ANNALES DE L'INSTITUT FOURIER

JEAN-JACQUES PAYAN

Contribution à l'étude des corps abéliens absolus de degré premier impair

Annales de l'institut Fourier, tome 15, n° 2 (1965), p. 133-199

<http://www.numdam.org/item?id=AIF_1965__15_2_133_0>

© Annales de l'institut Fourier, 1965, tous droits réservés.

L'accès aux archives de la revue « Annales de l'institut Fourier » (http://annalif.ujf-grenoble.fr/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Ann. Inst. Fourier, Grenoble
15, 2 (1965), 133-199.

CONTRIBUTION A L'ÉTUDE DES CORPS ABÉLIENS ABSOLUS DE DEGRÉ PREMIER IMPAIR

par Jean-Jacques PAYAN

Introduction.

J'ai entrepris le travail qui suit, après avoir lu le mémoire d'Albert Châtelet [2] consacré aux corps abéliens de degré 3. J'en ai d'abord étendu les résultats aux corps abéliens absolus de degré 5, [10], [11] et ensuite aux corps abéliens absolus de degré premier impair.

Certains des résultats obtenus étaient déjà connus, mais comme conséquence de la théorie du corps de classe. Les méthodes que j'ai utilisées ici sont plus élémentaires et permettent une exploitation numérique plus poussée pour les corps de degré l, tels que le corps des racines $l^{\text{ièmes}}$ de l'unité soit principal.

Dans le premier chapitre, après avoir rappelé quelques résultats sur les corps circulaires, je précise la formation des idéaux essentiels définis par Albert Châtelet [3].

Dans le second chapitre, j'associe à chaque polynôme abélien de degré premier l, deux $(l-1)$-uples de paramètres non indépendants (éléments conjugués du corps des racines $l^{\text{ièmes}}$ de l'unité), le premier étant attaché au corps algébrique engendré par les zéros d'un tel polynôme. La détermination des polynômes abéliens de degré l impair se ramène au calcul d'un déterminant d'ordre l, calcul que je mène à son terme pour $l = 3$ et $l = 5$.

Le troisième chapitre traite des entiers des corps abéliens de degré premier: après avoir mis en évidence des bases

d'entiers privilégiées et avoir étudié le groupe multiplicatif des matrices unitaires qui permettent de passer des unes aux autres, on peut calculer le discriminant d'un tel corps et le nombre de corps abéliens de discriminant donné.

Le quatrième et le cinquième chapitre sont consacrés à l'étude des idéaux d'un corps abélien de degré premier. Je précise d'abord, à l'aide de la composition des corps de discriminants premiers entre eux, dans quels corps circulaires est contenu un corps de discriminant donné. J'étudie ensuite la décomposition des idéaux rationnels dans un corps de degré premier et je donne enfin une démonstration élémentaire de la loi de réciprocité.

Dans le dernier chapitre, je me suis intéressé à la construction des corps abéliens de degré premier sur le complété par la valeur absolue p-adique du corps des nombres rationnels. Là encore, on peut obtenir des résultats numériques assez précis.

Qu'il me soit permis de dire ma gratitude au Professeur François Châtelet pour l'attention et la bienveillance avec lesquelles il a suivi la progression de ce travail et pour les nombreux conseils et encouragements qu'il m'a prodigués; de dire également mes remerciements au Professeur Charles Pisot : après m'avoir communiqué son goût pour la Théorie des Nombres, il n'a cessé de m'encourager aux différentes étapes de cette étude.

Que les Professeurs Paul Dubreil et Jean-Pierre Kahane qui ont bien voulu faire partie du Jury, et pour ce dernier choisir mon second sujet, trouvent ici l'expression de ma reconnaissance.

Je dois aussi remercier les membres du Comité de Rédaction des *Annales de l'Institut Fourier* d'avoir accepté ce mémoire.

TABLE DES MATIÈRES

CHAPITRE PREMIER. — CORPS CIRCULAIRES ET IDÉAUX ESSENTIELS 137

1. Propriétés arithmétiques de $C(l)$ 137
2. Idéaux essentiels de $C(l)$ 139

CHAPITRE II. — CONSTRUCTION DES CORPS ABÉLIENS DE DEGRÉ PREMIER l IMPAIR 143

1. l-uples d'éléments conjugués irrationnels 143
2. Ordres compatibles avec les permutations circulaires..... 148
3. Polynômes abéliens de degré premier impair l..... 150

CHAPITRE III. — ENTIERS D'UN CORPS ABÉLIEN DE DEGRÉ PREMIER l.. 155

1. Corps unitaires..... 157
2. Corps non-unitaires 161
3. Discriminants..... 166
4. Exemples 167

CHAPITRE IV. — COMPOSITION DES CORPS ABÉLIENS DE DEGRÉ PREMIER l. 170

1. Composition de deux corps 170
2. Inclusion dans les corps circulaires 171

CHAPITRE V. — ÉTUDE DES IDÉAUX DES CORPS ABÉLIENS DE DEGRÉ PREMIER l 175

1. Critère de décomposition 175
2. Loi de réciprocité 182
3. Exemples 184

CHAPITRE VI. — ÉTUDE LOCALE 186

1. Étude locale des polynômes abéliens de degré l sur Q..... 186
2. Étude de $Q_p(l)$ 187
3. Extensions abéliennes de Q_p de degré l impair..... 189
4. Dénombrement des extensions abéliennes de degré l de Q_p.... 195

BIBLIOGRAPHIE 199

CHAPITRE PREMIER

CORPS CIRCULAIRES ET IDÉAUX ESSENTIELS

On notera dans ce qui suit, $C(m)$ le corps circulaire engendré par une racine primitive $m^{\text{ième}}$ de l'unité ε. On sait que ε est zéro d'un polynôme à coefficients entiers, normé, irréductible sur le corps Q des nombres rationnels. Le degré de ce polynôme est égal à $\varphi(m)$.

Les $\varphi(m)$ éléments du groupe de Galois $G(m)$ de $C(m)$ sont les $\varphi(m)$ automorphismes notés $[i]$ et définis par l'égalité $[i]f(\varepsilon) = f(\varepsilon^i)$ (i mod m, premier avec m).

Si $\alpha \in C(m)$, on notera α_i son conjugué $[i]\alpha$.

1. Propriétés arithmétiques de $C(l)$.

1) *Idéaux premiers de* $C(l)$. — l premier, impair.

Les idéaux premiers apparaissent quand on cherche à décomposer les nombres premiers naturels dans le domaine des entiers de $C(l)$. Nous rappelons les résultats suivants [8] que nous utiliserons dans la suite de cet exposé :

Si p désigne un nombre premier naturel et f l'exposant minimum tel que $p^f \equiv 1 \bmod l$, f divise $l - 1$. De plus, l'idéal (p) se décompose en $e = \dfrac{l-1}{f}$ idéaux premiers distincts de degré f :

$$(p) = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_e.$$

Si F désigne le groupe de décomposition des $\mathfrak{p}_i$ et G un ensemble de représentants des classes du groupe quotient $G(l)/F$, on peut écrire :

$$(p) = \prod_{i' \in G} \mathfrak{p}_{i'}.$$

L'idéal (l) est totalement ramifié, $(l) = \mathfrak{l}^{l-1}$ avec $\mathfrak{l} = (1 - \varepsilon)$, $\mathfrak{l}$ est encore un idéal du premier degré.

Nous savons que les idéaux de $C(l)$ ne sont pas forcément principaux. Cependant l'indice h du sous-groupe des idéaux principaux dans le groupe multiplicatif des idéaux d'un corps algébrique est fini [8]. Le nombre de classes h d'un corps circulaire $C(l)$ se met sous la forme $h = h_0 h_1$ où h_0 désigne le nombre de classes du sous-corps réel maximum de $C(l)$ et h_1 un nombre entier naturel. On montre [4] que $h_1 = 1$ si $3 \leqslant l \leqslant 19$ et que $h_1 > 1$ si $23 \leqslant l < 100$. En outre les majorations classiques du nombre de classes d'un corps de nombres algébriques [5], [12] entraînent $h_0 = 1$ si $3 \leqslant l \leqslant 19$. On en déduit que $C(l)$ est principal si $3 \leqslant l \leqslant 19$ et ne l'est pas si $23 \leqslant l < 100$.

2) *Congruences dans* $C(l)$.

L'ensemble des entiers de $C(l)$ est réparti en $N(\mathfrak{m})$ classes par la congruence modulo un idéal entier $\mathfrak{m}$. En particulier si $\mathfrak{m}$ est un idéal premier du premier degré, nous remarquerons que tout entier de $C(l)$ est congru modulo $\mathfrak{m}$ à un entier rationnel. Plus généralement si n est un entier rationnel et $\mathfrak{p}$ un idéal premier, la congruence

$$n \equiv 0 \bmod \mathfrak{p} \qquad \text{équivaut à} \qquad n \equiv 0 \bmod N(\mathfrak{p}).$$

Le nombre des classes mod $\mathfrak{m}$ premières avec $\mathfrak{m}$ est égal à $\varphi[N(\mathfrak{m})]$.

3) *Unités de* $C(l)$.

Les unités de $C(l)$ forment un groupe multiplicatif avec un nombre fini de générateurs.

Les unités de $C(l)$ s'écrivent de façon unique sous la forme :

$$u = (-1)^{n_1} \varepsilon^{n_2} \xi_1^{r_1} \xi_2^{r_2} \dots \xi_q^{r_q}$$

où
$$\begin{cases} \xi_1, \xi_2, \dots, \xi_q & \text{unités fondamentales} \\ q = \dfrac{l-3}{2}, & \\ & n_1 \bmod 2 \\ & n_2 \bmod l \\ r_1, r_2, \dots, r_q & \text{entiers rationnels.} \end{cases}$$

Si on note $C_0(l)$ le sous-corps réel maximum de $C(l)$, E le groupe des unités de $C(l)$, U le sous-groupe des racines $l^{\text{ièmes}}$ de

l'unité et E_0 le groupe des unités de $C_0(l)$, l'indice $[E : UE_0]$ est égal à 1 [5]. Ceci revient à dire que l'on peut choisir comme système d'unités fondamentales des unités fondamentales de $C_0(l)$.

Exemples :

— Pour $l = 3$ les seules unités sont les racines sixièmes de 1.

— Pour $l = 5$ toute unité est le produit d'une racine dixième de 1 par une puissance entière de $\varepsilon_1 + \varepsilon_4$.

— Pour $l = 7$ le corps $C_0(7)$ est un corps abélien de degré 3 dont les unités s'écrivent comme produit de puissances entières de deux des zéros du polynôme $x^3 - x^2 - 2x + 1$ ou encore de deux des 3 nombres $\varepsilon_1 + \varepsilon_6$, $\varepsilon_2 + \varepsilon_5$, $\varepsilon_3 + \varepsilon_4$ [2], [6].

2. Idéaux essentiels de C(*l*).

1) *Définition.*

Nous appellerons essentiel [3] un idéal $\mathfrak{m}$ qui vérifie les deux conditions :

1. Pour tout i le produit $\mathfrak{m}_1^i \mathfrak{m}_i^{-1}$ est une puissance entière d'exposant l d'un idéal $\mathfrak{n}_{1,i}$.

$$\mathfrak{m}_1^i \mathfrak{m}_i^{-1} = \mathfrak{n}_{1,i}^l.$$

2. Les idéaux $\mathfrak{m}_i$ et $\mathfrak{n}_{1,i}$ sont principaux.

2) *Caractérisation des idéaux essentiels de* C(l).

Étudions d'abord les conséquences de la première condition. Tout idéal d'un corps algébrique est produit de puissances d'idéaux premiers, nous désignerons par facteurs simples les produits de ceux de ses facteurs qui divisent un même nombre premier naturel. Pour qu'un idéal vérifie la première condition, il faut et il suffit que celle-ci soit vérifiée par chacun de ses facteurs simples.

Soit alors p un nombre premier naturel congru à 1 modulo l; notons P le facteur simple correspondant avec

$$P = \prod_{i=1}^{p-1} \mathfrak{p}_i^{h(i)}$$

les $\mathfrak{p}_i$ étant des idéaux premiers du premier degré.

Pour que P vérifie la condition (1), il faut et il suffit que $ih(i) \equiv a \bmod l$. En effet, exprimons que $P_1^j P_j^{-1}$ est une puissance $l^{\text{ième}}$:

$$P_1^j P_j^{-1} = \left(\prod_{i=1}^{l-1} \mathfrak{p}_i^{jh(i)}\right)\left(\prod_{i=1}^{l-1} \mathfrak{p}_{ij}^{-h(i)}\right) = \prod_{i=1}^{l-1} \mathfrak{p}_i^{jh(i)-h(ij^{-1})}$$

la première condition équivaut donc à :

$$jh(i) - h(ij^{-1}) \equiv 0 \bmod l \ \forall i \text{ et } \forall j$$

cela entraîne en prenant $j = i$:

$$ih(i) \equiv h(1) \bmod l.$$

On voit immédiatement que cette condition nécessaire est suffisante.

Soit maintenant p un nombre premier naturel, différent de l, et incongru à 1 modulo l. Le facteur simple correspondant s'écrira :

$$P = \prod_{i' \in G} \mathfrak{p}_{i'}^{h(i')}$$

où G désigne un système complet de représentants des classes de $G(l)/F$, F étant le groupe de décomposition des $\mathfrak{p}_{i'}$. Désignons par j_0 un élément de F autre que 1, il existe certainement puisque les $\mathfrak{p}_{i'}$ sont de degré supérieur à 1.

Appliquons la condition (1) pour l'indice j_0

$$\Rightarrow P_1^{j_0} P_{j_0}^{-1} = \left(\prod_{i' \in G} \mathfrak{p}_{i'}^{j_0 h(i')}\right)\left(\prod_{i' \in G} \mathfrak{p}_{i'j_0}^{-h(i')}\right) = \prod_{i' \in G} \mathfrak{p}_{i'}^{(j_0-1)h(i')}$$
$$= \mathfrak{n}_{1,j_0}^{l} \leftrightarrow (j_0 - 1)h(i') \equiv 0 \bmod l \quad \forall i'.$$

D'après le choix de j_0 cette condition équivaut à $h(i') \equiv 0 \bmod 1$ soit encore $P = P_1^l$.

Si $p = l$, $P = L = (1 - \varepsilon)^h$ et L vérifie la condition (1) si et seulement si $h \equiv 0 \bmod l$.

En rassemblant ces résultats et en numérotant convenablement les idéaux premiers du premier degré, nous voyons qu'une condition nécessaire et suffisante pour qu'un idéal $\mathfrak{m}$ de $C(l)$ vérifie la condition (1) est qu'il se mette sous la forme :

$$\mathfrak{m} = \mathfrak{n}^l \prod_{i=1}^{l-1} \mathfrak{p}_i^{i-{}^1h(1)} \mathfrak{p}'^{i-{}^1h'(1)}_i \cdots \mathfrak{p}_i^{(n)i-{}^1h^{(n)}(1)}$$

avec $h(1), h'(1), \ldots, h^{(n)}(1) \not\equiv 0 \bmod l$. On peut mettre $\mathfrak{m}$ sous une forme plus simple en remplaçant $\mathfrak{p}_i^{(k)}$ par $\mathfrak{p}_{ih^{(k)}(1)^{-1}}^{(k)}$ (ce qui revient à indexer différemment les $\mathfrak{p}_i^{(k)}$)

$$\mathfrak{m} = \mathfrak{n}^l \prod_{i=1}^{l-1} \mathfrak{a}_i^{i^*}$$

où $\mathfrak{a}_i$ est un produit d'idéaux premiers du premier degré tel que $N(\mathfrak{a}_i)$ soit sans facteur carré et premier avec l et où i^* est défini par :

$$\begin{cases} i.i^* \equiv 1 \bmod l \\ 1 \leqslant i^* \leqslant p-1. \end{cases}$$

Étudions maintenant les conséquences de la deuxième condition.

Soit $p \equiv 1 \bmod l$ un nombre premier naturel et $\mathfrak{p}_i$ ses diviseurs premiers dans $C(l)$. On note ω une racine primitive $p^{\text{ième}}$ de l'unité et $\tau = \sum_x \omega^x \varepsilon^{\operatorname{ind} x}$ $\begin{cases} x \text{ de } 1 \text{ à } p-1 \\ \operatorname{ind} x \bmod p-1 \end{cases}$ où ind x est défini à l'aide d'une classe primitive $g \bmod p$ par :

$$x \equiv g^{\operatorname{ind} x} \bmod p$$

τ appartient *a priori* au corps $C(p, l)$ composé de $C(p)$ et $C(l)$, nous pouvons cependant énoncer [3] :

$\theta = \tau^l$ est un entier de $C(l)$, l'idéal (θ) est essentiel et égal à l'un des conjugués de l'idéal

$$\mathfrak{a} = \prod_{i=1}^{l-1} \mathfrak{p}_i^{i^*}.$$

Nous appellerons formellement essentiel un idéal qui vérifie la condition (1) et facteur banal d'un idéal formellement essentiel $\mathfrak{m} = \mathfrak{n}^l \prod_{i=1}^{l-1} \mathfrak{a}_i^{i^*}$ l'idéal $\mathfrak{n}^l$.

Le théorème précédent montre que tout idéal formellement essentiel sans facteur banal est essentiel.

Si $\mathfrak{m} = \mathfrak{n}^l \prod_{i=1}^{l-1} \mathfrak{a}_i^{i^*}$ est un idéal formellement essentiel nous venons de voir que $\prod_{i=1}^{l-1} \mathfrak{a}_i^{i^*}$ est un idéal essentiel, pour que $\mathfrak{m}$ soit essentiel il faut et il suffit donc que $\mathfrak{n}^l$ soit essentiel,

c'est-à-dire que $\mathfrak{n}$ soit principal. Compte tenu de la propriété [3] : si la puissance $l^{\text{ième}}$ d'un idéal $\mathfrak{n}$ est un idéal essentiel, cet idéal est principal; nous pouvons caractériser les idéaux essentiels de $C(l)$.

THÉORÈME 1. — *Pour qu'un idéal* $\mathfrak{m}$ *de* $C(l)$ *soit essentiel, il faut et il suffit qu'il puisse s'écrire sous la forme :*

$$\mathfrak{m} = (\lambda^l) \prod_{i=1}^{l-1} \mathfrak{a}_i^{i*}$$

λ *étant un élément de* $C(l)$ *et* $\mathfrak{a}_i$ *un produit d'idéaux premiers du premier degré tel que* $N(\mathfrak{a}_i)$ *soit sans facteur carré et premier avec* l.

Un idéal essentiel de la forme $\prod_{i=1}^{l-1} \mathfrak{a}_i^{i*}$ sera appelé canonique.

Cas particulier. — L'étude que nous allons poursuivre se simplifiera notablement dans le cas où $C(l)$ est à idéaux principaux. Les idéaux $\mathfrak{a}_i$ sont alors principaux et on définira des $(l-1)$-uples canoniques d'entiers conjugués de $C(l)$:

DÉFINITION. — *On appellera* $(l-1)$*-uple canonique de* $C(l)$ *un ensemble de* $l-1$ *entiers conjugués premiers entre eux* $||\alpha_1, \alpha_2, \ldots, \alpha_{p-1}||$ *de* $C(l)$ *tels que* $N(\alpha_i)$ *soit sans facteur carré et sans facteur commun avec* l.

Les résultats obtenus ci-dessus montrent que les bases d'un idéal essentiel canonique sont les entiers associés à $\alpha_1^{1*}, \alpha_2^{2*}, \ldots, \alpha_{p-1}^{(p-1)*}$. Tout idéal essentiel s'écrira alors sous la forme :

$$\mathfrak{m} = \left(\lambda^l \prod_{i=1}^{l-1} \alpha_i^{i*}\right).$$

Exemples. — Les idéaux essentiels de $C(3)$ sont engendrés par les nombres de la forme $\lambda^3\alpha_1\alpha_2^2$ [2].

Les idéaux essentiels de $C(5)$ sont engendrés par les nombres de la forme $\lambda^5\alpha_1\alpha_2^3\alpha_3^2\alpha_4^4$.

Ceux de $C(7)$ sont obtenus à partir des nombres $\lambda^7\alpha_1\alpha_2^4\alpha_3^5\alpha_4^2\alpha_5^3\alpha_6^6$.

CHAPITRE II

CONSTRUCTION DES CORPS ABÉLIENS DE DEGRÉ PREMIER *l* IMPAIR

1. *l*-Uples d'éléments conjugués irrationnels.

Soit K un corps abélien absolu de degré premier l impair. Le groupe de Galois de K est isomorphe au groupe des permutations circulaires de l éléments. Nous supposerons que les éléments θ_u d'un l-uple de conjugués irrationnels de K sont numérotés modulo l de façon que les automorphismes de K notés $1, \sigma, \ldots, \sigma^{l-1}$ satisfassent aux équations :

$$\sigma^h(\theta_u) = \theta_{u+h}.$$

Nous utiliserons dans ce qui suit les résolvantes de Lagrange :

$$\overline{\theta_{u,j}} = \sum_{t \bmod l} \varepsilon_j^t \theta_{u+t}.$$

Ces résolvantes appartiennent au corps $\mathfrak{k}$ composé de K et de $C(l)$. $\mathfrak{k}$ est un corps abélien absolu de degré $l(l-1)$, [1] et si $P(\theta_u, \varepsilon)$ désigne un de ses éléments on pourra noter $[j]\sigma^h$ (j premier avec l mod l et h mod l) ses automorphismes avec l'égalité :

$$[j]\sigma^h(P(\theta_u, \varepsilon)) = P(\theta_{u+h}, \varepsilon_j).$$

Pour qu'un élément A de $\mathfrak{k}$ appartienne à $C(l)$ (resp K) il faut et il suffit que $\sigma^h(A) = A \forall h$ (resp $[j]A = A \forall j$).

Remarquons enfin que :

$$[k]\overline{\theta_{u,j}} = \overline{\theta_{u,kj}}$$

$$\sigma^h\,\overline{\theta_{u,j}} = \sum_{t \bmod l} \varepsilon_j^t\, \theta_{u+t+h} = \sum_{t'=t+h} \varepsilon_j^{t'-h}\, \theta_{u+t'}$$

ce qui entraîne :

$$\sigma^h \overline{\theta_{u,j}} = \overline{\theta_{u+h,j}} = \varepsilon_j^{-h} \overline{\theta_{u,j}}.$$

THÉORÈME 2. — *Si* $\{\theta_u\}$ *est un l-uple de conjugués irrationnels de* K, *le nombre* $\overline{\theta_{u,j}}^l$ *appartient à* $C(l)$, *ce n'est pas une puissance* $l^{\text{ième}}$ *exacte dans* $C(l)$, *c'est une base d'un idéal essentiel* $\mathfrak{m}_j$ *et il existe* $\lambda_j \in C(l)$ *tel que :*

$$\overline{\theta_{u,j}}\,\overline{\theta_{u,l-j}} = \lambda_j \lambda_{l-j}\, p_1 p_2 \ldots p_n$$

les p_i *étant des entiers premiers deux à deux distincts tels que* $p_i \equiv 1 \mod l$.

