$ avec $(I(\theta), \sqrt{D_K}) = 1$, donc $p \neq 5$, si s = 1 , puisque $5c \equiv 1 \pmod{p}$, $p \neq 5$) .

Nous avons alors $f(c) \equiv 0 \pmod{p}$ avec $5c - s \equiv 0 \pmod{p}$. La formule (III-1) montre que :

$$5^5 f(c) \equiv -5^{5(1-s)} m \sum_{i=1}^{i=4} \alpha_{2i}^2 \alpha_{3i} \alpha_{4i}^3 \equiv 0 \pmod{p}$$

et comme $p \neq 5$ et p est premier à m (car m divise D_K et p divisant $I(\theta)$ est premier à D_K) , on a :

$$\sum_{i=1}^{i=4} \alpha_{2i}^2 \alpha_{3i} \alpha_{4i}^3 \equiv 0 \pmod{p}$$

Condition suffisante .

Soit p un nombre premier , $p \neq 2$ et $p \neq 5$ tel que

$m_1 \equiv 0 \equiv m_2 \pmod{p}$ et $\sum_{i=1}^{i=4} \alpha_{2i}^2 \alpha_{3i} \alpha_{4i}^3 \equiv 0 \pmod{p}$.

Puisque p divise m_1 (et m_2) , p divise $I(\theta)$ et la congruence $f(x) \equiv 0 \pmod{p}$ admet au moins une racine multiple (proposition II.5) . Compte-tenu des propositions III.1 et III.2 , il y a, a priori, deux possibilités : la congruence $f(x) \equiv 0 \pmod{p}$ admet

- soit deux racines doubles a et b et une racine simple c .
- soit une racine a d'ordre 4 et une racine simple c .

Démontrons que ce deuxième cas est impossible . Puisque , par hypothèse , $p \neq 5$, il existe $\lambda \in \mathbb{Z}$, tel que $5d \equiv s \pmod{p}$.

$\sum_{i=1}^{i=4} \alpha_{2i}^2 \alpha_{3i} \alpha_{4i}^3 \equiv 0 \pmod{p} \Rightarrow 5^5 f(d) \equiv 0 \pmod{p} \Rightarrow f(d) \equiv 0 \pmod{p}$.

Supposons que $f(x) \equiv (x-a)^4 (x-c) \pmod{p}$, avec $4a + c \equiv s \pmod{p}$, $a \not\equiv c \pmod{p}$.

Alors $f(d) \equiv 0 \pmod{p} \Rightarrow d \equiv a$ ou $d \equiv c \pmod{p}$

- si $d \equiv a \pmod{p}$, $4a + c \equiv 4d + c \equiv s \equiv 5d \pmod{p}$

d'où $a \equiv d \equiv c \pmod{p}$, ce qui est impossible .

- si $d \equiv c \pmod{p}$, $4a + c \equiv 4a + d \equiv s \equiv 5d \pmod{p}$,

d'où $4(a-d) \equiv 0 \pmod{p}$ avec $p \neq 2$ par hypothèse ,

donc $a \equiv d \equiv c \pmod{p}$, ce qui est impossible .

Par suite le seul cas possible est :

$$f(x) \equiv (x-a)^2 (x-b)^2 (x-c) \pmod{p} .$$

Corollaire :

Soit p un nombre premier , $p \neq 2$ et $p \neq 5$, tel que : $m_1 \equiv 0 \equiv m_2 \pmod{p}$ et $\sum_{i=1}^{4} \alpha_{2i}^2 \alpha_{3i} \alpha_{4i}^3 \equiv 0 \pmod{p}$, alors la congruence $f(x) \equiv 0 \pmod{p}$ admet deux racines doubles a et b et une racine simple c . Cette dernière est déterminée par :

$$5c \equiv s \pmod{p} .$$

Donc : si $s = 0$, $c \equiv 0 \pmod{p}$; si $s = 1$, c est l'inverse de s mod. p .

Existence d'une racine d'ordre 4 et d'une racine simple pour la congruence fondamentale mod. p .

Remarquons d'abord que , si $I(\theta) \equiv 0 \pmod{2}$, la congruence $f(x) \equiv 0 \pmod{2}$ admet une racine multiple (proposition II.5) et comme , modulo 2 , il n' y a que deux racines incongrues , nécessairement f admet une racine d'ordre 4 et une racine simple .

Il résulte immédiatement des propositions III.2 et III.3:

Proposition III.4 :

Soit p un diviseur premier impair de $I(\theta)$.

