THEORIE DES NOMBRES
BESANCON

Années 1984/85-1985/86
Fascicule 2

DETERMINATION NUMERIQUE DU GROUPE D'ARTIN DES EXTENSIONS CYCLIQUES DE $\mathbb{Q}$ A RAMIFICATION DONNEE (PROGRAMME FORTRAN IV - GALCYCL)

Georges GRAS

Détermination numérique du groupe d'Artin des extensions cycliques de $\mathbb{Q}$ à ramification donnée

(Programme FORTRAN IV - GALCYCL)

Georges Gras

Introduction. On se propose de fournir ici un programme FORTRAN IV donnant numériquement, pour tout corps K cyclique sur $\mathbb{Q}$ de conducteur m (i.e. contenu dans le corps $\mathbb{Q}^{(m)}$ des racines m-ièmes de l'unité), le groupe d'Artin $H = Gal(\mathbb{Q}^{(m)}/K)$ ainsi que les différentes classes de $Gal(\mathbb{Q}^{(m)}/\mathbb{Q})$ modulo H (tous les groupes de Galois étant vus à partir de l'isomorphisme canonique $Gal(\mathbb{Q}^{(m)}/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^*$). On sait que cette information numérique est le point de départ indispensable à la recherche pratique de tout "invariant arithmétique" du corps K, dès lors que ce corps a une caractérisation du type "corps de classes" (i.e. comme corps associé à un sous-groupe de $(\mathbb{Z}/m\mathbb{Z})^*$). Par exemple, on pourra déterminer soit les nombres de Bernoulli généralisés de K (si K est imaginaire), soit ses unités cyclotomiques (s'il est réel), en vue de calculer le nombre de classes de K ; l'utilisateur aura la possibilité d'utiliser le programme en question à bien d'autres fins, sans modification (bases d'entiers, sommes de Gauss, décomposition des nombres premiers, fonctions L p-adiques ou non, etc ...).

"Le" corps K (fourni en donnée au programme) sera "défini" par la donnée de son degré, et de la famille des nombres premiers ramifiés avec leurs indices de ramification respectifs ; une telle donnée conduit en général à plusieurs corps K, précisément caractérisés par leurs groupes d'Artin H ; c'est cependant la seule façon pratique de définir K, qui ne suppose pas le problème résolu. Le programme fournit alors toutes les solutions K, et l'ensemble des calculs demandés pour chaque solution.

Pour justifier le programme et permettre au lecteur de le contrôler, nous avons cru bon de rédiger en détail, à la fois la partie théorique, et son aboutissement algorithmique, de telle sorte que ce travail n'apparaisse pas comme destiné aux seuls spécialistes de la théorie algébrique des nombres.

Plan

§1. Etude directe par le corps de classes :

Soit K une extension cyclique de $\mathbb{Q}$ de degré d. On suppose connus, outre le degré d, les nombres premiers ramifiés dans $K/\mathbb{Q}$ ainsi que leurs indices de ramification (la ramification en 2 étant scindée en deux types de ramification). On se propose alors de déterminer explicitement toutes les solutions K en calculant numériquement le conducteur m de K puis $H = Gal(\mathbb{Q}^{(m)}/K)$ comme sous-groupe de $(\mathbb{Z}/m\mathbb{Z})^*$, et les classes de $(\mathbb{Z}/m\mathbb{Z})^*$ modulo H.

On va d'abord rappeler les règles qui assurent l'existence d'un tel corps K au moins (le lecteur voulant omettre cette partie peut reprendre à partir du théorème de la fin du § c, p. 6).

a) Rappels des éléments du corps de classes sur $\mathbb{Q}$ (cf. [1], [2], [3]).
Le conducteur de K est l'entier minimum m tel que $K \subset \mathbb{Q}^{(m)}$. Considérons $G = (\mathbb{Z}/m\mathbb{Z})^*$ et posons

$$m = \prod_{p|m} p^{n(p)} \quad , \quad n(p) \geq 1 \ ;$$

on rappelle que si $2|m$ alors $4|m$.

Soit χ un caractère de degré 1 associé à K (i.e. un caractère de $(\mathbb{Z}/m\mathbb{Z})^*$ à valeurs dans $\mathbb{C}^\times$, dont le noyau est $H = Gal(\mathbb{Q}^{(m)}/K)$) ; on sait que l'ensemble $\{\chi^a$, a mod d, $(a, d) = 1\}$ caractérise K.

Puisque $m = \prod_{p|m} p^{n(p)}$, on a $(\mathbb{Z}/m\mathbb{Z})^* \simeq \prod_{p|m} (\mathbb{Z}/p^{n(p)}\mathbb{Z})^*$; on a donc, en désignant de façon générale par $(\mathbb{Z}/q\mathbb{Z})^{*\perp}$ le groupe des caractères de $(\mathbb{Z}/q\mathbb{Z})^*$, l'isomorphisme canonique $(\mathbb{Z}/m\mathbb{Z})^{*\perp} \simeq \prod_{p|m} (\mathbb{Z}/p^{n(p)}\mathbb{Z})^{*\perp}$. On peut ainsi écrire tout caractère χ de $(\mathbb{Z}/m\mathbb{Z})^*$ sous la forme $\chi = (\ldots, \chi_p, \ldots)$, $\chi_p \in (\mathbb{Z}/p^{n(p)}\mathbb{Z})^{*\perp}$.

Précisons ces isomorphismes en vue du calcul numérique : on peut écrire $G = (\mathbb{Z}/m\mathbb{Z})^* = \bigoplus_{p|m} G_p$ (somme directe interne), où les G_p correspondent aux sous-groupes $\mathrm{Gal}(\mathbb{Q}^{(m)}/\mathbb{Q}^{(m/p^{n(p)})}) \simeq \mathrm{Gal}(\mathbb{Q}^{(p^{n(p)})}/\mathbb{Q})$; posons pour simplifier $m_p = p^{n(p)}$ et ${}_pm = m/m_p$, pour tout $p|m$;

on a alors :

$$G_p = \{a \in (\mathbb{Z}/m\mathbb{Z})^*,\ a \equiv 1 \bmod {}_pm\}.$$

On a de même $(\mathbb{Z}/m\mathbb{Z})^{*\perp} = \bigoplus_{p|m} G_p^{\perp}$, où les éléments de $G_p^{\perp}$ (notés encore χ_p) sont les caractères de $(\mathbb{Z}/m\mathbb{Z})^*$ qui sont triviaux sur $\bigoplus_{q\neq p} G_q \simeq \mathrm{Gal}(\mathbb{Q}^{(m)}/\mathbb{Q}^{(m_p)})$; ce sont donc par définition des caractères de $\mathbb{Q}^{(m_p)}$, et tout caractère χ de $(\mathbb{Z}/m\mathbb{Z})^*$ s'écrit de façon unique

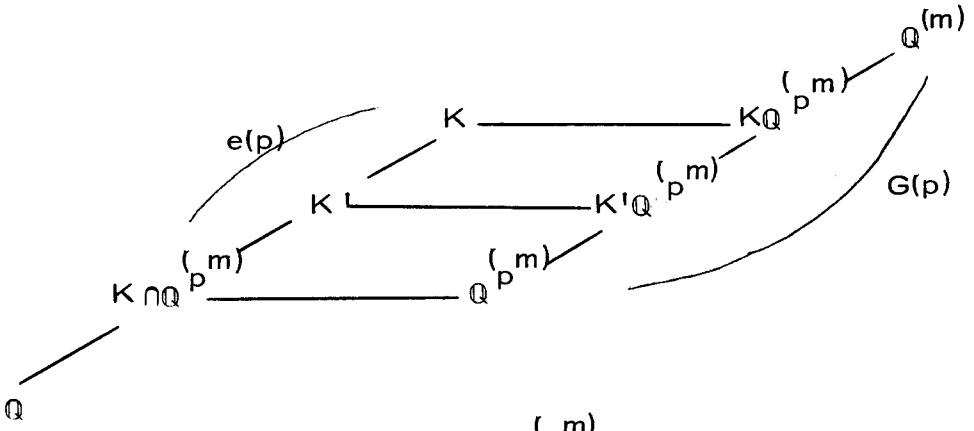
$$\chi = \prod_{p|m} \chi_p\ ,\ \chi_p \in G_p^{\perp} \text{ pour tout } p|m.$$

b) Caractères et ramification. Relativement au caractère χ associé à K, posons une fois pour toutes $\chi = \prod_{p|m} \chi_p$, $\chi_p \in G_p^{\perp}$ pour tout $p|m$, et appelons $e(p)$, $e(p)|d$, $e(p)>1$, les indices de ramification, dans $K/\mathbb{Q}$, des $p|m$.

Proposition 1. Soit $K/\mathbb{Q}$ une extension cyclique de degré d de $\mathbb{Q}$, de conducteur $m = \prod_{p|m} m_p$, $m_p = p^{n(p)}$, $n(p)\geq 1$, de caractère $\chi = \prod_{p|m} \chi_p$, et soient $e(p)|d$ les indices de ramification dans $K/\mathbb{Q}$ des $p|m$; pour $p\neq 2$, posons $e(p) = \bar{e}(p)\, p^{\lambda(p)}$, $p \nmid \bar{e}(p)$, $\lambda(p)\geq 0$. Alors $n(p) = \lambda(p)+1$ et $\bar{e}(p)\,|\,p-1$; enfin χ_p est d'ordre $e(p)$ $(p\neq 2)$.