Démonstration. — On peut écrire :

$$\sigma^h \overline{\theta_{u,j}}^l = (\sigma^h \overline{\theta_{u,j}})^l = (\varepsilon_j^{-h} \overline{\theta_{u,j}})^l = \overline{\theta_{u,j}}^l$$

ce qui montre que $\overline{\theta_{u,j}}^l \in C(l)$. Montrons alors que l'idéal principal $(\overline{\theta_{u,j}}^l) = \mathfrak{m}_j$ vérifie la première propriété des idéaux essentiels :

$$\mathfrak{m}_j^i \mathfrak{m}_{ji}^{-1} = (\overline{\theta_{u,j}}^{li}\, \overline{\theta_{u,ij}}^{-l}) = (\overline{\theta_{u,j}}^{i}\, \overline{\theta_{u,ij}}^{-1})^l$$

mais $\overline{\theta_{u,j}}^i\, \overline{\theta_{u,ij}}^{-1} \in C(l)$ car les automorphismes σ^h le laissent invariant, les conditions (1) et (2) sont donc vérifiées.

$\overline{\theta_{u,j}}^l$ n'est certainement pas une puissance $l^{\text{ième}}$ exacte dans $C(l)$ sinon $\overline{\theta_{u,j}} \in C(l) \forall_j \Leftrightarrow \theta_u \in C(l)$ et l'intersection de K et de $C(l)$ ne se réduirait pas à Q ce qui est impossible en raison des degrés respectifs de K et de $C(l)$.

On peut écrire :

$$\overline{\theta_{u,j}}^l = (\lambda_j^l) \prod_{i=1}^{l-1} \mathfrak{a}_{ij}^{i*}.$$

Supposons que $N(\mathfrak{a}_{ij}) = p_1 p_2 \ldots p_n$ et notons P_k le facteur simple de p_k, nous avons vu que ce facteur simple est un idéal ayant pour base une puissance $l^{\text{ième}} \tau_{kj}^l$ d'un élément de $C(l, p_k)$. On peut écrire :

$$\overline{\theta_{u,j}}^l = u \varepsilon_j^n \lambda'^l_j \prod_{k=1}^{r} \tau_{kj}^l$$

où u désigne une unité réelle de $C(l)$.

On en déduit :

$$\overline{\theta_{u,j}}^l\, \overline{\theta_{u,l-j}}^l = u^2 (\lambda'_j \lambda'_{l-j})^l \prod_{k=1}^{r} (\pm p_k)^l$$

mais $\overline{\theta_{u,j}}\,\overline{\theta_{u,l-j}}$ appartient à C(l) donc u^2 est une puissance $l^{\text{ième}}$ exacte, ce qui est également vrai pour u et on peut écrire :

$$\overline{\theta_{u,j}}^{\,l} = \varepsilon_j^n \lambda_j^l \prod_{k=1}^{r} \tau_{kj}^l = \varepsilon_j^n \lambda_j^l \mu_j$$

en remarquant que $\overline{\theta_{u,j}}\,\overline{\theta_{u,l-j}}$ est un nombre réel positif on en déduit que :

$$\overline{\theta_{u,j}}\,\overline{\theta_{u,l-j}} = \lambda_j \lambda_{l-j} p_1 p_2 \ldots p_n.$$

Dans le cas particulier où C(l) est à idéaux principaux μ_j s'exprime simplement à l'aide des $(l-1)$-uples canoniques :

$$\mu_j = \prod_{i=1}^{l-1} \alpha_{ji}^{i^*}$$

La réciproque s'énonce de la façon suivante :

THÉORÈME 3. — *Si $\mathfrak{m}_j$ est un idéal essentiel de* C(l), *on peut en choisir une base $\lambda_j^l \mu_j$ non puissance $l^{\text{ième}}$ exacte dans* C(l) *qui vérifie*

$$\lambda_j^l \lambda_{l-j}^l \mu_j \mu_{l-j} = \mathrm{A}^l (p_1 p_2 \ldots p_n)^l$$

où A *désigne un élément du sous-corps réel de* C(l). *A chaque base de $\mathfrak{m}_j$ satisfaisant à la condition précédente et à chaque nombre rationnel s correspond un l-uple de conjugués irrationnels d'un corps abélien* K *de degré l sur* Q, *de trace s, tel que*

$$\overline{\theta_{u,j}}^{\,l} = \lambda_j^l \mu_j.$$

Démonstration. — Nous avons vu que tout idéal essentiel $\mathfrak{m}$ est de la forme :

$$\mathfrak{m} = (\lambda^l) \prod_{i=1}^{l-1} \mathfrak{a}_i^{i^*}.$$

Si C(l) est à idéaux principaux on pourra choisir comme base : $\lambda_j^l \prod_{i=1}^{l-1} \alpha_i^{i^*}$ où α_i est un entier base de $\mathfrak{a}_i$, elle répond bien à la condition puisque $\prod_{i=1}^{l-1} \alpha_i = p_1 p_2 \ldots p_n$. Dans le cas où $\mathfrak{m}$ est l'idéal unité de C(l) ou un idéal essentiel banal on choisira $\mu_j = \varepsilon_j$.

Dans les autres cas on peut écrire :

$$\mathfrak{m} = (\lambda^l) \prod_{k=1}^{n} \prod_{i=1}^{l-1} \mathfrak{p}_{i,k}^{i^*}$$

Nous avons vu que $\prod_{i=1}^{l-1} \mathfrak{p}_{i,k}^{i^*}$ est un facteur simple dont une base est un conjugué de τ_k^l élément défini à partir de $C(l, p_k)$. Par ailleurs $\tau_k^l . [l-1] (\tau_k^l) = \pm p_k$, la base $\lambda^l \mu$ obtenue en posant $\mu = \prod_{k=1}^{n} \tau_k^l$ satisfait donc à la condition

$$\lambda_j^l \lambda_{l-j}^l \mu_j \mu_{l-j} = A^l p_1 p_2 \ldots p_n$$

et ce n'est pas une puissance $l^{\text{ième}}$ exacte.

Désignons maintenant par r un élément défini modulo l qui engendre le groupe multiplicatif modulo l.

$(\lambda_r^l \mu_r)$ étant essentiel, la première propriété entraîne $\left(\frac{\mu_r}{\mu^r}\right)$ est puissance $l^{\text{ième}}$ d'un idéal principal de $C(l)$ ce que l'on peut écrire :

$\frac{\mu_r}{\mu^r} = \varepsilon^h u A_r^l$ où u désigne une unité réelle de $C(l)$. On en déduit :

$\frac{\mu_{l-r}}{\mu_{l-1}^r} = \varepsilon^{l-h} u A_{l-r}^l$ le produit membre à membre de ces deux égalités montre que u est une puissance $l^{\text{ième}}$ exacte dans $C(l)$ et on peut le faire entrer dans le terme A_r^l.

Montrons que $h \equiv 0 \bmod l$, nous pouvons écrire :

$$\begin{cases} \frac{\mu_r}{\mu^r} = \varepsilon^h B_r^l \\ \frac{\mu_{r^2}}{\mu_r^r} = \varepsilon^{rh} B_{r^2}^l \\ \vdots \\ \frac{\mu_{r^{l-1}}}{\mu_{r^{l-2}}^r} = \varepsilon^{r^{l-2}h} B_{r^{l-1}}^l \end{cases}$$

d'où il résulte :

$$\frac{\mu_{r^{l-1}}}{\mu^{r^{l-1}}} = \varepsilon^{hr^{l-2}(l-1)} [B_r^{r^{l-2}} B_{r^2}^{r^{l-3}} \ldots B_{r^{l-1}}]^l$$

mais $\mu_{r^{l-1}} = \mu$ entraîne que $\frac{\mu_{r^{l-1}}}{\mu^{r^{l-1}}}$ est une puissance $l^{\text{ième}}$ exacte

dans $C(l)$. On en déduit que :

$$hr^{l-2}(l-1) \equiv 0 \mod l$$

donc

$$h \equiv 0 \mod l.$$

L'égalité $\left(\frac{\mu^r}{\mu_r}\right)^{r^{n-1}} \cdot \left(\frac{\mu_r}{\mu_{r^2}}\right)^{r^{n-2}} \cdots \frac{\mu_{r^{n-1}}^r}{\mu_{r^n}} = \frac{\mu^{r^n}}{\mu_{r^n}}$ valable pour tout entier n, montre que si $\frac{\mu^r}{\mu_r}$ est une puissance $l^{\text{ième}}$ exacte dans $C(l)$, il en est de même pour $\frac{\mu^j}{\mu_j}$ $\forall j \in \{1, 2, \ldots, l-1\}$.

Considérons le corps $\mathfrak{k}$ obtenu par adjonction à $C(l)$ des racines $l^{\text{ièmes}}$ de $\lambda^l\mu$, d'après ce qui vient d'être dit $\mathfrak{k}$ contient également les racines $l^{\text{ièmes}}$ de $\lambda_j^l\mu_j$ pour tout j. Notons enfin $\omega_{0,1}, \omega_{1,1}, \ldots, \omega_{l-1,1}$ les racines $l^{\text{ièmes}}$ de $\lambda^1\mu$ avec $\omega_{u,1} = \varepsilon^{-u}\omega_{0,1}$. $\omega_{0,1}$ est un élément primitif de $\mathfrak{k}$ relativement à Q et $\mathfrak{k}$ est abélien relativement à $C(l)$. Les automorphismes de $\mathfrak{k}$ relativement à Q substituent à $\omega_{0,1}$ les racines $l^{\text{ièmes}}$ des $\lambda_j^l\mu_j$.

Notons σ l'automorphisme qui substitue $\omega_{1,j}$ à $\omega_{0,j}$. $\sigma(\lambda^l\mu) = \sigma(\omega_{0,1}^l) = (\varepsilon^{-1}\omega_{0,1})^l = \lambda^l\mu$ montre que σ laisse invariant l'élément primitif $\lambda^l\mu$ de $C(l)$, donc $C(l)$ tout entier. Il en résulte que $\sigma^h.\omega_{0,1} = \omega_{h,1}$.

Soit alors ω_j une racine $l^{\text{ième}}$ de $\lambda_j^l\mu_j$ nous savons que $\omega_j = A\omega_{0,1}^j$ avec $A \in C(l)$ donc $\sigma\omega_j = \sigma.A.\sigma\omega_{0,1}^j = \varepsilon^{-j}\omega_j$. Considérons maintenant les l automorphismes de $\mathfrak{k}$ qui substituent à $\omega_{0,1}$ une des racines $l^{\text{ième}}$ de $\lambda_j^l\lambda_j$, la restriction de ces automorphismes à $C(l)$ coïncide avec $[j]$, notons-les provisoirement $\varphi_1, \varphi_2, \ldots, \varphi_l$. Nous remarquerons que $\varphi_2 = \sigma^{h_2}\varphi_1, \ldots, \varphi_l = \sigma^{h_l}\varphi_1$ et que ces automorphismes commutent avec les puissances de σ, leurs puissances $(l-1)^{\text{ièmes}}$ sont donc deux à deux distinctes et font correspondre à $\omega_{0,1}$ des racines $l^{\text{ièmes}}$ de

$$\lambda_{j^{l-1}}^l\mu_{j^{l-1}} = \lambda^l\mu,$$

l'une de ces puissances $(l-1)^{\text{ièmes}}$ est donc l'automorphisme identité, notons $[j]$ le φ_i correspondant et posons $\omega_{0,1} = [j]\omega_{0,1}$. On voit alors que $\mathfrak{k}$ est un corps abélien absolu de degré $l(l-1)$.

Les nombres $\theta_u = \frac{1}{l}\left(\sum_j \omega_{u,j} + s\right)$ appartiennent au sous-corps K réel de degré l et forment bien un l-uple de conjugués irrationnels de trace s de ce corps.

COROLLAIRE 1. — *Pour que deux l-uples* $||\theta_u||$, $||\vartheta_u||$ *ordonnés appartiennent à une même extension abélienne de degré* l *de* Q, *il faut et il suffit que le quotient* $\dfrac{\overline{\theta_{u,j}}^{\,l}}{\vartheta_{u,j}^{\,l}}$ *soit une puissance* $l^{\text{ième}}$ *exacte dans* $C(l)$.

COROLLAIRE 2. — *Pour qu'une base de* $\mathfrak{m}$ *soit puissance* $l^{\text{ième}}$ *d'une résolvante de Lagrange d'un l-uple de conjugués irrationnels d'un corps abélien de degré* l *il faut et il suffit qu'elle soit de la forme:*

$\varepsilon^n u^l \lambda^l \mu$ *où* u *désigne une unité réelle et qu'elle ne soit pas puissance* $l^{\text{ième}}$ *exacte dans* $C(l)$.

Cette propriété résulte immédiatement de la condition nécessaire :

$$\overline{\theta_{u,j}}\,\overline{\theta_{u,l-j}} = \lambda_j \lambda_{l-j} p_1 p_2 \ldots p_n.$$

2. Ordres compatibles avec les permutations circulaires.

Nous avons choisi au départ une numérotation des θ_u telle que les automorphismes de K correspondent aux permutations circulaires des u, quelles sont les numérotations qui conviennent?

Soit Σ l'automorphisme de K représenté par la permutation σ : $\sigma(\theta_u) = \theta_{u+1}$ dans la numérotation initiale. Nous voulons que Σ soit encore représenté par une permutation circulaire dans la nouvelle numérotation $\theta_{\varphi(u)}$. Écrivons de deux façons différentes l'image de θ_u par Σ dans la nouvelle numérotation :

$\Sigma(\theta_u) = \theta_{\varphi\sigma(u)}$ et supposons que Σ est représenté par la permutation circulaire σ^h dans la nouvelle numérotation

$$\Longrightarrow \theta_{\varphi\sigma(u)} = \theta_{\sigma^h\varphi(u)} \Longleftrightarrow \varphi\sigma = \sigma^h\varphi.$$

On peut supposer en multipliant éventuellement par une permutation circulaire que $\varphi(0) = 0$ nous en déduisons :

$$\varphi\sigma(0) = \varphi(1) = \sigma^h(0) = h$$

supposons que :

$$\varphi(n) \equiv hn \bmod l$$

nous en déduisons :

$$\varphi\sigma(n) = \sigma^h(hn) \equiv hn + n = \varphi(n+1)$$

donc :

$$\varphi(n+1) \equiv h(n+1) \bmod l$$

cela entraîne $\varphi(n) \equiv hn \forall n$. Cette nouvelle numérotation est évidemment une numérotation telle que Σ soit représenté par une permutation circulaire.

Il y a donc $l-1$ façon d'ordonner convenablement à une permutation circulaire près les l-uples de conjugués d'un corps abélien K de degré l.

THÉORÈME 4. — *Si φ est une permutation des entiers modulo l correspondant à un ordre compatible avec les permutations circulaires* $\Longleftrightarrow \varphi(u) \equiv hu \bmod l$ *alors :*

$$\overline{\theta_{\varphi(u),j}}^{\,l} = \overline{\theta_{u,h*j}}^{\,l}.$$

Nous pouvons écrire :

$$\overline{\theta_{\varphi(u),j}} = \sum_t \theta_{\varphi(u+t)}\varepsilon_j^t = \sum_t \theta_{hu+ht}\varepsilon_j^t$$

d'où on tire :

$$\overline{\theta_{\varphi(u),j}} = \sum_{ht=t'} \theta_{hu+t'}\varepsilon_{h*j}^{t'} = \overline{\theta_{hu,h*j}}.$$

On en déduit bien que :

$$\overline{\theta_{\varphi(u),j}}^{\,l} = \overline{\theta_{hu,h*j}}^{\,l} = \overline{\theta_{u,h*j}}^{\,l}.$$

En rassemblant les résultats qui précèdent nous pouvons énoncer :

THÉORÈME 5. — *Si* K *est un corps abélien de degré l et si ses l-uples d'éléments conjugués irrationnels sont ordonnés à une permutation circulaire près il leur correspond un idéal essentiel canonique, si on change l'ordre des l-uples on obtient les idéaux essentiels canoniques conjugués.*

Réciproquement à un idéal essentiel canonique non banal (cf. Chapitre I, § II) correspondent l corps K avec des l-uples ordonnés à une permutation circulaire près. A ses conjugués correspondent les mêmes corps K mais des ordres différents pour les l-uples de conjugués. A l'idéal essentiel canonique banal : idéal unité ne correspond qu'un corps abélien de degré l avec les différents ordres possibles.

La correspondance est l'association à l'ensemble des puissances $l^{\text{ièmes}}$ des résolvantes de Lagrange $\overline{\theta_{u,j}}^{\,l}$ d'un corps K

du facteur canonique $\prod_{j=1}^{l-1} \mathfrak{a}_i^{i^*}$ de l'idéal essentiel contenant les $\overline{\theta_{u,j}}^{\,l}$.

Le théorème résulte alors des corollaires 1 et 2 et du fait qu'un idéal essentiel canonique non banal ne possède que l bases à une puissance $l^{\text{ième}}$ près qui satisfont aux conditions du théorème 3. Si μ en est une, les autres sont

$$\{\varepsilon_i \mu\} \, i = 1, \ldots, l-1.$$

Les bases de l'idéal unité qui conviennent sont à un facteur puissance $l^{\text{ième}}$ près : $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{l-1}$.

3. Polynômes abéliens de degré premier impair *l*.

Dans la construction des polynômes abéliens de degré l nous devrons distinguer deux cas suivant que les idéaux de C(l) sont tous principaux ou non, la première éventualité se prêtant à une étude plus précise et à une exploitation numérique éventuelle.

1) C(l) *est à idéaux principaux.*

On peut alors définir des $(l-1)$-uples canoniques (cf. Chapitre I) et les idéaux essentiels sont de la forme $\left(\lambda^l \prod_{i=1}^{l-1} \alpha_i^{i^*}\right)$, la base $\lambda^l \prod_{i=1}^{l-1} \alpha_i^{i^*}$ satisfait aux conditions du théorème 3 car $\prod_{i=1}^{l-1} \alpha_i = p_1 p_2 \ldots p_n$ et $i^* + (l-i)^* = l$. En outre $\prod_{i=1}^{l-1} \varepsilon_{ij}^{i^*} = \varepsilon_j^{l-1}$ ce qui montre que toutes les bases d'un idéal essentiel qui satisfont aux conditions du théorème 3 sont de la forme $\lambda^l \prod_{i=1}^{l-1} \alpha_i^{i^*}$.

Nous désignerons encore dans ce qui suit par r un élément dont la classe modulo l est primitive dans le groupe multiplicatif des classes modulo l.

LEMME 1. — *Les éléments* $\overline{\theta_{u,j}}\,\overline{\theta_{u,l-j}}$ *et* $\dfrac{\overline{\theta_{u,j}}\,\overline{\theta_{u,j-i}}}{\overline{\theta_{u,j}}}$ *où* $i \neq j$ *sont des monômes en* $\overline{\theta_{u,j'}}^{\,l}$ *et* $\dfrac{\overline{\theta_{u,j'}}^{\,r}}{\overline{\theta_{u,rj'}}}$.

Nous avons déjà montré (Chapitre II, § I) que les éléments

$\dfrac{\overline{\theta_{u,kj}}}{\overline{\theta_{u,j}}^{k}}$ sont des monômes en $\overline{\theta_{u,j'}}^{l}$, $\dfrac{\overline{\theta_{u,j'}}^{r}}{\overline{\theta_{u,rj'}}}$, il suffit de remarquer que $\dfrac{\overline{\theta_{u,i}}\,\overline{\theta_{u,j-i}}}{\overline{\theta_{u,j}}} = \dfrac{\overline{\theta_{u,i}}^{ji^*}}{\overline{\theta_{u,j}}} \times \dfrac{\overline{\theta_{u,j-i}}}{\overline{\theta_{u,i}}^{ji^*-1}}$ pour démontrer le lemme.

LEMME 2. — *Si* $\overline{\theta_{u,j}}^{l} = \lambda_j^l \prod_{i=1}^{l-1} \alpha_{ij}^{i^*}$ *alors*

$$\frac{\overline{\theta_{u,i}}\,\overline{\theta_{u,j-i}}}{\overline{\theta_{u,j}}} = \frac{\lambda_i\lambda_{j-i}}{\lambda_j} \prod_{k=1}^{l-1} \alpha_{ik}^{\frac{k^*+[ki(j-i)]^*-(kj^*)^*}{l}} \quad \begin{cases} \forall i, j \\ \text{et } i \neq j. \end{cases}$$

En effet $\overline{\theta_{u,j}}^{l} = \lambda_j^l \prod_{i=1}^{l-1} \alpha_{i-j^*}^{i^*}$ entraîne $\dfrac{\overline{\theta_{u,j}}^{r}}{\overline{\theta_{u,rj}}} = \varepsilon^n \dfrac{\lambda_j^r}{\lambda_{rj}} \prod_{i=1}^{l-1} \alpha_{ij}^{\frac{ri^*-(r^*i)^*}{l}}$ égalité obtenue en prenant une racine $l^{\text{ième}}$ de $\dfrac{\overline{\theta_{u,j}}^{lr}}{\overline{\theta_{u,rj}}}$.

