JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

J. HERBRAND

Sur les classes des corps circulaires

Journal de mathématiques pures et appliquées 9^e série, tome 11 (1932), p. 417-441.
<http://www.numdam.org/item?id=JMPA_1932_9_11__417_0>

Sur les classes des corps circulaires

PAR J. HERBRAND.

INTRODUCTION ET SOMMAIRE.

Les moyens fournis par la théorie du corps de classes (¹) permettent de reprendre et de compléter, tout en évitant les longueurs de calcul dont il n'avait pu se passer, les résultats obtenus par Kummer il y a 75 ans sur les corps circulaires. Le présent Mémoire y est consacré. On commence par prouver le théorème non encore démontré de Kummer sur la divisibilité du nombre des classes de $k(\zeta)$ par celui de ses sous-corps (§ 1). On y continue par l'étude approfondie de la divisibilité de ces nombres par l, dans le cas où l est premier, ζ racine $l^{ième}$ primitive de l'unité (§ 4); cette étude conduit à celle des surcorps non ramifiés de degré l de $k(\zeta)$, qui est conduite jusqu'au bout dans un cas particulier (§ 5). On montre pour finir comment ces recherches permettent d'étendre sans peine la deuxième démonstration de Kummer pour le théorème de Fermat à des cas plus généraux que ceux qu'il a considérés (§ 6).

(¹) Pour tout ce qui concerne la théorie du corps de classes, on pourra consulter les deux rapports de Hasse (*Jahresbericht der Deutsch. Math. Ver.*, t. 35. 1926, et t. 36, 1927); pour la théorie générale des corps algébriques, nous renverrons au rapport de Hilbert (même périodique, t. 4, 1897; traduction française aux *Annales de Toulouse*, 1909, également éditée à part; quand nous renverrons à « Hilbert », il s'agira de cet Ouvrage, les numéros de page seront ceux de l'édition française qui contient en outre plusieurs Notes de MM. Got et Lévy).

Malgré la disparition presque complète des calculs (sauf au paragraphe 6), l'emploi des logarithmes de Kummer reste indispensable; on n'y utilise que les propriétés les plus simples que nous avons eu soin d'énumérer en rappelant succinctement leurs démonstrations (§ 3).

NOTATIONS. — Désormais, sauf quand le contraire sera explicitement indiqué, désignons par :

k le corps des rationnels;
l un nombre premier impair;
$\mu = \frac{l-1}{2}$;
ζ une racine $l^{\text{ième}}$ primitive de l'unité;
$\lambda = 1 - \zeta$;
$\mathfrak{l}$ l'idéal (λ), tel que $(l) = \mathfrak{l}^{l-1}$;
r une racine primitive module l;
s la substitution $(\zeta \to \zeta^r)$ engendrant le groupe de $k(\zeta)$ par rapport à k;
ε l'unité circulaire suivante :

$$\varepsilon = +\sqrt{\frac{(\zeta^r-1)(\zeta^{-r}-1)}{(\zeta-1)(\zeta^{-1}-1)}},$$

$$E_\nu = \varepsilon^{1+sr^{-2\nu}+s^2r^{-4\nu}+\ldots+s^{\mu-1}r^{-2\nu(\mu-1)}} \qquad \left(\text{où } \nu = 1, 2, 3, \ldots, \mu-1 = \frac{l-3}{2}\right).$$

1. DÉMONSTRATION D'UN THÉORÈME DE KUMMER. — Kummer (1) a énoncé le théorème suivant :

THÉORÈME 1. — *Le nombre des classes de tout sous-corps de $k(\zeta)$ divise le nombre des classes de $k(\zeta)$, ζ étant une racine primitive $l^{\text{ième}}$ de l'unité.*

Sa démonstration était fausse [il suppose implicitement que tout idéal non principal du sous-corps reste non principal dans $k(\zeta)$].

Dans ce qui suit, on peut indifféremment prendre la notion de classe au sens ordinaire, ou au sens restreint, où seuls les idéaux (α) tels que α soit totalement positif, sont dans la classe principale : dans le deuxième cas, il faudra seulement dans les démonstrations ne

(1) KUMMER. *Journal de Crelle*, t. 40, p. 114.

pas tenir compte des idéaux infinis pouvant intervenir dans les conducteurs des corps abéliens considérés.

Le théorème 1 résulte du théorème général suivant :

THÉORÈME 2. — *Soient k un corps, K un surcorps de k, $\overline{\overline{k}}$ le plus grand surcorps de k compris dans K, qui soit abélien non ramifié par rapport à k; p son degré par rapport à k.*

Alors il y a un sous-groupe d'indice p du groupe des classes de k isomorphe au groupe quotient du groupe des classes de K par un de ses sous-groupes.

Appelons $\overline{k}$ le corps de classes absolu de k, $\overline{\mathrm{K}}$ celui de K.

$\overline{k}$ contient $\overline{\overline{k}}$; le groupe de $\overline{k}$ par rapport à k est isomorphe au groupe des classes de k; donc le groupe de $\overline{\overline{k}}$ par rapport à $\overline{k}$ est un sous-groupe d'indice p de ce groupe.

Soit $\overline{\mathrm{K}} = \mathrm{K}\overline{k}$ le plus petit corps contenant K et $\overline{k}$. Le groupe de $\overline{\mathrm{K}}$ par rapport à K est isomorphe à celui de $\overline{k}$ par rapport à $\overline{\overline{k}}$; donc $\overline{\mathrm{K}}$ est abélien sur K. D'après un théorème de Hasse (1), le conducteur de $\overline{\mathrm{K}}$ par rapport à K divise celui de $\overline{k}$ par rapport à k, c'est-à-dire 1. Donc $\overline{\mathrm{K}}$ est abélien non ramifié sur K, et est donc compris dans $\overline{\overline{\mathrm{K}}}$.

Or le groupe de $\overline{\overline{\mathrm{K}}}$ par rapport à K est isomorphe au groupe des classes de K. Donc le groupe de $\overline{\overline{\mathrm{K}}}$ par rapport à K est isomorphe au groupe quotient du groupe des classes de K par un de ses sous-groupes.

D'où le théorème.

Si h est le nombre des classes de k, H celui de K, on voit que h divise $p\mathrm{H}$.

Si, en particulier, K est galoisien par rapport à k, appelons g le plus petit groupe contenant tous les groupes d'inertie, g est évidemment invariant et *p est l'indice du groupe des commutateurs du groupe quotient.*

Si K est un corps à groupe de Galois cyclique (par rapport au

(1) HASSE, *Ein Satz über relativ Galois'scher Zahlkörper...* (*Math. Zeitschrift*, t. 31, p. 563).

corps des rationnels), on vérifie immédiatement que g est identique au groupe de Galois lui-même. D'où le théorème 1.

On voit immédiatement que l'on peut le généraliser ainsi (1) :

THÉORÈME 1 *bis*. — K *étant un corps cyclique* [*par exemple le corps des racines* $l^{\text{èmes}}$ *de l'unité* (l *premier*)], k *un sous-corps, le groupe des classes de* k *est isomorphe* (*en général mériédriquement*) *au groupe des classes de* K.

Des considérations analogues ont été développées indépendamment par M. Chevalley. Elles ont été publiées dans une Note aux *Comptes rendus* du 2 février 1931.

