

THÉORIE DES NOMBRES

BESANÇON

Année 1983 - 1984

NON MONOGÉNÉITÉ DE L'ANNEAU DES ENTIERS  
DE CERTAINES EXTENSIONS ABÉLIENNES DE  $\mathbb{Q}$

Marie-Nicole GRAS

Non monogénéité de l'anneau des entiers  
de certaines extensions abéliennes de  $\mathbb{Q}$

par Marie-Nicole GRAS

0) Introduction .

Soit  $E$  un corps de nombres et soit  $Z_E$  l'anneau des entiers de  $E$ . On dit que  $Z_E$  est monogène s'il existe  $\theta \in Z_E$  tel que  $Z_E = \mathbb{Z}[\theta]$ . Par abus, on dit aussi que  $E$  est monogène .

La monogénéité des extensions de  $\mathbb{Q}$  de degré 2, 3 ou 4 a souvent été étudiée ; en degré plus grand, et dans le cas abélien, les seuls corps connus dont l'anneau des entiers soit monogène sont les corps cyclotomiques  $\mathbb{Q}^{(f)} = \mathbb{Q}(\xi)$  et leur sous-corps réel maximal  $\mathbb{Q}(\xi + \xi^{-1})$  ; il est facile de vérifier qu'il en est de même pour le corps ( d'indice 2 dans  $\mathbb{Q}^{(f)}$  si  $f \equiv 0 \pmod{4}$  ) égal à  $\mathbb{Q}(\xi - \xi^{-1})$  .

Dans [G(MN)1], nous avons montré que si  $E/\mathbb{Q}$  est une extension cyclique de degré premier  $\ell \geq 5$ , alors  $Z_E$  n'est pas monogène, sauf si  $E$  est le sous-corps réel maximal d'un corps cyclotomique ( ce qui donne au plus un corps pour  $\ell$  fixé ) .

Dans [G(MN)2], en généralisant la méthode utilisée dans [G(MN)1], nous avons établi une condition nécessaire pour que l'anneau des entiers d'une extension abélienne de  $\mathbb{Q}$  soit monogène ; nous rappelons les principales étapes conduisant à l'énoncé de cette condition nécessaire :

Soit  $E/\mathbb{Q}$  une extension abélienne de degré  $n$ . On suppose que  $Z_E$  est monogène, c'est-à-dire qu'il existe  $\theta \in Z_E$  tel que  $\{1, \theta, \dots, \theta^{n-1}\}$  soit une  $\mathbb{Z}$ -base d'entiers de  $Z_E$ . Dans ce cas, on a :

$$\Delta(\theta) = \prod_{\substack{g, g' \in G \\ g \neq g'}} (\theta^g - \theta^{g'}) = \pm D_E,$$

où  $G = \text{Gal}(E/\mathbb{Q})$  et où  $D_E$  désigne le discriminant de  $E/\mathbb{Q}$  .

Pour tout  $g \in G$ ,  $g \neq 1$ , on pose  $\Delta_g(\theta) = N_{E/\mathbb{Q}}(\theta - \theta^g)$ ; alors  $\Delta(\theta) = \prod_{\substack{g \in G \\ g \neq 1}} \Delta_g(\theta)$ , et l'hypothèse  $Z_E = \mathbb{Z}[\theta]$  entraîne que pour tout  $g, g' \in G$  tels que  $\langle g \rangle = \langle g' \rangle \neq (1)$ , on a  $\frac{\Delta_g(\theta)}{\Delta_{g'}(\theta)} = \pm 1$ . On choisit alors convenablement  $g$  et  $g'$  en fonction de la ramification dans  $E/\mathbb{Q}$ .

Soit  $p$  un nombre premier ne divisant pas  $n$  et ramifié dans  $E/\mathbb{Q}$ . Soit  $e$  l'indice de ramification de  $p$  et soit  $\sigma$  un générateur du groupe d'inertie de  $p$  dans  $E/\mathbb{Q}$ .

On étudie d'abord  $\Delta_{\sigma^x}(\theta)$ ,  $x = 1, \dots, e-1$ . On exprime  $\theta$  sur les  $\chi$ -coordonnées de H.W. Leopoldt [L], et on montre que l'on peut choisir un idéal  $\mathfrak{P}$  de  $\mathbb{Q}^{(f)} \mathbb{Q}^{(n)}$  (où  $f$  désigne le conducteur de  $E$ ) au-dessus de  $p$ , et une uniformisante  $\pi$  en  $\mathfrak{P}$  telle que

$$\Delta_{\sigma^x}(\theta) \equiv \pi^n (1 - \zeta_e^x)^n w \pmod{(\pi^{n+1})},$$

où  $w$  est inversible modulo  $(\pi)$  et ne dépend pas de  $x = 1, \dots, e-1$ , et où  $\zeta_e$  est une racine de l'unité d'ordre  $e$ .

Soit  $d$  un diviseur de  $e$ ,  $d \neq 1$ ; on pose  $\zeta_d = \zeta_e^{e/d}$ ; en choisissant pour  $g$  et  $g'$  deux générateurs quelconques de  $\langle \sigma^{e/d} \rangle$ , on obtient la condition suivante ([G(MN)2], théorème 1) :

Pour que  $Z_E$  soit monogène, il est nécessaire que l'on ait :  
 pour tout nombre premier  $p$  ne divisant pas  $n$ , ramifié dans  $E/\mathbb{Q}$   
 et d'indice de ramification  $e$ ,  
 pour tout diviseur  $d$  de  $e$ ,  $d \neq 1$ ,  
 pour tout  $k$  premier à  $d$ ,

$$(1) \quad \left( \frac{1 - \zeta_d^k}{1 - \zeta_d} \right)^{2n} \equiv 1 \pmod{p \mathbb{Z}[\zeta_d]}.$$

Lorsque  $d$  est impair, on peut choisir  $k = 2$ , et alors il est nécessaire que l'on ait (avec  $p$  et  $d$  comme ci-dessus) :

$$(2) \quad (1 + \zeta_d)^{2n} \equiv 1 \pmod{p\mathbb{Z}[\zeta_d]} .$$

Lorsque  $d = 2, 3, 4$  ou  $6$  , les conditions (1) et (2) sont toujours vérifiées .

Dans [G(MN)2] , nous avons déduit des conditions (1) et (2) que si  $\ell$  est un nombre premier , presque toutes les  $\ell$ -extensions cycliques de  $\mathbb{Q}$  ne sont pas monogènes .

Le présent travail se divise en deux parties :

Dans une première partie , en utilisant toujours ces conditions (1) et (2) , nous montrons qu'il n'existe qu'un nombre fini d'extensions abéliennes monogènes de degré  $n$  fixé , sous la seule condition que ni 2 ni 3 ne divisent  $n$  .

Puis nous montrons ( théorème 2 ) qu'une extension abélienne  $E/\mathbb{Q}$  de degré  $n = m \ell^r$  ,  $\ell$  premier ,  $\ell^r \geq 5$  ,  $m \in \mathbb{N}^*$  , est non monogène dès que les deux conditions suivantes sont vérifiées :

$$(i) \quad \begin{cases} \text{si } \ell = 2 , & 2^{r-2} \geq 2m + 1 \\ \text{si } \ell \text{ est impair ,} & \frac{\ell-1}{2} \ell^{r-1} \geq m + 1 , \end{cases}$$

(ii) il existe un nombre premier  $p$  ,  $p \equiv 1 \pmod{\ell^r}$  ,  $p$  ramifié dans  $E/\mathbb{Q}$  avec un indice de ramification multiple de  $\ell^r$  , et vérifiant  $p > 2n + 1$  .

Pour conclure cette partie , nous précisons les résultats obtenus dans le cas des extensions abéliennes de  $\mathbb{Q}$  de degré  $2 \ell^r$  ,  $3 \ell^r$  ( $\ell$  premier  $\geq 5$ ) et  $5m$  .

Dans une deuxième partie , nous montrons que les sous-corps  $E$  de  $\mathbb{Q}^{(p)}$  ,  $p$  nombre premier impair , ne sont pas monogènes , exceptés les cas déjà connus ( les corps  $\mathbb{Q}^{(p)}$  ,  $\mathbb{Q}_o^{(p)}$  et le sous-corps quadratique de  $\mathbb{Q}^{(p)}$  qui sont monogènes , et si  $p \equiv 1 \pmod{3}$  , le sous-corps cubique de  $\mathbb{Q}^{(p)}$  qui est le seul à pouvoir être ou non monogène ) .

1) Extensions abéliennes de  $\mathbb{Q}$  .

a) Théorème de finitude .

Si  $n$  est un entier divisible par 2 ( resp. 3 ), on peut trouver une infinité d'extensions abéliennes  $E/\mathbb{Q}$  de degré  $n$  dans lesquelles on a un nombre premier  $p$  ne divisant pas  $n$ , ramifié avec un indice de ramification égal à 2 ( resp. 3 ), et pour lequel la condition (1) est donc toujours vérifiée . En effet, soit  $K_n$  le sous-corps de degré  $n$  du composé des  $\mathbb{Z}_\ell$ -extensions de  $\mathbb{Q}$  et soit  $p$  premier,  $p \nmid n$ . Soit  $L_p$  le sous-corps quadratique ( resp. cubique si  $p \equiv 1 \pmod{3}$  ) de  $\mathbb{Q}^{(p)}$ ; alors tout sous-corps  $E$ ,  $E \neq K_n$ , d'indice 2 ( resp. 3 ) de  $K_n L_p$  convient .