On en déduit :

$$\begin{cases} \dfrac{\overline{\theta_{u,j}}^{r}}{\overline{\theta_{u,rj}}} = \varepsilon^n \dfrac{\lambda_j^r}{\lambda_{rj}} \prod_{i=1}^{l-1} \alpha_{ij}^{\frac{ri^*-(r^*i)^*}{l}} \\ \dfrac{\overline{\theta_{u,rj}}^{r}}{\overline{\theta_{u,r^2j}}} = \varepsilon^{nr} \dfrac{\lambda_{rj}^r}{\lambda_{r^2j}} \prod_{i=1}^{l-1} \alpha_{rij}^{\frac{ri^*-(r^*i)^*}{l}} \\ \vdots \\ \dfrac{\overline{\theta_{u,r^{l-2}j}}^{r}}{\overline{\theta_{u,r^{l-1}j}}} = \varepsilon^{nr^{l-2}} \dfrac{\lambda_{r^{l-2}j}^r}{\lambda_{r^{l-1}j}} \prod_{i=1}^{l-1} \alpha_{r^{l-2}ij}^{\frac{ri^*-(r^*i)^*}{l}} \end{cases}$$

En combinant ces égalités on obtient

$$\frac{\overline{\theta_{u,j}}^{r^{l-1}}}{\overline{\theta_{u,r^{l-1},j}}} = \overline{\theta_{u,j}}^{r^{l-1}-1} = \varepsilon^{n(l-1)r^{l-2}} \lambda_j^{r^{l-1}-1} \prod_{i=1}^{l-1} (\alpha_{ij}^{r^{l-2}}\, \alpha_{irj}^{r^{l-3}} \ldots \alpha_{r^{l-2}ij})^{\frac{ri^*-(r^*i)^*}{l}}$$

$r^{l-1} - 1$ est un multiple de l, et le membre de droite est nécessairement une puissance entière de $\lambda_j^l \prod_{i=1}^{l-1} \alpha_{ij}^{i^*}$ on en déduit $n \equiv 0 \bmod 1$. Le lemme 1 entraîne que $\dfrac{\overline{\theta_{u,i}}\,\overline{\theta_{u,j-i}}}{\overline{\theta_{u,j}}}$ est une expression rationnelle en $\lambda_{j'}$, et $\alpha_{ij'}^{i^*}$ ce qui précise laquelle des racines $l^{\text{ièmes}}$ de $\dfrac{\overline{\theta_{u,i}}^{l} \cdot \overline{\theta_{u,j-i}}^{l}}{\overline{\theta_{u,j}}^{l}}$ il faut choisir. Notons $\beta_{i,j}$ cette

racine $l^{\text{ième}}$ et posons $m = \alpha_1\alpha_2 \dots \alpha_{l-1}$, nous pouvons démontrer le :

THÉORÈME 6. — *Le polynôme abélien dont les racines* θ_u *de trace s vérifient* $\overline{\theta_{u,j}}^{l} = \lambda_j^l \prod_{i=1}^{l-1} \alpha_{ij}^{i^*}$ *s'écrit :*

$$\Delta = \begin{vmatrix} -(lx-s) & 1 & 1 & 1 & \dots & 1 \\ \lambda_1\lambda_{l-1}m & -(lx-s) & \beta_{1,2} & \beta_{1,3} & \dots & \beta_{1,l-1} \\ \lambda_2\lambda_{l-2}m & \beta_{2,1} & -(lx-s) & \beta_{2,3} & \dots & \beta_{2,l-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ \lambda_{l-1}\lambda_1 m & \beta_{l-1,1} & \beta_{l-1,2} & \beta_{l-1,3} & & -(lx-s) \end{vmatrix}$$

Démonstration. — Nous pouvons écrire :

$$l\theta_u - s = \overline{\theta_{u,1}} + \overline{\theta_{u,2}} + \dots + \overline{\theta_{u,l-1}}$$

et
$$(l\theta_u - s)\,\overline{\theta_{u,j}} = \overline{\theta_{u,1}}\,\overline{\theta_{u,j}} + \overline{\theta_{u,2}}\,\overline{\theta_{u,j}} + \dots + \overline{\theta_{u,l-1}}\,\overline{\theta_{u,j}}$$
$$= \beta_{j,1+j}\,\overline{\theta_{u,1+j}} + \beta_{j,2+j}\,\overline{\theta_{u,2+j}} + \dots \lambda_j\lambda_{l-j}m$$

le système :

$$\begin{cases} -(l\theta_u - s) + \overline{\theta_{u,1}} + \overline{\theta_{u,2}} + \dots + \overline{\theta_{u,l-1}} = 0 \\ \lambda_1\lambda_{l-1}m - (l\theta_u - s)\,\overline{\theta_{u,1}} + \beta_{1,2}\,\overline{\theta_{u,2}} + \dots + \beta_{1,l-1}\,\overline{\theta_{u,l-1}} = 0 \\ \vdots \\ \lambda_{l-1}\lambda_1 m + \beta_{l-1,1}\,\overline{\theta_{u,1}} + \dots - (l\theta_u - s)\,\overline{\theta_{u,l-1}} = 0 \end{cases}$$

admet la solution non banale 1, $\overline{\theta_{u,1}}$, $\overline{\theta_{u,2}}$, $\dots$ $\overline{\theta_{u,l-1}}$ et le déterminant associé est nul.

Pour vérifier que le polynôme obtenu en développant le déterminant est à coefficients rationnels il suffit de montrer que $[r]\Delta = \Delta$.

Numérotons les l lignes et colonnes du déterminant de 0 à $l-1$, les nombres β_{ij} sont alors situés dans la ligne et la colonne qui correspondent à leur indice. Posons en outre $\beta_{i,0} = \lambda_i\lambda_{l-i}\alpha_1\alpha_2 \dots \alpha_{l-1}$.

$[r]\Delta$ se déduit du déterminant initial en remplaçant $\beta_{i,j}$ par $[r]\beta_{i,j}$ mais la définition de $\beta_{i,j}$ montre que $[r]\beta_{i,j} = \beta_{ri,rj}$.

Notons $\hat{r}^*$ la permutation des lignes et des colonnes du déterminant qui fait correspondre à l'élément $\beta_{i,j}$ l'élément de la ligne r^*i et de la colonne r^*j (mod l).

$\hat{r}^*\Delta = \Delta$ car la signature de cette permutation produit de deux permutations de même parité est égale à $+1$. Dans cette transformation l'élément de la ligne ri et de la colonne

$rj \pmod{l}$ ira à l'intersection de la $i^{\text{ième}}$ ligne et de la $j^{\text{ième}}$ colonne, ce qui entraîne :

$$[r]\Delta = \hat{r}^*\Delta = \Delta.$$

2) *Les idéaux de* $C(l)$ *ne sont pas tous principaux.*

Il existe encore des $(l-1)$-uples canoniques mais leurs normes ne parcourent pas l'ensemble des produits, sans facteur carré, de nombres premiers congrus à 1 modulo l. Si $p_1p_2 \dots p_n$ est un tel produit et s'il n'existe pas d'élément de $C(l)$ de norme $p_1p_2 \dots p_n$ on ne peut pas déterminer explicitement la valeur de $\dfrac{\overline{\theta_{u,j}}^r}{\overline{\theta_{u,rj}}}$ à partir de celle de $\overline{\theta_{u,j}}^l$. On pourra cependant appliquer la méthode précédente qui donnera des polynômes abéliens de degré l à partir des $(l-1)$-uples canoniques mais nous n'obtiendrons pas tous les polynômes abéliens de degré l. Il sera toujours possible de déterminer les polynômes abéliens admettant comme racines des éléments conjugués du sous-corps de degré l de $C(l^2)$, on prendra $\alpha_i = \varepsilon_i$.

3) *Applications.*

a) Les polynômes abéliens de degré 3 sont de la forme [2] :

$$\begin{vmatrix} s-3x & 1 & 1 \\ \lambda_1\lambda_2\alpha_1\alpha_2 & s-3x & \dfrac{\lambda_1^2}{\lambda_2}\alpha_2 \\ \lambda_1\lambda_2\alpha_1\alpha_2 & \dfrac{\lambda_2^2}{\lambda_1}\alpha_1 & s-3x \end{vmatrix}$$
$$= (s-3x)^3 - 3\lambda_1\lambda_2\alpha_1\alpha_2(s-3x) + \alpha_1\alpha_2(\lambda_1^3\alpha_2 + \lambda_2^3\alpha_1).$$

b) Les polynômes abéliens de degré 5 sont de la forme [10] :

$$\begin{aligned}(5x-s)^5 &- 5m(\lambda_1\lambda_4 + \lambda_2\lambda_3)(5x-s)^3 \\ &- 5m\Big[\sum_{i=1}^{4}\lambda_i^2\lambda_{3i}\alpha_{2i}\alpha_{4i}\Big](5x-s)^2 \\ &+ 5m\Big[m(\lambda_1^2\lambda_4^2 + \lambda_2^2\lambda_3^2 - \lambda_1\lambda_2\lambda_3\lambda_4) \\ &- \sum_{i=1}^{4}\lambda_i\lambda_{3i}^3\alpha_i\alpha_{2i}^2\alpha_{4i}\Big](5x-s) \\ &- m\Big[\sum_{i=1}^{4}\lambda_i^5\alpha_{2i}^2\alpha_{3i}\alpha_{4i}^3 \\ &+ 5m\sum_{i=1}^{4}\alpha_i\alpha_{2i}(\lambda_i\lambda_{3i}^2\lambda_{4i}^2 - \lambda_{3i}^3\lambda_{2i}\lambda_{4i})\Big].\end{aligned}$$

c) Les polynômes abéliens de degré 7 sont de la forme :

$$\begin{vmatrix}
s-7x & 1 & 1 & 1 & 1 & 1 & 1 \\
\lambda_1\lambda_6 m & s-7x & \frac{\lambda_1^2}{\lambda_2}\alpha_2\alpha_3\alpha_6 & \frac{\lambda_1\lambda_2}{\lambda_3}\alpha_3\alpha_5\alpha_6 & \frac{\lambda_1\lambda_3}{\lambda_4}\alpha_2\alpha_4\alpha_6 & \frac{\lambda_1\lambda_4}{\lambda_5}\alpha_3\alpha_5\alpha_6 & \frac{\lambda_1\lambda_5}{\lambda_6}\alpha_2\alpha_3\alpha_6 \\
\lambda_2\lambda_5 m & \frac{\lambda_2\lambda_6}{\lambda_1}\alpha_4\alpha_1\alpha_5 & s-7x & \frac{\lambda_2\lambda_1}{\lambda_3}\alpha_6\alpha_3\alpha_5 & \frac{\lambda_2^2}{\lambda_4}\alpha_4\alpha_6\alpha_5 & \frac{\lambda_2\lambda_3}{\lambda_5}\alpha_4\alpha_6\alpha_5 & \frac{\lambda_2\lambda_4}{\lambda_6}\alpha_6\alpha_3\alpha_5 \\
\lambda_3\lambda_4 m & \frac{\lambda_3\lambda_5}{\lambda_1}\alpha_2\alpha_1\alpha_4 & \frac{\lambda_3\lambda_6}{\lambda_2}\alpha_2\alpha_1\alpha_4 & s-7x & \frac{\lambda_3\lambda_1}{\lambda_4}\alpha_6\alpha_2\alpha_4 & \frac{\lambda_3\lambda_2}{\lambda_5}\alpha_6\alpha_5\alpha_4 & \frac{\lambda_3^2}{\lambda_6}\alpha_6\alpha_2\alpha_4 \\
\lambda_3\lambda_4 m & \frac{\lambda_4^2}{\lambda_1}\alpha_1\alpha_5\alpha_3 & \frac{\lambda_4\lambda_5}{\lambda_2}\alpha_1\alpha_2\alpha_3 & \frac{\lambda_4\lambda_6}{\lambda_3}\alpha_1\alpha_5\alpha_3 & s-7x & \frac{\lambda_4\lambda_1}{\lambda_5}\alpha_5\alpha_6\alpha_3 & \frac{\lambda_4\lambda_2}{\lambda_6}\alpha_5\alpha_6\alpha_3 \\
\lambda_2\lambda_5 m & \frac{\lambda_5\lambda_3}{\lambda_1}\alpha_1\alpha_4\alpha_2 & \frac{\lambda_5\lambda_4}{\lambda_2}\alpha_3\alpha_1\alpha_2 & \frac{\lambda_5^2}{\lambda_3}\alpha_3\alpha_1\alpha_2 & \frac{\lambda_5\lambda_6}{\lambda_4}\alpha_1\alpha_4\alpha_2 & s-7x & \frac{\lambda_5\lambda_1}{\lambda_6}\alpha_3\alpha_6\alpha_2 \\
\lambda_1\lambda_6 m & \frac{\lambda_6\lambda_2}{\lambda_1}\alpha_5\alpha_4\alpha_1 & \frac{\lambda_6\lambda_3}{\lambda_2}\alpha_4\alpha_2\alpha_1 & \frac{\lambda_6\lambda_4}{\lambda_3}\alpha_5\alpha_3\alpha_1 & \frac{\lambda_6\lambda_5}{\lambda_4}\alpha_4\alpha_2\alpha_1 & \frac{\lambda_6^2}{\lambda_5}\alpha_5\alpha_4\alpha_1 & s-7x
\end{vmatrix}$$

CHAPITRE III

ENTIERS D'UN CORPS ABÉLIEN DE DEGRÉ PREMIER *l*

Nous avons vu au chapitre précédent qu'un corps abélien pouvait être caractérisé par une base μ_j convenable d'un idéal essentiel canonique.

Nous avons également montré que l'on pouvait choisir $\mu_j = \varepsilon_{jk}\tau^l_{j_1,i_1}.\tau^l_{j_2,i_2}\ldots\tau^l_{j_r,i_r}$, les nombres $\tau_{j,i}$ désignant des conjugués des éléments $\tau_{1,i} = \sum_{x=1}^{p_i-1} \omega^x \varepsilon^{\text{ind } x}$ (ind x mod $p_i - 1$). On en déduit :

$$\tau^l_{1,i} \equiv \sum_{x=1}^{p_i-1} \omega^{lx}\varepsilon^{l \text{ ind } x} \bmod l$$

soit encore :

$$\tau^l_{1,i} \equiv \sum_{x=1}^{p_i-1} \omega^{lx} \bmod l, \quad \text{mais} \quad \sum_{x=1}^{p_i-1} \omega^{lx} = -1$$

entraîne :

$$\mu_j \equiv \pm\, \varepsilon_{jk} \bmod l.$$

La donnée des restes $\pm\varepsilon_{jk}$ des nombres μ_j modulo l détermine les restes des μ_j modulo $(1-\varepsilon)^l$.

PROPOSITION. — *Si* $\mu_j \equiv \pm 1$ *mod* l *la congruence*

$$\mu_j \equiv \xi^l \text{ mod } (1-\varepsilon)^l$$

est soluble dans $C(l)$.

Si $\mu_j \equiv \pm\, \varepsilon_{jk}$ *mod* l, $k \not\equiv 0$ *mod* l *la congruence*

$$\mu_j \equiv \xi^l \text{ mod } (1-\varepsilon)^l$$

est insoluble dans $C(l)$.

Si $\mu_j \equiv \pm 1 \bmod l$ nous pouvons écrire :

$$\mu_j \equiv \pm 1 + el \bmod (1-\varepsilon)^l$$

où e est un entier rationnel, on en déduit :

$$\mu_{l-j} \equiv \pm 1 + el \bmod (1-\varepsilon)^l$$

ce qui entraîne :

$$\mu_j \mu_{l-j} \equiv 1 \pm 2el \bmod (1-\varepsilon)^l$$

mais nous savons que :

$$\mu_j \mu_{l-j} = (p_1 p_2 \dots p_r)^l \quad \text{avec} \quad p_i \equiv 1 \bmod l \forall i$$

mais

$$p_i \equiv 1 \bmod l \Longrightarrow p_i^l \equiv 1 \bmod l^2 \Longrightarrow \mu_j \mu_{l-j} \equiv 1 \bmod l^2.$$

En rapprochant cette congruence de l'expression du reste de $\mu_j \mu_{l-j}$ modulo $(1-\varepsilon)^l$ on en déduit que $e \equiv 0 \bmod l$ d'où il résulte :

$$\mu_j \equiv \pm 1 \bmod (1-\varepsilon)^l.$$

Si $\mu_j \equiv \pm \varepsilon_{jk} \bmod l$, $k \not\equiv 0 \bmod l$, la congruence $\mu_j \equiv \xi_l \bmod l$ (et à fortiori mod $(1-\varepsilon)^l$) est insoluble, car si $\xi = \sum_{i=1}^{l-1} a_i \varepsilon_i$, a_i entier rationnel, $\xi^l \equiv \sum_{i=1}^{l-1} a_i^l \bmod l$ comme ε_{jk} n'est pas congru à un nombre rationnel mod l on en déduit que la congruence n'admet pas de solution dans C(l).

Les décompositions de $(1-\varepsilon)$ dans $\mathfrak{k}$ et de (l) dans K suivant le reste de $\mu_j \bmod l$ s'en déduisent [7].

THÉORÈME. — a) *Si* $\mu_j \equiv \xi^l \bmod (1-\varepsilon)^{l+1}$ *est soluble dans* C(l) *alors* $(1-\varepsilon) = \mathfrak{l}_1 \mathfrak{l}_2 \dots \mathfrak{l}_l$ *dans* $\mathfrak{k}$.

b) *Si* $\mu_j \equiv \xi^l \bmod (1-\varepsilon)^l$ *est soluble dans* C(l) *sans que la congruence précédente le soit :* $(1-\varepsilon)$ *reste premier dans* $\mathfrak{k}$.

c) *Si* $\mu_j \equiv \xi^l \bmod (1-\varepsilon)^l$ *est insoluble dans* C(l) *alors* $(1-\varepsilon) = \mathfrak{l}^l$ *dans* $\mathfrak{k}$.

Les décompositions correspondantes de (l) dans K s'en déduisent immédiatement :

a) $(l) = \mathfrak{l}_1 \mathfrak{l}_2 \dots \mathfrak{l}_l$.

b) (l) premier.

c) $(l) = (\mathfrak{l})^l$.

1. Corps unitaires.

DÉFINITION. — *Nous dirons qu'un corps abélien* K *de degré premier l est unitaire si on peut le construire à l'aide d'un nombre* $\mu_j \equiv 1 \bmod l$.

1) THÉORÈME 7. — *Le l-uple de conjugués de* K *construit avec* $\mu_j \equiv 1 \bmod l$, *la trace* $s = 1$ *et* $\lambda_j = 1$ *forme une base des entiers de* K.

Démonstration. — La congruence $\mu_j \equiv \xi^l \bmod (1-\varepsilon)^l$ est soluble, $(1-\varepsilon)$ se décompose donc dans $\mathfrak{k}$ de l'une des deux façons suivantes :

$$(1-\varepsilon) = \mathfrak{l}_1\mathfrak{l}_2 \ldots \mathfrak{l}_l$$
$$(1-\varepsilon) = \mathfrak{l} \text{ premier.}$$

Les θ_u sont déterminés à l'aide de $\overline{\theta_{u,j}}^l = \mu_j$. Si $(1-\varepsilon)$ est premier dans $\mathfrak{k}$

$$X^l - 1 \equiv 0 \bmod l \Longrightarrow X - \varepsilon_i \equiv 0 \bmod (1-\varepsilon)$$

mais comme $\varepsilon_i \equiv \varepsilon_j \bmod (1-\varepsilon)$, on voit que :

$$X^l - 1 \equiv 0 \bmod l \Longleftrightarrow X - \varepsilon_i \equiv 0 \bmod (1-\varepsilon).$$

Si $(1-\varepsilon) = \mathfrak{l}_1\mathfrak{l}_2 \ldots \mathfrak{l}_l$

$$X^l - 1 \equiv 0 \bmod l \Longrightarrow X - \varepsilon_i \equiv 0 \bmod \mathfrak{l}_u$$
$$\Longrightarrow X - \varepsilon_j \equiv 0 \bmod \mathfrak{l}_u \forall_u \text{ et } \forall_j$$

on peut alors écrire que :

$$X^l - 1 \equiv 0 \bmod l \Longleftrightarrow X - \varepsilon_i \equiv 0 \bmod (1-\varepsilon).$$

Les entiers $\overline{\theta_{u,j}}$ (de $\mathfrak{k}$) vérifient donc $\overline{\theta_{u,j}} \equiv \varepsilon_{ij} \bmod (1-\varepsilon)$ on en déduit la congruence dans $\mathfrak{k}$:

$$\sum_{j=1}^{l-1} \overline{\theta_{u,j}} + 1 \equiv 0 \bmod (1-\varepsilon)$$

mais $\sum_{j=1}^{l-1} \overline{\theta_{u,j}} + 1 = l\theta_u$ est un nombre de K.

Si $(1-\varepsilon)$ premier dans $\mathfrak{k}$: $(l) = \mathrm{L} = (1-\varepsilon)^{l-1}$ et

$$l\theta_u \equiv 0 \bmod (1-\varepsilon) \Longrightarrow l\theta_u \equiv 0 \bmod \mathrm{L} = (l)$$

et θ_u est entier.

Si $(1-\varepsilon) = \mathfrak{l}_1\mathfrak{l}_2 \ldots \mathfrak{l}_l$ alors

$$l\theta_u \equiv 0 \bmod \mathfrak{l}_v \forall v \Longrightarrow l\theta_u \equiv 0 \bmod \mathrm{L}_v \forall v$$

$$\Longrightarrow l\theta_u \equiv 0 \bmod \prod_{v=1}^{l} \mathrm{L}_v = (l)$$

θ_u est encore entier.

Les θ_u dont la trace est égale à 1 forment évidemment une base de l'espace vectoriel K sinon il existerait des ρ_u rationnels non tous nuls tels que :

$$\sum_{i=0}^{l-1} \rho_i \theta_{u+i} = 0$$

égalité qui serait vérifiée pour tout u, elle entraînerait alors :

$$\begin{vmatrix} \theta_u & \theta_{u+1} & \ldots & \theta_{u+l-1} \\ \theta_{u+1} & \theta_{u+2} & \ldots & \theta_u \\ \vdots & & & \\ \theta_{u+l-1} & \theta_u & \ldots & \theta_{u+l-2} \end{vmatrix} = s \prod_{j=1}^{l-1} \overline{\theta_{u,j}} = s(p_1 p_2 \ldots p_n)^{\frac{l-1}{2}} = 0$$

ce qui est impossible.

Si $||\theta_u||$ est un l-uple d'entiers conjugués de K, nous pouvons écrire :

$$\vartheta_u = \sum_{i \bmod l} \rho_i \theta_{u+i} \quad \rho_i \text{ rationnel } \forall_i$$

on en déduit :

$$\overline{\vartheta_{u,j}} = \sum_{i \bmod l} \rho_i \overline{\theta_{u+i,j}} = \sum_{i \bmod l} \rho_i \varepsilon_j^{-i} \overline{\theta_{u,j}}$$

soit encore :

$$\overline{\vartheta_{u,j}} = \overline{\theta_{u,j}} \sum_{i=1}^{l-1} (\rho_i - \rho_0)\varepsilon_j^{-i} = \lambda_j \overline{\theta_{u,j}}$$

ϑ_u étant entier il en est évidemment de même pour $\overline{\vartheta_{u,j}}^{\,l} = \lambda_j^l \overline{\theta_{u,j}}^{\,l}$ mais comme μ_j est sans facteur puissance $l^{\text{ième}}$ cela entraîne que λ_j est entier, les nombres $\rho_i - \rho_0$ sont donc des entiers rationnels et on peut écrire :

$$\vartheta_u = \rho_0 + \sum_{i=1}^{l-1} (\rho_i - \rho_0)\theta_{u+i}$$

comme ϑ_u et $\sum_{i=1}^{l-1} (\rho_i - \rho_0)\theta_{u+i}$ sont entiers on en déduit que ρ_0 est également entier, comme ρ_0 était déjà rationnel, on en déduit que les ρ_i sont tous des entiers rationnels.