2. LEMME. — Nous utiliserons dans la suite un lemme dont un cas particulier a déjà été énoncé par Hasse (2) :

LEMME. — *Soient* k *un corps;* $\overline{\mathrm{K}}$ *un surcorps de* k, *de groupe* $\overline{g}$; K *un surcorps abélien de* $\overline{\mathrm{K}}$, *galoisien par rapport à* k, *de groupe* G *par rapport à* k, *et de groupe* g *par rapport à* $\overline{\mathrm{K}}$. *Soient* $\mathfrak{f}$ *le conducteur de* K *par rapport à* $\overline{\mathrm{K}}$, H *le groupe d'idéaux* (mod $\mathfrak{f}$), *pour lequel* K *est corps de classes. Il y a une correspondance biunivoque entre les éléments de* g, *et les éléments du groupe* h *quotient du groupe des idéaux premiers à* $\mathfrak{f}$, *par* H.

Une substitution de $\overline{g}$, *qui s'applique sur* z *dans l'isomorphisme appliquant* $\overline{g}$ *sur* G (*l'élément unité de* $\overline{g}$ *s'appliquant sur* g), *transforme un élément* H_β *de* h, *correspondant à* β *de* g, *en un élément* H_γ *correspondant à* γ *de* g.

---

(1) Après la rédaction de ce Mémoire, est venu à notre connaissance un Mémoire de J. Varmon (*Arkiv för Matem., Astr., och Fysik*, Band 22, 1930) où il démontre que le *nombre* des classes de k divise celui de $\overline{\mathrm{K}}$ (et même un théorème plus général). Ses méthodes reposent sur le calcul effectif du nombre des classes, et ne paraissent pas susceptibles d'être généralisées dans la direction du théorème 1 *bis*.

(2) HASSE, *Arithmetische Theorie der Kubischen Zahlkörper...* (*Math. Zeitsch.*, § 2, p. 572, Hilfsatz.) Comparer, ARTIN, *Hamb. Abh.*, t. 7.

On a alors :

$$\gamma = \alpha\beta\alpha^{-1}.$$

Démonstration. — Que α permute entre eux les éléments de h, cela résulte de ce que α conserve K, qui est galoisien sur k, donc H.

Soient maintenant $\mathfrak{P}$ un idéal premier de K, $\overline{\mathfrak{P}}$ l'idéal premier de $\overline{\mathrm{K}}$ divisible par $\mathfrak{P}$. Supposons que $\mathfrak{P}$ soit premier au discriminant de K par rapport à k, et corresponde à la substitution β de G (¹). Donc $\overline{\mathfrak{P}}$ est dans H_γ; $\alpha\overline{\mathfrak{P}}$ est dans H_γ; or la substitution correspondant à $\alpha\mathfrak{P}$, qui est un diviseur de $\alpha\overline{\mathfrak{P}}$, est $\alpha\beta\alpha^{-1}$; d'où le lemme.

Ce lemme, quoique sa démonstration soit très simple, nous sera d'une très grande utilité. Il revient à dire que les automorphismes engendrés par G dans g donnent des permutations des éléments de g identiques aux permutations des éléments de h.

3. Les logarithmes de Kummer. — Quoique nous évitions une grande partie des calculs de Kummer, nous serons pourtant obligés d'employer ses logarithmes. Mais ce sera seulement pour quelques calculs très simples, qui n'utiliseront que les propriétés que nous allons énoncer. (*Voir* pour cela Hilbert, § 131, nous modifions certains points.)

Soit $f(x)$ une fonction rationnelle à coefficients entiers; $f(\zeta)$ est un nombre α de $k(\zeta)$.

Posons

$$l^g(\alpha) = \frac{d_0^g \log f(e^u)}{du^g} \qquad \text{pour } g = 1, 2, \ldots, l-2$$

(l'indice o veut dire qu'on fait $u = 0$ après avoir pris la dérivée)

$$l^{l-1}(\alpha) = \frac{n(\alpha^{l-1}) - 1}{l},$$

$n(\alpha)$ étant la norme de α. Ces expressions sont définies modulo l et ne

(¹) Il y a toujours de tels idéaux d'après un théorème connu (*cf.* par exemple Artin, *Hamb. Abh.*, t. 3, p. 106 (Th. 4), ou Schreier, *Hamb. Abh.*, t. 5, p. 1). La démonstration de Schreier, ne concerne que le cas où le corps de base est le corps des rationnels; mais on passe aisément de là au cas général.

dépendent modulo l que de α, et non du choix particulier de la fonction $f(x)$, comme on le vérifie sans peine (1).

On vérifie aisément que :

$$l^i(\mu\nu) \equiv l^i(\mu) + l^i(\nu) \pmod{l}, \tag{1}$$

en particulier $l^{(i)}(\mu^l) \equiv 0 \pmod{l}$

$$l^i(s\mu) \equiv r^i l^i(\mu) \pmod{l}, \tag{2}$$

d'où

$$l^{(i)}\left[s^{\frac{l-1}{2}}\mu\right] \equiv (-1)^i l^i(\mu) \pmod{l};$$

donc : *si μ est réel, $l^{(i)}(\mu)$ pour i impair est nul.*

Si

$$\mu \equiv a + \alpha l^b \pmod{l^{b+1}} \quad (b \leq l-2). \tag{3}$$

a étant rationnel, premier à l, α pouvant être pris rationnel, on a :

$$l^i(\mu) \equiv 0 \pmod{l} \quad \text{pour } \mu < b.$$

$$l^b(\mu) \equiv \frac{\alpha}{a}(-1)^b b! \pmod{l}.$$

On déduit sans peine de là que $l^{(i)}(\mu)$ est le même pour deux μ congrus entre eux modulo l^{i+1} ; et ce résultat reste vrai pour $i = l-1$.

De plus si

$$l^i(\mu) \equiv 0 \quad (l) \qquad \text{quel que soit } i \leq l-2.$$

on a (2)

$$\mu \equiv a \quad (l^{l-1})$$

pour un certain rationnel.

Donc

$$\mu = a - \alpha l$$

et par conséquent

$$\mu \equiv a' \quad (l^l).$$

a' étant rationnel. Or

$$a' \equiv a'^{l(l-1)} \quad (l^2);$$

---

(1) On ne définit ordinairement ces logarithmes que pour $x \equiv 1 \pmod{l}$. c'est là une restriction inutile, si l'on procède comme nous l'indiquons.

(2) Nous écrirons souvent $a \equiv b\ (p)$ au lieu de $a \equiv b \pmod{p}$.

donc

$$a' \equiv (a'^{l-1})^{l} \quad (l').$$

Ainsi :

Si

$$l^{i}(\mu) \equiv 0 \quad (l) \qquad \textit{quel que soit } i \leqq l-2,$$

μ est congru à une $l^{ième}$ puissance modulo l'.

Soit

$$(4) \qquad \varepsilon(x) = \left[\frac{(x^{2}-1)(x^{-2}-1)}{(x-1)(x^{-1}-1)}\right]^{\frac{1}{2}},$$

de sorte que $\varepsilon(\zeta) = \varepsilon$.