Par contre, si  $n$  est premier à 2 et 3, on va montrer le résultat suivant :

Théorème 1 : Soit  $n \in \mathbb{N}$ ,  $n \geq 5$ ,  $n$  premier à 2 et 3 .

Il n'existe qu'un nombre fini d'extensions abéliennes de  $\mathbb{Q}$  de degré  $n$  dont l'anneau des entiers soit monogène .

Définition : L'entier  $n$  étant fixé, soit  $\ell \geq 5$  un nombre premier divisant  $n$  et soit  $\zeta_\ell = \exp(2i\pi/\ell)$  . On pose

$$\mathfrak{P}_\ell = \left\{ p \text{ premier, } p \equiv 1 \pmod{\ell}, \text{ tel que } (1 + \zeta_\ell)^{2n} \equiv 1 \pmod{p \mathbb{Z}[\zeta_\ell]} \right\} .$$

Lemme : L'ensemble  $\mathfrak{P}_\ell$  est fini .

Démonstration du lemme :

On sait que  $\text{Irr}(\zeta_\ell, \mathbb{Q}) = X^{\ell-1} + X^{\ell-2} + \dots + X + 1$ , ce qui

permet d'écrire  $(1 + \zeta_\ell)^{2n} - 1 = \sum_{j=0}^{\ell-2} a_j \zeta_\ell^j$ ,  $a_j \in \mathbb{Z}$ , où les coeffi-

cients  $a_j$  ne sont pas tous nuls, car  $\ell \neq 3$ . On a alors  $(1 + \zeta_\ell)^{2n} \equiv 1 \pmod{p \mathbb{Z}[\zeta_\ell]}$  si et seulement si  $p$  divise tous les  $a_j$ ,  $j = 0, \dots, \ell-2$ . Donc  $\mathfrak{P}_\ell$  est fini, et la méthode pour déterminer  $\mathfrak{P}_\ell$  est effective; elle sera développée au b) .

Démonstration du théorème :

Soit  $E/\mathbb{Q}$  une extension abélienne de degré  $n$ ,  $n$  premier à 2 et 3; tout nombre premier  $\ell$  divisant  $n$  est donc tel que  $\ell \geq 5$  .

On pose  $\mathcal{P}_0 = \{\ell, \ell \mid n\}$ . Pour démontrer le théorème, il suffit de montrer que s'il existe  $p$  premier ramifié dans  $E/\mathbb{Q}$  et tel que  $p \notin \mathcal{P}_0 \cup \left( \bigcup_{\ell \mid n} \mathcal{P}_\ell \right)$ , alors  $Z_E$  n'est pas monogène.

En effet,  $p \notin \mathcal{P}_0$ , donc  $p \nmid n$ ; soit  $e$  l'indice de ramification de  $p$  dans  $E/\mathbb{Q}$ , et soit  $L$  le corps d'inertie de  $p$ ; alors  $E/L$  est cyclique d'ordre  $e$ ,  $p$  est totalement ramifié dans  $E/L$  et  $p \equiv 1 \pmod{e}$ ; puisque  $e \mid n$ , il existe  $\ell' \mid n$  tel que  $\ell' \mid e$  et  $\ell' \geq 5$ ; comme par hypothèse  $p \notin \mathcal{P}_{\ell'}$ ,  $Z_E$  n'est pas monogène d'après (2), puisque  $(1 + \zeta_{\ell'})^{2n} \not\equiv 1 \pmod{p \mathbb{Z}[\zeta_{\ell}]}$ .

La méthode employée montre que les extensions abéliennes de degré  $n$  monogènes ont un conducteur explicitement borné en fonction des  $p \in \mathcal{P}_\ell$ , d'où l'importance de la détermination effective de  $\mathcal{P}_\ell$ . Nous déterminerons d'abord dans un cadre plus général un ensemble  $\mathcal{P}_{m, \ell^r}$  et nous appliquerons les résultats obtenus à la non monogénéité des extensions abéliennes de  $\mathbb{Q}$ .

b) Détermination de l'ensemble  $\mathcal{P}_{m, \ell^r}$ .

Dans ce paragraphe nous étudions les nombres premiers  $p$  vérifiant (1) avec les notations suivantes :

$$(3) \quad \left[ \begin{array}{l} \ell \text{ est un nombre premier, } r, m \in \mathbb{N}^*, \ell^r \geq 5, \\ \zeta_r = \exp(2i\pi/\ell^r), \\ \mathcal{P}_{m, \ell^r} = \left\{ p \text{ premier tel que } \left( \frac{1 - \zeta_r^k}{1 - \zeta_r} \right)^{2m\ell^r} \equiv 1 \pmod{p \mathbb{Z}[\zeta_r]} \right. \\ \left. \text{pour tout } k \text{ premier à } \ell \right\}. \end{array} \right.$$

Si  $p \in \mathcal{P}_{m, \ell^r}$ , on a, pour tout  $k$  premier à  $\ell$ ,

$$(1 - \zeta_r^k)^{2m\ell^r} \equiv (1 - \zeta_r)^{2m\ell^r} \pmod{p \mathbb{Z}[\zeta_r]} ; \text{ on en déduit que}$$

$$(1 - \zeta_r)^{2m\ell^r} \equiv \frac{1}{(\ell-1)\ell^{r-1}} \text{Tr}_{\mathbb{Q}(\zeta_r)/\mathbb{Q}} (1 - \zeta_r)^{2m\ell^r} \pmod{p \mathbb{Z}[\zeta_r]},$$

et donc que (la réciproque étant évidente) :

$$(3') \quad \begin{cases} p \in \mathcal{P}_{m, \ell^r} \text{ si et seulement si il existe } c \in \mathbb{Z} \text{ tel que} \\ (1 - \zeta_r)^{2m \ell^r} \equiv c \pmod{p \mathbb{Z}[\zeta_r]} . \end{cases}$$

Remarque 1 : Pour tout diviseur  $m'$  de  $m$ , si  $p \in \mathcal{P}_{m', \ell^r}$ , alors il est évident que  $p \in \mathcal{P}_{m, \ell^r}$ , et ceci a lieu, en particulier pour tout nombre

$p$  de la forme  $m' \ell^r + 1$  ou  $2m' \ell^r + 1$ . Pour chaque valeur de  $m$  considérée, les nombres premiers  $p$ ,  $p < 2m \ell^r + 1$ , feront l'objet d'une étude à part (voir à ce sujet la proposition 2), et dans la suite on supposera  $p \geq 2m \ell^r + 1$ ; alors les entiers qui interviennent dans le calcul des coef-

ficients du binôme  $\binom{2m \ell^r}{x}$  sont inversibles modulo  $p$ . Avec cette hypothèse on va développer  $(1 - \zeta_r)^{2m \ell^r}$ ; mais si  $\ell$  est impair, on peut aussi utiliser  $(1 + \zeta_r)^{2m \ell^r} \equiv 1 \pmod{p \mathbb{Z}[\zeta_r]}$ , ce qui simplifie les calculs; on va donc distinguer deux cas.

1<sup>er</sup> cas :  $\ell = 2$  (et nécessairement  $r \geq 3$ )

On pose  $N = 2^{r-2}$  et alors  $\text{Irr}(\zeta_r, \mathbb{Q}) = X^{2N} + 1$ ; donc

$$(1 - \zeta_r)^{8mN} = a_0 + \sum_{s=1}^{2N-1} (-1)^s a_s \zeta_r^s, \text{ et (3') entraîne que :}$$

$$a_s \equiv 0 \pmod{p} \text{ pour tout } s = 1, \dots, 2N - 1 .$$

$$\text{On calcule } a_s = \sum_{k=0}^{4m-1} (-1)^k \binom{8mN}{s+2kN}$$

$$= \sum_{j=0}^{2m-1} \left[ \binom{8mN}{s+4jN} - \binom{8mN}{s+(4j+2)N} \right], \quad s = 1, \dots, 2N - 1 .$$

Mais  $a_N = 0$  et  $a_{2N-s} = a_s$ ; on obtient donc  $N - 1$  congruences qui sont :  $a_t \equiv 0 \pmod{N}$ ,  $t = N+1, \dots, 2N - 1$ .

Si  $N \leq 2m$ , on étudie directement les  $N - 1$  congruences ci-dessus. Si  $N > 2m$ , on considère les  $2m$  congruences obtenues pour  $t = N + i$ ,  $i = 1, \dots, 2m$ . Puisque :

$$\binom{8mN}{(4j+2)N+N+i} = \binom{8mN}{8mN-4jN-4N+N-i},$$

on obtient, après renumérotation, les  $2m$  congruences

$$\sum_{j=0}^{2m-1} \left[ \binom{8mN}{4jN+N+i} - \binom{8mN}{4jN+N-i} \right] \equiv 0 \pmod{p}.$$

$$\text{On pose } \delta = \det \left( \binom{8mN}{4jN+N+i} - \binom{8mN}{4jN+N-i} \right)_{\substack{i=1, \dots, 2m \\ j=0, \dots, 2m-1}};$$

si les  $2m$  congruences ci-dessus sont vérifiées, on a  $\delta \equiv 0 \pmod{p}$ .