2) *Bases normales d'un corps unitaire.*

Pour qu'un l-uple de conjugués ϑ_u de K forme une base des entiers de K(base normale) il faut et il suffit que la matrice carrée M qui permet de passer de la matrice unicolonne (θ_u) à la matrice unicolonne (ϑ_u) soit de la forme :

$$M = \begin{vmatrix} a_0 & a_1 & \dots & a_{l-1} \\ a_{l-1} & a_0 & \dots & a_{l-2} \\ a_{l-2} & a_{l-1} & \dots & \\ \vdots & & & \\ a_1 & a_2 & \dots & a_0 \end{vmatrix}$$

avec a_i entier rationnel $\forall_i$ et det. $M = \pm 1$.

Si N est la matrice obtenue en remplaçant a_i par b_i on voit que :

$$MN = \begin{vmatrix} c_0 & c_1 & \dots & c_{l-1} \\ c_{l-1} & c_0 & \dots & c_{l-2} \\ \vdots & & & \\ c_1 & c_2 & \dots & c_0 \end{vmatrix}$$

où $c_{l-i+j} = \sum_h a_{l-i+h} b_{j-h}$. L'ensemble de ces matrices forme donc un groupe multiplicatif abélien. L'étude des bases normales se ramène à l'étude de ce groupe.

Nous pouvons remarquer que :

$$\det M = (a_0 + a_1 + \dots + a_{l-1}) \prod_{j=1}^{l-1} \left[\sum_i (a_i - a_0)\varepsilon_j^i \right]$$

la condition $\begin{Bmatrix} \det M = \pm 1 \\ a_i \text{ entier rationnel} \end{Bmatrix}$ équivaut à :

$$\begin{cases} a_0 + a_1 + \dots + a_{l-1} = \pm 1 \\ \sum_{i=1}^{l-1} (a_i - a_0)\varepsilon_j^i = \lambda_j \quad \text{unité de } C(l). \end{cases}$$

Remarquons que :

$$\mathrm{Tr}(\lambda_j) = \sum_{i=1}^{l-1} (a_0 - a_i) = la_0 - (a_0 + a_1 + \dots + a_{l-1})$$

$$\Longrightarrow \mathrm{Tr}(\lambda_j) \equiv \pm 1 \bmod l.$$

A une matrice M correspond donc une unité de trace congrue

à $\pm 1 \bmod l$. Soit alors $\lambda_j = b_1\varepsilon_j + \cdots + b_{l-1}\varepsilon_j^{l-1}$ une unité de $C(l)$ telle que $\mathrm{Tr}(\lambda_j) \equiv \pm 1 \bmod l$.
La dernière condition équivaut à :

$$b_1 + b_2 + \cdots + b_{l-1} = \pm 1 + ml.$$

On recherche des entiers rationnels $a_0, a_1, \ldots, a_{l-1}$ tels que :

$$\begin{cases} a_0 + a_1 + \cdots + a_{l-1} = \pm 1 \\ a_i - a_0 = b_i \quad \forall i = 1, \ldots l-1 \end{cases}$$

les conditions posées montrent que :
$a_0 = -m$, $a_i = b_i - m$ est la solution de ce système d'équations.

La correspondance entre les matrices M et les unités λ_j de trace congrue à $\pm 1 \bmod l$ est donc biunivoque. Cette correspondance est un isomorphisme en raison de l'égalité :

$$\left(\sum_{i=0}^{l-1} a_i\varepsilon_j^i\right)\left(\sum_{i'=0}^{l-1} b_{i'}\varepsilon_j^{i'}\right) = \sum_{i''=0}^{l-1} \varepsilon_j^{i''} \sum_{i=0}^{l-1} a_i b_{l-i+i''}.$$

On peut voir directement que si α et β sont des entiers de $C(l)$

$$\mathrm{Tr}(\alpha)\,\mathrm{Tr}(\beta) \equiv \mathrm{Tr}(\alpha\beta) \bmod l$$

il suffit de remarquer que $\mathrm{Tr}(\varepsilon\alpha) \equiv \mathrm{Tr}(\alpha) \bmod l$ et que $\mathrm{Tr}(n\,\varepsilon\alpha) = n\,\mathrm{Tr}(\varepsilon\alpha)$ si n est entier rationnel.

Pour obtenir toutes les bases normales d'un corps abélien de degré l premier à partir de l'une d'elles il suffit donc de connaître le groupe multiplicatif des unités de $C(l)$ de trace congrue à $\pm 1 \bmod l$. Ce groupe contient le groupe multiplicatif des unités puissances $\dfrac{l-1}{2}$ ièmes exactes et les racines $l^{\text{ièmes}}$ de l'unité il est donc isomorphe au groupe des unités de $C(l)$.

Exemples :

Pour $l = 3$ il n'y aura que deux bases normales à une permutation circulaire près.

Pour $l = 5$, $\dfrac{1+\sqrt{5}}{2} = -(\varepsilon_2 + \varepsilon_3)$ est une unité fondamentale, et le groupe des unités de trace congrue à ± 1 modulo 5 admettra $1 - \varepsilon_2 - \varepsilon_3 = (\varepsilon_2 + \varepsilon_3)^2$ comme généra-

teur d'ordre infini, la matrice correspondante s'écrit :

$$\begin{vmatrix} 1 & 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & -1 & -1 \\ -1 & 0 & 1 & 0 & -1 \\ -1 & -1 & 0 & 1 & 0 \\ 0 & -1 & -1 & 0 & 1 \end{vmatrix}.$$

Pour $l = 7$ on peut choisir $\varepsilon_1 + \varepsilon_6$ et $\varepsilon_2 + \varepsilon_5$ comme unités fondamentales, et le groupe des unités de trace congrue à ± 1 mod 7 admettra $(\varepsilon_1 + \varepsilon_6)^3$ et $(\varepsilon_2 + \varepsilon_5)^3$ comme générateurs d'ordre infini, les matrices correspondantes s'écrivent :

$$\begin{vmatrix} -1 & 2 & -1 & 0 & 0 & -1 & 2 \\ 2 & -1 & 2 & -1 & 0 & 0 & -1 \\ -1 & 2 & -1 & 2 & -1 & 0 & 0 \\ 0 & -1 & 2 & -1 & 2 & -1 & 0 \\ 0 & 0 & -1 & 2 & -1 & 2 & -1 \\ -1 & 0 & 0 & -1 & 2 & -1 & 2 \\ 2 & -1 & 0 & 0 & -1 & 2 & -1 \end{vmatrix}$$

et

$$\begin{vmatrix} -1 & 0 & 2 & -1 & -1 & 2 & 0 \\ 0 & -1 & 0 & 2 & -1 & -1 & 2 \\ 2 & 0 & -1 & 0 & 2 & -1 & -1 \\ -1 & 2 & 0 & -1 & 0 & 2 & -1 \\ -1 & -1 & 2 & 0 & -1 & 0 & 2 \\ 2 & -1 & -1 & 2 & 0 & -1 & 0 \\ 0 & 2 & -1 & -1 & 2 & 0 & -1 \end{vmatrix}.$$

2. Corps non-unitaires.

DÉFINITION. — *Un corps abélien* K *de degré premier* l *est non-unitaire s'il peut être construit à l'aide d'un nombre* $\mu_j \equiv \varepsilon_{ij} \bmod l$ *avec* $i \not\equiv 0 \bmod l$.

THÉORÈME 8. — *Pour que le* l*-uple* $||\theta_u||$ *de trace* s *construit avec* $\lambda'_j \mu_j$ *soit formé d'entiers il faut et il suffit que les* λ_j *et* s *soient entiers et que* $\lambda_j \equiv 0 \bmod l$, $s \equiv 0 \bmod l$.

Démonstration. — Cette condition est manifestement suffisante car

$$\lambda_j \equiv 0 \bmod l \Longrightarrow \overline{\theta_{u,j}}' \text{ entier}$$

et

$$\overline{\theta_{u,j}}^{\,l} \equiv 0 \bmod l^l \Longrightarrow \overline{\theta_{u,j}} \equiv 0 \bmod l$$

donc

$$\theta_u = \frac{1}{l}\left(\sum_{j=1}^{l-1} \overline{\theta_{u,j}} + s\right) \quad \text{est entier.}$$

Pour mettre en évidence que cette condition est nécessaire, considérons :

$P = \prod_u (\theta_u - \theta_{u-1})$ comme $\sigma P = P$ ce nombre est un entier rationnel.

Par ailleurs :

$$\theta_u - \theta_{u-1} = \frac{1}{l}\left[\overline{\theta_{u,1}}(1-\varepsilon) + \overline{\theta_{u,2}}(1-\varepsilon_2) + \cdots + \overline{\theta_{u,l-1}}(1-\varepsilon_{l-1})\right]$$

ce qui entraîne :

$$P = \frac{1}{l^l} \prod_u \left(\sum_j \overline{\theta_{u,j}}(1-\varepsilon^j)\right).$$

En développant ce produit on obtient :

$$P = \frac{1}{l^l}\left[\sum_{j=1}^{l-1}\left(\prod_u \overline{\theta_{u,j}}\right)(1-\varepsilon^j)^l + \cdots + \sum_{j=1}^{l-1} \overline{\theta_{0,j}}^{n_1}\,\overline{\theta_{0,k_2 j}}^{n_2} \cdots \overline{\theta_{0,k_r j}}^{n_r}(1-\varepsilon^j)^{n_1}\cdots(1-\varepsilon^{k_r j})^{n_r} \times \sum_{E_1, E_2, \ldots, E_r} \varepsilon_j^{-\left[\sum_{u\in E_1} u + \sum_{u\in E_2} u+k_2 + \cdots + \sum_{u\in E_r} u+k_r\right]} + \cdots\right.$$

où $n_1 + n_2 + \cdots + n_r = l$, $n_i > 0$ et où le signe $\sum_{E_1, E_2 \ldots E_r}$ signifie que l'on étend la somme aux partitions $E_1, \ldots, E_r$ de $\{0, 1, \ldots, l-1\}$ telles que $\mathfrak{C}(E_i) = n_i$, où $\mathfrak{C}(E_i)$ désigne le nombre d'éléments de E_i.

LEMME. — *L'expression* $\sum_{E_1, E_2, \ldots, E_r} \varepsilon_j^{-\left[\sum_{u\in E_1} u + \sum_{u\in E_2} u+k_2 + \cdots + \sum_{u\in E_r} u+k_r\right]}$ *est toujours rationnelle; elle est nulle si*

$$n_1 + k_2 n_2 + \cdots + k_r n_r \not\equiv 0 \bmod l$$

et congrue à 0 *modulo* l *si* $n_1 + k_2 n_2 + \cdots + k_r n_r \equiv 0 \bmod l$.

Supposons $n_1 + k_2 n_2 + \cdots + k_r n_r \equiv h \not\equiv 0 \bmod l$ et notons

N(i) le nombre de partitions telles que :

$$\sum_{u\in E_1} u + k_2 \sum_{u\in E_2} u + \cdots + k_r \sum_{u\in E_r} u \equiv i \bmod l$$

alors $N(i) = N(i')\forall i'$. En effet, si on considère la partition $(E_1, E_2, \ldots, E_r)$ et la partition $\mathfrak{C}_t(E_1, E_2, \ldots E_r)$ obtenue en ajoutant à chaque u le nombre t mod l, $\mathfrak{C}_t$ matérialise une correspondance biunivoque entre les partitions de « somme » i et les partitions de somme $i + ht = i'$ comme $h \not\equiv 0 \bmod l$ cette dernière équation a toujours une solution $\Longrightarrow N(i) = N(i')$.

L'expression totale peut donc se mettre sous la forme :

$$\sum_{E_1 \cdots E_r} \varepsilon_j^{-\left[\sum_{u\in E_1} u + \cdots + k_r \sum_{u\in E_r} u\right]} = N(i)[1 + \varepsilon + \varepsilon_2 + \cdots + \varepsilon_{l-1}] = 0.$$

Si $n_1 + k_2 n_2 + \cdots + k_r n_r \equiv 0 \bmod l$ et si $N(i)$ désigne le nombre de partitions de somme $i \not\equiv 0 \bmod l$, désignons par $\mathcal{S}_h (h \not\equiv 0 \bmod l)$ la transformation qui fait correspondre à la partition $\{E_1, \ldots, E_r\}$ la partition obtenue en faisant le produit de u par h mod l. La nouvelle partition aura une somme égale à ih mod l et $N(i) = N(ih)$, la somme des termes correspondant à des partitions de « somme » incongrue à 0 modulo l est égale à $-N(i)$ et il reste $C_l^{E_1, E_2 \cdots E_r} - (l-1)N(i)$ termes égaux à 1, $C_l^{E_1, E_2 \cdots E_r}$ désignant le nombre de partitions $\{E_1 \ldots E_r\}$. Il est évident que $C_l^{E_1, E_2 \cdots E_r} \equiv 0 \bmod l$ et il résulte :

$$C_l^{E_1, E_2, \ldots, E_r} - (l-1)N(i) - N(i) \equiv 0 \bmod l.$$

Remarque. — La condition $n_1 + k_2 n_2 + \cdots + k_r n_r = 0$ est nécessaire et suffisante pour que :

$$\overline{\theta_{0,j}}^{n_1} \overline{\theta_{0,k_2 j}}^{n_2} \ldots \overline{\theta_{0,k_r j}}^{n_r} \in C(l).$$

Exprimons alors que P est entier

$$\Longrightarrow \sum_{j=1}^{l-1} \overline{\theta_{u,j}}^{l} (1 - \varepsilon_j)^l \equiv 0 \bmod l(1-\varepsilon)^l$$

mais $\overline{\theta_{u,j}}^{l} = \lambda_j^l \mu_j$ et $\lambda_j \equiv e \bmod 1 - \varepsilon$ avec e rationnel donc $\lambda_j^l \equiv e \bmod l$. On en déduit :

$$\sum_{j=1}^{l-1} \overline{\theta_{u,j}}^{l} (1 - \varepsilon_j)^l \equiv e \sum_{j=1}^{l-1} \varepsilon_{ij} (1 - \varepsilon_j)^l \equiv 0 \bmod l(1-\varepsilon)^l.$$

Étudions la congruence plus générale :

$$e\sum_{j=1}^{l-1}\varepsilon_{ij}(1-\varepsilon_j)^{nl}\equiv 0 \bmod l(1-\varepsilon_j)^{nl}$$

avec n entier rationnel mais $\left(\frac{1-\varepsilon_j}{1-\varepsilon}\right)=1+\varepsilon+\cdots+\varepsilon_{j-1}$ et la congruence équivaut à :

$$e\sum_{j=1}^{l-1}\varepsilon_{ij}(1+\varepsilon+\cdots+\varepsilon_{j-1})^{nl}\equiv 0 \bmod l$$

soit encore : $e\sum_{j=1}^{l-1} j^n\varepsilon_{ij}\equiv 0 \bmod l$ mais $\sum_{j=1}^{l-1} j^n\varepsilon_{ij}\not\equiv 0 \bmod l$ donc $e\equiv 0 \bmod l$. On en déduit donc que $\lambda'_j\equiv 0 \bmod (1-\varepsilon)^{l(l-2)}$ donc $\overline{\theta_{u,j}}^{\,l}\equiv 0 \bmod (1-\varepsilon)^{l(l-2)}$ ce qui entraîne $\overline{\theta_{u,j}}\equiv 0 \bmod \mathfrak{l}$ dans $\mathfrak{k}$ et comme θ_u est supposé entier avec

$$l\theta_u=\sum_{j=1}^{l-1}\overline{\theta_{u,j}}+s\Longrightarrow s\equiv 0 \bmod \mathfrak{l},$$

s étant un entier rationnel, on en déduit $s\equiv 0 \bmod l$.

$$\prod_u\left(\theta_u-\frac{s}{l}\right)=\frac{1}{l^l}\prod_u\left(\sum_j\overline{\theta_{u,j}}\right)$$

est alors entier.

Il nous reste à étudier l'expression :

$$A=\frac{1}{l^l}\prod_u\sum_j\overline{\theta_{0,j}}\,\varepsilon_j^{-u}$$

de la même façon que précédemment on peut écrire :

$$A=\frac{1}{l^l}\Big[\sum_j\overline{\theta_{0,j}}^{\,l}+\sum_j\sum_{E_1,E_2}\overline{\theta_{0,j^{n_1}}}\,\overline{\theta_{0,k_2j^{n_2}}}\,\varepsilon_j^{-\left[\sum_{u\in E_1}u+k_2\sum_{u\in E_2}u\right]}+\cdots$$

posons $\lambda_j=(1-\varepsilon_j)^{l-2}\lambda'_j$ avec λ'_j entier. Pour que A soit entier il faut et il suffit que :

$$\sum_j\mu_j\lambda'_j(1-\varepsilon_j)^{l(l-2)}\equiv 0 \bmod (1-\varepsilon)^{l(l-1)}$$

Comme précédemment on en déduit :

$$\lambda'_j\equiv 0 \bmod 1-\varepsilon\Longrightarrow\lambda_j\equiv 0 \bmod (1-\varepsilon)^{l-1}\simeq l.$$

COROLLAIRE. — *Si* $||\theta_u||$ *désigne le l-uple de conjugués obtenus avec* $\lambda_j = l$, μ_j *et* $s = 0$ *les entiers* $\{1, \theta_{u+1}, \ldots, \theta_{u+l-1}\}$ *forment une base des entiers de* K.

K n'admet pas de base normale puisque la somme d'un l-uple de conjugués entiers est congrue à 0 modulo l.

L'ensemble $\{1, \theta_{u+1}, \ldots, \theta_{u+l-1}\}$ forme évidemment une base de l'espace vectoriel K. En effet, s'il existait une relation linéaire à coefficients rationnels entre ces éléments on pourrait écrire :

$$a_0 + \sum_i a_i \theta_{u+i} = 0,$$

relation vraie pour tout u.

Ces relations entraîneraient alors :

$$\begin{vmatrix} 1 & \theta_1 & \theta_2 & \ldots & \theta_{l-1} \\ 1 & \theta_2 & \theta_3 & \ldots & \theta_0 \\ 1 & \theta_3 & \theta_4 & \ldots & . \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \theta_0 & \theta_1 & & \theta_{l-2} \end{vmatrix} = 0$$

mais ce déterminant est égal à $\prod_{j=1}^{l-1} \overline{\theta_{u,j}}$ et son égalité à zéro est impossible.

Posons

$$\vartheta_u = a_0 + \sum_{i=1}^{l-1} a_i \theta_{u+i}$$

et supposons que ϑ_u est un entier.

$$\overline{\vartheta_{u,j}} = \overline{\theta_{u,j}} \, (a_1 \varepsilon_j^{-1} + a_2 \varepsilon_j^{-2} + \cdots + a_{l-1} \, \varepsilon_j^{l-1}) = \overline{\theta_{u,j}} \, \nu_j.$$

On en déduit :

$$\overline{\vartheta_{u,j}}^{\,l} = \mu_j l^l \nu_j^l$$

nous venons de voir que ϑ_u entier entraîne $l\nu_j$ est un entier de C(l) congru à 0 mod l $\Longleftrightarrow$ ν_j est un entier de C(l)

$$\Longrightarrow \text{les } a_i \; 1 \leqslant i \leqslant l-1$$

sont des entiers, par différence on voit que a_0 est également entier.

3. Discriminants.

1) Si K est un corps unitaire un l-uple formant une base d'entiers permet de calculer son discriminant :

$$\Delta = \begin{vmatrix} \theta_u & \theta_{u+1} & \dots & \theta_{u+l-1} \\ \theta_{u+1} & \theta_{u+2} & \dots & \theta_u \\ \vdots & \vdots & & \vdots \\ \theta_{u+l-1} & \theta_u & & \theta_{u+l-2} \end{vmatrix}^2 = \left(\prod_{j=1}^{l-1} \overline{\theta_{u,j}}\right)^2 \left(\sum_u \theta_u\right)^2 = (p_1 p_2 \dots p_n)^{l-1}$$

le discriminant d'un corps unitaire de degré l est la puissance $(l-1)^{\text{ième}}$ d'un produit de nombres premiers rationnels distincts congrus à 1 modulo l.

Pour déterminer le nombre de corps unitaires dont le discriminant est égal à $(p_1 p_2 \dots p_n)^{l-1}$ il suffit de connaître le nombre des idéaux essentiels canoniques de norme égale à $(p_1 p_2 \dots p_n)^{\frac{l(l-1)}{2}}$ sans distinguer les idéaux conjugués qui correspondent au même corps mais avec des l-uples ordonnés différemment. Ce nombre est évidemment égal à $(l-1)^{n-1}$.

2) Si K est un corps non-unitaire on obtiendra son discriminant à l'aide d'une base d'entiers de la forme trouvée au 2.

$$\Delta = \begin{vmatrix} 1 & \theta_{u+1} & \theta_{u+2} & \dots & \theta_{u+l-1} \\ 1 & \theta_{u+2} & \theta_{u+3} & \dots & \theta_u \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \theta_u & \theta_{u+1} & \dots & \theta_{u+l-2} \end{vmatrix} = \left(\prod_{j=1}^{l-1} \overline{\theta_{u,j}}\right)^2 = (l^2 p_1 p_2 \dots p_n)^{l-1}$$

le discriminant d'un corps non-unitaire de degré l est la puissance $(l-1)^{\text{ième}}$ du produit de l^2 par n nombres premiers rationnels distincts congrus à 1 modulo l (n peut éventuellement être nul). On déterminera encore le nombre des corps non-unitaires de discriminant $(l^2 p_1 p_2 \dots p_n)^{l-1}$ en recherchant le nombre des idéaux essentiels canoniques de norme

$$(p_1 p_2 \dots p_n)^{\frac{l(l-1)}{2}}.$$

On trouvera encore $(l-1)^n$ corps.