Un calcul aisé (Hilbert, édition française, p. 342) donne (B_n étant le $n^{ième}$ nombre de Bernoulli) :

$$\frac{1}{2}\log \varepsilon^{2}(e^{u}) = \log r + \frac{(r^{2}-1)B_{1}u^{2}}{2.2!} + \ldots + \frac{(-1)^{r-1}(r^{2n}-1)B_{n}u^{2n}}{2n.(2n)!} + \ldots;$$

donc

$$l^{2i}(\varepsilon) \equiv (-1)^{i}\frac{(r^{2i}-1)B_{i}}{2i} \pmod{l},$$
$$l^{2i-1}(\varepsilon) \equiv 0 \pmod{l},$$

si $i \leqq \frac{l-3}{2}$; et enfin par un calcul simple :

$$l^{2\nu}(E_{\nu}) \equiv \frac{(-1)^{\nu-1}(r^{2\nu}-1)B_{\nu}}{4\nu} \pmod{l},$$
$$l^{i}(E_{\nu}) \equiv 0 \pmod{l},$$

pour $i \neq 2\nu$ et $\leqq l-2$; la formule reste vraie pour $i = l-1$, étant donné qu'on a évidemment

$$n(E_{\nu}^{l-1}) = +1.$$

Dans ces calculs, il faut opérer sur $\varepsilon^{2}(x)$ et non sur $\varepsilon(x)$, car seul $\varepsilon^{2}(x)$ est rationnel en x.

4. ÉTUDE GÉNÉRALE DES SURCORPS NON RAMIFIÉS DE DEGRÉ l :

1° LEMME. — *Toute matrice d'ordre $l-1$, modulo l, est équivalente modulo l à une matrice diagonale.*

Posons $\varepsilon_{ij} = 1$ ou 0 suivant que $i = j$ ou $i \neq j$.

Soit la matrice

$$A = (a_{ij}) \qquad (i, j = 1, 2, \ldots, N).$$

telle que

$$A^{l-1} \equiv E \pmod{l}, \qquad \text{où } E = (\varepsilon_{ij}), \text{ la matrice unité.}$$

Donc

$$|a_{ij}| \not\equiv 0 \quad (l).$$

Toutes les égalités que nous écrirons désormais dans la démonstration de ce lemme devront être considérées comme des congruences, modulo l.

Au lieu de la matrice (a_{ij}), considérons (pour simplifier le langage) la transformation linéaire :

$$x'_i = \sum_j a_{ij} x_j \tag{1}$$

qui est donc d'ordre $l-1$.

Considérons l'équation en s :

$$|a_{ij}s - \varepsilon_{ij}| = 0. \tag{2}$$

Cette équation est de degré N ; ses racines définissent une extension du corps des restes modulo l. Soit s une de ces racines. Par une transformation linéaire ayant ses coefficients dans ce corps, on pourra dès lors remplacer les variables x par des variables y, la transformation (1) prenant la forme

$$y'_1 = s y_1,$$
$$y_i = \sum_{(j)} b_{ij} y_j \qquad (i = 2, 3, \ldots, N ; j = 1, 2, \ldots, N).$$

La puissance $(l-1)$ de cette substitution étant la substitution unité, on en déduit que

$$s^{l-1} = 1. \tag{3}$$

Toute racine de (2) satisfait donc à cette condition. L'équation (3) a comme racines les $(l-1)$ restes rationnels premiers à l modulo l. On en déduit que toute racine de (2) est dans le corps des restes modulo l, et non dans une extension algébrique de ce corps.

$s_1, s_2, \ldots, s_p$ étant les racines différentes de (2), la théorie des diviseurs élémentaires nous montre alors que par cette transformation à coefficients entiers, et à déterminant non nul modulo l, on peut

remplacer les variables x_i par des variables z_i pour lesquelles la transformation (1) a la forme suivante :

Les variables z_i se partageant en q groupes, de n_1, n_2, ..., n_q variables; les variables du $i^{\text{ième}}$ groupe, que nous désignons par z_1, z_2, ..., z_{n_i}, se transforment comme suit :

$$\begin{aligned} z'_1 &= sz_1, \\ z'_2 &= s(z_1 + z_2), \\ z'_3 &= s(z_2 + z_3), \\ &\cdots\cdots\cdots\cdots, \\ z'_{n_i} &= s(z_{n_i-1} + z_{n_i}). \end{aligned}$$

Itérons $(l-1)$ fois cette transformation; la transformée de z_2 est, on le voit sans peine,

$$s^{l-1}[(l-1)z_1 + z_2] \equiv z_2 - z_1.$$

Or on devrait trouver z_2, on en déduit que $n_i = 1$; le passage des variables x_i aux variables z_i réduit donc la matrice à la forme diagonale.

Remarque. — Rien dans cette démonstration ne suppose que $(l-1)$ est la plus petite puissance de la matrice congrue à la matrice unité. On peut donc énoncer le théorème :

Toute matrice d'ordre a, modulo l, est équivalente modulo l à une matrice diagonale, l étant un nombre premier tel que

$$l \equiv 1 \quad (a).$$

Conséquence. — Considérons un groupe abélien de type $(\underbrace{l, l, \ldots, l}_{p \text{ fois}})$ c'est-à-dire un groupe de la forme

$$A_1^{x_1} A_2^{x_2} \ldots A_p^{x_p},$$

les x_i prenant les valeurs 0, 1, 2, ..., $l-1$ et $A_i^l = 1$.

Tout automorphisme de ce groupe remplace A_i par un élément

$$A_1^{x_{1i}} A_2^{x_{2i}} \ldots A_p^{x_{pi}};$$

si la puissance $l-1$ de cet automorphisme est l'automorphisme unité,

la matrice (x_{ij}) est d'ordre $l-1$ modulo l; donc d'après le lemme on peut choisir une base du groupe $B_1, B_2, \ldots, B_p$, telle que cet automorphisme transforme B_i en $B_j^{a_i}$.

Ce fait va nous permettre une étude approfondie des surcorps non ramifiés de degré l.

2° Soient K le corps $k(\zeta)$; k' un sous-corps de K.

Soit $\overline{K}$ le plus petit surcorps de K contenant tous les surcorps galoisiens non ramifiés et de degré l sur K. Son groupe par rapport à K est abélien de type $(\underbrace{l, l, \ldots, l}_{p \text{ fois}})$. On sait dès lors que le groupe des classes de K étant mis sous la forme d'un produit direct de groupes cycliques de degrés puissances de nombres premiers, il y a exactement p de ces groupes où ce nombre premier est l (nous dirons alors que le l-rang de ce groupe est égal à p).

Soit $\overline{k'}$ le corps défini de la même manière à partir de k', et $\overline{\overline{k}} = K\overline{k'}$.

Les degrés de K et de $\overline{k'}$ par rapport à k' étant premiers entre eux (le premier divise $l-1$, et l'autre est une puissance de l), ces corps n'ont aucun élément commun en dehors de k'. De plus, $\overline{\overline{k}}$ est abélien par rapport à K, car son groupe par rapport à K est isomorphe à celui de $\overline{k'}$ par rapport à k'; et d'après un théorème de Hasse déjà utilisé (note 2, p. 420), il est corps de classes sur K pour une division des idéaux en classes de conducteur 1; il est donc compris dans $\overline{K}$.

$\overline{K}$ est galoisien par rapport à k car une substitution du groupe de K par rapport à k laisse sa définition invariante; il en est de même de $\overline{k'}$.

Soit $\overline{G}$ le groupe de $\overline{K}$ par rapport à k; dans ce groupe, aux corps k', K, $\overline{k'}$, $\overline{\overline{k}}$ correspondent les sous-groupes invariants G, g, $\overline{g}$, $\overline{\overline{g}}$.