On applique alors le lemme du e), avec  $\mu = 2m$ ,  $\lambda = 4N$  et  $x = N = 2^{r-2}$ ; il en résulte que si un nombre premier  $p$  divise  $\delta$  et vérifie  $p \geq m2^{r+1} + 1$ , alors  $p$  divise  $(m2^{r+1} + 1)(m2^{r+1} + 2)\dots(m2^{r+1} + 4m - 1)$ ; puisque  $4m - 1 < 2^{r-1}$  et que l'on ne considère que des nombres premiers  $p$ ,  $p \equiv 1 \pmod{2^r}$ , tous les entiers  $m2^{r+1} + 1 + i$  sont inversibles modulo  $p$ , et donc  $p$  divise  $m2^{r+1} + 1$ .

2<sup>ème</sup> cas :  $\ell$  est impair,  $\ell^r \geq 5$ .

On pose  $N = \ell^{r-1}$ , et alors  $\text{Irr}(\zeta_r, \mathbb{Q}) = X^{(\ell-1)N} + \dots + X^N + 1$ ; on écrit  $(1 - \zeta_r)^{2m\ell N} = a_0 + a_1 \zeta_r + \dots + a_{(\ell-1)N-1} \zeta_r^{(\ell-1)N-1}$  dans  $\mathbb{Z}[\zeta_r]$  et (3') entraîne  $a_s \equiv 0 \pmod{p}$ , pour tout  $s = 1, \dots, (\ell-1)N-1$ .

Mais puisque  $\ell$  est impair, on peut utiliser (2) et on a  $(1 + \zeta)^{2m\ell N} \equiv 1 \pmod{p} \mathbb{Z}[\zeta_r]$ . On écrit  $(1 + \zeta_r)^{2m\ell N} = b_0 + b_1 \zeta_r + \dots + b_{(\ell-1)N-1} \zeta_r^{(\ell-1)N-1}$  dans  $\mathbb{Z}[\zeta_r]$  et on a donc :  $b_s \equiv 0 \pmod{p}$ , pour tout  $s = 1, \dots, (\ell-1)N-1$ .

$$\text{Or } b_s = \sum_{k=0}^{2m-1} \binom{2m\ell N}{k\ell N+s} - \sum_{k=0}^{2m-1} \binom{2m\ell N}{k\ell N+(\ell-1)N+\bar{s}}$$

$$\text{et } a_s = \sum_{k=0}^{2m-1} (-1)^{k+s} \binom{2m\ell N}{k\ell N+s} - \sum_{k=0}^{2m-1} (-1)^{k+\bar{s}} \binom{2m\ell N}{k\ell N+(\ell-1)N+\bar{s}},$$

en désignant par  $\bar{s}$  le reste de la division de  $s$  par  $N$ .

$$\text{On pose } c_s = \sum_{k=0}^{2m-1} \binom{2m\ell N}{k\ell N+s} \text{ et } d_s = \sum_{k=0}^{2m-1} (-1)^{k+s} \binom{2m\ell N}{k\ell N+s},$$



$s = 1, \dots, \ell N - 1$  . Alors les congruences ci-dessus entraînent que pour  $s' \equiv s \pmod{N}$  on a  $c_{s'} \equiv c_s \pmod{p}$

et  $d_{s'} \equiv d_s \pmod{p}$  .

$$\text{On écrit alors } c_s = \sum_{j=0}^{m-1} \binom{2m\ell N}{2j\ell N + s} + \sum_{j=0}^{m-1} \binom{2m\ell N}{2j\ell N + \ell N + s}$$

$$\text{et } (-1)^s d_s = \sum_{j=0}^{m-1} \binom{2m\ell N}{2j\ell N + s} - \sum_{j=0}^{m-1} \binom{2m\ell N}{2j\ell N + \ell N + s} ;$$

puisque  $s$  et  $s + \ell N$  sont de parité différente , en faisant la somme et différence des congruences ci-dessus , on obtient , après renumérotation , les congruences suivantes :

$$(4) \quad \left[ \begin{array}{l} \text{Pour tout } t \in \{1, \dots, \ell N - 1, \ell N + 1, \dots, 2\ell N - 1\} \text{ soit} \\ u_t = \sum_{j=0}^{m-1} \binom{2m\ell N}{2j\ell N + t} ; \text{ alors pour } t' \equiv t \pmod{2N} , \text{ on a} \\ u_{t'} \equiv u_t \pmod{p} . \end{array} \right.$$

On écrit les  $m$  congruences obtenues pour  $t = \alpha N + i$  et  $t' = (2\ell - \alpha)N + i$  ,  $i = 1, \dots, m$  , où  $\alpha = (\ell - 1)/2$  , et ceci est possible si  $m \leq \alpha N - 1$  ( sinon , on étudie numériquement les congruences (4) ci-dessus ) .

$$\text{Puisque } \binom{2m\ell N}{2j\ell N + (2\ell - \alpha)N + i} = \binom{2m\ell N}{2m\ell N - 2j\ell N - 2\ell N + \alpha N - i}$$

on obtient , après renumérotation :

$$\sum_{j=0}^{m-1} \left[ \binom{2m\ell N}{2j\ell N + \alpha N + i} - \binom{2m\ell N}{2j\ell N + \alpha N - i} \right] \equiv 0 \pmod{p} .$$

Comme dans le cas  $\ell = 2$  , on pose

$$\delta = \det \left( \binom{2m\ell N}{2j\ell N + \alpha N + i} - \binom{2m\ell N}{2j\ell N + \alpha N - i} \right)_{\substack{i = 1, \dots, m \\ j = 0, \dots, m-1}} ,$$

et on a donc  $\delta \equiv 0 \pmod{p}$  .

On applique le lemme du e) avec  $\mu = m$ ,  $\lambda = 2\ell N$  et  $x = \alpha N = \frac{\ell-1}{2} \ell^{r-1}$ ; il en résulte que si un nombre premier  $p$  divise  $\delta$  et vérifie  $p \geq 2m\ell^r + 1$ , alors  $p$  divise  $(2m\ell^r + 1) \dots (2m\ell^r + 2m - 1)$ ; puisque  $2m - 1 < \frac{\ell-1}{2} \ell^{r-1}$  et que l'on ne considère que des nombres premiers  $p$ ,  $p \equiv 1 \pmod{2\ell^r}$ , on a encore  $p$  divise  $2m\ell^r + 1$ .

On a donc montré :

Proposition 1 : Les notations sont celles définies en (3) .

On suppose de plus que :

(i) si  $\ell = 2$ ,  $2^{r-2} \geq 2m + 1$

(ii) si  $\ell$  est impair,  $\frac{\ell-1}{2} \ell^{r-1} \geq m + 1$  .

Soit  $p$  un nombre premier,  $p \geq 2m\ell^r + 1$  et  $p \equiv 1 \pmod{\ell^r}$ ; si  $p \in \mathcal{P}_{m, \ell^r}$ , alors  $p = 2m\ell^r + 1$  .

Le cas des nombres premiers  $p$ ,  $p \equiv 1 \pmod{\ell^r}$ , tels que  $p < 2m\ell^r + 1$  va être précisé grâce à la propriété suivante :

Proposition 2 : Soit  $p$  un nombre premier,  $p \equiv 1 \pmod{\ell^r}$  .

Si  $p \in \mathcal{P}_{m, \ell^r}$ , alors  $p$  est nécessairement de la forme suivante :

(i) lorsque  $\ell$  est impair :

$$p = 2\ell^r + 1 \text{ ou } p = 2\lambda\ell^r + 1 \text{ avec } (\lambda, m) \neq 1 ,$$

(ii) lorsque  $\ell = 2$  :

$$p = 2^r + 1 \text{ ou } p = 2^{r+1} + 1 \text{ ou } p = \lambda 2^r + 1 , \text{ avec } (\lambda, 2m) \neq 1 .$$

Démonstration : soit  $p$  un nombre premier,  $p \equiv 1 \pmod{\ell^r}$ ; alors  $p$  est totalement décomposé dans  $\mathbb{Q}(\ell^r)$ ; en tout  $\mathfrak{p}$  au-dessus de  $p$  dans  $\mathbb{Q}(\ell^r)$ , le corps résiduel en  $\mathfrak{p}$  est isomorphe à  $\mathbb{F}_p$ . Si  $\ell^r + 1$  (lorsque  $\ell = 2$ ) ou  $2\ell^r + 1$  sont des nombres premiers, ils appartiennent à  $\mathcal{P}_{m, \ell^r}$ ; supposons  $p \neq \ell^r + 1$  et  $p \neq 2\ell^r + 1$ ; alors  $p \notin \mathcal{P}_{1, \ell^r}$ , et donc il existe  $k$  premier à  $\ell$  tel que  $\left(\frac{1 - \zeta_r^k}{1 - \zeta_r}\right)^{2\ell^r} \not\equiv 1 \pmod{p \mathbb{Z}[\zeta_r]}$ ; soit  $h$

l'ordre de l'image de cet élément dans le groupe multiplicatif du corps résiduel en  $p$ . La proposition résulte de ce que :

(i) si  $\ell$  est impair, et si  $p = 1 + 2\lambda\ell^r$ , avec  $(\lambda, m) = 1$ ,  $h$  ne peut pas être un diviseur de  $m$  et donc  $p \notin \mathcal{P}_{m, \ell^r}$ ,

(ii) si  $\ell = 2$  et si  $p = 1 + \lambda 2^r$ , avec  $(\lambda, 2m) = 1$ ,  $h$  ne peut pas être un diviseur de  $m$  et donc  $p \notin \mathcal{P}_{m, 2^r}$ .

Remarque 2 : L'ensemble  $\mathcal{P}_\ell$  du a) est l'ensemble des nombres premiers  $p$ ,  $p \equiv 1 \pmod{\ell}$ , qui appartiennent à  $\mathcal{P}_{m, \ell^r}$ , avec  $r = 1$ .