Démonstration.

Considérons le schéma suivant $(p\neq 2)$:



Comme $p\nmid {}_pm$, p est non ramifié dans $\mathbb{Q}^{({}_pm)}/\mathbb{Q}$, donc en particulier dans

$K \cap \mathbb{Q}^{(p^m)}/\mathbb{Q}$; comme de plus $\mathbb{Q}^{(m_p)}/\mathbb{Q}$ et $\mathbb{Q}^{(p^m)}/\mathbb{Q}$ sont linéairement disjointes, p est totalement ramifié dans $\mathbb{Q}^{(m)}/\mathbb{Q}^{(p^m)}$, ce qui fait que $K \cap \mathbb{Q}^{(p^m)}$ est le corps d'inertie pour p dans $K/\mathbb{Q}$; on a donc $[K\mathbb{Q}^{(p^m)} : \mathbb{Q}^{(p^m)}] = e(p) = \bar{e}(p)\, p^{\lambda(p)}$. Comme le sous-corps de $\mathbb{Q}^{(m)}$ de degré $p^{\lambda(p)}$ sur $\mathbb{Q}^{(p^m)}$ est unique (car $\mathrm{Gal}(\mathbb{Q}^{(m)}/\mathbb{Q}^{(p^m)})$ est cyclique sous l'hypothèse $p \neq 2$), il en résulte que $n(p) = \lambda(p)+1$ (sinon $K\mathbb{Q}^{(p^m)}$, donc K, serait contenue dans $\mathbb{Q}^{(m/p)}$, ce qui est contraire à la définition du conducteur). On en déduit aussi la relation $\bar{e}(p) \mid p-1$.

Montrons que χ_p est d'ordre e(p) : on sait que χ_p est trivial sur $\mathrm{Gal}(\mathbb{Q}^{(m)}/\mathbb{Q}^{(m_p)})$; si on écrit $\chi = \chi_p \psi$ ($\psi = \prod_{q \neq p} \chi_q$), ψ est trivial sur $\mathrm{Gal}(\mathbb{Q}^{(m)}/\mathbb{Q}^{(p^m)})$; comme χ est trivial sur $\mathrm{Gal}(\mathbb{Q}^{(m)}/K)$, on a aussi χ_p trivial sur $\mathrm{Gal}(\mathbb{Q}^{(m)}/K\mathbb{Q}^{(p^m)})$ et c'est donc un caractère de $\mathrm{Gal}(K\mathbb{Q}^{(p^m)}/\mathbb{Q}^{(p^m)})$ donc de $\mathrm{Gal}(K/K \cap \mathbb{Q}^{(p^m)})$ de façon canonique. Si χ_p était d'ordre inférieur à e(p) (donc diviseur strict de e(p)), χ_p serait trivial sur le groupe de Galois de K par rapport à un sous-corps K' tel que $K \cap \mathbb{Q}^{(p^m)} \subset K' \subsetneq K$. Donc χ_p serait un caractère de $K'\mathbb{Q}^{(p^m)}$; comme ψ est trivial sur $\mathrm{Gal}(\mathbb{Q}^{(m)}/\mathbb{Q}^{(p^m)})$ il en résulterait que χ serait un caractère de K', ce qui n'est pas, d'où le résultat.

Proposition 2. Soit $K/\mathbb{Q}$ une extension cyclique de degré d de $\mathbb{Q}$, de conducteur m, de caractère $\chi = \prod_{p \mid m} \chi_p$, et soient $e(p) \mid d$ les indices de ramification des $p \mid m$. On suppose que 2 est ramifié dans $K/\mathbb{Q}$. Alors χ_2 se décompose de façon unique sous la forme γc, où γ provient, dans l'isomorphisme $\mathrm{Gal}(\mathbb{Q}^{(m)}/\mathbb{Q}^{(2^m)}) \simeq \mathrm{Gal}(\mathbb{Q}^{(m_2)}/\mathbb{Q})$, d'un caractère du sous-corps réel maximal $\mathbb{Q}_+^{(m_2)}$ de $\mathbb{Q}^{(m_2)}$, et où c provient d'un caractère de $\mathbb{Q}^{(4)} = \mathbb{Q}(i)$. On définit les indices de γ et c-ramification par $e^{\gamma}(2)$ = ordre de γ et $e^{c}(2)$ = ordre de c. Alors la 2-partie m_2 de m est $2^{n(2)} = 4\, e^{\gamma}(2)$, quel que soit c.

Démonstration.

Si la composante G_2 est cyclique, c'est que $n(2) = 2$; sinon G_2 est somme directe de deux groupes cycliques (l'un d'ordre 2 et le second d'ordre $2^{n(2)-2}$). Considérons les schémas suivants :

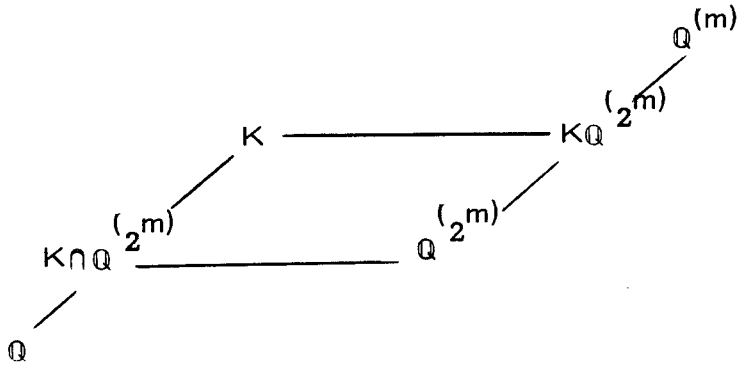


Schéma I

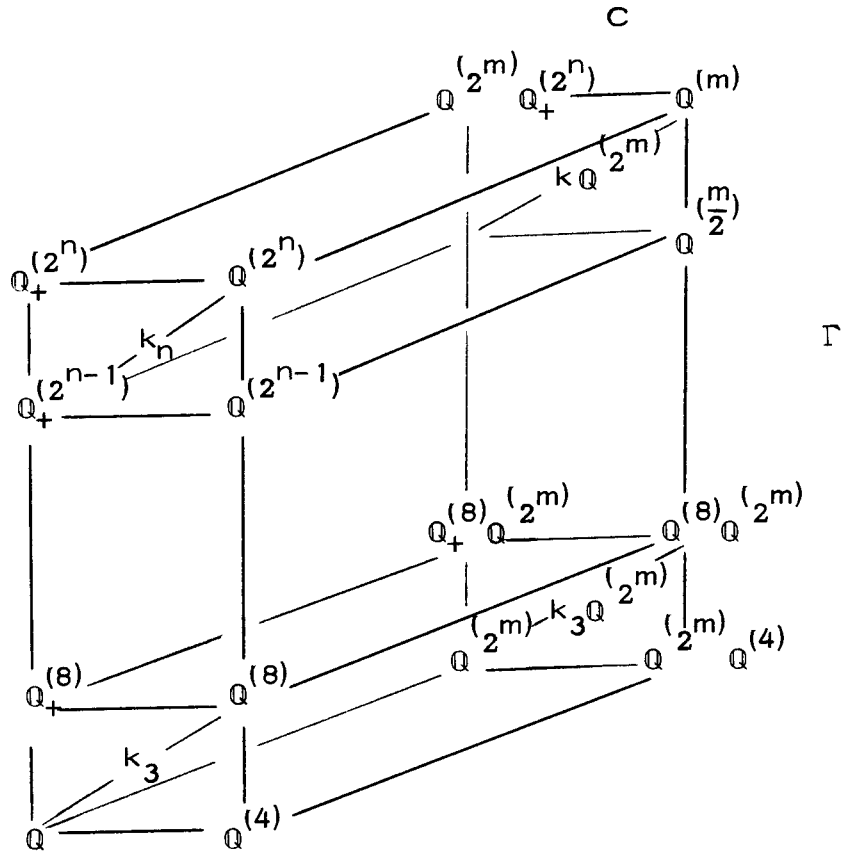


Schéma II

Pour simplifier on a posé $n(2)=n$ dans le schéma

Posons $\Gamma=Gal(\mathbb{Q}^{(m)}/\mathbb{Q}^{(2^m)}\mathbb{Q}^{(4)})$ et $C=Gal(\mathbb{Q}^{(m)}/\mathbb{Q}^{(2^m)}\mathbb{Q}_+^{(2^{n(2)})})$; on a donc $G_2=\Gamma\oplus C$ et $G_2^{\perp}=\Gamma^{\perp}\oplus C^{\perp}$.

Le composé $K\mathbb{Q}^{(2^m)}$ est donc de l'une des formes suivantes :

- si $n(2)=2$, c'est $\mathbb{Q}^{(2^m)}\mathbb{Q}^{(4)}$,
- si $n(2)\geq 3$, c'est le composé de $\mathbb{Q}^{(2^m)}$ avec l'un des corps $\mathbb{Q}_+^{(m_2)}$ ou $k_{n(2)}$ (car $K\mathbb{Q}^{(2^m)}/\mathbb{Q}^{(2^m)}$ est cyclique par hypothèse puisque $K/\mathbb{Q}$ l'est).