Le corps $\overline{\overline{k}}$ est abélien par rapport à k' : on voit donc que $G : \overline{\overline{g}}$ est abélien, et que $\overline{\overline{g}}$ contient le groupe des commutateurs de G.

Réciproquement appelons pour un instant $\overline{\overline{g}}'$ le groupe des commutateurs de G; $\overline{\overline{g}}$ contient $\overline{\overline{g}}'$; l'ordre de $G : g$ divise $l-1$, celui de $g : \overline{\overline{g}}'$ est une puissance de l; ces ordres étant premiers, $G : \overline{\overline{g}}'$ qui est abélien est produit direct de $g : \overline{\overline{g}}'$ et de $\overline{g}' : \overline{\overline{g}}'$ pour un groupe $\overline{g}'$

convenable. Prenons les corps $\bar{k}''$ et k' correspondant aux groupes $\bar{g}'$ et $\bar{\bar{g}}'$, on voit que $\bar{k}''$ est *galoisien* par rapport à k'.

Il est de plus *non ramifié*, car soit γ le groupe d'inertie d'un des facteurs de l dans $\bar{k}'$, dans le groupe G : $\bar{\bar{g}}'$; ce groupe étant un produit direct de $\bar{g}' : \bar{\bar{g}}'$ et de $g : \bar{\bar{g}}'$, dont les ordres sont premiers entre eux, γ est le produit direct d'un sous-groupe de $\bar{g}' : \bar{\bar{g}}'$ et d'un sous-groupe de $g : \bar{\bar{g}}'$; $\bar{k}'$ étant non ramifié sur K, le dernier est égal à l'unité; γ est donc dans $\bar{g}' : \bar{\bar{g}}'$, donc $\bar{k}''$ est non ramifié par rapport à k'.

De plus le groupe de $\bar{k}''$ par rapport à k' étant isomorphe à un sous-groupe de g, est *abélien de type* $(l, l, \ldots, l)$.

De toutes ces propriétés de $\bar{k}''$, on déduit que $\bar{k}''$ est dans $\bar{k}'$, et doit donc coïncider avec $\bar{k}'$.

Par conséquent $\bar{\bar{g}}$ *est le groupe des commutateurs de* G.

3° Soit s une substitution de $\bar{G}$, qui considérée dans le groupe quotient $\bar{G}$: g engendre ce groupe (par exemple $s\zeta = \zeta^r$). Le passage de β de g à $s\beta s^{-1}$ définit un automorphisme de g : une puissance $l-1$ de cet automorphisme est un automorphisme unité. D'après le lemme on peut choisir une base de g composée des éléments $\beta_1, \beta_2, \ldots, \beta_\mu$, telle que

$$s\beta_i s^{-1} = \beta_i^{\rho_i}.$$

Soit n le degré de k' par rapport à k; $mn = l-1$; G : g est engendré par s''; or

$$s''\beta_i s^{-n} = \beta_i^{\rho_i^n};$$

donc $\bar{\bar{g}}$ est engendré par les $\beta_i^{\rho_i^{n-1}}$.

Le groupe $g : \bar{\bar{g}}$ est donc isomorphe au groupe engendré par ceux des β tels que

$$\rho_i^n \equiv 1 \quad (l).$$

Soient $\beta_1, \beta_2, \ldots, \beta_q$ ces β. Le groupe G : γ est alors de la forme

$$\beta_1^{x_1}\beta_2^{x_2}\ldots\beta_q^{x_q} \qquad (0 \leq x_i < l-1)$$

et l'on a

$$s\beta_i s^{-1} = \beta_i^{\rho_i}.$$

Remarquons maintenant que $\overline{K}$ est corps de classes pour K par rapport au groupe des $l^{\text{èmes}}$ puissances d'idéaux. On peut mettre le groupe des classes de K sous la forme

$$A_1^{x_1} A_2^{x_2} \dots A_p^{x_p} B^l,$$

les B^l parcourant les $l^{\text{èmes}}$ puissances de classes, les A_i fixes, $0 \leq x_i < l$; et d'après le lemme 1, on peut supposer

$$s A_i \cong A_i^{\varrho_i}$$

(nous employons le signe $A \cong B$ pour exprimer que le quotient des classes A et B est une $l^{\text{ème}}$ puissance de classes).

On voit dès lors que $\varrho_1, \varrho_2, \dots, \varrho_p$ étant les ϱ_i tels que $\varrho_i'' \equiv 1 \ (l)$ le groupe des classes de k' est de forme

$$C_1^{x_1} C_2^{x_2} \dots C_q^{x_q} D^l.$$

les D^l parcourant les $l^{\text{èmes}}$ puissances de classes, les C_i fixes, $0 \leq x_i < l$; et l'on a

$$s C_i \cong C_i^{\varrho_i};$$

il nous reste à déterminer les ϱ_i.

4° Soient r_i le plus petit nombre > 0, congru à r^i (modulo l), et

$$q_i = \frac{r r_i - r_{i+1}}{l} \qquad (q_i \text{ est évidemment entier}).$$

D'après le théorème 136 de Hilbert, pour tout idéal $\mathfrak{p}$

$$\mathfrak{p}^{q_0 + q_{-1} s + \dots + q_{-l+2} s^{l-2}}$$

est principal. On en déduit que les ϱ_i sont racines de la congruence

$$(1) \qquad q_0 + q_{-1} x + \dots + q_{-l+2} x^{l-2} \equiv 0 \quad (l).$$

Résolvons cette congruence. Posons

$$x \equiv r^{-u} \quad (l) \qquad (u = 0, 1, \dots, l-2).$$

Reprenons le raisonnement de Kronecker reproduit par Hilbert (lemme 28).

En élevant à la puissance $u+1$ l'identité

$$rr_i = r_{i+1} + (rr_i - r_{i-1}),$$

où $rr_i - r_{i+1}$ est divisible par l, on obtient

$$r^{u(i-1)} r_i^{u-1} \equiv r_{i+1}^{u-1} + (u+1) r_{i+1}^{u} (rr_i - r_{i-1}) \quad (l^2);$$

donc :

$$(u+1)(rr_i - r_{i-1}) r_{i+1}^{u} \equiv r^{u(i-1)} r_i^{u-1} - r_{i+1}^{u+1} \quad (l^2)$$

ou

$$(u+1)(rr_i - r_{i+1}) r^{(i-1)u} \equiv r^{u(i-1)} r_i^{u-1} - r_{i+1}^{u+1} \quad (l^2).$$

Ajoutons ces congruences pour $i = 0, -1, \ldots, -(l-2)$, il vient :

$$(u+1) l r^{u} \sum_{i} q_i r^{-iu} \equiv r^{u(i-1)} \sum_{i} r_i^{u-1} - \sum_{i} r_{i+1}^{u+1} \quad (l^2).$$

Mais

$$\sum_{i} r_i^{u-1} = \sum_{i} r_{i+1}^{u-1} = 1^{u-1} + 2^{u-1} + \ldots + (l-1)^{u-1}.$$

Donc r^u n'est une racine que si

$$(r^{u-1} - 1)\left[1^{u-1} + 2^{u-1} + \ldots + (l-1)^{u-1}\right] \tag{2}$$

est divisible par l^2.