Si  $\ell \leq 2m + 1$ , on étudie numériquement les congruences (4) :

$$(4') \quad \left[ \begin{array}{l} \text{pour tout } t = 2, \dots, \ell - 2, \text{ on a } u_{t+1} \equiv u_{t-1} \pmod{p}, \text{ avec} \\ u_t = \sum_{j=0}^{m-1} \binom{2m\ell}{2j\ell + t} \end{array} \right.$$

et l'étude du cas  $\ell = 5$  au paragraphe d) montrera qu'il peut exister des nombres premiers  $p \in \mathcal{P}_\ell$  tels que  $p > 2m\ell + 1$ .

Par contre si  $\ell \geq 2m + 3$ , les nombres premiers qui appartiennent à  $\mathcal{P}_\ell$  sont :

ou bien des nombres  $p < 2m\ell + 1$  de la forme  $2\lambda\ell + 1$ ,  $\lambda = 1$  ou  $(\lambda, m) \neq 1$ ,

ou bien le nombre  $2m\ell + 1$ .

Donc si  $\ell \geq 2m + 3$ , les résultats sont plus simples, mais cette hypothèse n'est pas toujours vérifiée, d'où l'intérêt d'avoir la même propriété pour  $\ell^r$  car alors la condition  $(\ell - 1)\ell^{r-1} \geq 2m + 1$  est plus facilement réalisée, mais il faut supposer que le nombre premier  $p$  est ramifié avec un indice de ramification multiple de  $\ell^r$ .

c) Extensions abéliennes de degré  $m\ell^r$ ,  $\ell$  premier,  $\ell^r \geq 5$ .

Soit  $E/\mathbb{Q}$  une extension abélienne de degré  $n$ . Soit  $p$  un nombre premier ne divisant pas  $n$  et ramifié dans  $E/\mathbb{Q}$ . On suppose que l'indice de ramification  $e$  de  $p$  est multiple de  $\ell^r$ ,  $\ell$  premier,  $\ell^r \geq 5$  et on pose  $n = m\ell^r$ .

Pour simplifier, on définit :

(RAM) Définition : on dit que  $p$  vérifie (RAM) si  $p$  est un nombre premier,  $p \equiv 1 \pmod{\ell^r}$ , et s'il est ramifié dans  $E/\mathbb{Q}$  avec un indice de ramification multiple de  $\ell^r$ .

On pose encore  $\zeta_r = \exp(2i\pi/\ell^r)$ . D'après (1) une condition nécessaire pour que  $Z_E$  soit monogène est que pour tout  $p$  vérifiant (RAM) et ne divisant pas  $n$ , on ait  $p \in \mathfrak{P}_{m, \ell^r}$ , (cf. (3)). Il résulte donc des

propositions 1 et 2 :

Théorème 2 : Soit  $E/\mathbb{Q}$  une extension abélienne de degré  $n$ . On suppose que  $n = m\ell^r$ ,  $\ell$  premier,  $\ell^r \geq 5$ , et que :

- (i) si  $\ell = 2$ ,  $2^{r-2} \geq 2m + 1$ ,
- (ii) si  $\ell$  est impair,  $\frac{\ell-1}{2} \ell^{r-1} \geq m + 1$ .

Alors si  $Z_E$  est monogène, tous les nombres premiers  $p$ ,  $p \equiv 1 \pmod{\ell^r}$ , qui se ramifient dans  $E/\mathbb{Q}$  avec un indice de ramification multiple de  $\ell^r$  vérifient  $p \leq 2n + 1$ .

Remarque 3 : Si  $m = 1$  et  $\ell \geq 5$  est premier, la non monogénéité des extensions cycliques de  $\mathbb{Q}$  de degré  $\ell^r$  a été résolue dans [G(MN)1] et [G(MN)2] ; le théorème 2 permet de retrouver que si  $Z_E$  est monogène, seuls les nombres premiers égaux à  $\ell$  ou  $2\ell^r + 1$  peuvent se ramifier totalement dans  $E/\mathbb{Q}$  et le résultat est le même si  $\ell = 3$  et  $r \geq 2$ . Nous allons préciser les résultats complétant le théorème 2, d'abord lorsque  $\ell = 2$ , puis dans le cas du degré  $2\ell^r$  et  $3\ell^r$ ,  $\ell$  premier,  $\ell \geq 5$ . Le cas du degré  $5\ell$  sera traité dans le § e), exemple 1.

- (i) Degré  $n = m2^r$ ,  $r \geq 3$ .

Si  $m = 1$ , le théorème 2 s'applique lorsque  $2^{r-2} \geq 3$ , c'est-à-dire  $r \geq 4$  ; il reste donc à étudier le cas  $n = 8$  et on calcule

$$\binom{16}{1} - \binom{16}{5} + \binom{16}{9} - \binom{16}{13} = 2^7 \cdot 3 \cdot 17. \text{ Donc, dans tous les cas,}$$

si  $Z_E$  est monogène, seuls les nombres  $2^r + 1$  et  $2^{r+1} + 1$ , lorsqu'ils sont premiers, peuvent vérifier (RAM). On remarque aussi que  $2^\lambda + 1$  ne peut être premier que si  $\lambda$  est une puissance de 2 et si le nombre de Fermat correspondant est premier.

Si  $m \geq 2$  et  $n = 8m$ , il existe des nombres premiers  $p$ ,  $p \equiv 1 \pmod{8}$ , tels que  $p > 8m + 1$  et  $p \in \mathcal{P}_{m,8}$ ; en effet, dans ce cas,  $p \in \mathcal{P}_{m,8}$  si et seulement si

$$a(m) = \sum_{j=0}^{2m-1} \left[ \binom{16m}{8j+1} - \binom{16m}{8j+5} \right] \equiv 0 \pmod{p};$$

et on calcule, par exemple :

$$a(2) = 2^{12} \cdot 3 \cdot 17 \cdot \underline{577},$$

$$a(3) = 2^{15} \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot \underline{1153},$$

et  $a(4) = 2^{21} \cdot 3 \cdot 17 \cdot \underline{577} \cdot \underline{665857}$ , d'où les exemples annoncés.

(ii) Degré  $n = 2\ell^r$ ,  $\ell$  premier  $\geq 5$ .

Les hypothèses entraînent que l'extension  $E/\mathbb{Q}$  est cyclique. On désigne par  $L$  le sous-corps quadratique de  $E$  et par  $K$  le sous-corps de  $E$  de degré  $\ell^r$  sur  $\mathbb{Q}$ ; un nombre premier  $p$  vérifie (RAM) si et seulement si  $p$  est totalement ramifié dans  $K/\mathbb{Q}$ .

Le théorème 2 s'applique, sauf si  $r = 1$  et  $\ell = 5$ , et l'étude du cas  $n = 5m$  (cf. § d), montre que si  $m = 2$  alors  $\mathcal{P}_5 = \{11\}$ .

De plus, lorsque  $E$  est non inclus dans  $\mathbb{R}$ , ce qui a lieu si et seulement si  $L$  est imaginaire, alors pour tout  $\theta \in Z_E$ , tous les  $\Delta_K(\theta)$  sont positifs, et une condition nécessaire pour que  $Z_E$  soit monogène est que pour tout  $p$  totalement ramifié dans  $K/\mathbb{Q}$ ,  $p \equiv 1 \pmod{\ell^r}$ , on ait  $(1 + \zeta_p)^{2\ell^r} \equiv 1 \pmod{p} \mathbb{Z}[\zeta_p]$  (au lieu de  $(1 + \zeta_p)^{4\ell^r}$ ); la condition trouvée est celle écrite dans le cas cyclique de degré  $\ell^r$  ([G(MN)2], § 2); elle ne peut avoir lieu que si  $p = 2\ell^r + 1$ . On a donc :

Théorème 3 : Soit  $E/\mathbb{Q}$  une extension cyclique de degré  $2\ell^r$ ,  $\ell$  premier  $\geq 5$ . Soit  $K$  le sous-corps de  $E$  de degré  $\ell^r$  sur  $\mathbb{Q}$ . S'il existe un nombre premier  $p$ ,  $p \equiv 1 \pmod{\ell^r}$ , totalement ramifié dans  $K$  et vérifiant  $p \neq 2\ell^r + 1$  et  $p \neq 4\ell^r + 1$ , alors  $Z_E$  n'est pas monogène.

Si de plus  $E/\mathbb{Q}$  est imaginaire, il suffit alors que  $p$  vérifie  $p \neq 2\ell^r + 1$ .

Remarque 4 : Puisque  $\ell \geq 5$ , en raisonnant modulo 3, on vérifie que le nombre  $2\ell^r + 1$  n'est pas premier si  $r$  est pair ou si  $\ell \equiv 1 \pmod{3}$ , et que le nombre  $4\ell^r + 1$  n'est pas premier si  $r$  est impair et  $\ell \equiv 2 \pmod{3}$ .

Lorsque  $E/\mathbb{Q}$  est imaginaire, on obtient la non monogénéité de certaines extensions sauvagement ramifiées ; en effet, on a :

Proposition 3 : Soit  $E/\mathbb{Q}$  une extension imaginaire cyclique de degré  $2\ell^r$ ,  $\ell$  premier  $\geq 5$ . Si  $\ell$  est totalement ramifié dans  $K/\mathbb{Q}$ , alors  $Z_E$  n'est pas monogène, sauf peut-être dans les deux cas suivants :  $\ell = 5$ ,  $L = \mathbb{Q}(\sqrt{-1})$  et  $\ell = 7$ ,  $L = \mathbb{Q}(\sqrt{-3})$ .