La congruence $f(x) \equiv 0 \pmod{p}$ admet une racine d'ordre 4 et une racine simple si et seulement si :

$$\begin{cases} m_1 \equiv 0 \equiv m_2 \pmod{p} \\ \sum_{i=1}^{i=4} \alpha_{2i}^2 \alpha_{3i} \alpha_{4i}^3 \not\equiv 0 \pmod{p} . \end{cases}$$

Dans le cas des corps cycliques de degré 5 , le calcul des polynomes g_h (formule I-3) se fait effectivement en utilisant les formules donnant les produits deux à deux et les carrés des éléments d'une

base d'entiers ([16]) . L'application à ce cas particulier de la proposition II.9 et du théorème II.4 permet alors de construire les approximations p-adiques des racines de f dans $\mathbb{Q}_p$ et d'obtenir des $\mathbb{Z}$-bases des idéaux primaires canoniques $\mathfrak{P}^k$, lorsque $p = N(\mathfrak{P})$ divise $I(\theta)$.

II.3.- Exemples de développements p-adiques des racines du polynome f pour des nombres premiers p divisant $I(\theta)$.

Dans les exemples suivants , nous donnons le discriminant D_K du corps K considéré , le nombre α de $\mathbb{Q}^{(5)}$ utilisé pour construire K , le polynome fondamental f correspondant , la valeur de $I(\theta)$ avec celle de chacun des facteurs m_1 et m_2 , et le début des développements p-adiques des racines Θ_i de f dans $\mathbb{Z}_p$ pour des nombres p divisant $I(\theta)$.

A) Cas où la congruence fondamentale admet une racine d'ordre 4 et une racine simple .

1°) K est le corps unitaire de discriminant $D_K = 151^4$,

$\alpha = -\epsilon^2 + 3\epsilon^3 + 2\epsilon^4$; $f(x) = x^5 - x^4 - 60x^3 + 12x^2 + 784x - 128$

$I(\theta) = 2^9$; $m_1 = 2^3$, $m_2 = 2^6$

Dans $\mathbb{Z}_2$:

$$\Theta_1 = 1 + 0 \times 2 + 0 \times 2^2 + 0 \times 2^3 + \ldots$$
$$\Theta_2 = 0 + 0 \times 2 + 0 \times 2^2 + 1 \times 2^3 + \ldots$$
$$\Theta_3 = 0 + 1 \times 2 + 0 \times 2^2 + 0 \times 2^3 + \ldots$$
$$\Theta_4 = 0 + 0 \times 2 + 1 \times 2^2 + 1 \times 2^3 + \ldots$$
$$\Theta_5 = 0 + 1 \times 2 + 0 \times 2^2 + 1 \times 2^3 + \ldots$$

2°) K est un corps non unitaire de discriminant $D_K = 5^8 \times 61^4$

$\alpha = 3\epsilon^2 + \epsilon^3$; $f(x) = x^5 - 610x^3 + 4880x^2 + 5185x + 976$

$I(\theta) = 2^{11} \times 41$, $m_1 = 2^6 \times 41$, $m_2 = 2^5$

Dans $\mathbb{Z}_2$:

$$\Theta_1 = 0 + 0 \times 2 + 0 \times 2^2 + 0 \times 2^3 + 1 \times 2^4 + \ldots$$
$$\Theta_2 = 1 + 0 \times 2 + 1 \times 2^2 + 0 \times 2^3 + 0 \times 2^4 + \ldots$$
$$\Theta_3 = 1 + 1 \times 2 + 1 \times 2^2 + 0 \times 2^3 + 1 \times 2^4 + \ldots$$
$$\Theta_4 = 1 + 1 \times 2 + 1 \times 2^2 + 0 \times 2^3 + 0 \times 2^4 + \ldots$$
$$\Theta_5 = 1 + 0 \times 2 + 1 \times 2^2 + 1 \times 2^3 + 0 \times 2^3 + \ldots$$

B) Cas où la congruence fondamentale admet deux racines doubles et une racine simple .

3°) K est le corps unitaire de discriminant $D_K = 41^4$

$\alpha = \epsilon^2 + 2\epsilon^3 + 3\epsilon^4$; $f(x) = x^5 - x^4 - 16x^3 - 5x^2 + 21x + 9$

$I(\theta) = 3^3$, $m_1 = 3$, $m_2 = 3^2$.