1° Si $u = 0$, on vérifie directement que ceci n'est divisible que par l et non par l^2. On pourrait ainsi montrer que $u = 0$ entraînerait l'existence d'un surcorps non ramifié sur k.

2° Si $u = l-2 \equiv -1\ (l)$, on vérifie directement que

$$x \equiv r^{-l-2} \equiv r \quad (l)$$

fournit une solution de l'équation (1). Mais nous démontrerons plus loin (Remarque 2° de ce paragraphe) que cette solution ne peut intervenir.

3° Pour les autres valeurs de $u\ (1 \leqq u \leqq l-3)$,

$$1^{u-1} + 2^{u-1} + \ldots + (l-1)^{u-1} + l^{u-1}$$

n'est divisible par l^2, d'après les formules sommatoires connues (¹) que si $u = 2t$; ou bien $u = 2t+1$ à condition que

$$B_{t-1} \equiv 0 \quad (l)$$

(B_k étant le $k^{\text{ième}}$ nombre de Bernoulli). Revenons maintenant aux considérations qui terminaient la troisième partie de ce paragraphe.

Si $\varrho_i = r^{-u_i}$, la congruence $\varrho_i'' \equiv 1\ (l)$ revient à

$$nu_i \equiv 0 \qquad (l-1).$$

donc

$$u_i \equiv 0 \qquad (m).$$

Des considérations précédentes résulte alors :

Théorème 3. — *Les classes de $k(\zeta)$ peuvent être représentées sous la forme*

$$\mathfrak{A}_1^{x_1}\mathfrak{A}_2^{x_2}\dots\mathfrak{A}_\rho^{x_\rho}\mathfrak{B}.$$

$\mathfrak{B}$ *parcourant un certain ensemble de classes, les $\mathfrak{A}_i$ étant fixes, les x_i soumis à la seule condition : $0 \leq x_i < l$ de telle manière que*

$$s\mathfrak{A}_i \sim \mathfrak{A}_i^{r^{-u_i}}.$$

les u_i ne pouvant prendre que les valeurs $1, 2, \dots, l-3$; de plus $u_i = 2t+1$ n'est possible que si $B_{t+1} \equiv 0(l)$; k' étant le sous-corps de $k(\zeta)$ par rapport

---

(¹) En effet, on sait que :

$$1^{2t} + 2^{2t} + \dots + (l-1)^{2t} + l^{2t}$$
$$= \frac{l^{2t+1}}{2t+1} + \frac{l^{2t}}{2} + B_1 \frac{2t}{2!} l^{2t-1} + \dots$$
$$+ (-1)^{n-1} l^{2t-2n+1} B_n \frac{2t(2t-1)\dots(2t-2n+2)}{(2n)!} + \dots + (-1)^{t-1} l B_t;$$

$$1^{2t-1} + 2^{2t-1} + \dots + (l-1)^{2t-1} + l^{2t-1}$$
$$= \frac{l^{2t}}{2t} + \frac{l^{2t-1}}{2} + B_1 \frac{2t-1}{2!} l^{2t-2} + \dots$$
$$+ (-1)^{n-1} l^{2t-2n} B_n \frac{(2t-1)2t\dots(2t-2n+2)}{(2n)!} + \dots + (-1)^{t-1} l^t B_t \frac{2t-1}{2}.$$

De plus, $B_1, B_2, \dots, B_{\frac{l-3}{2}}$ ont des dénominateurs premiers à l, ce qui permet de passer aux congruences modulo l.

auquel $k(\zeta)$ est de degré m, les classes de k' peuvent se mettre de même sous la forme $C_1^{x_1}C_2^{x_2}\dots C_q^{x_q}D^l$ (D variable, les C_i fixes, $0 \leqq x_i < l$; q est le l-rang du groupe des classes de k') de telle manière que

$$sC_i \simeq C_i^{-u_{x_i}},$$

les x_i étant tous différents entre eux, les u_{x_i} n'étant autres que tous les u_i divisibles par m.

En résumé, les u impairs ne peuvent intervenir que si des nombres de Bernoulli sont divisibles par l, les u pairs que si le nombre de classes de $k(\zeta+\zeta^{-1})$ est divisible par l. Mais on démontre aisément (théorème 154 de Hilbert) que, dans ce cas, un des $\frac{l-3}{2}$ premiers nombres de Bernoulli est divisible par l.

Donc nous trouvons une démonstration légèrement modifiée du théorème de Kummer, affirmant que si aucun de ces nombres n'est divisible par l, le nombre des classes de $k(\zeta)$ est premier à l (on évite le lemme 28 de Hilbert).

Remarques. — 1° Nous pourrions étudier par la même méthode le p-rang du groupe des classes, p étant un nombre premier tel que $p \equiv 1 \ (l-1)$.

Nous serions conduits à résoudre l'équation (1) modulo p et non plus modulo l. Mais nous n'avons pu en faire la résolution effective dans ce cas ; aussi avons-nous préférer nous limiter au cas simple où $p = l$.

2° Nous avons annoncé plus haut que $u_1 = -1$ était impossible. Démontrons-le.

Supposons pour fixer les idées $u_1 = -1$. Prenons le corps de classes pour le groupe des idéaux de toutes les classes :

$$A_2^{x_2}\dots A_p^{x_p}B^l \qquad (0 \leqq x_i < l).$$

Il est engendré par $\sqrt[l]{z}$. Soit $\mathfrak{p}$ un idéal de la classe A_1. On a

$$\left(\frac{z}{\mathfrak{p}}\right) = \zeta^{l} \qquad [\text{avec } l \text{ entier } (\bmod l)].$$

$s\mathfrak{p}$ étant dans une classe $\sim A_1^r$, on a

$$\left(\frac{z}{s\mathfrak{p}}\right) = \zeta^{lr}$$

Donc

$$\left(\frac{s^{-1}\alpha}{\mathfrak{p}}\right)=\zeta^{l}=\left(\frac{\alpha}{\mathfrak{p}}\right).$$

Mais $\sqrt[l]{\alpha}$ et $\sqrt[l]{s^{-1}\alpha}$ donnant donc le même surcorps, on a une relation

$$s^{-1}\alpha.\alpha'^{l}=\beta^{l}$$

avec un β et un α' convenable. Dès lors :

$$\left(\frac{s^{-1}\alpha}{\mathfrak{p}}\right)=\left(\frac{\alpha}{\mathfrak{p}}\right)^{x},$$

ce qui entraîne, en comparant avec (1),

$$x\equiv -1 \pmod{l}.$$

Donc

$$\frac{s\alpha}{\alpha'}=\beta^{l}.$$

On aura (la norme étant prise par rapport à k)

$$N(\beta)=-1.$$

Donc β est de forme γ^{1-s} (d'après le théorème 90 de Hilbert, dont la démonstration est valable pour tout corps relatif cyclique, même de degré non premier). $\alpha\gamma^{l}=a$ est alors rationnel: c'est de plus la $l^{\text{ième}}$ puissance d'un idéal de $k(\zeta)$. En décomposant a en facteurs premiers on voit immédiatement que a serait la puissance $l^{\text{ième}}$ d'un nombre rationnel; α serait donc une $l^{\text{ième}}$ puissance, ce qui est impossible.

5. Génération effective des surcorps non ramifiés de degré l. — *Supposons désormais que le nombre de classes de* $k(\zeta+\zeta^{-1})$ *est premier à* l.