Dans la décomposition $G_2^{\perp} = \Gamma^{\perp} \oplus C^{\perp}$, écrivons $\chi_2 = \gamma c$, avec $\gamma \in \Gamma^{\perp}$ et $c \in C^{\perp}$ (γ est donc trivial à la fois sur C et sur $Gal(\mathbb{Q}^{(m)}/\mathbb{Q}^{(m_2)})$ tandis que c est trivial sur Γ et sur $Gal(\mathbb{Q}^{(m)}/\mathbb{Q}^{(m_2)})$). On appelle $e^{\gamma}(2)$ et $e^{c}(2)$ les ordres respectifs de γ et c. Examinons les trois cas possibles, en vue de relier $m_2 = 2^{n(2)}$ avec $e^{\gamma}(2)$ et $e^{c}(2)$:

(i) $K\mathbb{Q}^{(2m)} = \mathbb{Q}^{(2m)}\,\mathbb{Q}_+^{(m_2)}$ $\qquad (n(2) \geq 3)$;

(ii) $K\mathbb{Q}^{(2m)} = \mathbb{Q}^{(2m)}\,k_{n(2)}$ $\qquad (n(2) \geq 3)$;

(iii) $K\mathbb{Q}^{(2m)} = \mathbb{Q}^{(2m)}\,\mathbb{Q}^{(4)}$ $\qquad (n(2) = 2)$.

En utilisant le fait que $m_2 = 2^{n(2)}$ est la 2-participation au conducteur et en utilisant le schéma II, on obtient :

cas (i) : $\chi_2 = \gamma$ et $2^{n(2)} = 4\, e^{\gamma}(2)$ (on a $e^{c}(2) = 1$, car $c = 1$) ;

cas (ii) : $\chi_2 = \gamma c$ et $2^{n(2)} = 4\, e^{\gamma}(2)$ ($e^{\gamma}(2) = 2^{n(2)-2}$ et $e^{c}(2) = 2$) ;

cas (iii) : $\chi_2 = c$ et $2^{n(2)} = 4 = 4 e^{\gamma}(2)$ ($e^{\gamma}(2) = 1$, $e^{c}(2) = 2$).

On a donc bien dans tous les cas $2^{n(2)} = 4\, e^{\gamma}(2)$. Remarquons que e(2) n'est pas le produit $e^{\gamma}(2)\, e^{c}(2)$ mais que l'on a $e(2) = p.p.c.m.\ (e^{\gamma}(2), e^{c}(2))$.

Corollaire. Sous les hypothèses des propositions 1 et 2, on a $p.p.c.m._{p \mid m}\ (e(p)) = d$.

En effet, soit ℓ un nombre premier divisant d, et soit K_ℓ le sous-corps de K tel que $[K_\ell : \mathbb{Q}]$ soit la puissance de ℓ maximum qui divise d, on sait qu'il existe un nombre premier totalement ramifié dans $K_\ell/\mathbb{Q}$. Ceci conduit immédiatement au résultat.

c) Etude de la réciproque. Nous allons vérifier que les propositions précédentes conduisent bien à une condition nécessaire et suffisante pour l'existence de corps K à ramification donnée ; nous donnerons aussi le conducteur de ces corps K, ainsi que le nombre de solutions à attendre. En vue de l'aboutissement numérique nous utilisons des notations appropriées à partir de maintenant.

Théorème. Soit $d > 1$ un entier. Soient $p_1, \ldots, p_k$, $k > 0$ nombres premiers, et $e_1, \ldots, e_k$, k entiers strictement positifs. On convient du fait que les p_i impairs sont distincts et que les e_i correspondants sont différents de 1 ; si 2 est dans la liste des p_i, alors on suppose que $p_1, \ldots, p_{k-2}$ sont impairs, que $p_{k-1} = p_k = 2$ et que e_{k-1} et e_k ne sont pas tous deux égaux à 1.

Alors une condition nécessaire et suffisante pour qu'il existe au moins un corps K, cyclique de degré d sur $\mathbb{Q}$, tel que $\{p_1,\dots,p_k\}$ soit exactement l'ensemble des nombres premiers ramifiés dans $K/\mathbb{Q}$ avec les indices de ramification respectifs $e_1,\dots,e_k$ (e_{k-1} et e_k représentant respectivement la γ et la c-ramification lorsque $p_{k-1}=p_k=2$), est que l'on ait les deux conditions suivantes :

(i) $e_i \mid d$, et si on pose $e_i = \bar{e}_i\, p_i^{\lambda_i}$, $p_i \nmid \bar{e}_i$, $\lambda_i \geq 0$, alors $\bar{e}_i \mid p_i - 1$, pour tout $i = 1,\dots,k$;

(ii) $\underset{i=1,\dots,k}{\text{p. p. c. m.}}\,(e_i) = d$.

Si ces conditions sont réalisées, alors le conducteur commun m des corps K solutions est :

$$m = \prod_{i=1}^{k} p_i^{\lambda_i+1}, \text{ si 2 n'est pas ramifié dans } K/\mathbb{Q}\ (n(p_i)=\lambda_i+1),$$

$$m = \Big(\prod_{i=1}^{k-2} p_i^{\lambda_i+1}\Big)\, 4\, e_{k-1} \text{ sinon } (n(p_i)=\lambda_i+1,\ 1\leq i\leq k-2\ ;\ n(2)=\lambda_{k-1}+2).$$

Enfin, le nombre de corps K solutions est égal à $\dfrac{\varphi(e_1)\dots\varphi(e_k)}{\varphi(d)}$, en désignant par φ la fonction d'Euler.

Démonstration.

Montrons la condition suffisante (la condition nécessaire résultant des propositions 1 et 2 ainsi que de leur corollaire).

Soit m l'entier défini à la fin de l'énoncé ; c'est un conducteur de corps cyclotomique ; posons $n_i = n(p_i)$, pour $1\leq i\leq k$, considérons, pour chaque $p_i \mid m$, $G_i = \mathrm{Gal}(\mathbb{Q}^{(m)}/\mathbb{Q}^{(p_i^{n_i})})$ avec la convention $G_{k-1}=\Gamma$, $G_k = C$ si 2 est ramifié, et distinguons deux cas :

(i) Si $p_i \neq 2$, G_i est cyclique d'ordre $p_i^{n_i-1}(p_i-1)$, et il existe un caractère χ_i, trivial sur $\mathrm{Gal}(\mathbb{Q}^{(m)}/\mathbb{Q}^{(m_{p_i})})$ d'ordre e_i, car par hypothèse $e_i = \bar{e}_i\, p_i^{\lambda_i}$ avec $\bar{e}_i \mid p_i-1$ et $\lambda_i = n_i - 1$ précisément ;

(ii) si $p_{k-1}=p_k=2$, alors $2^{n_{k-1}} = 2^{n_k} = 4\, e_{k-1}$; considérons alors $\mathrm{Gal}(\mathbb{Q}^{(m)}/\mathbb{Q}^{(2^m)}) = G_{k-1}\oplus G_k$. En utilisant à nouveau le schéma II, on voit que l'on peut choisir $\chi_{k-1}=\gamma$ et $\chi_k = c$ d'ordres respectifs e_{k-1} et e_k et tels que χ_{k-1} soit un caractère de $G_{k-1}=\Gamma$ et χ_k un caractère de $G_k = C$ (l'un des deux caractères pouvant être trivial).

Considérons alors $\chi = \prod_{i=1}^{k} \chi_i$ et soit H le noyau de χ dans $(\mathbb{Z}/m\mathbb{Z})^*$; on remarque que χ est d'ordre égal au p. p. c. m. des ordres des χ_i, soit dans tous les cas p. p. c. m. $_{i=1,\ldots,k}(e_i) = d$.

Le corps K fixe par H est donc cyclique de degré d sur $\mathbb{Q}$ et l'étude directe (Prop. 1 et 2) montre que les indices de ramification des p_i sont bien les e_i (les χ_i sont les composantes de χ dans $(\mathbb{Z}/m\mathbb{Z})^{*\perp}$ et sont d'ordre e_i).

Tout caractère solution χ est de la forme $\chi = \chi_1^{a_1} \ldots \chi_k^{a_k}$, $a_i \bmod e_i$, $(a_i, e_i) = 1$, pour tout i, $1 \leq i \leq k$, ce qui donne $\varphi(e_1) \ldots \varphi(e_k)$ solutions ; comme les caractères "conjugués" χ^a ($a \bmod d$, $(a, d) = 1$) définissent le même corps K, on obtient bien le résultat annoncé sur le nombre de solutions.

Dans le paragraphe suivant, nous allons préciser la classification des corps K solutions et préciser un point important : à savoir si les corps obtenus sont réels ou imaginaires.

§2. Recherche pratique des solutions :

On suppose donc donnés les nombres premiers $p_1, \ldots, p_k$ (p_{k-1} et p_k pouvant être égaux à 2) ; on se donne les entiers $e_1, \ldots, e_k$ et on suppose que les hypothèses et les conventions du théorème sont vérifiées. On calcule m comme indiqué dans le théorème.

a) Recherche des caractères solutions. Soient $g_1, \ldots, g_k \in (\mathbb{Z}/m\mathbb{Z})^*$ des générateurs des sous-groupes $G_i = \{a \in (\mathbb{Z}/m\mathbb{Z})^*,\ a \equiv 1 \bmod m(p_i)\}$, avec la convention que, lorsque $p_{k-1} = p_k = 2$, $G_{k-1} = \Gamma$ et $G_k = C$.