Dans $\mathbb{Z}_3$:

$$\Theta_1 = 1 + 2 \times 3 + 0 \times 3^2 + 1 \times 3^3 + \ldots$$
$$\Theta_2 = 1 + 1 \times 3 + 0 \times 3^2 + 0 \times 3^3 + \ldots$$
$$\Theta_3 = 0 + 1 \times 3 + 1 \times 3^2 + 2 \times 3^3 + \ldots$$
$$\Theta_4 = 2 + 0 \times 3 + 0 \times 3^2 + 0 \times 3^3 + \ldots$$
$$\Theta_5 = 0 + 1 \times 3 + 0 \times 3^2 + 2 \times 3^3 + \ldots$$

4°) K est un corps non unitaire de discriminant $D_K = 5^8 \times 71^4$

$\alpha = 3\epsilon + \epsilon^2 + 2\epsilon^3$; $f(x) = x^5 - 710x^3 - 3195x^2 + 71710x + 69651$

$I(\theta) = 3^4 \times 1087$, $m_1 = 3 \times 1087$, $m_2 = 3^3$

Dans $\mathbb{Z}_3$:

$$\Theta_1 = 1 + 0 \times 3 + 0 \times 3^2 + 2 \times 3^3 + \ldots$$
$$\Theta_2 = 1 + 1 \times 3 + 1 \times 3^2 + 1 \times 3^3 + \ldots$$
$$\Theta_3 = 2 + 0 \times 3 + 0 \times 3^2 + 0 \times 3^3 + \ldots$$
$$\Theta_4 = 0 + 0 \times 3 + 1 \times 3^2 + 1 \times 3^3 + \ldots$$
$$\Theta_5 = 2 + 0 \times 3 + 0 \times 3^2 + 1 \times 3^3 + \ldots$$

C) Cas où la congruence fondamentale admet une racine double et trois racines simples .

5°) K est le corps de l'exemple 2°) de A) .

Dans $\mathbb{Z}_{41}$:

$$\Theta_1 = 33 + 12 \times 41 + \ldots$$

$$\Theta_2 = 33 + 40 \times 41 + \ldots$$

$$\Theta_3 = 7 + 15 \times 41 + \ldots$$

$$\Theta_4 = 16 + 15 \times 41 + \ldots$$

$$\Theta_5 = 34 + 38 \times 41 + \ldots$$

BIBLIOGRAPHIE

[1] P. APPELL - E. GOURSAT :

Théorie des fonctions algébriques. Tome 1 .
Chelsea Publishing Company, Inc. New York, N.Y.
1976 .

[2] E. ARTIN :

Galois Theory .
Notre-Dame , 1953 .

[3] Z.I. BOREVITCH - I.R. CHAFAREVITCH :

Théorie des nombres .
Gauthier-Villars Paris , 1967 .

[4] N. BOURBAKI :

Eléments de mathématiques, fascicule XI, Algèbre.
Hermann .

[5] D. CHATELAIN :

Bases des entiers des corps composés par des ex - tensions quadratiques de $\mathbb{Q}$.
Fascicule 6 des Annales Scientifiques de l'Université de Besançon, 3^{è} série , Mathématiques , 1973 .

[6] A. CHATELET :

Arithmétique et Algèbre modernes , tome II .
Presses universitaires de France , 1956 .

[7] HASSE :

Zahlentheorie .
Akademie Verlag , Berlin .

[8] HILBERT :

Théorie des corps de nombres algébriques
(théorèmes 87 et 88) .

[9] S. LANG :

Algebraic Numbers . IV. § 1 et 2 .

[10] LELONG-FERRAND-ARNAUDIES :

Cours de mathématiques , tome 1 : algèbre .
Dunod , Paris , 1971 .

[11] T. NAGELL :

Introduction to Number Theory . Uppsala 1951 .

[12] T. NAGELL :

Quelques résultats sur les diviseurs fixes de l'index des nombres entiers d'un corps de nombres algébriques. Arkiv för matematik, Band 6 nr. 15, 1965.

[13] C. PARIS :

C.R.A.S. Paris, t.274, ser.A, p.289-291 , 1972 .

[14] C. PARIS :

C.R.A.S. Paris, t.274, ser.A, p.610-611, 1972 .

[15] C. PARIS :

Approximations p-adiques de certains entiers de degré 3 .
Fascicule 6 des Annales Scientifiques de l'Université de Besançon, 3^{è} série, Mathématiques 1973 .

[16] J.J. PAYAN :

Contribution à l'étude des corps abéliens de degré premier impair .
Annales de l'Institut Fourier, Grenoble , 15 , 2 , (1965) , 133-199 .

[17] P. SAMUEL :

Théorie algébrique des nombres .
Hermann , Paris, 1967 .

Colette PARIS
Faculté des Sciences
Mathématiques
25030 Besançon Cedex