Démonstration : Les hypothèses faites entraînent que  $\ell$  est totalement ramifié dans  $E/L$ . Il en résulte que  $Z_E$  n'est pas monogène sur  $Z_L$  : cette propriété a été démontrée lorsque  $r = 1$  dans [P] et généralisée au cas  $r$  quelconque lorsque  $L = \mathbb{Q}$  dans [G(MN) 2]. Lorsque  $L$  est un corps quadratique imaginaire, les résultats sont les mêmes que lorsque  $r = 1$ . Enfin si  $Z_E$  n'est pas monogène sur  $Z_L$ , il n'est pas monogène sur  $\mathbb{Z}$ , d'où le résultat.

(iii) Degré  $n = 3\ell^r$ ,  $\ell$  premier  $\geq 5$ .

L'extension  $E/\mathbb{Q}$  est encore cyclique et le théorème 2 s'applique sauf si  $r = 1$  et  $\ell = 5$  ou  $7$ . Si  $\ell = 5$ , l'étude du cas  $n = 5m$  du § d) montre que si  $m = 3$ , alors  $\mathcal{P}_5 = \{11, 31\}$ .

Si  $\ell = 7$ , alors  $p \in \mathcal{P}_7$  si et seulement si (cf. (4')) :

$u_1 \equiv u_3 \equiv u_5 \pmod{p}$  et  $u_2 \equiv u_4 \equiv u_6 \pmod{p}$ , avec  $u_t = \binom{42}{t} + \binom{42}{t+14} + \binom{42}{t+28}$  et ces congruences ne permettent pas de former le déterminant d'ordre 3 égal à  $\delta$  ( $\delta$  devrait être construit à partir de  $u_4 - u_2 \equiv 0 \pmod{p}$  et  $u_5 - u_1 \equiv 0 \pmod{p}$ ). Par contre, si on forme un déterminant  $\delta'$  à partir des congruences  $u_4 - u_2 \equiv 0 \pmod{p}$ ,  $u_5 - u_3 \equiv 0 \pmod{p}$  et  $u_6 - u_4 \equiv 0 \pmod{p}$ , on obtient un déterminant d'ordre 3 qui vaut

$$\delta' = \det \left( \binom{42}{i+4+14j} - \binom{42}{i+2+14j} \right)_{i,j=0,1,2}.$$

$$\text{Or } \binom{42}{i+4+14j} - \binom{42}{i+2+14j} = \frac{42 \dots (41-i-14j)}{1 \dots (i+4+14j)} 2 \cdot 43 \cdot (18-i-14j) ;$$

comme dans le e), on met en facteur dans chaque colonne  $\frac{42 \dots (41-14j)}{1 \dots (6+4j)}$ , et ces quantités sont inversibles modulo  $p$ ,  $p \geq 43$ ; on obtient

$$\delta^1 = w \cdot 43^3 \begin{vmatrix} 5 \cdot 6 \cdot 18 & 19 \cdot 20 \cdot 4 & 33 \cdot 34 \cdot (-10) \\ 40 \cdot 6 \cdot 17 & 26 \cdot 20 \cdot 3 & 12 \cdot 34 \cdot (-11) \\ 40 \cdot 39 \cdot 16 & 26 \cdot 25 \cdot 2 & 12 \cdot 11 \cdot (-12) \end{vmatrix}$$

$$= w \cdot 43^3 \cdot 2^7 \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 11^2 \cdot 61, \text{ d'où } \mathfrak{P}_7 = \{43\}; \text{ donc :}$$

**Proposition 4 :** Soit  $E/\mathbb{Q}$  une extension cyclique de degré  $3\ell^r$ ,  $\ell$  premier  $\geq 5$ . Soit  $K$  le sous-corps de  $E$  de degré  $\ell^r$  sur  $\mathbb{Q}$ . S'il existe un nombre premier  $p$ ,  $p \equiv 1 \pmod{\ell^r}$ , totalement ramifié dans  $K/\mathbb{Q}$  et vérifiant  $p \neq 2\ell^r + 1$  et  $p \neq 6\ell^r + 1$ , alors  $Z_E$  n'est pas monogène.

d) Extensions abéliennes de degré  $5m$ ,  $m \in \mathbb{N}^*$ .

Si on reprend les notations du a), et si  $p \in \mathfrak{P}_\ell$ , alors  $(1 + \zeta_\ell)^{2m\ell} \equiv 1 \pmod{p \mathbb{Z}[\zeta_\ell]}$ ; mais  $(1 + \zeta_\ell)^{2m\ell}$  est une unité de  $\mathbb{Q}_0^{(\ell)}$ , ce qui fait que la congruence  $(1 + \zeta_\ell)^{2m\ell} \equiv 1 \pmod{p \mathbb{Z}[\zeta_\ell]}$  a lieu si et seulement si  $(\ell-3)/2$  entiers rationnels sont congrus à zéro modulo  $p$ . Le cas  $\ell = 5$  est donc particulier, car alors  $p \in \mathfrak{P}_5$  si et seulement si  $p$  divise un entier rationnel que l'on va calculer explicitement en fonction de  $m$ .

Soit  $\zeta = \exp(2i\pi/5)$ ; on pose

$$(5) \quad \mathfrak{R}_m = \left\{ p \text{ premier tel que } (1 + \zeta)^{10m} \equiv 1 \pmod{p \mathbb{Z}[\zeta]} \right\}.$$

Au lieu d'exprimer, comme dans b),  $(1 + \zeta)^{10m}$  en fonction des coefficients  $\binom{10m}{x}$ , on va calculer cette quantité en fonction des nombres de Lucas et Fibonacci. En effet, pour tout entier  $m$ , on a

$$(1 + \zeta)^{10m} = (\zeta^2 + \zeta^3)^{10m} = \left( \frac{1 + \sqrt{5}}{2} \right)^{10m} = \frac{L_{10m} + F_{10m} \sqrt{5}}{2},$$

où les suites  $(L_j)_{j \geq 0}$  et  $(F_j)_{j \geq 0}$  sont définies par :

$$\begin{aligned} L_0 &= 2 & L_1 &= 1 & L_{j+2} &= L_{j+1} + L_j & , \\ F_0 &= 0 & F_1 &= 1 & F_{j+2} &= F_{j+1} + F_j & . \end{aligned}$$

Donc  $(1 + \zeta)^{10m} \equiv 1 \pmod{p} \in \mathbb{Z}[\zeta]$  si et seulement si  
 $L_{10m} - 2 \equiv 0 \pmod{p}$  et  $F_{10m} \equiv 0 \pmod{p}$ .

Mais  $\left(\frac{1 + \sqrt{5}}{2}\right)^{10m}$  est une unité de norme 1 de  $\mathbb{Q}(\sqrt{5})$ , et donc  
 $L_{10m}^2 - 5F_{10m}^2 = 4$ ; il en résulte que si  $L_{10m} - 2 \equiv 0 \pmod{p}$ , alors  
 $F_{10m} \equiv 0 \pmod{p}$ ; donc

(6)  $p \in \mathcal{R}_m$  si et seulement si  $p$  divise  $L_{10m} - 2$ .

Les identités vérifiées par les nombres de Lucas et Fibonacci vont permettre de préciser (6). En effet les relations

$$\frac{L_{10m} + F_{10m}\sqrt{5}}{2} = \left(\frac{L_{5m} + F_{5m}\sqrt{5}}{2}\right)^2 \quad \text{et} \quad L_{5m}^2 - 5F_{5m}^2 = 4(-1)^m$$

permettent de montrer que si  $m$  est impair,  $L_{10m} - 2 = L_{5m}^2$  et que si  $m$  est pair,  $L_{10m} - 2 = 5F_{5m}^2$ . D'où, en tenant compte de (2) :

Proposition 5 : Soit  $E/\mathbb{Q}$  une extension abélienne de degré  $5m$ ,  $m \in \mathbb{N}^*$ . Une condition nécessaire pour que  $Z_E$  soit monogène est, que pour tout nombre premier  $p$  ne divisant pas  $m$ ,  $p \equiv 1 \pmod{5}$  et  $p$  ramifié dans  $E/\mathbb{Q}$  avec un indice de ramification multiple de 5, on ait

$p$  divise  $L_{5m}$  si  $m$  est impair,  
 $p$  divise  $F_{5m}$  si  $m$  est pair.

Remarque 5 : En utilisant la relation  $\frac{L_{5m} + F_{5m}\sqrt{5}}{2} = \left(\frac{L_m + F_m\sqrt{5}}{2}\right)^5$ , on montre que :

$$\text{si } m \text{ est impair, } L_{5m} = L_m (5F_m^2 + 5F_m + 1) (5F_m^2 - 5F_m + 1)$$

$$\text{et si } m \text{ est pair } F_{5m} = F_m (L_m^2 + L_m - 1) (L_m^2 - L_m - 1),$$

ce qui permet de factoriser plus facilement  $L_{5m}$  et  $F_{5m}$ .