Soit ξ une racine primitive d-ième de l'unité ; définissons, pour chaque i, $1 \leq i \leq k$, un caractère χ_i d'ordre e_i de G_i en posant $\chi_i(g_i) = \xi^{d/e_i}$ et $\chi_i(g_j) = 1$ pour tout $j \neq i$. Il est clair que l'on obtient tous les caractères χ solutions en posant : $\chi = \prod_{i=1}^{k} \chi_i^{a_i}$, avec $1 \leq a_i \leq e_i$, $(a_i, e_i) = 1$, pour i, $1 \leq i \leq k$.

Soit $g \in (\mathbb{Z}/m\mathbb{Z})^*$; on a $g = g_1^{x_1} \ldots g_k^{x_k}$, où l'on peut supposer que les intervalles de variation des x_i sont définis par les inégalités $0 \leq x_i < \nu_i$, avec $\nu_i = p_i^{n_i - 1}(p_i - 1)$ pour tout i tel que $p_i \neq 2$ et (éventuellement) $\nu_{k-1} = 2^{n_{k-1}-2}$, $\nu_k = 2$.

On a $\chi(g) = \chi_1^{a_1} \ldots \chi_k^{a_k}(g_1^{x_1} \ldots g_k^{x_k}) = \prod_{i=1}^{k} \chi_i(g_i)^{a_i x_i} = \prod_{i=1}^{k} \xi^{(d/e_i) a_i x_i}$, soit

$\chi(g) = \xi^{s(g)}$ avec $s(g) = \sum_{i=1}^{k} a_i x_i(d/e_i)$; la somme $s(g)$ est à calculer modulo d.

On aura $g \in H$ si et seulement si $s(g) \equiv 0 \bmod d$. Donnons un moyen de reconnaître les différentes classes de $(\mathbb{Z}/m\,\mathbb{Z})^*$ mod H ; pour cela on doit définir (et trouver numériquement) un élément de $(\mathbb{Z}/m\,\mathbb{Z})^*$ qui définisse un élément de $Gal(\mathbb{Q}^{(m)}/\mathbb{Q})$ dont la restriction à K engendre $Gal(K/\mathbb{Q})$ (i.e. soit d'ordre d) :

b) Générateur de $Gal(K/\mathbb{Q})$. On appelle R un système (à r éléments) de p_i tels que $\text{p.p.c.m.}_{i=1,\ldots,r}(e_i) = d$ (r existe : on peut toujours prendre $r = k$, mais on aura $r = 1$ s'il existe un p_i totalement ramifié dans $K/\mathbb{Q}$). On recherche alors un nombre de la forme $g_K = g_1^{\alpha_1} \ldots g_r^{\alpha_r}$ de telle sorte que g_K ait la propriété requise ; celle-ci est équivalente au fait que $\chi(g_K)$ soit une racine d-ième d'ordre d, autrement dit que $s(g_K)$ soit inversible modulo d. Pour un tel choix des α_i (en remarquant qu'il suffit de faire varier les α_i modulo e_i), notons $a = \sum_{i=1}^{k} a_i \alpha_i (d/e_i)$ ($\alpha_{r+1} = \ldots = \alpha_k = 0$) cet élément modulo d, étranger à d. On a donc $\chi(g_K) = \xi^a$; pour un élément g quelconque, $\chi(g) = \xi^{s(g)}$, ce qui s'écrit $\chi(g) = \xi^{a a^* s(g)}$, en désignant par a^* l'inverse de a modulo d ; posons $y(g) = a^* s(g)$ modulo d, on remarque alors que $\chi(g\, g_K^{-y(g)}) = \xi^{s(g)}\, \xi^{-a\, y(g)} = \xi^{s(g)-s(g)} = 1$ et $g \in g_K^{y(g)} H$, ce qui précise la classe de g, comme souhaité.

Lorsqu'un caractère χ a été défini au moyen d'une famille $(a_1, \ldots, a_k)$ ($1 \le a_i \le e_i$, $(a_i, e_i) = 1$, $1 \le i \le k$,) on doit éliminer les caractères conjugués χ^a, $(a, d) = 1$; on est donc amené à considérer comme équivalents les k-uples :

$$([a\, a_1]_{e_1}, \ldots, [a\, a_k]_{e_k}),$$

où $[\ ]_{e_i}$ désigne la fonction résidu modulo e_i, a parcourant l'ensemble des résidus modulo d étrangers à d.

c) Nature des solutions. On sait que K est réel si et seulement si la conjugaison complexe de $Gal(\mathbb{Q}^{(m)}/\mathbb{Q})$ appartient à H, donc si et seulement si $\chi(-1) = 1$.

Supposons d pair sinon le résultat est trivial : K est réel. Calculons $\chi(-1) = \prod_{i=1}^{k} \chi_i^{a_i}(-1)$, en calculant les $\chi_i(-1)$:

(i) cas $p_i \neq 2$. On sait que χ_i est le caractère d'ordre e_i de G_i défini par $\chi_i(g_i) = \xi^{d/e_i}$; on calcule alors $\chi_i(-1)$ en déterminant la projection u de -1 dans G_i puis en calculant $\chi_i(u)$; on remarque que $u \neq 1$, car sinon on

aurait $-1 \in \mathrm{Gal}(\mathbb{Q}^{(m)}/\mathbb{Q}^{(p_i^{n_i})})$, ce qui n'est pas car $\mathbb{Q}^{(p_i^{n_i})}$ est imaginaire ; donc $u = g_i^{\frac{\nu_i}{2}}$ (car $\mathrm{Gal}(\mathbb{Q}^{(m)}/\mathbb{Q}^{(p_i^{n_i})})$ est cyclique et l'on recherche son unique élément u d'ordre 2); or $\chi_i(u) = \xi^{(d/e_i)\frac{\nu_i}{2}}$ et $\frac{d\,\nu_i}{2\,e_i} = \frac{d}{2}\, p_i^{n_i-1}\, \frac{(p_i-1)}{e_i}$; comme $\xi^{d/2} = -1$ on constate que $\chi_i(u) = (-1)^{(p_i-1)/\bar{e}_i}$, puisque p_i est impair.

(ii) Cas de 2. On a alors $\chi_{k-1} = \gamma$ et $\chi_k = c$ pour lesquels on a $\chi_k(-1) = -1$ si et seulement si $e_k = 2$ et $\chi_{k-1}(-1) = 1$ dans tous les cas. On a donc $\chi(-1) = (-1)^u$ où $u = \sum_{i=1}^{k} a_i (p_i-1)/\bar{e}_i$ (resp. $u = 2\,a_k/e_k + \sum_{i=1}^{k-2} a_i (p_i-1)/\bar{e}_i$) si 2 n'est pas (resp. est) ramifié dans $K/\mathbb{Q}$. Comme les a_i sont étrangers à e_i, $1 \le i \le k$, et que pour $1 \le i \le k$ lorsque 2 est non ramifié (resp. $1 \le i \le k-2$ lorsque 2 est ramifié) $e_i/\bar{e}_i$ est impair, on peut écrire $a_i(p_i-1)/\bar{e}_i \equiv (p_i-1)/\bar{e}_i$ mod 2 ; de plus, si 2 est ramifié, $a_k = 1$ quel que soit e_k (= 1 ou 2). D'où finalement $\chi(-1) = (-1)^u$, où u modulo 2 vaut :

$$\sum_{i=1}^{k} (p_i-1)/\bar{e}_i \text{ , si 2 n'est pas ramifié dans } K/\mathbb{Q},$$

$$2/e_k + \sum_{i=1}^{k-2} (p_i-1)/\bar{e}_i \text{, si 2 est ramifié dans } K/\mathbb{Q}.$$

Ainsi les corps correspondants sont ou bien tous réels ou bien tous imaginaires.

d) Demi-système de représentants. Dans le seul cas où les corps K sont réels, il est souvent nécessaire de connaître $H_+ = \mathrm{Gal}(\mathbb{Q}_+^{(m)}/K)$, où $\mathbb{Q}_+^{(m)}$ désigne le sous-corps réel maximal de $\mathbb{Q}^{(m)}$, ainsi que les différentes classes de $\mathrm{Gal}(\mathbb{Q}_+^{(m)}/\mathbb{Q})$ modulo H_+. Autrement dit, on est amené à déterminer un système de représentants de $(\mathbb{Z}/m\mathbb{Z})^*$ modulo le sous-groupe $\{1, -1\}$.

Proposition 3. Soit j un indice fixé compris entre 1 et k, et distinct de k-1 lorsque 2 est ramifié. Alors l'ensemble :

$$\{g = g_1^{x_1} \dots g_k^{x_k},\ 0 \le x_i < \nu_i,\ \text{pour } i \ne j,\ 0 \le x_j < \frac{\nu_j}{2}\}$$

est un système exact de représentants de $\mathrm{Gal}(\mathbb{Q}_+^{(m)}/\mathbb{Q})$.

Démonstration.

On remarque que $\frac{\nu_j}{2}$ est toujours un entier et que ainsi l'ensemble défini a bien le bon nombre d'éléments. Il suffit de voir que deux quelconques de ses éléments ne sont pas équivalents modulo $\{-1, +1\}$.

Supposons que $g_1^{x_1} \dots g_k^{x_k} \equiv -g_1^{y_1} \dots g_k^{y_k} \bmod m$, où les x_i et y_i sont compris entre 0 et $\nu_i - 1$ pour tout $i \neq j$, et entre 0 et $\frac{\nu_j}{2} - 1$ pour $i = j$.