Supposons que $B_{n_1}, B_{n_2}, \ldots, B_{n_\nu}$ *soient les seuls nombres de Bernoulli parmi les* $\frac{l-3}{2}$ *premiers, qui soient divisibles par* l.

1° D'après le paragraphe **3**, 4°, on voit que :

$$l^{i}(E_{n_j})\equiv 0 \pmod{l}$$

quels que soient i et j.

Donc d'après le paragraphe **3**, 3°, E_{n_j} *est congru à une* $l^{\text{ième}}$ *puissance mod* l'.

Au contraire, si j est différent de tous les ν_i on a :

$$l^{i}(E_j) \equiv 0 \quad (l) \qquad \text{pour } i \neq j,$$
$$l^{j}(E_j) \not\equiv 0 \quad (l).$$

Enfin :

$$l^{i}(\zeta) \not\equiv 0 \quad (l),$$
$$l^{i}(\zeta) \equiv 0 \quad (l) \qquad \text{pour } i \neq 1.$$

2° E_j *ne peut être la* $l^{ième}$ *puissance d'une unité.*

Cette unité pourrait être supposée réelle positive (car toute unité de $k(\zeta)$ est le produit de ζ^{i} par une unité réelle positive). Il suffit de montrer que l'indice du groupe engendré par les E_j est d'un indice premier à l dans le groupe de toutes les unités réelles positives. Il en résultera que les E_j sont des unités indépendantes (puisqu'elles sont au nombre de $\frac{l-3}{2}$).

Or le groupe engendré par $\varepsilon, s\varepsilon, \ldots, s^{p-2}\varepsilon$ est d'indice premier à l dans le groupe de toutes les unités réelles positives ; car il résulte de l'expression donnée par Kummer du nombre de classes de $k(\zeta+\zeta^{-1})$, que cet indice est précisément égal à ce nombre de classes.

Reste à montrer qu'il en est de même de l'indice du groupe engendré par les E_j dans le groupe engendré par $\varepsilon, s\varepsilon, \ldots, s^{p-2}\varepsilon$. Or

$$E_j = \varepsilon^{1-s^{2j}+s^{2j+1}-\cdots-s^{p-2}+s^{p-2+2j}}$$

mais

$$\varepsilon^{1-s+s^2-\cdots-s^{p-1}} = 1;$$

donc

$$E_j = \varepsilon^{1-s^{2j}+s^{2j+1}-s^{4j}+s^{4j+1}-\cdots-s^{p-2+2j}+s^{p-2+4j}}.$$

L'indice cherché est égal au déterminant

$$\left| s^{2kj} - s^{2(k+1)j} \right| \qquad (0 \leq k \leq p-2,\ 1 \leq j \leq p-1).$$

Si ce déterminant était divisible par l, les congruences

$$\sum_{k} x_k (s^{2kj} - s^{2(k+1)j}) \equiv 0 \quad (l)$$

auraient des solutions x_k non toutes nulles. Multiplions ces congruences

par r^{2-k}, et ajoutons : on en déduit

$$x_k \equiv 0 \quad (l) \qquad (\text{pour } k = 2, 3, \ldots, \mu - 2);$$

$k = 2, 3, \ldots, \mu - 2$) ; d'où également

$$x_1 \equiv 0 \quad (l).$$

Donc ce déterminant est premier à l. C. Q. F. D.

Appelons a l'indice du groupe engendré par les $\pm E_i$ dans le groupe de toutes les unités réelles positives. La puissance $a^{\text{ième}}$ de toute unité est un produit d'une racine de l'unité par des puissances des E_i. On en déduit que, *pour toute unité* ε, *on ne peut avoir*

$$l^l(\varepsilon) \not\equiv 0 \quad (l)$$

que pour i *pair, différent de* $2\nu_1, 2\nu_2, \ldots, 2\nu_\mu, l-1$ *et pour* $i = 1$.

De plus, il y a toujours des unités telles que tous ces logarithmes aient des valeurs fixées d'avance (mod l*) satisfaisant aux conditions précédentes.*

3° D'après ce qui précède, $k(\zeta, \sqrt[l]{E_{\nu_i}})$ *est non ramifié sur* $k(\zeta)$: il est corps de classes pour un groupe d'idéaux composé de toutes les classes d'idéaux d'un sous-groupe H d'indice l du groupe des classes. Le groupe des classes est donc de forme

$$A^x H \qquad (x = 0, 1, \ldots, l-1).$$

Supposons A choisi de telle manière que, pour $\mathfrak{p}$ dans AH, on ait :

$$\left(\frac{E_{\nu_i}}{\mathfrak{p}}\right) = \zeta.$$

On a

$$sE_{\nu_i} = E_{\nu_i}^{r^{\nu_i}}.$$

Donc

$$\left(\frac{E_{\nu_i}}{s\mathfrak{p}}\right) = \left(\frac{sE_{\nu_i}^{r^{\nu_i}}}{s\mathfrak{p}}\right) = \left(\frac{sE_{\nu_i}}{s\mathfrak{p}}\right)^{r^{\nu_i}} = \zeta^{r^{\nu_i}}.$$

donc sA est égal au produit de $A^{r^{\nu_i}}$ par un élément de H.

4° On peut donc supposer que A est un des A_j de l'énoncé du théorème 3. On voit donc que, parmi les u_j, figurent tous les $2\nu_i - 1$. Nous pourrons donc mettre le groupe des classes sous la forme suivante :

$$V_1^{x_1} V_2^{x_2} \ldots V_\mu^{x_\mu} B \qquad (0 \leq x_i < l).$$

A_i' étant dans le groupe B, sA_i étant égal au produit de $A_i'^{-x_{i,i+1}}$ par un élément de B.

Or dans le cas où le nombre de classes de $k(\zeta+\zeta^{-1})$ est premier à l, Takagi (1) a démontré d'une manière remarquablement simple que tout surcorps non ramifié était donné par la racine $l^{\text{ième}}$ d'une unité (2). Soient τ_i une telle unité; a l'indice du groupe des E_i par rapport au groupe de toutes les unités réelles positives; prenons b tel que $b\equiv 1\ (l)$, $b\equiv 0(a)$; alors $\sqrt[l]{\tau_i^b}$ et $\sqrt[l]{\tau_i}$ engendrent le même corps; τ_i^b est congru à une $l^{\text{ième}}$ puissance modulo l', donc à un rationnel. Les valeurs des logarithmes des E_i montrent que τ_i^b est (à une puissance $l^{\text{ième}}$ près) un produit de $E_{i,i}$.

Soit

$$\tau_i^b = E_{i,1}^{e_1} E_{i,2}^{e_2} \dots E_{i,p}^{e_p} x^l.$$

On a

$$\left(\frac{\tau_i^b}{\mathfrak{p}}\right) = \zeta^{x_1 e_1 + x_2 e_2 + \dots + x_p e_p}$$

si la classe de $\mathfrak{p}$ est de forme

$$A_1^{x_1} A_2^{x_2} \dots A_p^{x_p} B.$$

$k(\zeta, \sqrt[l]{\tau_i^b})$ est donc corps de classes par rapport à $k(\zeta)$ pour le groupe des classes de la forme ci-dessus, caractérisées par

$$x_1 e_1 - x_2 e_2 - \dots + x_p e_p \equiv 0 \quad (l).$$

Comme il n'y a pas d'autre sous-groupe non ramifié de degré l, on déduit :

THÉORÈME 1. — *$B_{\nu_1}, B_{\nu_2}, \dots, B_{\nu_p}$ étant les seuls nombres de Bernoulli divisibles par l parmi les $\frac{l-3}{2}$ premiers, si le nombre des classes de $k(\zeta+\zeta^{-1})$ est premier à l, le groupe des classes de $k(\zeta)$ a la forme*

$$A_1^{x_1} A_2^{x_2} \dots A_p^{x_p} B.$$

---

(1) TAKAGI, *Journal für reine und ang Math.*, t. 157, p. 235.