Si  $m$  varie de 1 à 25, la liste des nombres premiers  $p$ ,  $p \equiv 1 \pmod{10}$ ,  $p \in \mathcal{R}_m$ , est la suivante :



m	p
1	11
2	11
3	11, 31
4	11, 41
5	11, 101, 151
6	11, 31, 61
7	11, 71, 911
8	11, 41, 2161
9	11, 31, 181, 541
10	11, 101, 151, 3001
11	11, 331, 39161
12	11, 31, 41, 61, 2521
13	11, 131, 521, 2081, 24571
14	11, 71, 911, 141961
15	11, 31, 101, 151, 12301, 18451
16	11, 41, 1601, 2161, 3041
17	11, 3571, 1158551, 12760031
18	11, 31, 61, 181, 541, 109441
19	11, 191, 41611, 87382901
20	11, 41, 101, 151, 401, 3001, 570601
21	11, 31, 71, 211, 911, 21211, 767131
22	11, 331, 661, 39161, 474541
23	11, 461, 1151, 5981, 324301, 686551
24	11, 31, 41, 61, 241, 2161, 2521, 20641
25	11, 101, 151, 251, 112128001, 28143378001

Cette table montre qu'il existe des nombres premiers  $p$ ,  $p \equiv 1 \pmod{10}$ ,  $p > 10m + 1$ , tels que  $(1 + \zeta)^{10m} \equiv 1 \pmod{p\mathbb{Z}[\zeta]}$  (cf. remarque 2). Pour les corps correspondants, on a  $\Delta_{2m}(\psi)/\Delta_m(\psi) \equiv 1 \pmod{p}$  pour tout  $\psi \in \mathbb{Z}_E$ . Ces exemples montrent que le résultat trouvé dans la proposition 1 peut être faux si  $\ell$  et  $m$  ne vérifient pas les hypothèses (i) ou (ii).

Pour conclure cette partie, donnons deux exemples qui illustrent à la fois le cas  $5m$  et le théorème de finitude.

Exemple 1 : Soit  $E/\mathbb{Q}$  une extension (cyclique) de degré  $5\ell$ ,  $\ell$  premier  $\geq 7$ . Soit  $K$  le sous-corps de  $E$  de degré 5 sur  $\mathbb{Q}$  et soit  $L$  le sous-corps de  $E$  de degré  $\ell$  sur  $\mathbb{Q}$ .

D'après les résultats concernant le cas "5 m", si  $Z_E$  est monogène, les nombres premiers  $p$  qui peuvent se ramifier dans  $K/\mathbb{Q}$  sont : 5,  $\ell$  (si  $\ell \equiv 1 \pmod{5}$ ), 11 et les  $p$ ,  $p \equiv 1 \pmod{10\ell}$  (cf. prop 2) qui divisent le nombre de Lucas  $L_{5\ell}$ .

D'après le théorème 2, si  $\ell \geq 2 \times 5 + 3 = 13$ , les nombres premiers  $q$  qui peuvent se ramifier dans  $L/\mathbb{Q}$ , si  $Z_E$  est monogène, sont  $q = \ell$ ,  $q = 2\ell + 1$  et  $q = 10\ell + 1$ .

Il reste à étudier les cas  $\ell = 7$  et  $\ell = 11$ .

Si  $\ell = 7$ , on cherche les nombres premiers  $q$ ,  $q \equiv 1 \pmod{70}$  (d'après la proposition 2),  $q \in P_{5,7}$ . D'après (4'),  $q$  divise  $u_6 - u_4$ , avec

$$u_6 = \binom{70}{6} + \binom{70}{20} + \binom{70}{34} + \binom{70}{48} + \binom{70}{62} \quad \text{et}$$

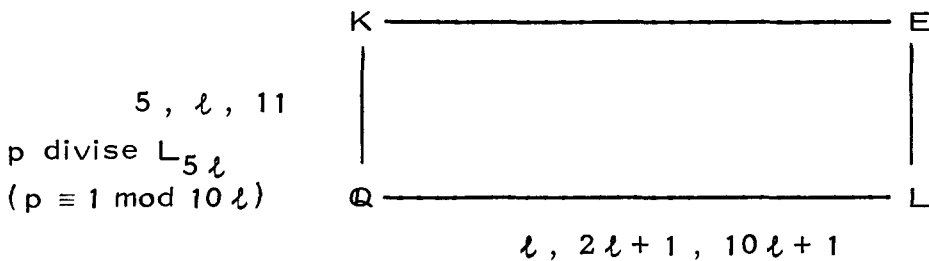
$$u_4 = \binom{70}{4} + \binom{70}{18} + \binom{70}{32} + \binom{70}{46} + \binom{70}{60} ; \quad \text{on calcule}$$

$$\begin{aligned} u_6 - u_4 &= 19519808413970050410 \\ &= 2.3.5.7.67.71.2819.74797.92671, \end{aligned}$$

et le seul nombre premier congru à 1 modulo 70 qui divise  $u_6 - u_4$  est 71. Le résultat est donc le même que dans le cas général.

Si  $\ell = 11$ , alors  $10\ell + 1 = 111$ , et on vérifie numériquement qu'il n'y a pas de nombre premier  $q$ ,  $q > 111$ , qui divise tous les  $u_{t+1} - u_{t-1}$ ,  $t = 2, \dots, 9$  (cf. (4')).

En conclusion, si  $Z_E$  est monogène, les nombres premiers qui peuvent se ramifier dans  $K/\mathbb{Q}$  et  $L/\mathbb{Q}$  sont indiqués sur le schéma ci-dessous :



Exemple 2 : Soit  $E/\mathbb{Q}$  une extension abélienne de degré 125 . Tout nombre premier  $p$  ,  $p \neq 5$  , qui est ramifié dans  $E/\mathbb{Q}$  vérifie  $p \equiv 1 \pmod{5}$  , et l'indice de ramification de  $p$  est multiple de 5 . D'après les résultats obtenus dans la table précédente , avec  $m = 25$  , s'il existe  $p$  ramifié dans  $E/\mathbb{Q}$  ,  $p \neq 5$  , 11 , 101 , 151 , 251 ,  $p_1$  et  $p_2$  , avec  $p_1 = 112128001$  et  $p_2 = 28143378001$  , alors  $Z_E$  n'est pas monogène .

Détaillons le cas cyclique de degré 125 ; les nombres premiers qui peuvent se ramifier dans  $E/\mathbb{Q}$  , si  $Z_E$  est monogène , sont indiqués sur le schéma ci-dessous :

E		Les raisons en sont les suivantes :
	251, 5, 11, 101, 151, $p_1, p_2$	(i) D'après [G(MN)2] , seul 251 peut se ramifier totalement dans $E/\mathbb{Q}$ ;
L		(ii) les nombres premiers suivants ne peuvent pas avoir un indice de ramification égal à 25 :
	251, 5	11 car $11 \not\equiv 1 \pmod{25}$ ,
K		101 et 151 d'après la proposition 2 ;
	251	en effet $101 = 2 \times 50 + 1$ et $(2, 5) = 1$ ,
Q		$151 = 3 \times 50 + 1$ et $(3, 5) = 1$ ;
		$p_1$ et $p_2$ d'après le théorème 2 ; en

effet celui-ci s'applique car  $\ell^r = 25$  ,  $m = 5$  et donc  $\frac{\ell-1}{2} \ell^{r-1} = 10 \geq m+1$ .

e) Calcul d'un déterminant .

Lemme : Soit  $n \in \mathbb{N}^*$  tel que  $2n = \lambda \mu$  ,  $\lambda \geq 2\mu + 2$  , et soit  $x$  vérifiant  $\mu + 1 \leq x \leq \lambda - \mu - 1$  et  $\lambda \neq 2x$  . Soit  $p \geq 2n + 1$  un nombre premier , et soit

$$\delta = \det \left( \binom{2n}{x+i+j\lambda} - \binom{2n}{x-i+j\lambda} \right)_{\substack{i=1, \dots, \mu \\ j=0, \dots, \mu-1}} ;$$

alors  $\delta = w (2n + 1)^\mu \prod_{k=1}^{\mu-1} \left[ (2n + 2k) (2n + 2k + 1) \right]^{\mu-k}$  ,

où  $w$  est inversible modulo  $p$  .

Démonstration : Les hypothèses faites entraînent que

$1 \leq x - i + j \lambda \leq x + i + j \lambda \leq 2n - 1$  pour tout  $i = 1, \dots, \mu$  et  $j = 0, \dots, \mu - 1$ .

Désignons par  $a_{ij}$  le terme général du déterminant  $\delta$ , et pour simplifier, posons  $x' = x + j \lambda$ . En ajoutant à la ligne n°  $i$  une combinaison

linéaire convenable des lignes n° 1 à  $i-1$ , et  $\binom{2i-1}{i}$  fois le terme

$\binom{2n}{x'} - \binom{2n}{x'}$ , on obtient  $\det(a_{ij}) = \det(b_{ij})$ , avec

$$b_{ij} = \sum_{k=0}^{2i-1} \binom{2i-1}{k} \binom{2n}{x'+i-k} - \sum_{k=0}^{2i-1} \binom{2i-1}{k} \binom{2n}{x'-i-k} ;$$

on utilise les relations  $\binom{2n+a}{x' \pm i - k} + \binom{2n+a}{x' \pm i - k - 1} = \binom{2n+a+1}{x' \pm i - k}$ ,

$k, a = 0, \dots, 2i - 2$ , pour en déduire que :

$$b_{ij} = \binom{2n+2i-1}{x'+i} - \binom{2n+2i-1}{x'+i-1} .$$

On calcule

$$b_{ij} = \frac{(2n+2i-1) \dots (2n+i-x')}{1 \dots (x'+i)} - \frac{(2n+2i-1) \dots (2n+i-x'+1)}{1 \dots (x'+i-1)}$$

$$= \frac{(2n+2i-1) \dots (2n+1) 2n \dots (2n-x'+i+1)}{1 \dots (x'+i)} (2n-2x')$$

$$= (2n+2i-1) \dots (2n+1) c(x') f_i(x') , \text{ avec}$$

$$c(x') = \frac{2n \dots (2n-x'+\mu+1)}{1 \dots (x'+\mu)} (2n-2x') \text{ et}$$

$$f_i(x') = [(2n-x'+\mu) \dots (2n-x'+i+1)] [(x'+i+1) \dots (x'+\mu)] .$$

On met en facteur dans chaque ligne le terme  $(2n+2i-1) \dots (2n+1)$ , puis dans chaque colonne le terme  $c(x')$ . Mais toutes les quantités

$\frac{2n \dots (2n-x'+\mu+1)}{1 \dots (x'+\mu)}$  sont inversibles modulo  $p$ , et l'hypothèse  $\lambda \neq 2x$

entraîne  $2n - 2x' = 2n - 2x - 2j \lambda \neq 0$ , et donc  $2(n - x')$  est inversible

modulo  $p$ ; d'où  $\delta = v \left[ \prod_{i=1}^{\mu} (2n+1) \dots (2n+2i-1) \right] \delta'$ , où  $v$  est in-

versible modulo  $p$  et où  $\delta' = \det \left( f_i(x + j \lambda) \right)_{\substack{i=1, \dots, \mu \\ j=0, \dots, \mu-1}}$ .