(i) cas $p_j \neq 2$. Alors en raisonnant modulo $p_j^{n_j}$, on obtient (puisque $g_i \equiv 1 \bmod p_j^{n_j}$ pour tout $i \neq j$) : $g_j^{x_j} \equiv -g_j^{y_j} \bmod p_j^{n_j}$, soit $g_j^{x_j - y_j} \equiv -1 \bmod p_j^{n_j}$; ceci entraîne $x_j - y_j \equiv \frac{\nu_j}{2} \bmod \nu_j$, or ceci est absurde car x_j et y_j sont compris entre 0 et $\frac{\nu_j}{2} - 1$.

(ii) cas $p_j = 2$ (i.e. $j = k$). Dans ce cas, g_k est le générateur de $C(g_k \equiv -1 \bmod 2^{n_k})$ et on a donc, modulo 2^{n_k}, $(-1)^{x_k} \equiv -(-1)^{y_k} \bmod 2^{n_k}$; or ici x_k et y_k sont nuls ($\nu_k = 2$), d'où une absurdité.

En pratique, compte tenu de la façon dont est listé le groupe de Galois dans le programme, on prendra systématiquement l'indice j égal à k pour obtenir le demi-système de représentants.

§3. Structure globale du programme :

Le programme proprement dit est constitué essentiellement par le sous-programme appelé GALCYCL ; de ce fait il faut un programme principal, très court, destiné à l'appel de GALCYCL pour les différentes données envisagées.

Voici un exemple de tel programme principal, avec à la suite un bref commentaire pour l'utilisateur (on a souligné en pointillé ce que l'utilisateur devra modifier) :

```
      IMPLICIT DOUBLE PRECISION (Y-Z), INTEGER (A-X)
      COMMON LEC, IMP, MK, MDG, MFD, MS
      LEC = 105
      IMP = 108
      MK = 10
      MDG = 400
      MFD = 100
      MS = 30
      READ (LEC, 1) FIN
1     FORMAT (I5)
      DO 2 I = 1, FIN
2     CALL GALCYCL
      STOP
      END
      SUBROUTINE GALCYCL
          :
      RETURN
      END
```

a) On commence par affecter (à LEC et IMP) les numéros des organes d'entrées-sorties propres à l'ordinateur utilisé (105 et 108 pour l'IRIS 50 de Besançon en 1978 !).

b) Les 4 variables suivantes sont des dimensions maximum de tableaux à prévoir en fonction des données numériques que l'on envisage de traiter. Ce sont les variables

MK, MDG, MFD et MS.

L'utilisateur doit donc effectuer les affectations suivantes :

(i) Affecter à ces variables des valeurs numériques, dans le programme principal (ici on a pris les valeurs respectives 10, 400, 100, 30) ; ces variables (déclarées en COMMON) sont utilisées par GALCYCL pour des tests, vérifiant si ces dimensions sont suffisantes, et le cas échéant pour écrire un message d'erreur.

(ii) Affecter ces <u>mêmes valeurs</u> numériques dans l'ordre DIMENSION de GALCYCL, selon la liste suivante (cf. p. 15) :

α) tableaux de dimension MK :

P, E, EB, PN, N, G, MP, B, AAB, DEA, AL, X.

β) tableaux de dimension MDG :

YH,

et tout autre tableau, introduit par l'utilisateur, dont l'indice peut varier de 1 à D (le degré des corps considérés).

γ) tableaux de dimension MFD :

AA,

et tout autre tableau, introduit par l'utilisateur, dont l'indice peut varier entre 1 et $\varphi(D)$.

δ) tableaux à deux dimensions (MS et MK) :

A.

Donnons l'interprétation des variables MK, MDG, MFD, MS :

(i) MK est la valeur maximum prise par k (qui est le nombre de nombres premiers ramifiés, 2 étant compté deux fois s'il est ramifié) ;

(ii) MDG est la valeur maximum du degré d des corps mis en données.

L'utilisateur doit donc contrôler lui-même (en fonction de ses données) que les valeurs affectées à MK et MDG (p. 11 et 15) sont assez grandes. Pour les

deux suivantes, la procédure GALCYCL est sensée s'assurer que les nombres qui leur sont affectés, sont assez grands :

(iii) MFD est la valeur maximum de $\varphi(d)$ (fonction d'Euler du degré d) ;

(iv) MS est la valeur maximum du nombre de corps solutions à une même donnée : $\frac{\varphi(e_1)\ldots\varphi(e_k)}{\varphi(d)}$.

L'utilisateur devra donner à MFD et MS (p. 11 et 15) des valeurs adaptées à celles données à MK et MDG.

On voit donc qu'il y a intérêt à regrouper, à chaque utilisation, les données correspondant à des degrés d'un ordre de grandeur commun. Compte tenu du fait que le temps d'exécution, pour un corps, est lié essentiellement au conducteur m (en fait à $\varphi(m)$), on aura intérêt à classer ses données en tenant compte de cette remarque.

c) Ensuite, on lit FIN qui est le nombre ≥ 1 de données (cf. p. 31 pour voir ce que l'on entend par "donnée").

d) Le reste du programme principal est alors le simple appel de GALCYCL un nombre de fois égal à FIN (signalons que c'est GALCYCL elle-même qui contient l'ordre de lecture des données et non le programme principal).

§4. Listing commenté de GALCYCL :

a) Boucles à imbrication de profondeur variable.

Nous décrivons ici, une fois pour toutes, un principe algorithmique élémentaire qui est utilisé plusieurs fois dans GALCYCL ; il s'agit de la programmation des boucles DO imbriquées qui seraient formellement de la forme suivante (où l'indice $K \geq 1$ est une variable dont les valeurs sont susceptibles de dépendre des données ou d'un calcul) :

```
||  DO   1  J(K) = 0,  S(K)-1
||  DO   1  J(K-1) = 0,  S(K-1)-1
||     :
||     :
||  DO   1  J(1) = 0,  S(1)-1
||  Instructions, fonctions du K-uple (J(1), J(2), ..., J(K))
1 ||  CONTINUE
```

Les S(I) sont des entiers supérieurs ou égaux à 1.

Le principe de parcours de l'ensemble $[0, S(1)[\times \ldots \times [0, S(K)[$ utilise l'écriture des nombres en "base multiple" (S(1), S(2), ..., S(K)) et l'addition dans ce cadre : c'est-à-dire que si l'on représente symboliquement par $\overline{J(K)\ldots J(1)}$

le développement d'un nombre (appartenant à l'intervalle $[0, S(1)...S(K)[$) dans cette base (avec $0 \leq J(I) \leq S(I)-1$, pour tout I) et si l'on ajoute 1, par exemple, on obtient le développement $\overline{J'(K)...J'(1)}$ (avec $0 \leq J'(I) \leq S(I)-1$, pour tout I), grâce au processus de "retenue".

On vérifie facilement que l'incrémentation systématique d'une unité, à partir de $\overline{0...0}$, donne tous les K-uples désirés, et que le test d'arrêt est constitué par la comparaison de J(K) à S(K).

Il en résulte le programme FORTRAN suivant (dans le cas le plus simple où les instructions, fonctions du K-uple (J(1),...,J(K)), ont une exécution indépendante des valeurs prises par le K-uple antérieur) :

```
      KK = K-1
      DO 10 I = 1,K
10    J(I) = 0
[20   IF (J(K).EQ.S(K)) GOTO 30
      Instructions F, fonctions du K-uple (J(1),...,J(K))  ]
11    J(1) = J(1)+1
      IF(KK.EQ.0) GOTO 20
      DO 12 I = 1,KK
      IF (J(I).LT.S(I)) GOTO 20
{     J(I) = 0                                             }
{12   J(I+1) = J(I+1)+1                                    }
[     GOTO 20   ]

      GOTO 11
30      :
```

On remarquera que l'on peut initialiser le tableau J à d'autres valeurs que 0, sans changement du programme (qui ne décrit alors qu'une partie de l'ensemble $[0, S(1)[\times ... \times [0, S(K)[$).

On remarquera enfin qu'il revient au même d'échanger les deux parties entre crochets (on trouvera les deux versions, au cours du programme GALCYCL).

Lorsque les instructions F, fonctions du K-uple (J(1),...,J(K)), sont obtenues sous une forme "récurrente" utilisant leur "valeur" au niveau du K-uple précédent, le programme a une forme analogue, mais les instructions entre accolades sont alors accompagnées d'instructions opérant la modification correspondante sur les instructions F.

b) GALCYCL.

On adopte la convention suivante : les explications précèdent les instructions concernées ; les notations employées dans le "commentaire" sont de nature FORTRAN ; on utilisera donc, éventuellement, la table de concordance (§5, a, p. 30) pour les significations mathématiques. Les différentes parties du programme sont encadrées pour éviter toute interférence avec les commentaires.

La juxtaposition séquentielle des différentes parties encadrées constitue par définition GALCYCL.

Description et écriture de GALCYCL.