DÉFINITION. — *Nous appellerons primaire un corps abélien dont le discriminant est puissance d'un nombre premier.*

l étant fixé, il existe un seul corps primaire non-unitaire de degré l et une infinité de corps primaires unitaires. Le corps primaire non-unitaire est obtenu à l'aide du $(l-1)$-uple $\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{l-1}\}$.

4. Exemples.

Nous appellerons polynôme fondamental d'un corps abélien de degré premier l un polynôme dont les racines θ_u forment une base d'entiers ou, si le corps n'est pas unitaire, tel que $\{1, \theta_{u+1}, \ldots, \theta_{u+l-1}\}$ forme une base des entiers du corps. Il y a une infinité de tels polynômes si $l > 3$. On trouvera des exemples pour les corps de degré 3 dans l'« Arithmétique des corps abéliens du troisième degré » d'Albert Châtelet. Pour le cas du degré 5, j'indique un élément du $(l-1)$-uple canonique, la valeur du discriminant et le polynôme fondamental correspondant pour les premiers corps primaires. Je donne également des polynômes fondamentaux des corps primaires non-unitaires de degré 7 et 11.

α_1	Δ	Polynôme fondamental
ε	5^8	$x^5 - 10x^3 + 5x^2 + 10x + 1$
$2\varepsilon_3 + \varepsilon_4$	11^4	$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$
$2\varepsilon - \varepsilon_2$	31^4	$x^5 - x^4 - 12x^3 + 21x^2 + x - 5$
$2 + 2\varepsilon + \varepsilon_2 - \varepsilon_4$	41^4	$x^5 - x^4 - 16x^3 - 5x^2 + 21x + 9$
$3\varepsilon + \varepsilon_2$	61^4	$x^5 - x^4 - 24x^3 + 13x^2 + 41x + 13$
ε	7^{12}	$x^7 - 21x^5 + 21x^4 + 91x^3 + 112x^2 - 84x - 97$
ε	11^{20}	$x^{11} - 55x^9 + 33x^8 + 825x^7 - 396x^6 - 4\,972x^5 + 1\,287x^4 + 12\,760x^3 - 924x^2 - 10\,989x + 243$

Les formules qui permettent d'exprimer les nombres $\overline{\theta_{u,j}}^2$ (resp. $\overline{\theta_{u,j_r}}.\overline{\theta_{u,j_1}}$, $j_1 + j_2 \neq l$) comme produits de $\overline{\theta_{u,2j}}$ (resp $\overline{\theta_{u,j_1+j_2}}$) par un nombre de $C(l)$ permettent de construire la table de

multiplication des entiers d'un corps abélien de degré l en calculant les produits deux à deux et les carrés des éléments d'une base d'entiers.

Examinons le cas des corps de degré 5.

Corps unitaires. — Désignons par θ_u, θ_{u+1}, θ_{u+2}, θ_{u+3}, θ_{u+4} les éléments de la base normale construite à l'aide du quadruplet canonique α_1, α_2, α_3, α_4, du facteur banal $\lambda = 1$, et de la trace $s = \pm 1$, $s \equiv \alpha_1\alpha_2^3\alpha_3^2\alpha_4^4 \bmod 5$. On peut écrire :

$$\begin{aligned}\theta_u^2 &= \frac{1}{5^2}\left[\sum_{j=1}^{4}\overline{\theta_{u,j}} + s\right]^2 \\ &= \frac{1}{5^2}\Big[\sum_{j=1}^{4}\alpha_{2j}\alpha_{4j}\,\overline{\theta_{u,2j}} + 2s\sum_{j=1}^{4}\overline{\theta_{u,j}} + 2\sum_{j=1}^{4}\alpha_{3j}\alpha_{4j}\,\overline{\theta_{u,3j}} \\ &\quad + 4\alpha_1\alpha_2\alpha_3\alpha_4 + 1\Big]\end{aligned}$$

soit encore :

$$\begin{aligned}\theta_u^2 = \frac{1}{5^2}\Big[&\Big(10s + \sum_{j=1}^{4}\alpha_j(\alpha_{2j} + 2\alpha_{3j})\Big)\theta_u \\ &+ \theta_{u+1}\sum_{j=1}^{4}\alpha_j\varepsilon_j(\alpha_{2j} + 2\alpha_{3j}) \\ &+ \theta_{u+2}\sum_{j=1}^{4}\alpha_j\varepsilon_j^2(\alpha_{2j} + 2\alpha_{3j}) + \theta_{u+3}\sum_{j=1}^{4}\alpha_j\varepsilon_j^3(\alpha_{2j} + 2\alpha_{3j}) \\ &+ \theta_{u+4}\sum_{j=1}^{4}\alpha_j\varepsilon_j^4(\alpha_{2j} + 2\alpha_{3j}) + 4\alpha_1\alpha_2\alpha_3\alpha_4 - 1\Big].\end{aligned}$$

On obtient de la même façon l'expression de $\theta_u\theta_{u+h}$ pour $h = 1, 2, 3, 4$.

$$\begin{aligned}\theta_u\theta_{u+h} = \frac{1}{5^2}\Big[&5s\theta_u + 5s\theta_{u+h} + \theta_u\sum_{j=1}^{4}\alpha_j(\alpha_{2j}\varepsilon_j^{2h} + \alpha_{3j}\varepsilon_j^h + \alpha_{3j}\varepsilon_j^{3h}) \\ &+ \theta_{u+1}\sum_{j=1}^{4}\alpha_j(\alpha_{2j}\varepsilon_j^{2h+1} + \alpha_{3j}\varepsilon_j^{h+1} + \alpha_{3j}\varepsilon_j^{3h+1}) \\ &+ \theta_{u+2}\sum_{j=1}^{4}\alpha_j(\alpha_{2j}\varepsilon_j^{2h+2} + \alpha_{3j}\varepsilon_j^{h+2} + \alpha_{3j}\varepsilon_j^{3h+2}) \\ &+ \theta_{u+3}\sum_{j=1}^{4}\alpha_j(\alpha_{2j}\varepsilon_j^{2h+3} + \alpha_{3j}\varepsilon_j^{h+3} + \alpha_{3j}\varepsilon_j^{3h+3}) \\ &+ \theta_{u+4}\sum_{j=1}^{4}\alpha_j(\alpha_{2j}\varepsilon_j^{2h+4} + \alpha_{3j}\varepsilon_j^{h+4} + \alpha_{3j}\varepsilon_j^{3h+4}) \\ &- \alpha_1\alpha_2\alpha_3\alpha_4 - 1\Big].\end{aligned}$$

Corps non-unitaires. — Désignons par θ_u, θ_{u+1}, θ_{u+2}, θ_{u+3}, θ_{u+4} les éléments construits avec le quadruplet $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ le facteur banal $\lambda = 5$ et une trace nulle.

On obtient alors :

$$\theta_u^2 = \frac{1}{5}\Big[\theta_u \sum_{j=1}^{4} \alpha_j(\alpha_{2j} + 2\alpha_{3j}) + \theta_{u+1} \sum_{j=1}^{4} \alpha_j\varepsilon_j(\alpha_{2j} + 2\alpha_{3j}) + \theta_{u+2} \sum_{j=1}^{4} \alpha_j\varepsilon_j^2(\alpha_{2j} + 2\alpha_{3j}) + \theta_{u+3} \sum_{j=1}^{4} \alpha_j\varepsilon_j^3(\alpha_{2j} + 2\alpha_{3j}) + \theta_{u+4} \sum_{j=1}^{4} \alpha_j\varepsilon_j^4(\alpha_{2j} + 2\alpha_{3j}) + 20\alpha_1\alpha_2\alpha_3\alpha_4\Big]$$

et pour $h = 1, 2, 3, 4$:

$$\begin{aligned}\theta_u\theta_{u+h} = \frac{1}{5}\Big[&\theta_u \sum_{j=1}^{4} \alpha_j(\alpha_{2j}\varepsilon_j^{-3h} + \alpha_{3j}\varepsilon_j^{-2h} + \alpha_{3j}\varepsilon_j^{-4h}) \\ &+ \theta_{u+1} \sum_{j=1}^{4} \alpha_j(\alpha_{2j}\varepsilon_j^{-3h+1} + \alpha_{3j}\varepsilon_j^{-2h+1} + \alpha_{3j}\varepsilon_j^{-4h+1}) \\ &+ \theta_{u+2} \sum_{j=1}^{4} \alpha_j(\alpha_{2j}\varepsilon_j^{-3h+2} + \alpha_{3j}\varepsilon_j^{-2h+2} + \alpha_{3j}\varepsilon_j^{-4h+2}) \\ &+ \theta_{u+3} \sum_{j=1}^{4} \alpha_j(\alpha_{2j}\varepsilon_j^{-3h+3} + \alpha_{3j}\varepsilon_j^{-2h+3} + \alpha_{3j}\varepsilon_j^{-4h+3}) \\ &+ \theta_{u+4} \sum_{j=1}^{4} \alpha_j(\alpha_{2j}\varepsilon_j^{-3h+4} + \alpha_{3j}\varepsilon_j^{-2h+4} + \alpha_{3j}\varepsilon_j^{-4h+4}) \\ &- 5\alpha_1\alpha_2\alpha_3\alpha_4\Big].\end{aligned}$$

CHAPITRE IV

COMPOSITION DES CORPS ABÉLIENS DE DEGRÉ PREMIER *l*

1. Composition de deux corps.

Considérons deux corps abéliens de degré l : K_1 et K_2 dont les discriminants sont premiers entre eux. Désignons par ξ_u éléments d'un l-uple de conjugués irrationnels de K_1 et par η_u les éléments d'un l-uple de conjugués irrationnels de K_2.

Considérons alors les nombres :

$$\theta_u = \sum_{\nu \bmod l} \xi_\nu \eta_{u-\nu}$$

on peut écrire :

$$\begin{aligned}\overline{\theta_{u,j}} &= \sum_{t \bmod l} \theta_{u+t}\, \varepsilon_j^t = \sum_{t \bmod l} \varepsilon_j^t \sum_{\nu \bmod l} \xi_\nu \eta_{u+t-\nu} \\ &= \sum_{\nu \bmod l} \xi_\nu \sum_{t \bmod l} \eta_{u+t-\nu}\, \varepsilon_j^t = \sum_{\nu} \xi_\nu \overline{\eta_{u-\nu,j}} \\ &= \sum_{\nu} \xi_\nu \varepsilon_j^\nu \overline{\eta_{u,j}}\end{aligned}$$

soit encore :

$$\overline{\theta_{u,j}} = \overline{\xi_{0,j}}\ \overline{\eta_{u,j}}.$$

Si on note que :

$$\overline{\xi_{u,j}}^{\,l} = \lambda_j' \mu_j \qquad \text{et} \qquad \overline{\eta_{u,j}}^{\,l} = \lambda'^{l}_j \mu_j'$$

on en déduit que $\overline{\theta_{u,j}}^{\,l} = (\lambda_j \lambda_j')^l \mu_j \mu_j'$ les discriminants de K_1 et K_2 étant supposés premiers entre eux, le produit $\mu_j \mu_j'$ est base d'un idéal essentiel canonique et les θ_u forment un l-uple de conjugués irrationnels du corps abélien de degré l construit à l'aide de $\mu_j \mu_j'$. On notera $K_1 \circ K_2$ ce corps. Les égalités précédentes montrent que le discriminant de $K_1 \circ K_2$ est le produit des discriminants de K_1 et K_2, il suffit pour le voir

de choisir les ξ_u et les η_u racines de polynômes fondamentaux de K_1 et K_2, les θ_u seront alors les racines d'un polynôme fondamental de $K_1 \circ K_2$. Remarquons encore que si on change l'ordre des éléments conjugués des l-uples de K_1 sans changer l'ordre des l-uples de K_2, on obtient un corps différent. On peut grâce à cette remarque montrer que tout corps abélien de degré l est composé de corps primaires et retrouver le nombre de corps de discriminant donné.

2. Inclusion dans les corps circulaires.

THÉORÈME 9. — *Un corps abélien* K *de degré* l *premier de discriminant* m^{l-1} *est sous-corps de* C(m).

a) $m = l^2$.

Le corps non-unitaire primaire est obtenu avec le $(l-1)$-uple $||\varepsilon_1\varepsilon_2 \ldots \varepsilon_{l-1}||$ il est donc sous-corps de C(l^2). Le groupe de Galois de C(l^2) est formé des éléments notés $[\omega^x.(1+l)^y]$ où ω est un représentant d'une classe primitive modulo l tel que $\omega^{l-1} \equiv 1 \bmod l^2$, x défini mod $l-1$, y défini modulo l. Désignons par ξ une racine primitive $l^{2\text{ième}}$ de l'unité, racine $l^{\text{ième}}$ de ε. Nous poserons :

$$[\omega^x(1+l)^y]\xi = \xi_{\omega^x(1+l)^y}.$$

Considérons les éléments $\theta_u = \sum_{x \bmod l-1} \xi_{\omega^x(1+l)^u}$ ce sont des éléments du corps primaire non-unitaire de degré l.

Formons l'expression $\overline{\theta_{u,j}}\,\overline{\theta_{u,l-j}}$:

$$\overline{\theta_{u,j}}\,\overline{\theta_{u,l-j}} = \sum_{\substack{x \bmod l-1 \\ x' \bmod l-1 \\ t,t' \bmod l}} \xi_{\omega^x(1+l)^{u+t}+\omega^{x'}(1+l)^{u+t'}+lj(t-t')}$$

pour étudier cette somme, remarquons que $\omega^{\frac{l-1}{2}} = -1 \bmod l^2$.

$$\overline{\theta_{u,j}}\,\overline{\theta_{u,l-j}} = \sum_{\substack{x \bmod l-1 \\ t,t' \bmod l}} \xi_{\omega^x(1+l)^u(t-t')+lj(t-t')} + \sum_{\substack{x,x' \bmod l-1 \\ x'-x \neq \frac{l-1}{2} \\ t,t' \bmod l}} \xi_{\omega^x(1+l)^{u+t}+\omega^{x'}(1+l)^{u+t'}+lj(t-t')}.$$

On peut écrire :

$$\sum_{\substack{x \bmod l-1 \\ t,\, t' \bmod l}} \xi_{\omega^x(1+l)^u l(t-t')+lj(t-t')} = \sum_{\substack{x \bmod l-1 \\ t,\, t' \bmod l}} \varepsilon_{(t-t')[\omega^x+j]}$$

cette somme est égale visiblement à l^2.

Par ailleurs, la seconde somme s'écrit :

$$\sum_{\substack{k \bmod l \\ h \bmod l-1 \\ h \neq \frac{l-1}{2}}} \sum_{\substack{x \bmod l-1 \\ t \bmod l}} \xi_{\omega^x(1+l)^{u+t}[1+\omega^h(1+l)^k]+ljk}$$

où l'on a posé $x' = x + h$, $t' = t - k$.

La somme

$$\sum_{\substack{x \bmod l-1 \\ t \bmod l}} \xi_{\omega^x(1+l)^{u+t}[1+\omega^h(1+l)^k]+ljk}$$

est nulle car la somme des racines primitives $l^{2\text{ièmes}}$ de l'unité est nulle.

De l'égalité $\overline{\theta_{u,j}}\,\overline{\theta_{u,l-j}} = l^2$ on déduit, que les θ_u ne sont pas rationnels, que $\overline{\theta_{u,j}}^{\,l} = l^l\varepsilon_k$, $k \not\equiv 0 \bmod l$ et que les θ_u sont racines d'un polynôme fondamental.

b) $m = p$, *p premier*, $p \equiv 1$ *mod l.*

Nous savons qu'il existe un seul corps abélien de degré l, de discriminant p^{l-1}. Le groupe de Galois de C(p) est formé des éléments notés $[\gamma^x]$, x modulo $p-1$, où γ désigne un représentant d'une classe primitive modulo p. Considérons le sous-groupe formé des éléments $[\gamma^x]$ avec $x \equiv 0 \bmod l$, c'est un sous-groupe d'indice l, le sous-corps de C(p) qui lui est associé est donc un corps abélien de degré l dont le discriminant est forcément une puissance de p (p est le seul nombre premier qui se ramifie sur C(p)). Notons ω_p une racine primitive $p^{\text{ième}}$ de l'unité, et considérons la somme :

$$\theta_u = \sum_{x \bmod \frac{p-1}{l}} [\gamma^{lx+u}]\omega_p$$

on obtient ainsi un l-uple de conjugués du corps abélien de degré l de discriminant p^{l-1}. Remarquons que $\sum_{u \bmod l} \theta_u = -1$ par ailleurs :

$$\overline{\theta_{u,j}} = \sum_{\substack{x \bmod \frac{p-1}{l} \\ t \bmod l}} \varepsilon_j^t[\gamma^{lx+u+t}]\omega_p.$$

On en déduit :

$$\overline{\theta_{0,j}}\,\overline{\theta_{0,l-j}} = \sum_{\substack{x \bmod \frac{p-1}{l} \\ t \bmod l}} \varepsilon_j^t[\gamma^{lx+t}]\omega_p \sum_{\substack{x' \bmod \frac{p-1}{l} \\ t' \bmod l}} \varepsilon_j^{-t'}[\gamma^{lx'+t'}]\omega_p$$

posons :

$$x' = x + \frac{p-1}{2l} + h$$
$$t' = t + k$$

nous pouvons alors écrire :

$$\begin{aligned}\overline{\theta_{0,j}}\,\overline{\theta_{0,l-j}} &= \sum_{\substack{x \bmod \frac{p-1}{l} \\ t \bmod l}} 1 + \sum_{k \bmod l} \varepsilon_j^{-k} \sum_{\substack{h,x \bmod \frac{p-1}{l} \\ t \bmod l \\ h \neq 0}} \omega_p^{\gamma^{lx+t}[1-\gamma^{lh+k}]} \\ &+ \sum_{\substack{k \bmod l \\ k \neq 0}} \varepsilon_j^{-k} \sum_{\substack{x \bmod \frac{p-1}{l} \\ t \bmod l}} \omega_p^{\gamma^{lx+t}[1-\gamma^k]} \\ &= p - 1 - \left(\frac{p-1}{l} - 1\right) \sum_{k \bmod l} \varepsilon_j^{-k} - \sum_{\substack{k \bmod l \\ k \neq 0}} \varepsilon_j^{-k} \\ &= p.\end{aligned}$$

Les θ_u forment donc un l-uple de racines d'un polynôme fondamental.

c) *m est composé.*

Considérons deux corps abéliens de degré l : K_1 et K_2 de discriminants respectifs m^{l-1} et n^{l-1} premiers entre eux. Supposons que K_1 et K_2 soient sous-corps respectivement de $C(m)$ et $C(n)$, notons G_m et G_n les groupes de Galois de $C(m)$ et $C(n)$ et g_m et g_n les sous-groupes d'indice l associés aux corps K_1 et K_2, notons σ et τ des représentants de classes primitives de G_m/g_m et G_n/g_n et supposons que :

$$\xi_u = \sum_{s \in g_m} s\sigma^u(\omega_m)$$
$$\eta_u = \sum_{t \in g_n} t\tau^u(\omega_n)$$

forment des l-uples de racines de polynômes fondamentaux de K_1 et K_2 (ω_m et ω_n désignent des racines primitives $m^{\text{ièmes}}$ et $n^{\text{ièmes}}$ de l'unité).

Nous pouvons alors énoncer :

LEMME. — *Le corps* $K_1 \circ K_2$ *est sous-corps de* $C(m.n)$.

Le groupe de Galois de $C(m.n)$ est produit direct des groupes G_m et G_n, nous noterons ses éléments (S, T) avec $S \in G_m$ et $T \in G_n$. Nous désignerons par I les éléments unités de G_m et G_n. Considérons :

$$\theta_u = \sum_{\nu \bmod l} \xi_\nu \eta_{u-\nu} = \sum_{\nu \bmod l} \sum_{\substack{s \in g_m \\ t \in g_n}} (s\sigma^\nu, t\tau^{u-\nu})\omega_m\omega_n$$

remarquons que $\omega_m\omega_n = \omega_{mn}$ est une racine primitive $mn^{\text{ième}}$ de l'unité et que les éléments $(s\sigma^\nu, t\tau^{-\nu})$ avec $s \in g_m$, $t \in g_n$ forment un sous-groupe g_{mn} d'indice l de $G_m \times G_n$ les éléments (I, τ^u) formant un système complet de représentants du groupe quotient.

On peut alors écrire :

$$\theta_u = \sum_{(S,T) \in g_{mn}} (S, T)\,(I, \tau^u)\omega_{mn}$$

les θ_u appartiennent donc à $C(m, n)$ et forment un l-uple de racines d'un polynôme fondamental de $K_1 \circ K_2$.

Comme un corps abélien non primaire peut être obtenu en composant des corps primaires, le lemme précédent achève la démonstration.

CHAPITRE V

ÉTUDE DES IDÉAUX DES CORPS ABÉLIENS DE DEGRÉ PREMIER

Décomposition d'un idéal rationnel.

La décomposition d'un idéal rationnel (a) dans K abélien de degré l et de discriminant m^{l-1} est donnée par la décomposition des idéaux rationnels (p) où p désigne un nombre premier naturel. Si $\mathfrak{p}$ est un idéal premier de K, son groupe de décomposition, s'il n'est pas égal au groupe de Galois de K, se réduit à l'élément unité de ce groupe, nous noterons dans ce cas $\mathfrak{p}_u$, $u \bmod l$ les conjugués de $\mathfrak{p}$. Les décompositions possibles de (p) s'écriront :

$(p) = \mathfrak{p}$, $\mathfrak{p}$ premier de degré l.

$(p) = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_l$ où les $\mathfrak{p}_u$ sont des idéaux premiers du premier degré deux à deux distincts.

$(p) = \mathfrak{p}^l$, $\mathfrak{p}$ premier du premier degré.

On sait que ce dernier cas se présente si et seulement si p divise m.

1. Critère de décomposition.

Soit p un nombre premier naturel qui ne divise pas le discriminant de K, alors si μ_j désigne une base de l'idéal essentiel canonique qui permet de construire K, (p) se décompose en un produit d'idéaux premiers du premier degré ou reste premier dans K suivant que la congruence [dans $C(l)$]

$$x^l - \mu_j \equiv 0 \quad \begin{cases} \bmod p & \text{si} \quad p \neq l \\ \bmod l^2 & \text{si} \quad p = l \end{cases} \quad \text{est soluble ou non.}$$

Nous noterons $||\theta_u||$ le l-uple de racines conjuguées d'un polynôme fondamental, vérifiant :

$$\begin{cases} \overline{\theta_{u,j}}^{l} = \mu_j & \text{si K est unitaire,} \\ \Sigma\theta_u = 1 \\ \overline{\theta_{u,j}}^{l} = l^l\mu_j & \text{si K est non-unitaire.} \\ \Sigma\theta_u = 0. \end{cases}$$

Remarquons que les congruences $x^l - \mu_j \equiv 0 \bmod p$ et $y^l - l^l\mu_j \equiv 0 \bmod p$ sont solubles pour les mêmes valeurs de p différentes de l.