Or  $(2n - x - j\lambda + k)(x + j\lambda + k) = -(x + j\lambda - n)^2 + (n + k)^2$  ;  
 on pose  $y_j = -(x + j\lambda - n)^2$  et alors  $\delta' = \det(g_i(y_j))$  ,

$$\text{avec } g_i(y_j) = \prod_{k=i+1}^{\mu} (y_j + (n+k)^2)$$

$$= y_j^{\mu-i} + \sum_{k=0}^{\mu-i-1} c_{ik} y_j^{\mu-i-k} , \quad c_{ik} \in \mathbb{N} ,$$

$$\text{et donc } (g_i(y_j)) = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & c_{ik} & \\ & 0 & & & 1 \end{pmatrix} \begin{pmatrix} y_0^{\mu-1} & \dots & y_{\mu-1}^{\mu-1} \\ \vdots & & \vdots \\ y_0 & \dots & y_{\mu-1} \\ 1 & \dots & 1 \end{pmatrix} ;$$

le deuxième déterminant est un déterminant de Vandermonde ; c'est un produit de termes de la forme

$$(x + k\lambda - n)^2 - (x + j\lambda - n)^2 = (k - j)\lambda(2n - 2x - (k + j)\lambda), \quad j \neq k,$$

et l'hypothèse  $\lambda \neq 2x$  entraîne que tous ces termes sont inversibles modulo  $p$  , d'où le résultat .

## 2) Sous-corps de $\mathbb{Q}^{(p)}$ , $p$ premier .

Le cas des sous-corps de  $\mathbb{Q}^{(p)}$  est contenu dans le résultat plus général suivant :

Théorème 4 : Soit  $E/\mathbb{Q}$  une extension cyclique de degré  $n \geq 4$  .

On suppose que tout nombre premier  $p$  ramifié dans  $E/\mathbb{Q}$  vérifie les hypothèses suivantes :  $p \equiv 1 \pmod{n}$  et  $p$  est totalement ramifié dans  $E/\mathbb{Q}$  .

Alors l'anneau des entiers  $Z_E$  de  $E$  n'est pas monogène sauf si

$E = \mathbb{Q}^{(n+1)}$  lorsque  $n+1$  est un nombre premier ,

ou  $E = \mathbb{Q}_0^{(2n+1)}$  lorsque  $2n+1$  est un nombre premier .

Démonstration : On reprend les notations de l'introduction .

On suppose que  $Z_E$  est monogène , et on appelle  $\theta$  un entier de  $E$  tel que  $Z_E = \mathbb{Z}[\theta]$  . Les hypothèses faites entraînent que tous les sous-corps ( différents de  $\mathbb{Q}$  ) de  $E$  ont le même conducteur  $f$  ( égal au produit des nombres premiers ramifiés dans  $E/\mathbb{Q}$  ) , que le discriminant de  $E$  est égal à  $f^{n-1}$  et que pour tout  $g \in \text{Gal}(E/\mathbb{Q})$  ,  $g \neq 1$  ,  $\Delta_g(\theta) = N_{E/\mathbb{Q}}(\theta - \theta^g) = \pm f$  .

Soit  $p$  ,  $p \equiv 1 \pmod{n}$  , l'un des nombres premiers divisant  $f$  ;  $p$  est totalement ramifié dans  $E/\mathbb{Q}$  , donc  $e = n$  , et le groupe d'inertie de  $p$  est égal à  $\text{Gal}(E/\mathbb{Q})$  ; on en désigne toujours par  $\sigma$  un générateur .

En écrivant que tous les rapports  $\Delta_{\sigma^\lambda}(\theta) / \Delta_{\sigma^\mu}(\theta)$  doivent être égaux à  $\pm 1$  , pour  $\lambda , \mu = 1, \dots, n-1$  , on obtient que pour que  $Z_E$  soit monogène , il est nécessaire que pour tout  $k = 1, \dots, n-1$  , on ait

$$\left( \frac{1 - \zeta_n^k}{1 - \zeta_n} \right)^{2n} \equiv 1 \pmod{p\mathbb{Z}[\zeta]} .$$

On pose  $\zeta = \zeta_n = \exp(2i\pi/n)$  , alors pour tout  $k = 1, \dots, n-1$  , on a  $(1 - \zeta^k)^{2n} \equiv (1 - \zeta)^{2n} \pmod{p\mathbb{Z}[\zeta]}$  . Il en résulte qu'il existe  $c \in \mathbb{Z}$  (  $c \equiv \frac{1}{\varphi(n)} \text{Tr}_{\mathbb{Q}^{(n)}/\mathbb{Q}}(1 - \zeta)^{2n} \pmod{p}$  ) , tel que pour tout  $k = 1, \dots, n-1$  ,

on ait :

$$(7) \quad (1 - \zeta^k)^{2n} \equiv c \pmod{p\mathbb{Z}[\zeta]} .$$

Puisque  $p \equiv 1 \pmod{n}$  ,  $p$  est totalement décomposé dans  $\mathbb{Q}^{(n)}$  . Soit  $\mathfrak{p}$  un idéal fixé au-dessus de  $p$  dans  $\mathbb{Q}^{(n)}$  ; on identifie le corps résiduel en  $\mathfrak{p}$  à  $\mathbb{F}_p$  , et on désigne par  $\bar{u}$  l'image de  $u \in \mathbb{Z}[\zeta]$  dans  $\mathbb{F}_p$  .

On considère le polynome

$$P = (1 - X)^{2n} - c \text{ de } \mathbb{Z}[X]$$

et son image  $\bar{P}$  dans  $\mathbb{F}_p[X]$  .

D'après (7) , on a  $\bar{P}(\bar{\zeta}^k) = \bar{0}$  pour tout  $k = 1, \dots, n-1$  . Or  $\bar{\zeta}$  ,  $\bar{\zeta}^2$  ,  $\dots$  ,  $\bar{\zeta}^{n-1}$  sont les  $n-1$  racines ( deux à deux distinctes ) du polynome  $\bar{\phi} = X^{n-1} + X^{n-2} + \dots + X + \bar{1}$  de  $\mathbb{F}_p[X]$  ; donc  $\bar{P} = \bar{\phi} \bar{h}$  dans  $\mathbb{F}_p[X]$  , et donc  $P = \phi h + p h'$  ,  $h , h' \in \mathbb{Z}[X]$  .

Soit  $R$  le reste de la division de  $P$  par  $\phi$  ; on doit avoir

$$\underline{R \equiv 0 \pmod{p\mathbb{Z}[X]} .}$$

Or  $(1 - X)^{2n} = \sum_{j=0}^{2n} (-1)^j \binom{2n}{j}$  . On en déduit que

$$R = a_0 + \sum_{j=1}^{n-2} a_j X^j , \text{ avec pour tout } j \geq 1 ,$$

$$a_j = (-1)^j \left[ \binom{2n}{j} + (-1)^n \binom{2n}{j+n} \right] - \left[ (-1)^{n-1} \binom{2n}{n-1} - \binom{2n}{2n-1} \right] .$$

La suite des calculs est alors analogue au calcul fait lorsque  $n$  est un nombre premier . Il faut distinguer deux cas :

1<sup>er</sup> cas :  $n$  est impair ,  $n = 2t + 1$  ,  $t \geq 2$

On exprime que  $a_t \equiv 0 \pmod{p}$  et  $a_{t-1} \equiv 0 \pmod{p}$  ; on en déduit que

$$u = \binom{2n}{t+1} - \binom{2n}{t} + \binom{2n}{t+2} - \binom{2n}{t-1} \equiv 0 \pmod{p} .$$

$$\text{Or } u = \frac{(4t+2) \dots (3t+4)}{1 \cdot 2 \dots (t+2)} 4(t+1)(2t+1)(4t+3) . \text{ Puisque } p \text{ est un}$$

nombre premier, et que  $p \equiv 1 \pmod{2n}$  , tous les entiers  $\lambda$  ,  $1 \leq \lambda \leq 4t+2$  , sont inversibles modulo  $p$  ; donc  $u \equiv 0 \pmod{p}$  , c'est-à-dire que  $a_t \equiv a_{t-1} \pmod{p}$  si et seulement si  $2n+1 \equiv 0 \pmod{p}$  .