(2) Cette unité, devant d'ailleurs être $\equiv x^l \pmod{l'}$ pour que le surcorps soit non ramifié, peut être supposée réelle positive.

B *étant composé de* $l^{\text{èmes}}$ *puissances de classes,* A_i^l *étant dans* B. *On a*

$$sA_i \cong A_i^{r^{2\nu_i-1}}.$$

Les différents surcorps non ramifiés de degré l, sont corps de classe, pour les sous-groupes caractérisés par

$$\sum e_i x_i \equiv 0 \pmod{l}$$

et sont alors engendrés par

$$\sqrt[l]{E_{\nu_1}^{e_1} E_{\nu_2}^{e_2} \dots E_{\nu_p}^{e_p}}.$$

Le procédé du paragraphe 4 permet alors la génération effective de tous les surcorps non ramifiés de degré l des sous-corps de $k(\zeta)$.

5° Supposons maintenant le nombre des classes de $k(\zeta)$ *divisible par* l^p *et non par une puissance supérieure de* l.

Alors le groupe B a un ordre premier à l, et l'on peut supposer $A_i^l = 1$. Remarquons que dans ce cas, on peut démontrer le théorème 4 sans recourir au raisonnement de Takagi; car le groupe B défini au début du sous-paragraphe 4 est forcément d'un ordre premier à l.

Soit $\mathfrak{p}$ un idéal de A_1; $\mathfrak{p}'$ est principal; posons $\mathfrak{p}' = ([\mathfrak{p}'])$. $[\mathfrak{p}']$ est un entier défini à une unité près.

Il ne peut être congru à une $l^{\text{ième}}$ puissance modulo l'; car $\sqrt[l]{[\mathfrak{p}']}$ définirait un surcorps non ramifié, donc $[\mathfrak{p}']$ serait égal au produit d'une unité par une $l^{\text{ième}}$ puissance, et $\mathfrak{p}$ serait principal, ce qui est impossible.

D'après la remarque faite plus haut sur les logarithmes des unités on voit qu'on peut supposer $l^{\nu}([\mathfrak{p}'])$ nul, sauf pour

$$i \equiv 2\nu_1, 2\nu_2, \dots, 2\nu_p : 3, 5, \dots, l-2 : l-1 :$$

si l'on choisit $[\mathfrak{p}']$ de manière qu'il en soit ainsi, les autres logarithmes sont bien déterminés: et un au moins est non nul (d'après § 3, 3°).

$s[\mathfrak{p}']$ est dans une classe $\cong A_1^{r^{2\nu_1-1}}$; donc on déduit ses logarithmes de ceux de $[\mathfrak{p}']$ en les multipliant par $r^{2\nu_1-1}$.

D'après le paragraphe 3, 2°, on voit que le seul logarithme de $[\mathfrak{p}']$ non nul est alors $l^{l-2\nu_1}([\mathfrak{p}'])$.

Supposons d'une manière générale que $\mathfrak{p}$ est un idéal quelconque tel que $\mathfrak{p}^l$ soit principal. $\mathfrak{p}$ appartient à une classe de forme $A_1^{e_1} A_2^{e_2} \dots A_p^{e_p}$.

Il est donc égal au produit d'idéaux entiers des classes $A_i^{\nu_i}$ par un idéal principal entier ou non. On voit donc que les seuls logarithmes non nuls de $[\mathfrak{p}']$, sont les $l^{l'-2\nu_i}([\mathfrak{p}'])$ pour les i tels que $x_i \not\equiv 0\ (l)$ (pour un choix convenable de $[\mathfrak{p}']$).

Or d'après ce que nous avons vu, $x_i \equiv 0\ (l)$ est équivalent à $\left(\frac{E_{\nu_i}}{\mathfrak{p}}\right) = 1$.

Si nous remarquons qu'en multipliant $[\mathfrak{p}']$ par une unité quelconque, $l^{l'-2\nu_i}([\mathfrak{p}'])$ ne change pas, on obtient le théorème suivant :

THÉORÈME 5. — *Sous les hypothèses du théorème 4, et si de plus le nombre de classes de $k(\zeta)$ n'est pas divisible par l^{p-1}, pour que $\left(\frac{E_{\nu_i}}{\mathfrak{p}}\right) = 1$, $\mathfrak{p}'$ étant supposé principal, il faut et il suffit que*

$$l^{l'-2\nu_i}([\mathfrak{p}']) \equiv 0 \pmod{l}.$$

Ce résultat fut découvert par Kummer dans un cas particulier; il supposait $p = 1$, le nombre de classes de $k(\zeta)$ divisible par l, et supposait de plus qu'il y avait un idéal $\mathfrak{p}$ tel que $\left(\frac{E_\nu}{\mathfrak{p}}\right) \neq 1$. Cette deuxième hypothèse apparaît comme inutile, grâce à la théorie du corps de classe : nous verrons en effet que la supposition que p des $\frac{l-3}{2}$ nombres de Bernoulli sont divisibles par l, et que le nombre des classes de $k(\zeta)$ n'est pas divisible par l^{p-1}, entraîne que le nombre des classes de $k(\zeta+\zeta^{-1})$ est premier à l. Alors $\sqrt[l]{E_\nu}$ donne un surcorps non ramifié, et il y a des $\mathfrak{p}$ tels que $\left(\frac{E_\nu}{\mathfrak{p}}\right) \neq 1$.

La démonstration de Kummer repose sur le calcul, long et difficile de $\left(\frac{E_\nu}{\mathfrak{p}}\right)$.

Il résulte de la démonstration précédente que, si $\mathfrak{p}'$ est principal, $\mathfrak{p}$ étant dans une des classes $A_1^{\nu_1}, \ldots, A_p^{\nu_p}$, on a

$$l^{l'-2\mu}([\mathfrak{p}']) \equiv 0 \pmod{l},$$

si μ est différent d'un des ν_i.

Ce résultat est vrai sans aucune hypothèse restrictive sur le groupe des classes. Takagi (1) l'a déduit très simplement de la valeur qu'il a

(1) *Loc. cit.* ou *Proceedings of the Math. Phys. Soc. of Japan*, 1922, p. 180.

donnée du symbole normique $\left(\frac{\alpha, \beta}{l}\right)$; dans le cas particulier où le nombre des classes de $k(\zeta+\zeta^{-1})$ est premier à l, il en a donné une autre démonstration très profonde. Mais dans notre cas particulier, la réciproque est vraie : en effet, si $\mathfrak{p}'$ est principal, $\mathfrak{p}$ sera d'une classe de forme $A_1^{x_1}A_2^{x_2}\dots A_\rho^{x_\rho}$; donc, pour que $\mathfrak{p}$ le soit, il suffit que $\left(\frac{E_{\nu_i}}{p}\right)=1$ pour tout i, donc que $l^{(l-2\nu_i)}([\mathfrak{p}']\equiv 0)\,(l)$; mais cette condition est évidemment nécessaire (d'après § 3, 1°).