1) *Condition nécessaire.*

Supposons que $\mathfrak{p}$ premier du premier degré divise (p) et $p \neq l$. On en déduit $\theta_{u+h} \equiv a_{u+h} \bmod \mathfrak{p}$ où a_{u+h} désigne un entier rationnel. Notons $\bar{\mathfrak{p}}$ l'idéal de $\mathfrak{k}$ ($\mathfrak{k}$ désignant toujours le composé de K et C(l)) obtenu en faisant le produit de $\mathfrak{p}$ par les entiers de $\mathfrak{k}$. On en déduit :

$$\overline{\theta_{u,j}} \equiv \sum_{h \bmod l} \varepsilon_j^h a_{u+h} \bmod \bar{\mathfrak{p}} \Longrightarrow \overline{\theta_{u,j}}^{l} \equiv \Big(\sum_{h \bmod} \varepsilon_j^h a_{u+h}\Big)^l \bmod \bar{\mathfrak{p}}$$

la congruence $x^l - \mu_j \equiv 0 \bmod \bar{\mathfrak{p}}$ a donc des solutions dans C(l) ce qui entraîne $x^l - \mu_j = u\xi$ avec $u \in \mathfrak{p}$ et $\xi \in \mathfrak{k}$ mais $\mathfrak{p} \cap \mathrm{C}(l) = (p)$ donc :

$$x^l - \mu_j \equiv 0 \bmod p.$$

Si $p = l$ supposons que (l) soit divisible par $\mathfrak{l}$ premier du premier degré dans K, il en résulte :

$$\theta_{u+h} \equiv a_{u+h} \bmod \mathfrak{l} \qquad \text{soit} \qquad \overline{\theta_{u,j}} = \sum_{h \bmod l} \varepsilon_j^h a_{u+h} \bmod \bar{\mathfrak{l}}$$

et

$$\overline{\theta_{u,j}}^{l} \equiv \Big(\sum_{h \bmod l} \varepsilon_j^h a_{u+h}\Big)^l \bmod (\bar{\mathfrak{l}}^l \cap l\bar{\mathfrak{l}})$$

donc :

$$\overline{\theta_{u,j}}^{l} \equiv \Big(\sum_{h \bmod l} \varepsilon_j^h a_{u+h}\Big)^l \bmod \bar{\mathfrak{l}}^2.$$

Comme les deux termes de la congruence appartiennent à C(l) et que $\mathfrak{l}^2$ ne divise pas l puisque nous avons écarté les diviseurs du discriminant de K, on en déduit que :

$$\overline{\theta_{u,j}}^{l} = \Big(\sum_{h \bmod l} \varepsilon_j^h a_{u+h}\Big)^l + u\xi \qquad \text{avec} \qquad u \in \mathfrak{l}^2 \quad \text{et} \quad \xi \in \mathfrak{k}$$

ce qui entraîne :

$$\overline{\theta_{u,j}}^{l} \equiv \Big(\sum_{h \bmod l} \varepsilon_j^h a_{u+h}\Big) \bmod l^2$$

(compte tenu de $\mathfrak{l}^2 \cap C(l) = (l^2)$).

2) *Condition suffisante.*

Supposons que l'on ait γ_j tel que :

$$\gamma_j^l - \overline{\theta_{u,j}}^{l} \equiv 0 \bmod p \quad \text{si } p \neq l.$$
$$\gamma_j^l - \overline{\theta_{u,j}}^{l} \equiv 0 \bmod l^2 \quad \text{si } p = l.$$

[Dans ce cas, K est unitaire].

THÉORÈME 10. — *Si $p \neq l$, on peut trouver des γ'_j, tels que :*

$$\begin{cases} \gamma_j'^{l} - \overline{\theta_{u,j}}^{l} \equiv 0 \bmod p \\ \dfrac{\gamma'_i \gamma'_{j-i}}{\gamma'_j} \equiv \dfrac{\overline{\theta_{u,i}}\ \overline{\theta_{u,j-i}}}{\overline{\theta_{u,j}}} \bmod p \quad \forall i,j \in \{1, 2, \ldots, l-1\},\ j - i \neq 0 \\ \gamma'_j \gamma'_{l-j} \equiv \overline{\theta_{u,j}}\ \overline{\theta_{u,l-j}} \bmod p. \end{cases}$$

Désignons par r un générateur du groupe multiplicatif modulo l. Nous avons montré au chapitre II que les nombres $\dfrac{\gamma'_i \gamma'_{j-i}}{\gamma'_j}$ et $\gamma'_j \gamma'_{l-j}$ sont des monômes en γ_j^l, $\dfrac{\gamma_j'^{r}}{\gamma'_{rj}}$ et leurs conjugués.

LEMME. — *r ayant toujours la même signification, si γ_j vérifie $\gamma_j^l \equiv \overline{\theta_{u,j}}^{l} \bmod p$, on peut trouver γ'_j tel que :*

$$\gamma_j'^{l} \equiv \overline{\theta_{u,j}}^{l} \bmod p \qquad \text{et} \qquad \frac{\gamma_j'^{r}}{\gamma'_{rj}} \equiv \frac{\overline{\theta_{u,j}}^{r}}{\overline{\theta_{u,rj}}} \bmod p.$$

Désignons par $(p) = \mathfrak{p}_{(1)}\mathfrak{p}_{(2)} \ldots \mathfrak{p}_{(e)}$ la décomposition de (p) en idéaux premiers distincts de degré f sur $C(l)$ ($ef = l - 1$), et par H_p le groupe de décomposition des $\mathfrak{p}_{(i)}$. Les solutions de la congruence $X^l \equiv \overline{\theta_{u,j}}^{l} \bmod p$ se déduisent de γ_j en faisant le produit de γ_j par une racine $l^{\text{ième}}$ de l'unité modulo p. Les racines $l^{\text{ièmes}}$ de l'unité modulo p sont au nombre de l^e, une quelconque d'entre elles est déterminée par son système de restes modulo les $\mathfrak{p}_{(i)}$: $u \equiv \varepsilon_{x_i} \bmod \mathfrak{p}_{(i)}$.

H_p est un groupe d'ordre f, il est formé des éléments $[r^{ex}]$, x mod f, nous noterons $\mathfrak{p}_{r^i}$, i mod e les diviseurs premiers de (p) avec $[j]$. $\mathfrak{p}_{r^i} = \mathfrak{p}_{r^{ij}}$ et $[r^e].\mathfrak{p}_{r^i} = \mathfrak{p}_{r^i}$.

La congruence $\gamma_j^l \equiv \overline{\theta_{u,j}}^l \bmod p$ entraîne :

$$\begin{aligned}
&\frac{\gamma_1^r}{\gamma_r} \equiv \varepsilon_{h_0} \frac{\overline{\theta_{u,1}}^r}{\theta_{u,r}} \bmod \mathfrak{p}_{r^e} \\
&\frac{\gamma_1^r}{\gamma_r} \equiv \varepsilon_{h_1} \frac{\overline{\theta_{u,1}}^r}{\theta_{u,r}} \bmod \mathfrak{p}_r \\
&\quad\vdots \\
&\frac{\gamma_1^r}{\gamma_r} \equiv \varepsilon_{h_{e-1}} \frac{\overline{\theta_{u,1}}^r}{\theta_{u,r}} \bmod \mathfrak{p}_{r^{e-1}}
\end{aligned}$$

mais l'égalité :

$$\left(\frac{\gamma_1^r}{\gamma_r}\right)^{r^{l-2}} \times \left(\frac{\gamma_r^r}{\gamma_{r^2}}\right)^{r^{l-3}} \times \cdots \times \left(\frac{\gamma_{r^{l-3}}^r}{\gamma_{r^{l-2}}}\right)^r \times \frac{\gamma_{r^{l-2}}^r}{\gamma_{r^{l-1}}} = \gamma_1^{r^{l-1}-1}$$

jointe à la congruence $\overline{\theta_{u,1}}^{r^{l-1}-1} - \gamma_1^{r^{l-1}-1} \equiv 0 \bmod p$ entraîne en prenant les restes modulo $\mathfrak{p}_i$ des $\frac{\gamma_{r^{l-i-1}}^r}{\gamma_{r^{l-i}}}$:

$$\varepsilon^{f r^{l-2}(h_0 + h_1 + \cdots + h_{e-1})} \equiv 1 \bmod \mathfrak{p}_i$$

ce qui entraîne $h_0 + h_1 + \cdots + h_{e-1} \equiv 0 \bmod l$.

Déterminons alors une racine $l^{\text{ième}}$ de l'unité U_1 modulo p telle que si on pose $\gamma_1 = U_1 \gamma_1'$ mod p, on ait :

$$\frac{\gamma_1'^r}{\gamma_r'} \equiv \frac{\overline{\theta_{u,1}}^r}{\theta_{u,r}} \bmod p \iff \frac{\gamma_1'^r}{\gamma_r'} \equiv \frac{\overline{\theta_{u,1}}^r}{\theta_{u,r}} \bmod \mathfrak{p}_{r^i}$$

pour $i = 1, 2, \ldots, e$.

U_1 est déterminé par ses restes modulo les $\mathfrak{p}_{r^i}$, posons :

$$U_1 \equiv \varepsilon_{x_i} \bmod \mathfrak{p}_{r^i}.$$

La condition cherchée équivaut à :

$$\left\{\begin{array}{rcl}
rx_e - rx_{e-1} &\equiv& h_0 \bmod l \\
rx_1 - rx_e &\equiv& h_1 \bmod l \\
rx_2 - rx_1 &\equiv& h_2 \bmod l \\
\vdots \quad\quad \vdots &\equiv& \vdots \quad \vdots \\
rx_{e-1} - rx_{e-2} &\equiv& h_{e-1} \bmod l
\end{array}\right.$$

Les solutions sont de la forme :

$$\begin{cases} x_1 \equiv x_0 + h_1 r^* & \bmod l \\ x_2 \equiv x_0 + (h_1 + h_2) r^* & \bmod l \\ \vdots \\ x_{e-1} \equiv x_0 + (h_1 + h_2 + \cdots + h_{e-1}) r^* & \bmod l \end{cases}$$

où x_0 est arbitraire. La condition $\sum_{i=0}^{e-1} h_i \equiv 0 \bmod l$ assurant la compatibilité des l équations. Le lemme est établi et conjugué avec la propriété du chapitre II qui vient d'être rappelée, il entraîne le théorème, on peut encore remarquer que les γ'_j qui conviennent sont définis au produit près par une racine $l^{\text{ième}}$ de l'unité.

Considérons maintenant les nombres rationnels définis mod p par :

$$c_{u+h} \equiv \frac{1}{l} \left(\sum_{j=1}^{l-1} \varepsilon_j^{-h} \gamma'_j + s \right) \bmod p$$

où s désigne la somme des θ_u. Posons $lc_u - s = X$ on en déduit :

$$\begin{aligned} -X + \gamma'_1 + \gamma'_2 + \cdots + \gamma'_{l-1} &\equiv 0 \bmod p \\ \gamma'_1\gamma'_{l-1} - X\gamma'_1 + \gamma'^2_1 + \cdots + \gamma'_1\gamma'_{l-2} &\equiv 0 \bmod p \\ \vdots \qquad\qquad\qquad\qquad\qquad & \quad \vdots \\ \gamma'_{l-1}\gamma'_1 \ldots\ldots\ldots\ldots\ldots - X\gamma'_{l-1} &\equiv 0 \bmod p \end{aligned}$$

posons alors

$$\frac{\gamma'_i\gamma'_{j-i}}{\gamma'_j} = \beta_{i,j} \qquad \text{et} \qquad \frac{\overline{\theta_{u,j}}\,\overline{\theta_{u,j-i}}}{\overline{\theta_{u,j}}} = \alpha_{i,j}$$

on obtient :

$$\begin{aligned} -X + \gamma'_1 + \gamma'_2 + \cdots + \gamma'_{l-1} &\equiv 0 \bmod p \\ \gamma'_1\gamma'_{l-1} - X\gamma'_1 + \beta_{1,2}\gamma'_2 + \cdots + \beta_{1,l-1}\gamma_{l-1} &\equiv 0 \bmod p \\ \vdots \qquad\qquad\qquad\qquad\qquad & \quad \vdots \\ \gamma'_{l-1}\gamma'_1 + \beta_{l-1,1}\gamma'_1 + \cdots - X\gamma'_{l-1} &\equiv 0 \bmod p \end{aligned}$$

le théorème précédemment démontré nous permet de remplacer les $\beta_{i,j}$ par les $\alpha_{i,j}$ mod p et $\gamma'_j\gamma'_{l-j}$ par $\overline{\theta_{u,j}}\,\overline{\theta_{u,l-j}}$, on en déduit donc :

$$\begin{vmatrix} -X & 1 & 1 & \ldots & 1 \\ m & -X & \alpha_{1,2} & \ldots & \alpha_{1,l-1} \\ m & \alpha_{2,1} & -X & \ldots & \\ \vdots & & & & \\ m & \ldots\ldots\ldots\ldots & & & -X \end{vmatrix} \equiv 0 \bmod p.$$

Ce qui signifie que $P(c_u) \equiv 0 \bmod p$. Si γ_j est une solution de la congruence $X^l - \overline{\theta_{u,j}}^l \equiv 0 \bmod p$, il existe donc une solution c à la congruence $P(x) \equiv 0 \bmod p$, soit :

$$\prod_u (\theta_u - c) \equiv 0 \bmod p.$$

Comme $\{1, \theta_{u+1}, \ldots, \theta_{u+l-1}\}$ forme une base des entiers de K les idéaux $\mathfrak{p}_u = (p, \theta_u - c)$ sont des diviseurs non-banaux de p, du premier degré.

Supposons maintenant que K soit unitaire et que

$$\gamma_j^l - \overline{\theta_{u,j}}^l \equiv \bmod l^2,$$

on peut alors trouver γ'_j tel que

$$\gamma_j'^l \equiv \overline{\theta_{u,j}}^l \bmod l^{l+1} \qquad \text{et} \qquad \frac{\gamma_j'^r}{\gamma_{jr}'} \equiv \frac{\overline{\theta_{u,j}}^2}{\overline{\theta_{u,jr}}} \bmod l^{l+1}.$$

Supposons que l'on ait pu déterminer δ_j tel que :

$$\delta_j^l - \overline{\theta_{u,j}}^l \equiv 0 \bmod l^n \quad \text{avec} \quad n \geqslant 2,$$

on peut écrire : $\delta_j^l \equiv \overline{\theta_{u,j}}^l + l^n A_j \bmod l^{n+1}$ où A_j désigne un entier de $C(l)$. Déterminons alors B_j tel que

$$(\delta_j + l^{n-1}B_j)^l \equiv \overline{\theta_{u,j}}^l \bmod l^{n+1}$$

on peut écrire :

$$(\delta_j + l^{n-1}B_j)^l \equiv \delta_j^l + l^n B_j \bmod l^{n+1}.$$

Il nous suffit donc de choisir $B_j = -A_j$ pour que la condition soit vérifiée.

Choisissons alors γ'_j tel que $\gamma_j'^l \equiv \overline{\theta_{u,j}}^l \bmod l^{l+2}$ on en déduit :

$$\frac{\gamma_j'^r}{\gamma_{jr}'} \equiv \varepsilon_{k_j} \frac{\overline{\theta_{u,j}}^2}{\overline{\theta_{u,rj}}} \bmod l^{l+1}$$

l'égalité

$$\left(\frac{\gamma_j'^r}{\gamma_{rj}'}\right)^{r^{l-2}} \left(\frac{\gamma_{rj}'^r}{\gamma_{r^2j}'}\right)^{r^{l-3}} \cdots \frac{\gamma_{r^{l-2}j}'^r}{\gamma_{r^{l-1}j}'} = \gamma_j'^{r^{l-1}-1}$$

montre que $k \equiv 0 \bmod l$. Si on choisit r générateur du groupe

multiplicatif mod l, on déduit comme précédemment :

$$\begin{cases} \gamma_j'^{l} \equiv \overline{\theta_{u,j}}^{l} \bmod l^{l+1} \\ \gamma_j'\gamma_{l-j}' \equiv \overline{\theta_{u,j}}\ \overline{\theta_{u,l-j}} \bmod l^{l+1} \\ \dfrac{\gamma_i'\gamma_{j-i}'}{\gamma_j'} \equiv \dfrac{\overline{\theta_{u,i}}\ \overline{\theta_{u,j-i}}}{\overline{\theta_{u,j}}} \bmod l^{l+1}. \end{cases}$$

Remarquons que $\sum_{j=1}^{l-1} \gamma_j' \equiv \sum_{j=1}^{l-1} \gamma_j'^{l} \equiv \sum_{j=1}^{l-1} \overline{\theta_{u,j}}^{l} \equiv -s \bmod l$.
Posons alors :

$$X = lc_{u+h} \equiv \sum_{j=1}^{l-1} \varepsilon_j^{-h}\gamma_j' + s \bmod l^{l+1}$$

on en déduit :

$$\begin{vmatrix} -X & 1 & 1 & \dots & 1 \\ m & -X & \alpha_{1,2} & & \alpha_{1,l-1} \\ \vdots & & & & \\ m & \alpha_{l-1,1} & \dots\dots & & -X \end{vmatrix} \equiv 0 \bmod l^{l+1}$$

en divisant les deux membres de la congruence par l^l on en déduit que les c_{u+h} sont racines de $P(x) \equiv 0 \bmod l$ donc que l se décompose sur K en un produit d'idéaux du premier degré. Ce qui achève la démonstration.

Nous nous sommes servis des polynômes fondamentaux et de leurs racines modulo p pour mener notre démonstration, nous pouvons encore préciser :

THÉORÈME 11. — *Si* K *est un corps abélien de degré* l, P *un polynôme fondamental associé.*

$P(x) \equiv \prod_{u \bmod l} (x - c_u) \bmod p$ *et deux des racines* c_u, $c_{u'}$ *de* P mod p *sont incongrues* mod p *si* p *se décompose sur* K *en un produit d'idéaux premiers distincts.*

$P(x)$ *est irréductible* mod p *si* (p) *est premier sur* K.

$P(x) \equiv (x-c)^l \bmod p$ *et* $P(x) \not\equiv (x-c)^l \bmod p^2$ *si* p *se ramifie sur* K.

Soient $P(x)$ un polynôme fondamental de K, $||\theta_u||$ ses racines.

Supposons que p soit un produit d'idéaux premiers du premier degré distinct dans K :

$$p = \prod_{u \bmod l} \mathfrak{p}_u$$

on en déduit :

$$\theta_{u+h} \equiv c_{u+h} \bmod \mathfrak{p}_u$$

où les c_{u+h} sont des entiers rationnels, nous en déduisons :

$$P(x) = \prod_{h \bmod l} (x - \theta_{u+h}) \equiv \prod_{h \bmod l} (x - c_{u+h}) \bmod \mathfrak{p}_u$$

les deux membres de la congruence sont rationnels, on en déduit que :

$$P(x) \equiv \prod_{h \bmod l} (x - c_{u+h}) \bmod p.$$

Si tous les c_{u+h} étaient congrus modulo p, on en déduirait :

$$\theta_{u+h} \equiv c_u \bmod \mathfrak{p}_u \quad \forall\ h \bmod l$$

d'où $\theta_u \equiv c_u \bmod \mathfrak{p}_{u+h}\ \forall h \Longrightarrow \theta_u \equiv c_u \bmod p$ ce qui est impossible.

Si $p = \mathfrak{p}^l$ sur K, on écrit $\theta_{u+h} \equiv c_u \bmod \mathfrak{p}$ et

$$P(x) \equiv (x - c)^l \bmod p,$$

on ne peut pas avoir $P(x) \equiv (x - c)^l \bmod p^2$ sinon $\theta_u \equiv c \bmod \mathfrak{p}^2$ et tout élément de K serait congru modulo $\mathfrak{p}^2$ à un nombre rationnel.

Supposons enfin (p) indécomposable sur K, $P(x)$ n'admet pas de racine modulo p sinon il existerait un entier rationnel c tel que $\theta_u - c \equiv 0 \bmod p$ ce qui est impossible. Par ailleurs, p étant premier dans K, l'ensemble des classes d'entiers de K modulo p forme un corps à p^l éléments sur $\mathbf{Z}/p\mathbf{Z}$ et la classe de θ_u modulo p est un élément primitif de ce corps, $P(x)$ est donc irréductible modulo p.

2. Loi de réciprocité.

Les résultats déjà obtenus permettent de retrouver assez aisément la loi de réciprocité. Nous énoncerons :

THÉORÈME 12. — *Si* K *abélien de degré l impair admet le discriminant* m^{l-1} *tous les nombres premiers d'une progression arithmétique de raison m admettent le même type de décomposition sur* K.

Considérons le groupe de Galois G_m de $C(m)$, isomorphe au groupe multiplicatif des classes premières avec m modulo m et désignons par g_m le sous-groupe d'indice l associé à K.