Déclarations de GALCYCL (nom de la subroutine) ; déclarations de réels en double précision, déclaration des entiers ; ordres de dimensions des tableaux, ces dimensions étant les valeurs numériques de MK, MDG, MFD et MS affectées dans le programme principal p. 11. Sont mis en COMMON les variables LEC, IMP, MK, MDG, MFD, MS, afin d'éviter une nouvelle fois l'affectation numérique qui est faite dans le programme principal (p. 11) , la carte n°4 comprend les variables "utilisateur" ; ici nous l'avons laissée en blanc :

```
      |  | SUBROUTINE GALCYCL
      |  | IMPLICIT DOUBLE PRECISION (Y-Z), INTEGER (A-X)
      |  | DIMENSION P(10), E(10), EB(10), PN(10), N(10), G(10),
     1|  | MP(10), AA(100), A(30, 10), B(10), AAB(10), DEA(10),
     2|  | AL(10), X(10),
     3|  | YH(400),
     4|  |
      |  | COMMON LEC, IMP, MK, MDG, MFD, MS
```

Affectation du nombre π à YPI (n'est évidemment pas utilisé dans le calcul du groupe d'Artin mais est disponible pour l'utilisateur à toutes fins utiles (racines de l'unité)) :

```
      |  | YPI = 0.3141592653589793D+01
```

Lecture d'une donnée (cf. p. 31) (correspondant à une famille de corps) :

```
      |  | READ (LEC, 10) D, K, (P(I), I=1, K), (E(I), I=1, K)
   10 |  | FORMAT (16I5)
```

On teste si les variables MK et MDG ont été déclarées assez grandes en regard des nombres K et D qui viennent d'être lus :

```
      |  | IF (K.GT.MK) WRITE (IMP, 11)
11    |  | FORMAT (' ␣ DIMENSION MK INSUFFISANTE')
      |  | IF (D.GT.MDG) WRITE (IMP, 12)
12    |  | FORMAT (' ␣ DIMENSION MDG INSUFFISANTE')
```

On affecte à KP la valeur K ou K-1 selon que 2 est non ramifié ou est ramifié (KP est donc le nombre de nombres premiers distincts ramifiés dans l'extension). Ainsi lorsque 2 est ramifié, l'indice KP est relatif à la γ-ramification et l'indice K à la c-ramification.

On affecte à TEST le nombre (≥ 0) de nombres premiers impairs ramifiés dans l'extension : on remarque donc que si TEST=0 (i.e. K=2 et KP=1) on a donc P(1) = 2 et P(2) = 2 (corps de conducteur une puissance de 2). Si TEST $\neq 0$, c'est qu'il existe des nombres premiers impairs ramifiés dans l'extension : (P(1), ..., P(TEST)).

On affecte enfin à KK la valeur K-1 (on a donc KK ≥ 0) :

```
      |  | KP=K
      |  | IF (P(K).EQ. 2) KP=K-1
      |  | TEST =K
      |  | IF (KP.NE.K) TEST =K-2
      |  | KK =K-1
```

Calcul des EB(I), les parties "modérées" des indices de ramification E(I), et calcul des PN(I), les P(I)-participations au conducteur, ceci pour I = 1 à K. Le calcul est scindé en deux parties (cf. p. 7) :

(i) Pour I de 1 à TEST si ce dernier est non nul (première partie) : EB(I) est la partie étrangère à P(I) de E(I), PN(I) est la puissance de P(I) supérieure d'une unité à celle figurant dans E(I).

(ii) Si 2 est ramifié (cas où KP $\neq$ K) (deuxième partie) : on pose EB(KP) = EB(K) = 1, et PN(KP) = PN(K) = 4 * E(KP) (où E(KP) est l'indice de γ-ramification) :

```
      |  | IF (TEST.EQ.0) GOTO 70
      |  | DO 60 I=1,TEST
      |  | EB(I)=E(I)
      |  | PN(I)=P(I)
   50 |  | IF (EB(I)-EB(I)/P(I)*P(I).NE.0) GOTO 60
      |  | EB(I)=EB(I)/P(I)
      |  | PN(I)=P(I)*PN(I)
      |  | GOTO 50
   60 |  | CONTINUE
```

```
   70 |  | IF(KP.EQ.K) GOTO 80
      |  | EB(KP)=1
      |  | EB(K)=1
      |  | PN(KP)=4*E(KP)
      |  | PN(K)=PN(KP)
```

Calcul du conducteur $M = PN(1)*\ldots*PN(KP)$ (PN(K) ne doit pas être compté), puis calcul des quantités $MP(I) = M/PN(I)$, pour I = 1 à K (de sorte que lorsque 2 est ramifié, $MP(KP) = MP(K) = M/PN(K)$) (cf. p. 7) :

```
   80 |  | M=1
      |  | DO 90 I=1,KP
   90 |  | M=M*PN(I)
      |  | DO 100 I=1,K
  100 |  | MP(I)=M/PN(I)
```

Calcul de l'ordre N(I) (I de 1 à TEST, si ce dernier est non nul) des ordres des composantes $(\mathbb{Z}/PN(I)\mathbb{Z})^*$ (i.e. $\varphi(PN(I))$).

Si 2 est ramifié ($KP \neq K$), N(KP) vaut PN(K)/4 (ordre de Γ) et N(K) vaut 2 (ordre de C) :

```
      |  | IF(TEST.EQ.0) GOTO 120
      |  | DO 110 I=1,TEST
  110 |  | N(I)=(P(I)-1)*PN(I)/P(I)
  120 |  | IF (KP.EQ.K) GOTO 130
      |  | N(K)=2
      |  | N(KP)=PN(K)/4
```

Calcul des générateurs G(I) des sous-groupes de $(\mathbb{Z}/M\mathbb{Z})^*$ correspondant aux $(\mathbb{Z}/PN(I)\mathbb{Z})^*$, pour I = 1 à TEST (si ce dernier est non nul). Le but est donc de trouver G(I) tel que $G(I) \equiv 1 \bmod MP(I) = M/PN(I)$, et tel que G(I) engendre $(\mathbb{Z}/PN(I)\mathbb{Z})^*$ (on a MP(I) = 1 si et seulement si il n'y a qu'un seul premier ramifié, et la première condition a toujours lieu dans ce cas). On part donc du nombre auxiliaire GI = 1 que l'on incrémente d'abord de MP(I), et on teste si GI est bien d'ordre voulu (à savoir N(I)) sinon on incrémente GI à nouveau de MP(I) (étiquette 140) ; le principe est le suivant : on calcule les puissances successives de GI (dans la variable GG) modulo Q = PN(I) sans tester si la valeur utilisée est même étrangère à PN(I). La puissance est repérée au moyen du compteur décroissant NN qui vaut 0 si et seulement si on a dans GG la puissance N(I)-ième. A chaque stade on teste si GG = 1 et on change de valeur de GI si GG = 1 sans que l'ordre N(I) ait été atteint ; lorsque l'on a atteint l'ordre N(I) (i.e. NN = 0) on vérifie que l'on trouve GG=1 (sinon c'est que GI était non étranger à PN(I), et on écarte la valeur en retournant à l'étiquette 140 :

```
130     IF (TEST.EQ.0) GOTO 180
        DO 170 I=1,TEST
        GI=1
        Q=PN(I)
140     GI=GI+MP(I)
        NN=N(I)
        GG=GI
150     GG=GG-GG/Q*Q
        NN=NN-1
        IF(NN.EQ.0) GOTO 160
        IF(GG.EQ.1) GOTO 140
        GG=GG*GI
        GOTO 150
160     IF (GG.NE.1) GOTO 140
        G(I)=GI
170     CONTINUE
```

Calcul des générateurs de Γ et de C (lorsque 2 est ramifié, soit $KP \neq K$) :

(i) Calcul de G(KP) (première partie). On sait que Γ est engendré par un nombre G(KP) congru à 5 modulo la puissance de 2 divisant M (égale à PN(K)). On part donc du nombre auxiliaire GG = 5 que l'on incrémente mod PN(K) jusqu'à ce que GG soit congru à 1 mod MP(K) (on a MP(K) = 1 si

et seulement si 2 est le seul ramifié, auquel cas cette condition est vérifiée dès la première fois, et on trouve le générateur 5 dans ce cas).

(ii) Calcul de G(K) (deuxième partie). Le groupe C est engendré de façon analogue, en remplaçant 5 par -1 ; dans ce cas on part de GG=PN(K)-1 que l'on incrémente mod PN(K) jusqu'à avoir $GG \equiv 1 \bmod MP(K)$.

Dans les deux cas on réduit modulo M et on obtient G(KP) et G(K) :

```
180     IF (KP.EQ.K) GOTO 230
        GG=5
190     IF (GG-1-(GG-1)/MP(K)*MP(K).EQ.0) GOTO 200
        GG=GG+PN(K)
        GOTO 190
200     GG=GG-GG/M*M
        G(KP)=GG

        GG=-1+PN(K)
210     IF (GG-1-(GG-1)/MP(K)*MP(K).EQ.0) GOTO 220
        GG=GG+PN(K)
        GOTO 210
220     GG=GG-GG/M*M
        G(K)=GG
```

Dans le tableau AA suivant on calcule les nombres compris entre 1 et D étrangers à D ; Q est le nombre dont on teste la primarité avec D, J est le compteur qui donnera l'indice final de AA (donc la valeur $\varphi(D)$ qui sera affectée à F D).

Partant de Q=1 et J=1, on affecte 1 à AA(1) :

```
230     Q=1
        AA(1)=1
        J=1
```

Ensuite, on incrémente Q et on teste si la constitution du tableau est finie (ce qui est le cas si Q=D), ce qui donne FD, valeur finale de J.