Théorème 6. — *Sous les hypothèses du théorème 5, si $\mathfrak{p}'$ est principal, pour que $\mathfrak{p}$ soit principal il faut et il suffit que*

$$l^{(l-2\nu_i)}([\mathfrak{p}'])\equiv 0 \quad (l) \qquad \text{pour } i=1, 2, \dots, \rho.$$

Conséquence. — *Si $[\mathfrak{p}']\equiv a\,(l)$, a étant rationnel, $\mathfrak{p}$ est principal* (d'après le paragraphe 3, 2°).

Rémarque. — On sait que Kummer (*voir* Hilbert, th. 142) a mis le nombre des classes de $k(\zeta)$ sous la forme d'un produit de deux facteurs, dont le deuxième est le nombre des classes $k(\zeta+\zeta^{-1})$.

Si p nombres de Bernoulli parmi les $\frac{l-3}{2}$ premiers sont divisibles par l, on démontre aisément (en reprenant le raisonnement de Hilbert, lemme 28) que le premier facteur du nombre des classes est divisible par l^p; *donc l'hypothèse que le nombre des classes est divisible par l^p, et non par une puissance plus grande de l, entraine que le nombre des classes de $k(\zeta+\zeta^{-1})$ est premier à l.*

6. Application au dernier théorème de Fermat. — Kummer, en s'appuyant sur un cas particulier des résultats précédents, avait démontré que :

L'équation $x^l+y^l=z^l$ est impossible en nombres entiers du corps $k(\zeta+\zeta^{-1})$ dont un seul est divisible par l, sous les conditions suivantes :

1° *l divise un seul B_ν des $\frac{l-3}{2}$ premiers nombres de Bernoulli;*

2° *Le premier facteur du nombre de classes n'est pas divisible par l^2;*

3° *Il y a un idéal* $\mathfrak{p}$ *tel que* $\left(\frac{E_{2n}}{\mathfrak{p}}\right) \neq 1$;

4° B_{n} *n'est pas divisible par* l^2.

Les résultats obtenus précédemment permettent d'aller plus loin en utilisant la même méthode.

THÉORÈME 7. — *Supposons que, parmi les* $\frac{l-3}{2}$ *premiers nombres de Bernoulli, seuls* $B_{n_1}, B_{n_2}, \ldots, B_{n_r}$ *soient divisibles par* l. *On peut remplacer les conditions de Kummer par les suivantes :*

1° *Le nombre des classes de* $k(\zeta)$ *n'est pas divisible par* l^{r+1} :

2° *Aucun* B_{n_i} *n'est divisible par* l^2.

D'après la remarque terminant le paragraphe 5, la première hypothèse équivaut à l'ensemble des suivantes :

a. Le premier facteur du nombre de classes n'est pas divisible par l^{r+1}.

b. Le deuxième facteur est premier à l.

La condition *a* généralise la deuxième condition de Kummer. La condition *b* était chez Kummer une conséquence de sa troisième condition.

La démonstration de ce théorème est essentiellement celle de Kummer. Il n'y a à faire que quelques très légères modifications, que nous indiquons, et à utiliser notre théorème 6, au lieu des résultats sur lesquels s'appuie Kummer. Nous renvoyons pour le reste et pour les notations à l'exposé qu'en donne Got dans HILBERT, édition française, p. 359-365 (¹).

On commence par démontrer par la même méthode que Kummer, que dans notre cas plus général : *Toute unité congrue à un nombre rationnel* (mod l^2) *est la* $l^{ème}$ *puissance d'une unité.*

En effet, le deuxième facteur du nombre des classes est premier à l.

(¹) Got, en reproduisant le raisonnement de Kummer, oublie la deuxième hypothèse, faite explicitement par Kummer; elle est pourtant indispensable dans la démonstration du théorème XI, § 8, de HILBERT (éd. fr.).

On arrive alors aux congruences

$$M_n \frac{d_0^{2nl} \log \varepsilon(e^u)}{du^{2nl}} \equiv 0 \quad (l^2) \qquad (n = 1, 2, \ldots, \mu - 1).$$

Mais

$$\frac{d_0^{2nl} \log \varepsilon(e^u)}{du^{2nl}} = (-1)^{n+1}(r^{2nl} - 1)\frac{B_{nl}}{2nl} \qquad \text{(d'après § 3, 4°)}.$$

Donc

$$M_n \equiv 0 \quad (l),$$

c'est-à-dire

$$\sum_{k=0}^{k=\mu-2} m_k r^{2nkl} \equiv 0 \quad (l).$$

Multiplions ces congruences respectivement par r^{-2nls}, et ajoutons; il vient

$$m_s \equiv 0 \quad (l),$$

ce qui entraîne le résultat cherché.

Dans la démonstration du théorème lui-même, on fera les deux modifications suivantes :

1° $[I_r']$ est congru modulo l à un nombre réel; donc (th. 6, Conséquence) I_r est un idéal principal.

2° Pour démontrer que $I_r(\zeta).I_r(\zeta^{-1})$ est congru à $a\varepsilon \pmod{l}$, (a rationnel, ε unité), il est inutile d'employer les logarithmes de Kummer; on a en effet

$$I_r(\zeta)\, I_r(\zeta^{-1}) \equiv \varepsilon_l'(\zeta)\, \varepsilon_l''(\zeta^{-1}) [I_l'(\zeta)\, I_l''(\zeta^{-1})]^l \pmod{l};$$

or $I_l'(\zeta)\, I_l''(\zeta^{-1})$ étant principal, sa $l^{\text{ième}}$ puissance est évidemment congrue à un rationnel. Tout le reste est inchangé.

Remarques finales. — La question de la génération effective du corps de classes, qui est une des principales questions qui se posent actuellement dans cette théorie, paraît être en rapport étroit avec les propriétés des unités d'un corps algébrique. Nous venons de voir ce qui se passait dans un cas particulier. Une partie de nos méthodes s'étend avec des hypothèses moins restrictives; mais les résultats ne sont plus aussi complets.

On peut s'étonner du rôle spécial joué par les unités E_ν. Remarquons qu'il est bien mis en évidence, par le fait que dans le cas étudié, les seuls surcorps abéliens non ramifiés de degré l par rapport à $k(\zeta)$, et galoisiens par rapport à k, sont précisément des corps $k(\zeta, \sqrt[l]{E_\nu})$.

Nous terminerons par une question, dont la solution nous paraîtrait avoir, à titre d'exemple, une très grande portée : le nombre de classes de $k(\zeta+\zeta^{-1})$ est donné par une expression dépendant des unités; y a-t-il un lien, et quel est-il, entre le groupe quotient de toutes les unités réelles positives par celui engendré par ε et ses conjugués, et les groupes des classes de $k(\zeta+\zeta^{-1})$; par exemple, ces deux groupes sont-ils isomorphes et les unités permettent-elles d'engendrer effectivement le corps de classes absolu de $k(\zeta+\zeta^{-1})$?

Le 16 février 1931.

M. Cl. Chevalley a bien voulu nous seconder pour la correction des épreuves du présent travail, — Mémoire posthume du regretté J. Herbrand. Nous tenons à le remercier ici très vivement.

(*La Rédaction.*)