On peut préciser les structures de G_m et g_m :

a) Si $m = p$ premier et si γ désigne un élément primitif modulo p.

$$G_m = \{\gamma^x | x \bmod p - 1\}, \qquad g_m = \left\{\gamma^{lx} | x \bmod \frac{p-1}{l}\right\}$$
$$G_m/g_m = \{g_m, \gamma g_m, \ldots, \gamma^{l-1} g_m\}.$$

b) Si $m = l^2$ et si ω désigne un représentant d'une classe primitive modulo l telle que $\omega^{l-1} \equiv 1 \bmod l^2$:

$$G_m = \{\omega^x (1+l)^y | \; x \bmod l - 1, \quad y \bmod l\}$$
$$g_m = \{\omega^x | x \bmod l - 1\}$$
$$G_m/g_m = \{g_m, (1+l)g_m, \ldots, (1+l)^{l-1} g_m\}.$$

c) $m = p_0 p_1 \ldots p_r$ avec p_i nombre premier naturel $p_i \equiv 1 \bmod l \forall i \in \{1, \ldots, r\}$ et $p_0 = 1$ ou $p_0 = l^2$ suivant que K est unitaire ou non. On considère alors K comme le produit de corps primaires de discriminants p_i^{l-1}, chacun d'eux étant ordonné par le choix d'une classe primitive $\gamma_i \bmod p_i$. Déterminons alors les classes γ_i' par les congruences

$$\begin{cases} \gamma_i' \equiv \gamma_i \bmod p_i, \\ \gamma_i' \equiv 1 \bmod \dfrac{m}{p_i}. \end{cases}$$

Le groupe des classes modulo m, isomorphe à G_m, est donné par les expressions :

$$\prod_{i=0}^{r} \gamma_i'^{X_i} \; (X_i \bmod \varphi(p_i)).$$

Le sous-groupe g_m est défini par les expressions :

$$\prod_{i=0}^{r} \gamma_i'^{lx_i} \prod_{j=1}^{r} (\gamma_0' \gamma_j'^{-1})^{u_j} \bmod m \quad \left(x_i \bmod \frac{\varphi(p_i)}{l}, \; u_j \bmod l\right).$$

Les classes de G_m/g_m sont données par les éléments $\gamma_i', \gamma_i'^2, \ldots, \gamma_i'^l$ avec i arbitraire. Notons $\sigma, \sigma^2, \ldots, \sigma^1 = 1$ les éléments associés de G_m/g_m.

Nous sommes maintenant en mesure de préciser la relation

qui existe entre la classe modulo m à laquelle appartient p et la décomposition de p sur K.

Pour que p se décompose sur K en un produit d'idéaux premiers du premier degré, il faut et il suffit que p appartienne à l'une des classes modulo m de g_m.

Considérons p premier avec m, si p est divisible par $\mathfrak{p}$ du premier degré sur K et si $||\theta_u||$ est le l-uple de racines d'un polynôme fondamental de K défini par $\theta_u = \sum_{s\in g_m} s(\varepsilon_m)$, il existe un entier rationnel c tel que $\theta_u - c \equiv 0 \mod \mathfrak{p}$, en outre l'un des conjugués θ_{u+h} de θ_u vérifie

$$\theta_{u+h} - c \not\equiv 0 \mod \mathfrak{p}$$

il en résulte :

$$\begin{cases} \theta_u^p - \theta_u \equiv 0 \mod \mathfrak{p} \\ \theta_u^p - \theta_{u+h} \equiv 0 \mod \mathfrak{p}. \end{cases}$$

Par ailleurs :

$$\theta_u^p = \Big(\sum_{s\in g_m} s(\varepsilon_m)\Big)^p \equiv \sum_{s\in g_m} (s.(\varepsilon_m))^p \mod p.$$

Si p appartient à une classe $\gamma^h g_m$ (h défini modulo l) on en déduit :

$$\sum_{s\in g_m} [s(\varepsilon_m)]^p \equiv \sum_{s\in g_m} \sigma_h s.(\varepsilon_m) = \theta_{u+h} \mod p.$$

Donc $\theta_u \equiv \theta_{u+h} \equiv \theta_u^p \mod p$ en itérant ce procédé, on en déduit : $\theta_u \equiv \theta_{u+nh} \mod p$ ce qui entraîne : $h \equiv 0 \mod l$ c'est-à-dire $p \in g_m$.

Réciproquement, s'il en est ainsi, la congruence qui en résulte :

$$0 \equiv \theta_u^p - \theta_u \equiv \theta_u(\theta_u - 1) \ \ldots \ (\theta_u - p + 1) \mod p$$

montre qu'il existe c entier rationnel tel que :

$$\mathfrak{p} = (p, \theta_u - c) \quad \text{soit premier du premier degré.}$$

3. Exemples.

L'étude précédente nous permettra de déterminer effectivement les nombres premiers qui se décomposent dans une extension abélienne K de degré l et de discriminant m.

Si le groupe g_m peut être déterminé simplement, on en déduira les progressions arithmétiques contenant les nombres premiers décomposables, ce sera en particulier le cas si K est primaire.

Le corps primaire non-unitaire de degré 5 est sous-corps de $C(5^2)$, les éléments de g_m sont : $[7]$, $[-1]$, $[-7]$, $[+1]$. Les nombres premiers qui se décomposent sur ce corps appartiennent donc aux progressions arithmétiques $\pm 1 \bmod 25$ ou $\pm 7 \bmod 25$.

Si g_m ne se détermine pas de façon simple, on construit un polynôme fondamental $P(x)$ de K et en utilisant le fait que $P(x) \equiv 0 \bmod p$ a des solutions si et seulement si p se décompose sur K et la structure de groupe de g_m, on pourra en déduire les progressions arithmétiques modulo m contenant les nombres premiers décomposables sur K.

Considérons le corps K de degré 5, de discriminant $(11.31)^4$ déterminé par le polynôme fondamental

$$P = x^5 + x^4 - 136x^3 + 41x^2 + 3\,039\,x + 1\,431.$$

$P(0) = 3^3.53$. 3 est donc décomposable sur K et

$$3^n \equiv 1 \bmod 341 \leftrightarrow n \equiv 0 \bmod 30$$

comme g_m possède $\frac{\varphi(m)}{l} = 60$ éléments on en déduit que les classes qui contiennent les nombres premiers décomposables sur K sont de la forme :

$$\pm 3^x \text{ modulo } 341, \qquad x \text{ défini mod } 30.$$

CHAPITRE VI

ÉTUDE LOCALE

Nous allons maintenant étudier les extensions abéliennes de degré l du corps Q_p des nombres rationnels p-adiques.

1. Étude locale des polynômes abéliens de degré l sur Q.

Soit $\mathfrak{X}$ un polynôme à coefficients rationnels, irréductible, abélien et de degré l sur Q, K l'extension de Q obtenue en y adjoignant les racines de $\mathfrak{X}$. Désignons par P un polynôme fondamental de K et par K_p l'extension de Q_p obtenue en y adjoignant les racines de P.

Le polynôme $\mathfrak{X}$ reste abélien sur Q_g car si ϑ_u est une de ses racines, nous pouvons écrire :

$$\vartheta_{u+h} = R_h(\vartheta_u)$$

où R_h est un polynôme à coefficients rationnels de degré au plus égal à $l - 1$ et dire que $\mathfrak{X}$ est abélien sur Q c'est dire que :

$$\mathfrak{X}(R_h(x)) = \mathfrak{X}(x)S(x)$$

cette égalité reste valable sur Q_p, on en déduit que $\mathfrak{X}$ est soit irréductible sur Q_p, soit décomposé en un produit de facteurs du premier degré. En outre, $\mathfrak{X}$ et P sont simultanément réductibles ou irréductibles sur Q_p, et on peut énoncer :

THÉORÈME 13. — *Si* (p) *est premier sur* K, $\mathfrak{X}$ *est irréductible sur* Q_p.

Si $(p) = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_1$ *sur* K, *où les* $\mathfrak{p}_i$ *désignent des idéaux premiers du premier degré deux à deux distincts, alors* $\mathfrak{X}$ *se décompose en un produit de facteurs du premier degré sur* Q_p.

Si $(p) = \mathfrak{p}^l$ *sur* K, $\mathfrak{X}$ *est irréductible sur* Q_p.

Les deux premières assertions résultent de l'étude de P modulo p, de sa décomposition sur Z/pZ et du lemme de Hensel.

Dans le cas où $(p) = \mathfrak{p}^l$ sur K, nous avons vu que

$$P \equiv (x - c)^l \bmod p \quad \text{et} \quad P \not\equiv (x - c)^l \bmod p^2,$$

il en découle que le polynôme $P(x - c)$ satisfait au critère d'Eisenstein et que P, donc $\mathfrak{X}$ est irréductible sur Q_p.

2. Étude de $Q_p(l)$.

Nous noterons $Q_p(l)$ l'extension de Q_p obtenue en lui adjoignant les racines $l^{\text{ièmes}}$ de l'unité. Si $p \neq 1$ désignons par f l'ordre de la classe de p dans le groupe multiplicatif des entiers modulo l, la décomposition de p dans $C(l)$ entraîne :

$$x^{l-1} + x^{l-2} + \dots + x + 1 \equiv P_1P_2 \dots P_e \bmod p$$

où $e = \dfrac{l-1}{f}$ et où les P_i sont des polynômes irréductibles sur Z/pZ, de degré f, premiers entre eux deux à deux. Le lemme de Hensel montre que :

$$x^{l-1} + x^{l-2} + \dots + x + 1 = R_1R_2 \dots R_e \text{ sur } Q_p$$

où les R_i désignent des polynômes irréductibles de degré f sur Q_p, premiers entre eux deux à deux. On en déduit que $[Q_p(l) : Q_p] = f$ et que le groupe de Galois de $Q_p(l)$, relativement à Q_p, est isomorphe au groupe de décomposition des idéaux premiers diviseurs de p dans $C(l)$. En particulier si $p \equiv 1 \bmod l$, $Q_p(l) = Q_p$.

Si $p = l$, $Q_p(p)$ est de degré $p - 1$, relativement à Q_p et ne contient pas de racines de l'unité autres que les racines $p^{\text{ièmes}}$ [5].

Nous désignerons dans ce qui suit, par ε une racine primitive $l^{\text{ième}}$ de l'unité et par $\mathfrak{p}$ l'idéal premier de $Q_p(l)$.

Examinons la structure du groupe des unités de $Q_p(l)$ et distinguons deux cas suivant que p est égal ou non à l.

1) $p \neq l$.

Nous désignerons par ν l'entier positif défini par les conditions : $Q_p(l)$ contient les racines l^ν ièmes de l'unité et ne contient pas toutes les racines d'ordre $l^{\nu+1}$. Nous noterons η une racine primitive l^ν ième de l'unité telle que :

$$\eta^{\nu l-1} = \varepsilon.$$

PROPOSITION 1. — *Les nombres* η^x, $x \in \{0, 1, \ldots, l-1\}$ *forment un système complet de représentants des classes du groupe quotient du groupe des unités de* $Q_p(l)$ *par le sous-groupe des unités puissances* $l^{\text{èmes}}$.

Soit $Z/pZ(l)$ le corps des restes de $Q_p(l)$, l'ensemble des $p^f - 1$ éléments autres que 0 forme un groupe multiplicatif cyclique, l'indice du sous-groupe des puissances $l^{\text{èmes}}$ est donc égal à l. Les classes du groupe quotient sont engendrées par les restes des η^x, $x \in \{0, 1, \ldots, l-1\}$ puisque η n'est pas une puissance $l^{\text{ème}}$ exacte dans $Q_p(l)$.

Considérons une unité U de $Q_p(l)$ on déduit de ce qui précède que $U \equiv \eta^x V^l \bmod \mathfrak{p}$ où $\mathfrak{p}$ désigne l'idéal premier de $Q_p(l)$ et V un représentant d'une classe modulo $\mathfrak{p}$, il en résulte :

$$X^l - \frac{U}{\eta^x} \equiv X^l - V^l \bmod \mathfrak{p}.$$

Il suffit pour conclure de montrer que le polynôme $X^l - \dfrac{U}{\eta^x}$ possède une racine A dans $Q_p(l)$ ce qui entraîne $U = \eta^x A^l$. Comme $p \neq l$ les racines de $X^l - V^l$ sont deux à deux distinctes et $X^l - V^l$ se décompose sur $Z/pZ(l)$ en un produit de facteurs linéaires premiers entre eux deux à deux, le lemme de Hensel prouve alors l'existence d'une racine de $X^l - \dfrac{U}{\eta^x}$ dans $Q_p(l)$.

2) $p = l$.

Nous noterons Π_j l'élément premier $1 - \varepsilon^j$. Nous savons [5] que toute unité de $Q_p(p)$ s'écrit comme produit d'une unité distinguée (c'est-à-dire congrue à 1 modulo $\mathfrak{p}$) par un élément du système de restes multiplicativement stable, $\mathcal{R}$ isomorphe au groupe multiplicatif du corps des restes de $Q_p(p)$.

$\mathcal{R}$ est formé des racines $p-1^{\text{èmes}}$ de l'unité et tous ses éléments sont des puissances $p^{\text{èmes}}$ dans $Q_p(p)$. Les éléments

du groupe H des unités distinguées s'écrivent de manière unique sous la forme :

$$U = \prod_{h=1}^{p} (1 - \Pi^h)^{\alpha_h} \quad \begin{cases} \alpha_1 \quad \text{défini modulo } p \\ \alpha_h \in Z_p \quad \text{pour} \quad 2 \leqslant h \leqslant p \end{cases}$$

où Z_p désigne l'anneau des entiers p-adiques [5].

3. Extensions abéliennes de Q_p de degré l premier impair.

Dans ce paragraphe et dans le suivant, nous allons mener une étude analogue à celle du chapitre II. Après avoir introduit les résolvantes de Lagrange, nous construirons les corps abéliens de degré l sur Q_p en prenant d'abord une extension $\mathfrak{k}_p$ de degré l de $Q_p(l)$ et en cherchant à quelle condition une telle extension est abélienne relativement à Q_p. Comme dans le cas global, on caractérisera les $\alpha \in Q_p(l)$ dont les racines $l^{\text{ièmes}}$ engendrent les $\mathfrak{k}_p$ convenables, cette caractérisation se fera en deux temps, le premier consistera en l'étude des facteurs premiers de α, le second en l'étude des facteurs unités. Mais dans le cas présent, le premier temps sera notablement simplifié par la présence d'un seul idéal premier et le fait que tous les idéaux sont principaux.

Désignons par r un représentant d'une classe primitive du groupe multiplicatif modulo l et par $[r^{ex}]$, $x \bmod \dfrac{l-1}{e}$ les éléments du groupe de Galois de $Q_p(l)$ avec

$$[r^{ex}]\varepsilon = \varepsilon^{r^{ex}}, \qquad f = [Q_p(l) : Q_p] \qquad \text{et} \qquad ef = l - 1.$$

K_p désigne une extension de degré l impair abélienne de Q_p, $\{\theta_{u+h}\}_{h \bmod l}$ un l-uple d'éléments primitifs et conjugués de K_p. Les éléments du groupe de Galois de K_p seront notés σ^h et on supposera que l'indexation des θ_{u+h} est telle que $\sigma^h(\theta_u) = \theta_{u+h}$.

Nous considérons les résolvantes de Lagrange :

$$\overline{\theta_{u,j}} = \sum_{h \bmod l} \varepsilon^{jh} \theta_{u+h}$$

elles appartiennent au composé $\mathfrak{k}_p = (K_p, Q_p(l))$ dont le groupe de Galois est le produit direct des groupes de Galois de K_p et de $Q_p(l)$ [1].

Nous pouvons écrire :

$$\begin{cases} [r^{ex}]\overline{\theta_{u,j}} = \overline{\theta_{u,\,jr^{ex}}} \\ \sigma^h\,\overline{\theta_{u,j}} = \overline{\theta_{u+h,\,j}} = \varepsilon^{-j^h}\,\overline{\theta_{u,j}} \end{cases}$$

d'où on déduit que $\overline{\theta_{u,j}}^l \in Q_p(l)$.

Remarquons encore que les changements de l'indexation des θ_u compatibles avec la représentation des automorphismes de K_p comme des permutations circulaires sur les indices u, se ramènent comme dans l'étude globale, chapitre II, § 2, à la substitution des $\overline{\theta_{u,hj}}$ aux $\overline{\theta_{u,j}}$.

Pour déterminer le nombre d'extensions abéliennes de degré l de Q_p et les polynômes irréductibles associés, nous allons caractériser les éléments de $Q_p(l)$ dont les racines $l^{\text{ièmes}}$ engendrent des extensions de $Q_p(l)$ abéliennes relativement à Q_p.

PROPOSITION 2. — *Il existe j tel que $\overline{\theta_{u,j}}^l$ ne soit pas une puissance $l^{\text{ième}}$ exacte dans $Q_p(l)$.*

Si tous les $\overline{\theta_{u,j}}^l$ étaient des puissances $l^{\text{ièmes}}$ dans $Q_p(l)$, les $\overline{\theta_{u,j}}$ et la somme s des θ_u appartiendraient à $Q_p(l)$ et comme

$$l\theta_u = \sum_{j=1}^{l-1} \overline{\theta_{u,j}} + s$$

K_p serait contenu dans $Q_p(l)$ ce qui est impossible en raison des degrés respectifs de ces deux corps.

Il nous reste à préciser les valeurs possibles des $\overline{\theta_{u,i}}^l$. Remarquons que si $e = 1$ ou si $p = l$, $[Q_p(l) : Q_p] = l - 1$ et les $\overline{\theta_{u,i}}^l$ seront les conjugués (non nuls) de $\overline{\theta_{u,j}}^l$. Si $e \neq 1$ les $\overline{\theta_{u,\,jr^{ex}}}^l$ seront encore les conjugués de $\overline{\theta_{u,j}}^l$. La proposition suivante explique ce qui se passe pour les autres valeurs de i.

PROPOSITION 3. — *Supposons $e \neq 1$ et $\overline{\theta_{u,j}}^l$ non puissance $l^{\text{ième}}$ exacte dans $Q_p(l)$, si i n'est pas de la forme $i = jr^{ex}$ mod l, $\overline{\theta_{u,i}}^l$ quand elle diffère de zéro appartient à la classe puissance $(i.j^*)^{\text{ième}}$ de la classe de $\overline{\theta_{u,j}}^l$ dans le groupe multiplicatif de $Q_p(l)$ modulo le sous-groupe de ses puissances $l^{\text{ièmes}}$.*

Cela revient à montrer que $\dfrac{\overline{\theta_{u,i}}^l}{\overline{\theta_{u,j}}^{(i.j^*)l}}$ est une puissance $l^{\text{ième}}$

exacte dans $Q_p(l)$. Ce qui résulte de l'appartenance de $\dfrac{\overline{\theta_{u,i}}}{\overline{\theta_{u,j}}^{(i.j^*)}}$ à $Q_p(l)$.

Déterminons maintenant les facteurs premiers de $\overline{\theta_{u,j}}^l$.

PROPOSITION 4. — *Supposons* $p \not\equiv 1 \bmod l$ *et* $\overline{\theta_{u,j}}^l$ *non puissance* $l^{\text{ième}}$ *dans* $Q_p(l)$, *alors* $\overline{\theta_{u,j}}^l \equiv 0 \bmod \mathfrak{p}^h \Longrightarrow h \equiv 0 \bmod l$. $\overline{\theta_{u,j}}^l \equiv 0 \bmod \mathfrak{p}^h$ entraîne $[r^e]\overline{\theta_{u,j}}^l = \overline{\theta_{u,r^e j}}^l \equiv 0 \bmod \mathfrak{p}^h$ par ailleurs $\dfrac{\overline{\theta_{u,j}}^{r^e}}{\overline{\theta_{u,r^e j}}}$ est un élément de $Q_p(l)$ et on peut écrire :

$$\left(\frac{\overline{\theta_{u,j}}^{r^e}}{\overline{\theta_{u,r^e j}}}\right)^l \equiv 0 \bmod \mathfrak{p}^{h(r^e-1)}$$

en exprimant que le premier membre est une puissance $l^{\text{ième}}$ dans $Q_p(l)$ et compte tenu de $p \not\equiv 1 \bmod l$, on obtient $h \equiv 0 \bmod l$. Pour $p = l$ le raisonnement est valable en prenant $e = 1$.

THÉORÈME 14. — *Soient* ω *un élément de* $Q_p(l)$ *non puissance* $l^{\text{ième}}$ *tel que* $\dfrac{\omega^{r^e}}{[r^e]\omega}$ *soit une puissance* $l^{\text{ième}}$ *dans* $Q_p(l)$,

$$\lambda_i \quad i = 1, 2, \ldots, e-1$$

des éléments de $Q_p(l)$ *(éventuellement nuls pour certaines valeurs de* i*),* s *un élément de* Q_p *et* j *un entier* $\not\equiv 0 \bmod l$, *il existe un* l*-uple déterminé à une permutation circulaire près d'éléments conjugués* θ_u, *d'une extension abélienne* K_p *de degré* l *de* Q_p *tels que :*

$$\begin{cases} \overline{\theta_{u,\,jr^{ex}}}^l = [r^{ex}]\omega \\ \overline{\theta_{u,\,jr^{ex}+i}}^l = [r^{ex}]\lambda_i^l \omega^{r^i} \quad \forall i \in \{1, 2, \ldots, e-1\} \\ \sum\limits_{u \bmod l} \theta_u = s. \end{cases}$$

Considérons l'extension $\mathfrak{k}_p$ de $Q_p(l)$ obtenue en adjoignant à $Q_p(l)$ les racines $l^{\text{èmes}}$ de ω, elle est abélienne et de degré l relativement à $Q_p(l)$ [7].

En outre $\dfrac{\omega^{r^e}}{[r^e]\omega}$ étant une puissance $l^{\text{ième}}$ dans $Q_p(l)$, il en résulte que $\dfrac{\omega^{r^{ex}}}{[r^{ex}]\omega}$ est puissance $l^{\text{ième}}$ dans $Q_p(l)$, que $\mathfrak{k}_p$ contient égale-

ment les racines $l^{\text{ièmes}}$ des conjugués $[r^{ex}]\omega$ de ω relativement à Q_p et que ω est un élément primitif de $Q_p(l)$ relativement à Q_p. Le raisonnement du Chapitre II, § 1 s'applique ici encore et on en déduit que $\mathfrak{k}_p$ est galoisien relativement à Q_p et que son groupe de Galois est le produit direct des groupes de Galois de $Q_p(l)$ relativement à Q_p et de $\mathfrak{k}_p$ relativement à à $Q_p(l)$ [8]. Notons alors $\overline{\theta_{u,\,jr^{ex}}}$ les racines $l^{\text{ièmes}}$ de $[r^{ex}]\omega$, ce sont des éléments primitifs de $\mathfrak{k}_p$, notons enfin $\overline{\theta_{u,\,jr^{ex+i}}}$

$$i = 1, \ldots, e-1$$

les racines $l^{\text{ièmes}}$ de $\lambda_i^l \omega^{r^i}$ et supposons que les indices u sont choisis de façon que les automorphismes de $\mathfrak{k}_p$: $(\sigma^h, [r^{et}])$ vérifient les relations

$$(\sigma^h, [r^{et}])\,\overline{\theta_{u,\,jr^{ex+i}}} = \overline{\theta_{u+h,\,jr^{e(x+t)+i}}}.$$

Le l-uple formé des éléments

$$\theta_u = \frac{1}{l}\left[s + \sum_{i=0}^{l-1} \sum_{x \bmod \frac{l-1}{l}} \overline{\theta_{u,\,jr^{ex+i}}}\right]$$

répond aux conditions posées.