2<sup>ème</sup> cas :  $n$  est pair ,  $n = 2t$  ,  $t \geq 2$

On suppose que  $a_t \equiv 0 \pmod{p}$  et  $a_{t-1} \equiv 0 \pmod{p}$  ; on en déduit que

$$u = \binom{2n}{t} + \binom{2n}{t} + \binom{2n}{t-1} + \binom{2n}{t+1} \equiv 0 \pmod{p} .$$

$$\text{Or } u = \frac{4t \dots (3t+2)}{1 \cdot 2 \dots (t+1)} 2(2t+1)(4t+1) . \text{ Puisque } p \text{ est un nombre pre-}$$

mier, et que  $p \equiv 1 \pmod{n}$  , tous les entiers  $\lambda$  ,  $1 \leq \lambda \leq 2t$  ,  $2t+2 \leq \lambda \leq 4t$  sont inversibles modulo  $p$  ; donc  $u \equiv 0 \pmod{p}$  , c'est-à-dire que  $a_t \equiv a_{t-1} \pmod{p}$  si et seulement si  $(n+1)(2n+1) \equiv 0 \pmod{p}$  .

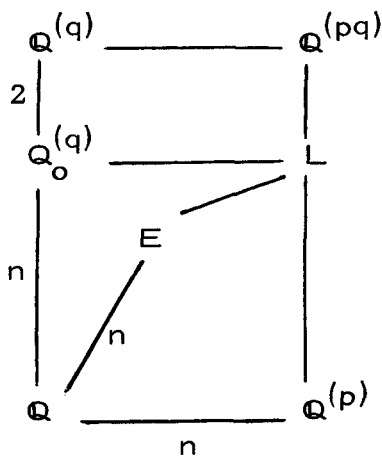
On a donc montré que si  $E/\mathbb{Q}$  vérifie les hypothèses du théorème 4, une condition nécessaire pour que  $Z_E$  soit monogène est que les seuls nombres premiers totalement ramifiés soient égaux à  $n+1$  ou  $2n+1$  ; il y a donc 3 cas :

(i)  $n$  est pair ,  $n+1$  est un nombre premier ,  $2n+1$  ne l'est pas , et alors  $E = \mathbb{Q}^{(n+1)}$  est le seul corps qui convienne .

(ii)  $n$  est pair ou impair,  $2n + 1$  est un nombre premier,  $n + 1$  ne l'est pas, et alors  $E = \mathbb{Q}_0^{(2n+1)}$  est le seul corps qui convienne.

(iii)  $n$  est pair,  $n + 1$  est un nombre premier  $p$ ,  $2n + 1$  est un nombre premier  $q$ , et  $E$  est un sous-corps cyclique de degré  $n$  de  $\mathbb{Q}^{(pq)}$ , avec  $p$  et  $q$  totalement ramifiés dans  $E$  (une telle situation existe : par exemple  $n = 6$ ,  $p = 7$ ,  $q = 13$ ;  $n = 18$ ,  $p = 19$ ,  $q = 37$ ;  $n = 30$ ,  $p = 31$ ,  $q = 61$ ; etc ...). Il reste à montrer que pour cette famille de corps,  $Z_E$  n'est pas monogène.

Montrons d'abord que  $E \not\subset \mathbb{R}$ .



Soit  $\mathbb{Q}_0^{(q)}$  le sous-corps réel maximal de  $\mathbb{Q}^{(q)}$  et soit  $L = \mathbb{Q}_0^{(q)} \mathbb{Q}_0^{(p)}$ .

Soit  $F = E \mathbb{Q}_0^{(p)}$ ; puisque  $p$  et  $q$  sont totalement ramifiés dans  $E$  et que seul  $p$  est ramifié dans  $\mathbb{Q}^{(p)}$ ,  $E \cap \mathbb{Q}^{(p)} = \mathbb{Q}$ , les extensions sont linéairement disjointes, et donc  $[F : \mathbb{Q}] = n^2$ . Mais  $F$  est une extension de  $\mathbb{Q}^{(p)}$ , et  $\mathbb{Q}^{(pq)} / \mathbb{Q}^{(p)}$  qui est cyclique contient une unique sous-extension d'indice 2; donc  $F = L$  et  $E \subset L$ .

Mais pour les mêmes raisons que ci-dessus,  $E$  et  $\mathbb{Q}_0^{(q)}$  sont linéairement disjointes; donc  $L = \mathbb{Q}_0^{(q)} E$ ; puisque  $L = \mathbb{Q}_0^{(q)} \mathbb{Q}_0^{(p)}$ ,  $L \not\subset \mathbb{R}$ ; donc  $E \not\subset \mathbb{R}$ .

Mais, si une extension  $E/\mathbb{Q}$  est telle que  $E \not\subset \mathbb{R}$ , alors pour tout  $k = 1, \dots, n - 1$ , on a  $\Delta_{\sigma^k}(\theta) > 0$  et  $Z_E$  est monogène si et seulement si pour tout  $k = 1, \dots, n - 1$ ,  $\Delta_{\sigma^k}(\theta) = f$ .

On refait un raisonnement analogue au précédent, mais cette fois avec le polynôme  $P = (1 - X)^n - c$ . Avec les mêmes notations que celles du cas  $n = 2t$ , on obtient que  $a_t \equiv a_{t-1} \pmod{p}$  si et seulement si

$$u = \binom{n}{t} + \binom{n}{t-1} \equiv 0 \pmod{p} \text{ . Or } \binom{2t}{t} + \binom{2t}{t-1} = \frac{2t \dots (t+2)}{1 \dots t} (2t+1)$$

et donc si  $E \not\subset \mathbb{R}$ , et si  $Z_E$  est monogène, seul le nombre premier  $n + 1$  peut totalement se ramifier.



Donc pour les extensions vérifiant (iii), on a bien, pour tout  $\psi \in Z_E$ ,  $\Delta_{\sigma^k}^2(\psi) \equiv \Delta_{\sigma^j}^2(\psi) \pmod{q}$ , pour tout  $k, j$  variant de 1 à  $n-1$ , mais on n'a pas  $\Delta_{\sigma^k}(\psi) \equiv \Delta_{\sigma^j}(\psi) \pmod{q}$ , pour tout  $k, j$ . Puisque les extensions (iii) ne sont pas réelles, elles ne sont pas monogènes, ce qui achève la démonstration du théorème 4.

Remarque 6 : Soit  $E/\mathbb{Q}$  une extension cyclique de degré premier  $l \geq 5$ ; si  $E/\mathbb{Q}$  est modérément ramifiée, elle vérifie les hypothèses du théorème 4; si  $E/\mathbb{Q}$  est sauvagement ramifiée, puisque son degré est premier, la démonstration du théorème 4 est encore valable si  $E \not\subset \mathbb{Q}^{(l^2)}$ . On retrouve ainsi le résultat démontré dans [G(MN)1].

Soit maintenant  $E$  un sous-corps de  $\mathbb{Q}^{(p)}$ ,  $p$  nombre premier impair; alors  $E/\mathbb{Q}$  est cyclique et vérifie les hypothèses du théorème 4; il en résulte :

Théorème 5 : Soit  $p$  un nombre premier impair et soit  $E$  un sous-corps de  $\mathbb{Q}^{(p)}$ . Soit  $Z_E$  l'anneau des entiers de  $E$ .

Alors :

(i) Si  $E = \mathbb{Q}^{(p)}$ ,  $\mathbb{Q}_0^{(p)}$ ,  $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2} p})$  ou  $\mathbb{Q}$ , alors  $Z_E$

est monogène ;

(ii) Si  $p \equiv 1 \pmod{3}$  et si  $E$  est le sous-corps cubique de  $\mathbb{Q}^{(p)}$ , alors  $Z_E$  est monogène si et seulement s'il existe  $x, y \in \mathbb{Z}$  tels que  $bx(x^2 - 9y^2) + ay(x^2 - y^2) = 1$ , où  $p = (a^2 + 27b^2)/4$ ,  $a$  et  $b$  de même parité (cf. [G(MN)3]).

(iii) Dans tous les autres cas,  $Z_E$  n'est pas monogène.

BIBLIOGRAPHIE

- [G(MN)1] M.-N. GRAS , Non monogénéité de l'anneau des entiers des extensions cycliques de  $\mathbb{Q}$  de degré premier  $l \geq 5$  ,  
Journal of Number Theory , à paraître .
- [G(MN)2] M.-N. GRAS , Condition nécessaire de monogénéité de l'anneau des entiers d'une extension abélienne de  $\mathbb{Q}$  ,  
Sém. de théorie des Nombres Paris , Birkhäuser , 1984-85 , à paraître .
- [G(MN)3] M.-N. GRAS , Sur les corps cubiques cycliques dont l'anneau des entiers est monogène ,  
C.R. Acad. Sc. Paris, t.278 (1974) , série A , 59-62 .
- [L] H.-W. LEOPOLDT , Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers ,  
J. reine angew. Math., 201 (1979) , 119-149 .
- [P] J.-J. PAYAN , Sur les classes ambiges et les ordres monogènes d'une extension cyclique de degré premier impair sur  $\mathbb{Q}$  ou sur un corps quadratique imaginaire ,  
Arkiv för Math., 11 (1973) , 239-244 .

Marie-Nicole GRAS  
Université de Besançon et C.N.R.S.  
Equipe de Mathématiques  
U.A. n° 040741  
Faculté des Sciences  
F - 25030 BESANÇON CEDEX