La partie centrale est l'algorithme du P.G.C.D. avec D et Q ; lorsque T=0 le P.G.C.D. positif se trouve dans S, d'où le test effectué dans la dernière ligne, qui renvoie à l'étiquette 240 (changement de valeur de Q) si $S \neq 1$:

```
240     Q =Q+1
        IF(Q.GE.D) GOTO 270

        S=Q
        R =D
250     T=R-R/S *S
        IF(T.EQ.0) GOTO 260
        R =S
        S=T
        GOTO 250
260     IF (S.NE. 1) GOTO 240

        J= J+1
        AA(J) =Q
        GOTO 240
270     FD =J
```

On teste si le nombre MFD est assez grand compte tenu de la valeur $\varphi(D)$ obtenue :

```
        IF (FD.GT.MFD) WRITE (IMP, 271)
271     FORMAT ('␣ DIMENSION MFD INSUFFISANTE')
```

Constitution du tableau A(L, I). Les lignes, indicées par L, sont constituées de nombres étrangers aux E(I) pour I = 1 à K, avec la convention A(L, I) = 0 si E(I) = 1 (cas qui se présente éventuellement pour la γ ou la c-ramification). On remarque donc que A(L, I) est toujours un plus petit résidu modulo E(I) étranger à E(I). En outre, parmi toutes les lignes possibles, on ne calcule qu'un système de représentants modulo l'équivalence que nous avons définie (cf. §2, p. 9). Le nombre de lignes MJ donne le nombre de corps solutions.

On part de la première ligne A(1, I) = 1 (ou la valeur 0 s'il y a lieu), pour I = 1 à K.

La ligne B(I) est la ligne générique testée ; on l'initialise à la ligne A(1, I). Le compteur J repère le nombre de lignes construites ; J est donc initialisé à 1 :

```
      |  |  DO  280 I = 1, K
      |  |  A(1, I) = 1
      |  |  IF (E(I). EQ. 1)  A(1, I) = 0
280   |  |  B(I) = A(1, I)
      |  |  J = 1
```

Le principe de la constitution séquentielle des lignes B (I) est celui du développement en "base" (S(1), . . . , S(K)), où ici le tableau S est le tableau E (première partie).

On retrouve ensuite l'algorithme du P. G. C. D. pour chacun des couples B(I), E(I), qui, éventuellement, permet de ne pas retenir la ligne B (I) (à savoir si l'un des B(I) est non étranger à E(I) ; signalons à ce sujet que lorsqu'un E(I) vaut 1, soit B(I) = 0, l'algorithme du P. G. C. D. trouve bien que 0 et 1 sont étrangers) :

```
290   |  |  B(1) = B (1) + 1
      |  |  IF (KK . EQ. 0)  GOTO  310
      |  |  DO 300 I = 1, KK
      |  |  IF (B(I). LT. E(I)) GOTO  310
      |  |  B(I) = 0
300   |  |  B(I+1) = B(I+1)+1
310   |  |  IF (B(K). EQ. E (K)) GOTO 380
```

```
      |  |  DO  340 I = 1, K
      |  |  S = E(I)
      |  |  R = B (I)
320   |  |  T = R-R/S * S
      |  |  IF (T. EQ. 0) GOTO 330
      |  |  R = S
      |  |  S = T
      |  |  GOTO  320
330   |  |  IF (S. NE. 1) GOTO 290
340   |  |  CONTINUE
```

Si la ligne B(I) est formée d'éléments étrangers aux E(I), alors on cherche si elle est équivalente à l'une des lignes précédentes, lignes de la forme A(L, I), pour L variant de 1 à J ; pour cela on constitue successivement les FD lignes AAB(I) = B I * AA(H) mod E(I) (les AA(H) sont les FD nombres étran-

gers à D), formées des résidus modulo E(I), et on compare, terme à terme, aux J lignes précédentes. Si l'une des FD lignes AAB(I) coïncide avec l'une des J lignes A(L, I), alors la ligne B(I) n'est pas retenue et on se renvoie à l'étiquette 290 :

```
      |  | DO  360 H = 1, FD
      |  | DO  345 I = 1, K
      |  | AAB(I) = B(I) * AA(H)
345   |  | AAB(I) = AAB(I) - AAB(I)/E(I) * E(I)
      |  | DO  360 L = 1, J
      |  | DO  350 I = 1, K
      |  | IF (A(L, I). NE. AAB(I)) GOTO 360
350   |  | CONTINUE
      |  | GO TO 290
360   |  | CONTINUE
```

Si le programme ci-dessus termine la boucle la plus extérieure (sur H), c'est que la ligne B(I) est retenue comme définissant un corps solution ; elle est alors chargée et on retourne ensuite à l'étiquette 290 (incrémentation de B(1) d'une unité). On est renvoyé à l'étiquette 380 dès que toutes les lignes, a priori possibles, ont été examinées (MJ est alors le nombre de lignes A(L, I) déterminées) :

```
      |  | J = J+1
      |  | DO  370 I = 1, K
370   |  | A(J, I) = B(I)
      |  | GOTO 290
380   |  | MJ = J
```

On teste si la variable MS est assez grande, compte tenu du nombre de corps solutions (MJ) que l'on vient de trouver :

```
      |  | IF (MJ. GT. MS) WRITE (IMP, 381)
381   |  | FORMAT ('␣ DIMENSION MS INSUFFISANTE')
```

La suite du programme a la structure suivante :

```
      DO 900 J = 1, MJ
     {Traitement complet du corps correspondant à la ligne A(J, I)}
900  CONTINUE
```

Nous allons essentiellement décrire, en plusieurs étapes, la partie entre accolades.

Elle commence par les ordres d'impression des données (degré D, nombres premiers ramifiés P(I), et leurs indices de ramification E(I), numéro J du corps traité, les générateurs G(I), le conducteur M et la ligne A(J, I) correspondant au corps traité) :

```
      |  | DO 900 J=1,MJ
      |  | WRITE (IMP, 382) D
      |  | WRITE (IMP, 383) (P(I), I = 1,K)
      |  | WRITE (IMP, 384) (E(I), I = 1,K)
382   |  | FORMAT (1H1///2X,'CORPS CYCLIQUE DE DEGRE ', 10X, I6)
383   |  | FORMAT (2X,'AVEC LA RAMIFICATION DE', 11X, 10I6)
384   |  | FORMAT (2X,'AVEC LES INDICES DE RAMIFICATION', 2X, 10I6)
      |  | WRITE (IMP, 385) J
385   |  | FORMAT (/105X,'CORPS NUMERO', I5)
      |  | WRITE (IMP, 390) (G(I), I = 1,K)
390   |  | FORMAT (/2X,'RACINES PRIMITIVES ', 16X, 10I6)
      |  | WRITE (IMP, 410) M
      |  | WRITE (IMP, 400) K, (A(J, I), I = 1,K)
400   |  | FORMAT (2X,'CE CORPS CORRESPOND AU', I2,'-UPLE', 5X, 10I6)
410   |  | FORMAT (/85X,'SON CONDUCTEUR EST', 8X, I8)
```

On calcule SGN qui vaut -1 (resp. 1) si le corps considéré est imaginaire (resp. réel). Le calcul se décompose en deux : une partie relative aux ramifiés impairs (si TEST $\neq$ 0), l'autre à 2 éventuellement (si KP $\neq$ K) (cf. p. 10) :

```
      |  | S = 0
      |  | SGN = 1
      |  | IF (TEST.EQ.0) GOTO 430
      |  | DO 420 I = 1, TEST
420   |  | S = S+(P(I)-1)/EB(I)
      |  | S= S-S/2*2
      |  | SGN = -1
      |  | IF (S.EQ. 0) SGN=1
430   |  | IF (KP.EQ.K) GOTO 440
      |  | SG = -1
      |  | IF (E(K).EQ.1) SG = 1
      |  | SGN = SGN*SG
```

On calcule dans DEA(I) les nombres (D/E(I)) * A(J, I) qui sont les coefficients permettant le calcul des valeurs du caractère χ associé au corps n°J ($\chi = \prod_I \chi_I^{DEA(I)}$, I de 1 à K) (cf. p. 8) :

```
440 |  | DO 450 I = 1, K
450 |  | DEA(I) = D/E(I) * A(J, I)
```

On calcule un élément GEN de la forme $GEN = \prod_I G(I)^{AL(I)} \bmod M$ (I de 1 à K) qui représente un générateur de Gal($K/\mathbb{Q}$) (i. e. tel que $\chi(GEN)$ soit d'ordre D) ; il faut donc trouver des coefficients AL(I) mod E(I), tels que $\chi(GEN) = \prod_I \xi^{AL(I)*DEA(I)}$ soit d'ordre D (I de 1 à K). De façon équivalente, on doit avoir $\sum_I AL(I)*DEA(I)$ étranger à D (cf. p. 9).