Construction des polynômes abéliens de degré l sur Q_p.

Nous utiliserons un calcul analogue à celui du théorème 6, Chapitre II, § 3-1). Pour cela, il faut calculer les produits $\dfrac{\overline{\theta_{u,i}}\,\overline{\theta_{u,j-i}}}{\overline{\theta_{u,j}}}$ et $\overline{\theta_{u,j}}.\overline{\theta_{u,l-j}}$ en fonctions linéaires des $\overline{\theta_{u,j}}$. Les produits $\dfrac{\overline{\theta_{u,j}}^r}{\overline{\theta_{u,rj}}}$ peuvent être d'abord calculés en fonction des λ_i et de ω grâce aux relations du théorème 14 et à l'égalité :

$$\left(\frac{\overline{\theta_{u,j}}^r}{\overline{\theta_{u,rj}}}\right)^{r^{l-2}} \left(\frac{\overline{\theta_{u,rj}}^r}{\overline{\theta_{u,r^2j}}}\right)^{r^{l-3}} \cdots \frac{\overline{\theta_{u,r^{l-2}j}}^r}{\overline{\theta_{u,r^{l-1}j}}} = \overline{\theta_{u,j}}^{r^{l-1}-1}.$$

On en déduit ensuite les produits recherchés au moyen du Lemme 1, Chapitre II, § 3-1). On obtient les polynômes sous forme de déterminants d'ordre l et le résultat est encore valable si certains des λ_i sont nuls.

Exemples. — Nous choisirons dans tous les cas $j = 1$.

1) $l = 3$.

r est alors égal à 2 et on pose $X = 3\theta - s$.

a) $p \equiv 1 \bmod 3$.

$$\begin{cases} \overline{\theta_{u,1}}^3 = \omega, \\ \overline{\theta_{u,2}}^3 = \lambda_1^3 \omega^2. \end{cases}$$

Choisissons λ_1 de façon que $\overline{\theta_{u,1}}\,\overline{\theta_{u,2}} = \lambda_1 \omega$.

On en déduit $\dfrac{\overline{\theta_{u,1}}^2}{\overline{\theta_{u,2}}} = \dfrac{1}{\lambda_1}\dfrac{\overline{\theta_{u,2}}^2}{\overline{\theta_{u,1}}} = \lambda_1^2 \omega$.

On peut écrire :

$$X^3 = (\overline{\theta_{u,1}} + \overline{\theta_{u,2}})^3$$

en utilisant les relations précédentes, on obtient :

$$X^3 - 3\lambda_1 \omega X - \omega - \lambda_1^3 \omega^2 = 0$$

b) $p \equiv -1 \bmod 3$ ou $p = 3$.

Nous désignerons par ω' le conjugué de ω.

$$\begin{cases} \overline{\theta_{u,1}}^3 = \omega, \\ \overline{\theta_{u,2}}^3 = \omega', \end{cases} \qquad \overline{\theta_{u,1}}\,\overline{\theta_{u,2}} = m$$

où m désigne la racine cubique de $\omega\omega'$ qui est contenue dans Q_p. Les polynômes en X s'écriront :

$$X^3 - 3mX - (\omega + \omega').$$

2) $l = 5$.

Choisissons $r = 2$ et posons $X = 5\theta - s$.

a) $p \equiv 1 \bmod 5$.

$$\begin{cases} \overline{\theta_{u,1}}^5 = \omega \\ \overline{\theta_{u,2}}^5 = \lambda_1^5 \omega^2 \\ \overline{\theta_{u,4}}^5 = \lambda_2^5 \omega^4 \\ \overline{\theta_{u,3}}^5 = \lambda_3^5 \omega^8 \end{cases}$$

et choisissons λ_1, λ_2, λ_3 de façon que :

$$\frac{\overline{\theta_{u,1}}^2}{\overline{\theta_{u,2}}} = \frac{1}{\lambda_1}, \qquad \frac{\overline{\theta_{u,2}}^2}{\overline{\theta_{u,4}}} = \frac{\lambda_1^2}{\lambda_2}, \qquad \frac{\overline{\theta_{u,4}}^2}{\overline{\theta_{u,3}}} = \frac{\lambda_2^2}{\lambda_3}$$

il en résulte :

$$\frac{\overline{\theta_{u,3}}^2}{\overline{\theta_{u,1}}} = \lambda_3^2 \omega^3$$

et

$$\overline{\theta_{u,1}}\,\overline{\theta_{u,4}} = \lambda_2\omega$$
$$\overline{\theta_{u,2}}\,\overline{\theta_{u,3}} = \lambda_1\lambda_3\omega^2$$
$$\frac{\overline{\theta_{u,1}}\,\overline{\theta_{u,2}}}{\overline{\theta_{u,3}}} = \frac{\lambda_1}{\lambda_3\omega}$$
$$\frac{\overline{\theta_{u,1}}\,\overline{\theta_{u,3}}}{\overline{\theta_{u,4}}} = \frac{\lambda_3}{\lambda_2}\,\omega$$
$$\frac{\overline{\theta_{u,2}}\,\overline{\theta_{u,4}}}{\overline{\theta_{u,1}}} = \lambda_1\lambda_2\omega$$
$$\frac{\overline{\theta_{u,3}}\,\overline{\theta_{u,4}}}{\overline{\theta_{u,2}}} = \frac{\lambda_3\lambda_2}{\lambda_1}\,\omega^2$$

le polynôme en X s'écrira :

$$\begin{vmatrix} -X & 1 & 1 & 1 & 1 \\ \lambda_2\omega & -X & \frac{1}{\lambda_1} & \frac{\lambda_1}{\lambda_3\omega} & \frac{\lambda_3}{\lambda_2}\omega \\ \lambda_1\lambda_3\omega^2 & \lambda_1\lambda_2\omega & -X & \frac{\lambda_1}{\lambda_3\omega} & \frac{\lambda_1^2}{\lambda_2} \\ \lambda_1\lambda_3\omega^2 & \lambda_3^2\omega^3 & \frac{\lambda_3\lambda_2}{\lambda_1}\,\omega^2 & -X & \frac{\lambda_3}{\lambda_2}\omega \\ \lambda_2\omega & \lambda_1\lambda_2\omega & \frac{\lambda_3\lambda_2}{\lambda_1}\,\omega^2 & \frac{\lambda_2^2}{\lambda_3} & -X \end{vmatrix}$$

soit après développement :

$$X^5 - 5\omega(\lambda_2 + \lambda_1\lambda_3\omega)X^3 - 5\omega(\lambda_3\omega + \lambda_1\lambda_2^2\omega + \lambda_1^2 + \lambda_2\lambda_3^2\omega^3)X^2$$
$$+ 5\omega X(\lambda_2^2\omega + \lambda_2^3\lambda_3\omega^3 - \lambda_3^3\omega^4 - \lambda_1\lambda_2\lambda_3\omega^2 - \lambda_1 - \lambda_1^3\lambda_2\omega$$
$$- \lambda_2^3\lambda_3\omega^3 - \lambda_3^3\omega^4)$$
$$- \omega[1 + \lambda_1^5\omega + \lambda_2^5\omega^3 + \lambda_3^5\omega^7 + 5\omega(\lambda_2^2\lambda_3^2\omega^3 + \lambda_1^2\lambda_2^2\lambda_3\omega^2$$
$$+ \lambda_1^2\lambda_2 + \lambda_1\lambda_3^2\omega^2$$
$$- \lambda_1\lambda_2^3\omega - \lambda_1\lambda_2\lambda_3^3\omega^4 - \lambda_2\lambda_3\omega - \lambda_1^3\lambda_3\omega)].$$

b) $p \equiv -1 \bmod 5$.

$Q_p(5)$ est de degré 2 relativement à Q_p, nous noterons α' le conjugué $[2^2]\alpha$ de α, on peut alors écrire :

$$\begin{cases} \overline{\theta_{u,1}}^5 = \omega \\ \overline{\theta_{u,4}}^5 = \omega' \\ \overline{\theta_{u,2}}^5 = \lambda_1^5\omega^2 \\ \overline{\theta_{u,3}}^5 = \lambda_1'^5\omega'^2 \end{cases} \Longrightarrow \begin{cases} \overline{\theta_{u,1}}\,\overline{\theta_{u,4}} = m \\ \text{où } m \text{ désigne la racine } 5^{\text{e}} \text{ de } \omega\omega' \\ \quad \text{située dans } Q_p \\ \overline{\theta_{u,2}}\,\overline{\theta_{u,3}} = \lambda_1\lambda_1' m^2 \end{cases}$$

Choisissons λ_1 de façon que $\dfrac{\overline{\theta_{u,1}}^2}{\overline{\theta_{u,2}}} = \dfrac{1}{\lambda_1}$ il en résulte :

$$\frac{\overline{\theta_{u,2}}^2}{\overline{\theta_{u,4}}} = \lambda_1 \frac{\omega}{m}, \quad \frac{\overline{\theta_{u,3}}^2}{\overline{\theta_{u,1}}} = \lambda_1' \frac{\omega'}{m}, \quad \frac{\overline{\theta_{u,4}}^2}{\overline{\theta_{u,3}}} = \frac{1}{\lambda_1'}$$

$$\frac{\overline{\theta_{u,1}}\,\overline{\theta_{u,2}}}{\overline{\theta_{u,3}}} = \frac{\lambda_1}{\lambda_1'}\frac{\omega}{m^2}, \quad \frac{\overline{\theta_{u,1}}\,\overline{\theta_{u,3}}}{\overline{\theta_{u,4}}} = \lambda_1' m$$

$$\frac{\overline{\theta_{u,2}}\,\overline{\theta_{u,4}}}{\overline{\theta_{u,1}}} = \lambda_1 m, \quad \frac{\overline{\theta_{u,3}}\,\overline{\theta_{u,4}}}{\overline{\theta_{u,2}}} = \frac{\lambda_1'}{\lambda_1}\frac{\omega'}{m^2}$$

d'où on déduit le polynôme en X sous la forme :

$$\begin{vmatrix} -X & 1 & 1 & 1 & 1 \\ m & -X & \dfrac{1}{\lambda_1} & \dfrac{\lambda_1}{\lambda_1'}\dfrac{\omega}{m^2} & \lambda_1' m \\ \lambda_1\lambda_1' m^2 & \lambda_1 m & -X & \dfrac{\lambda_1}{\lambda_1'}\dfrac{\omega}{m^2} & \dfrac{\lambda_1\omega}{m} \\ \lambda_1\lambda_1' m^2 & \dfrac{\lambda_1'\omega'}{m} & \dfrac{\lambda_1'}{\lambda_1}\dfrac{\omega'}{m^2} & -X & \lambda_1' m \\ m & \lambda_1 m & \dfrac{\lambda_1'}{\lambda_1}\dfrac{\omega'}{m^2} & \dfrac{1}{\lambda_1'} & -X \end{vmatrix}$$

c) $p \equiv \pm 2 \bmod 5$ ou $p = 5$.

On obtient une forme analogue à celle du cas global.

4. Dénombrement des extensions abéliennes de degré *l* de Q_p.

THÉORÈME 15. — *Soit* θ_u *un l-uple construit à l'aide de* ω *et de* $\lambda_i \neq 0\ \forall i \in \{1, \ldots, e-1\}$, *et* K_p *l'extension de* Q_p *associée aux* θ_u, *les éléments* ϑ_u *de* K_p *s'écrivent sous la forme :*

$$\vartheta_u = a_0 + \sum_{h=1}^{l-1} a_h \theta_{u+h}$$

avec $a_0, a_1, \ldots, a_{l-1}$ *éléments de* Q_p *et* $\overline{\vartheta_{u,j}}^{\,l} = \mu_j^l\, \overline{\theta_{u,j}}^{\,l}$.

Les éléments $1, \theta_{u+1}, \ldots, \theta_{u+l-1}$ forment une base de l'espace vectoriel K_p sur Q_p car le déterminant

$$\begin{vmatrix} 1 & \theta_{u+1} & \theta_{u+2} & \theta_{u+l-1} \\ 1 & \theta_{u+2} & \cdots & \theta_u \\ \vdots & & & \\ 1 & \theta_u & \theta_{u+1} & \theta_{u+l-2} \end{vmatrix} = \prod_{j=1}^{l-1} \overline{\theta_{u,j}}$$

est différent de zéro. On peut alors écrire :

$$\vartheta_{u+i} = a_0 + \sum_{h=1}^{l-1} a_h \theta_{u+h+i} \qquad \text{avec} \qquad a_0, \ldots, a_{l-1} \in Q_p$$

et en formant les résolvantes de Lagrange de ϑ_u on obtient :

$$\overline{\vartheta_{u,j}} = \sum_{x \bmod l} \varepsilon^{jx} \vartheta_{u+x} = \sum_{x \bmod l} \varepsilon^{jx} \sum_{h=1}^{l-1} a_h \theta_{u+h+x}$$
$$= \sum_{h=1}^{l-1} a_h \sum_{x \bmod l} \varepsilon^{jx} \theta_{u+h+x} = \sum_{h=1}^{l-1} a_h \theta_{u+h,j}$$

soit enfin $\overline{\vartheta_{u,j}} = \left(\sum_{h=1}^{l-1} a_h \varepsilon^{-jh} \right) \overline{\theta_{u,j}}$ ce qui achève la démonstration du théorème.

Nous sommes maintenant en mesure d'étudier le nombre d'extensions abéliennes de degré l de Q_p.

THÉORÈME 16. — *Si $p \neq l$ et $p \not\equiv 1 \bmod l$ il y a e extensions abéliennes de degré l de Q_p.*

Si $p \equiv 1 \bmod l$ il y a $l+1$ extensions abéliennes de degré l de Q_p.

D'après les propositions 1-2-3 et le théorème 15, le nombre d'extensions abéliennes de degré l de Q_p est au plus égal à l'indice du sous-groupe des puissances $l^{\text{ièmes}}$ du groupe des unités de $Q_p(l)$ si $e < l-1$, du groupe multiplicatif de Q_p si $p \equiv 1 \bmod l$. Il reste à examiner si chaque co-classe du sous-groupe des puissances $l^{\text{ièmes}}$ est formée d'éléments ω vérifiant les conditions du théorème 14.

Si $p \equiv 1 \bmod l$, le groupe des puissances $l^{\text{ièmes}}$ est d'indice l^2 dans le groupe multiplicatif de Q_p. Tout élément ω non puissance $l^{\text{ième}}$ engendre une extension abélienne de degré l de Q_p, le nombre de celles-ci est donc égal à $l+1$, compte tenu de ce que deux puissances entières, d'exposants premiers avec l, de ω engendrent la même extension de Q_p.

Si $p \not\equiv 1 \bmod l \Leftrightarrow e < l-1$, $\omega = \eta^x$ où $1 \leqslant x \leqslant l-1$ n'est pas une puissance $l^{\text{ième}}$ dans $Q_p(l)$ et $[r^e]\omega^{l^{\nu-1}} = [r^e]\varepsilon^x = \varepsilon^{r^e x}$ ce qui montre que $[r^e]\omega$ est une racine $l^{\nu-1\ \text{ième}}$ de $(\varepsilon^x)^{r^e}$, $\dfrac{[r^e]\omega}{\omega^{r^e}}$ est donc une racine $l^{\nu-1\ \text{ième}}$ de l'unité, c'est-à-dire une puissance $l^{\text{ième}}$ exacte dans $Q_p(l)$.

En tenant compte de ce qui a été dit sur le changement

des indices des l-uples de conjugués d'une extension de degré l de Q_p, on en déduit qu'il y en a $\frac{l-1}{f} = e$.

Le cas $p = l$ est un peu plus délicat.

THÉORÈME 17. — *Il y a* $p+1$ *extensions abéliennes de degré* p *de* Q_p. Si u désigne une unité distinguée nous devons examiner la valeur de $\frac{[r]u}{u^r}$.

u est de la forme, (cf. Prop. 1),

$$u = \sum_{h=1}^{p} (1 - \Pi^h)^{\alpha_h} \begin{cases} \alpha_1 \bmod p \\ \alpha_h \in Z_p \\ \text{pour } 2 \leqslant h \leqslant p \end{cases}$$

$$[r]u = \sum_{h=1}^{p} (1 - \Pi^h)^{\alpha' h}$$

il nous suffit pour avoir la valeur de $[r]u$ de calculer les $[r](1 - \Pi^h)$, remarquons que $[r](1 - \Pi) = (1 - \Pi)^r$ et que $[r](1 - \Pi^h) \equiv 1 \bmod \mathfrak{p}^h$.

Par ailleurs $[r](1 - \Pi^h) - 1 = \Pi^h(1 + \varepsilon + \cdots + \varepsilon^{r-1})^h$ d'où :

$$[r](1 - \Pi^h) \equiv 1 - r^h \Pi^h \bmod \mathfrak{p}^{h+1}$$

en outre

$$[r]u^\alpha = ([r]u)^\alpha \quad \forall \alpha \in Z_p$$

et

$$[r](u_1 . u_2) = [r]u_1 . [r]u_2.$$

Nous ne nous intéresserons qu'aux restes des unités distinguées modulo le sous-groupe de leurs puissances $p^{\text{ièmes}}$ c'est-à-dire aux restes mod p des α_h, les relations précédentes montrent que $[r]$ est un opérateur linéaire sur les systèmes d'exposants modulo p des $(1 - \Pi^h)$, systèmes qui forment un espace vectoriel isomorphe à $(Z/pZ)^p$, la matrice associée à $[r]$ dans la base canonique s'écrit alors :

$$M = \begin{vmatrix} r & 0 & 0 & 0 & \cdots & & \\ 0 & r^2 & 0 & 0 & \cdots & & \\ 0 & \beta_{3,2} & r^3 & 0 & \cdots & & \\ \vdots & & & & & & \\ 0 & \beta_{p-2,2} & \cdots & & r^{p-2} & 0 & 0 \\ 0 & \beta_{p-1,2} & \cdots & & \beta_{p-1,p-2} & 1 & 0 \\ 0 & \beta_{p,2} & & & & & r \end{vmatrix}$$

où les $\beta_{i,j}$ sont des entiers rationnels définis modulo p. Cette matrice triangulaire vérifie d'ailleurs :

$$M^{l-1} = 1.$$

Il est alors clair que les seules unités distinguées non puissances $p^{\text{ièmes}}$ qui satisfont à la condition $\frac{u^r}{[r]u}$ puissance $p^{\text{ième}}$ dans $Q_p(p)$ sont les produits par des puissances $p^{\text{ièmes}}$ des unités $(1-\Pi)^x (1-\Pi^p)^y$. $x, y \in \{0, 1, \ldots, p-1\}$, x, y non tous deux nuls. Compte tenu des remarques faites sur le changement d'indexation, il y a donc : $\frac{p^2-1}{p-1} = p+1$ extensions abéliennes de degré p de Q_p.

Exemples. — Nous nous servirons des résultats obtenus en particulier dans les théorèmes 14, 16 et 17 pour associer à chaque extension abélienne de degré l de Q_p un polynôme de degré l. Pour simplifier ce polynôme, nous choisirons les λ_i du théorème 14 égaux à 0 et ω égal à une puissance de η (cf. Chapitre VI, § 2) éventuellement multipliée par une puissance de p.

Nous examinerons le cas du degré 3.

a) $p \equiv 1 \mod 3$.

Les 4 extensions abéliennes sont associées biunivoquement aux polynômes :

$$x^3 - \eta, \quad x^3 - p\eta, \quad x^3 - p\eta^2, \quad x^3 - p,$$

b) $p \equiv -1 \mod 3$.

L'extension abélienne de degré 3 de Q_p est obtenue à l'aide du polynôme construit avec $\omega = 27\eta$ et $s = 0$, c'est-à-dire :

$$x^3 - 3x - \text{Trace de } \eta.$$

c) $p = 3$.

Les 4 extensions abéliennes de degré 3 de Q_3 seront obtenues à l'aide des polynômes construits à partir de $s = 0$ et des valeurs de ω suivantes :

$$\omega = 3^3\varepsilon, \quad \omega = 3^3\varepsilon(1 + 3\varepsilon - 3\varepsilon^2),$$
$$\omega = 3^3\varepsilon(1 + 3\varepsilon - 3\varepsilon^2)^2, \quad \omega = 3^3(1 + 3\varepsilon - 3\varepsilon^2)$$

nous obtenons :

$$x^3 - 3x + 1,$$
$$x^3 - 3\rho x + 10,$$
$$x^3 - 3\rho^2 x - 8,$$
$$x^3 - 3\rho x - 2$$

où ρ désigne la racine cubique de $1 + 3^3$ située dans Q_3.

Il est à remarquer que dans le cas *a*) les racines des polynômes trouvés sont bien des éléments primitifs de l'extension associée, mais elles ne donnent pas une base de l'extension considérée comme espace vectoriel sur Q_p (cf. Théorème 15).

BIBLIOGRAPHIE

[1] E. Artin, Galois Theory, Notre Dame, 1953.
[2] A. Chatelet, Arithmétique des corps abéliens du troisième degré, *Annales*, E.N.S., 63, 1946.
[3] A. Châtelet, Idéaux principaux dans les corps circulaires, *Colloque d'Algèbre et Théorie des nombres*, Paris, 1949, 103-106.
[4] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademie Verlag, Berlin, 1962.
[5] H. Hasse, Zahlentheorie, Akademie Verlag, Berlin, 1963.
[6] H. Hasse, Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen, kubischen und biquadratischen Zahlkörpern, Abh. Deutsche. Akad. Wiss, Berlin, *Math. Naturwiss. Jahrg.*, 1948, 2.
[7] E. Hecke, Vorlesungen über die Theorie der algebraischen Zahlen, Chelsea Pub. Co., 1948, 152-154.
[8] D. Hilbert, Théorie des corps de nombres algébriques trad. de T. Got et A. Levy, Hermann, 1913.
[9] H. W. Leopoldt, Zur Arithmetik in abelschen Zahlkörpern, *J. Reine u. Angew. Math.*, 209, 1961-1962, 8-11.
[10] J. J. Payan, Construction des corps abéliens de degré 5, *C. R.*, 254, 1962, 3617-3619.
[11] J. J. Payan, Entiers des corps abéliens de degré 5, *C. R.*, 255, 1962, 2345-2347.
[12] C. A. Rogers, The product of n real homogeneous linear forms, *Acta. math.*, 82, 1950, 185-208.

(*Thèse, Fac. Sciences*, Paris, 1964)

Jean-Jacques Payan,
Service de Mathématiques Pures,
Institut Fourier,
2, place du Doyen-Gosse,
Grenoble (Isère).