On applique encore le principe du développement en "base" E(I), avec incrémentation de 1, en initialisant AL(1) à 1 et AL(2), . . . , AL(K) à 0. On calcule chaque fois (dans C) $\sum_I AL(I)*DEA(I) \bmod D$; on teste alors si C est étranger à D (seconde partie). Ici on illustre une variante donnée au §a, p. 14 , qui évite de recalculer complètement C à chaque nouveau K-uple : on voit comment répercuter sur C l'addition de 1 au développement $\overline{AL(K)\ldots AL(1)}$: l'ancienne valeur de C est incrémentée de DEA(1) en général, sauf en cas de retenue qui se simplifie au niveau de C, car si AL(I) est réduit mod E(I), C est réduit mod D et l'instruction C = C - E(I) * DEA(I) qui devrait figurer après l'instruction AL(I) = 0, est inutile ici puisqu'alors E(I) * DEA(I) est multiple de D. Enfin, ici, un test d'arrêt est inutile puisque théoriquement une solution doit être trouvée avant que AL(K) ne dépasse E(K) :

```
    |  | DO 460 I = 1, K
460 |  | AL(I) = 0
    |  | AL(1) = 1
    |  | C = DEA(1)
```

```
470 |  | R = C
    |  | S = D
480 |  | T = R - R/S*S
    |  | IF (T. EQ. 0) GOTO 490
    |  | R = S
    |  | S = T
    |  | GOTO 480
490 |  | IF (S. EQ. 1) GOTO 510
```

```
      |  AL(1) = AL(1)+1
      |  C = C+DEA(1)
      |  C = C-C/D*D
      |  IF (KK. EQ. 0) GOTO 470
      |  DO 500 I = 1, KK
      |  IF (AL(I). LT. E(I)) GOTO 470
      |  AL(I) = 0
      |  AL(I+1) = AL(I+1)+1
      |  C = C+DEA(I+1)
      |  C = C-C/D*D
500   |  CONTINUE
      |  GO TO 470
```

Ayant trouvé C (étranger à D), on calcule CE mod D tel que $C*CE \equiv 1 \bmod D$; ceci se fait par multiplications successives :

```
510   |  DO 515 L = 1, D
      |  S = C*L
      |  S = S-S/D*D
      |  IF (S. EQ. 1) GOTO 516
515   |  CONTINUE
516   |  CE = L
```

On calcule maintenant $GEN = \prod_I G(I)^{AL(I)} \bmod M$, I de 1 à K, dans GG (initialisé à 1) par multiplications successives par G(1) (AL(1) fois),...,par G(K) (AL(K) fois) ; on teste si AL(I) = 0 puisque dans ce cas il n'y a pas de multiplication à effectuer. Le résultat de GG mod M donne GEN, et on a par définition $\chi(GEN) = \xi^C$.

Enfin dans GENIMP, on place celui des nombres GEN ou GEN+M qui est impair :

```
      |  | GG = 1
      |  | DO 530 I = 1, K
      |  | KAL = AL(I)
      |  | IF (KAL. EQ. 0) GOTO 530
      |  | DO 520 L = 1, KAL
  519 |  | GG = G G * G(I)
  520 |  | GG = G G-GG/M * M
  530 |  | CONT INUE
      |  | GEN = GG
      |  | S = GE N-G EN/2 * 2
      |  | GENIMP = GEN+(1-S) * M
```

Sorties relatives à la nature du corps traité (réel ou imaginaire), la valeur de GEN, les valeurs de C et CE :

```
      |  | IF (SGN. EQ. 1) WR ITE (IMP, 540)
  540 |  | FO RMAT (/85X, 'CE COR PS EST R EEL ')
      |  | IF (SGN. EQ. -1) WRITE (IMP, 550)
  550 |  | FORMAT (/85X, 'CE C OR PS E ST IMAGINAIRE')
      |  | WRITE (IMP, 560) GEN, C, CE
  560 |  | FORMAT (2X, 'CE CORPS ADMET LE GENERATEUR', 9X, I6
      |  1| /2X, 'ET LES CONSTANTES' 20X, 2I6)
```

Calcul de l'ordre $\varphi(M)$ de $(\mathbb{Z}/M\mathbb{Z})^*$, dans PHIM, puis de H = PHIM/D qui représente l'ordre du noyau de χ. On fait alors écrire ces valeurs :

```
      |  | PHIM = 1
      |  | DO 570 I = 1, K
  570 |  | PH IM = PH IM * N(I)
      |  | H = P HIM/D
      |  | WRITE (IMP, 580) PHIM, H
  580 |  | FO RMAT (2X, 'PHI DE M EST EGAL A', 18X, I6
      |  1| /2X, 'PH I DIV ISE PAR D = H', 17X, I6)
```

Pour l'initialisation des fonctions YH(L) choisies (L de 1 à D) (fonctions sur les D classes de $(\mathbb{Z}/M\mathbb{Z})^*$ modulo $Ker\chi$) se reporter au §5, c, p.32) ; l'exemple traité ici étant la sommation des résidus modulo M des éléments d'une même classe, on a initialisé ces fonctions à 0 :

```
      |  | DO 590 L = 1, D
  590 |  | YH (L) = 0
```

On aborde le calcul de l'élément générique de $(\mathbb{Z}/M\mathbb{Z})^*$ avec détermination de sa classe. On est donc amené à calculer, dans GG, le nombre $\prod_I G(I)^{X(I)} \bmod M$, I de 1 à K, et, dans SOM, le nombre $\sum_I DEA(I) * X(I) \bmod D$. Ces deux nombres sont liés par la relation $\chi(GG) = \xi^{SOM}$. Le principe de calcul sera comme d'habitude basé sur l'addition en "base S" avec, ici, S = N (cf. p. 9).

On commence par initialiser les X(I) à 0, et, en conséquence, GG à 1 et SOM à 0. On affecte à NN le nombre N(K) pour éviter l'appel fréquent d'une variable indicée. On pose aussi NNN = N(K)/2 qui sera utilisé pour la recherche d'un demi-système, ceci étant précisé par NF (cf. p. 33) :

```
        DO 600 I = 1,K
600     X(I) = 0
        NN = N(K)
        NNN = NN/2
601     NF = NN        NF = NNN
        GG= 1
        SOM= 0
        GOTO 630
```

Pour le calcul des valeurs successives de GG et SOM, on procède comme pour le calcul de GEN et C, en conduisant en parallèle les différentes opérations résultant de l'addition en "base N". On obtient donc au niveau de l'étiquette 620 :

```
610     X(1) = X(1)+1
        IF(X(K). EQ. NF) GOTO 640
611     GG = GG* G(1)
        GG = GG-GG/M*M
        SOM = SOM+DEA(1)
        SOM = SOM-SOM/D*D
        IF(KK. EQ. 0) GOTO 630
        DO 620 I = 1,KK
        IF(X(I). LT. N(I)) GOTO 630
        X(I) = 0
        X(I+1) = X(I+1) + 1
        IF(X(K). EQ. NF) GOTO 640
619     GG = GG *G(I+1)
        GG = GG-GG/M*M
        SOM = SOM+DEA(I+1)
620     SOM = SOM-SOM/D*D
```

On recherche alors la classe (indiquée par L, nombre compris entre 1 et D) de l'élément GG ; comme par définition de GEN, on a $\chi(GEN) = \xi^C$, et que l'on a obtenu $\chi(GG) = \xi^{SOM}$, on a donc $\chi(GEN^{CE}) = \xi$ (on rappelle que $C * CE \equiv 1 \bmod D$), soit $\chi(GG) = \chi(GEN^{CE * SOM})$ d'où $GG \in GEN^L \ \mathrm{Ker}\,\chi$, si l'on pose $L = CE * SOM \bmod D$. On prend L mod D entre 1 et D (cf. p. 9) :

```
630 |  | L = CE * SOM
    |  | L = L - L/D * D
    |  | IF (L.EQ.0) L = D
```

On calcule ensuite l'élément générique, correspondant à GG, d'un demi-système de représentants, uniquement si le corps est réel ; d'où le test de la première ligne.

On sait (§2, d, p. 10) que le demi-système est obtenu à partir du domaine suivant de variation des X(I) : si $I<K$, X(I) prend toutes les valeurs entre 0 et N(I) ; pour $I = K$ (qui correspond soit à la ramification d'un nombre premier impair soit à la C-ramification), on n'utilise que le demi-intervalle $[0, N(K)/2[$; lorsque cet intervalle a été parcouru, le demi-système est constitué et on saute systématiquement cette partie, d'où le test de la seconde ligne.

Le demi-système doit en outre avoir une propriété de cohérence expliquée au §5, d, p. 33 et qui est la suivante : l'élément considéré GG est donc de la forme $\prod_I G(I)^{X(I)} \bmod M$, avec $0 \le X(K) < N(K)/2$ et $U = GG * GEN^{-L} \in \mathrm{Ker}\,\chi$; il y a cohérence si cet élément U de Ker χ est aussi un élément du demi-système, autrement dit si et seulement si U s'écrit $\prod_I G(I)^{Y(I)}$, avec $0 \le Y(K) < N(K)/2$. On est donc amené à calculer $S = X(K) - L * AL(K) \bmod N(K)$ (en effet, on rappelle que $GEN = \prod_I G(I)^{AL(I)}$), d'où le calcul de S sous la forme $X(K) + (N(K) - L) * AL(K) \bmod NN$ ($= N(K)$) ; on teste sa valeur par rapport à $NNN = NN/2$ ($= N(K)/2$) : si $S < NNN$, alors GG appartient au demi-système, sinon, si $S \ge NNN$, il est clair que M-GG a la propriété voulue.

Le résultat (GG ou M-GG) est placé dans GGSYST.

Quant à GGIMP, c'est, parmi les nombres GGSYST ou GGSYST+M, celui qui est impair (on a donc un deuxième demi-système : si M est pair, les deux demi-systèmes coïncident ; si M est impair, ils sont distincts, mais GGIMP conserve la propriété de cohérence à condition de remplacer GEN par GENIMP (égal à celui des nombres GEN ou GEN+M qui est impair). Pour l'explication de la présence des pointillés précédant l'étiquette 637, voir p. 33 :