

ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

DAVID HILBERT

G. HUMBERT

TH. GOT

Théorie des corps de nombres algébriques

Annales de la faculté des sciences de Toulouse 3^e série, tome 3 (1911), p. 1-62

http://www.numdam.org/item?id=AFST_1911_3_3_1_0

© Université Paul Sabatier, 1911, tous droits réservés.

L'accès aux archives de la revue « Annales de la faculté des sciences de Toulouse » (<http://picard.ups-tlse.fr/~annales/>) 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/*

ANNALES
DE LA
FACULTÉ DES SCIENCES
DE L'UNIVERSITÉ DE TOULOUSE.

THÉORIE
DES
CORPS DE NOMBRES ALGÉBRIQUES

MÉMOIRE de M. DAVID HILBERT,
Professeur à l'Université de Göttingen.

NOTES DE MM. G. HUMBERT ET TH. GOT.

NOTE I (ANNEXE AU § 5),

PAR G. HUMBERT⁽¹⁾.

Démonstration du lemme 2. (Théorème d'Hurwitz.)

Soient

$$\begin{aligned} F &= \alpha_0 x^m + \alpha_1 x^{m-1} + \dots + \alpha_m, \\ G &= \beta_0 x^n + \beta_1 x^{n-1} + \dots + \beta_n, \end{aligned}$$

deux polynômes en x , à coefficients entiers algébriques quelconques; soit

$$FG = \gamma_0 x^{m+n} + \gamma_1 x^{m+n-1} + \dots + \gamma_{m+n};$$

je dis que si un même entier algébrique ω divise tous les γ_i (c'est-à-dire si les $\gamma_i : \omega$, qui sont algébriques, sont aussi entiers), ω divise tous les produits $\alpha_i \beta_k$.

⁽¹⁾ Cette Note et les suivantes n'ont rien de personnel; elles ont été rédigées, après lecture des Ouvrages ou Mémoires classiques, à l'occasion d'un cours professé au Collège de France en 1910-1911.

En effet, fixons i et k ; on a, en désignant par x_h les racines de $F=0$, par y_h celles de $G=0$,

$$\pm \frac{\gamma_i}{\alpha_0} \cdot \frac{\beta_k}{\beta_0} = (\Sigma x_1 x_2 \dots x_i) (\Sigma y_1 y_2 \dots y_k).$$

Or, considérons l'équation $FG=0$; soient ξ_1, ξ_2, \dots ses racines, qui sont les x_h et les y_h ; partageons les ξ en deux groupes de toutes les manières possibles, l'un de m racines, l'autre de n ; soient ζ_h et η_h les racines de deux groupes d'un même système. La fonction $u = (\Sigma \zeta_1 \zeta_2 \dots \zeta_i) (\Sigma \eta_1 \eta_2 \dots \eta_k)$ est une fonction rationnelle *non symétrique* des racines ξ ; en prenant tous les groupements possibles des $m+n$ racines ξ en deux groupes de m et n respectivement, on obtient un certain nombre de fonctions u , dont l'une est $\pm \frac{\gamma_i}{\alpha_0} \cdot \frac{\beta_k}{\beta_0}$. D'ailleurs, toute fonction symétrique des u l'est des ξ ; donc, les u sont racines d'une équation algébrique dont les coefficients sont rationnels par rapport aux coefficients γ de $FG=0$. D'une manière plus précise, les coefficients en question sont des polynômes en $\gamma_1 : \gamma_0$ à coefficients entiers ordinaires : cela résulte de la proposition suivante facile à démontrer :

Soit une équation algébrique $x^n + a_1 x^{n-1} + \dots + a_n = 0$; considérons la fonction symétrique des racines $x_i : \Sigma x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$, les a_i entiers ordinaires non négatifs : elle s'exprime par un polynôme en a_1, a_2, \dots, a_n , dont le degré est le plus grand des a_i et dont les coefficients sont entiers ordinaires.

Soit donc

$$u^M + d_1 u^{M-1} + \dots + d_M = 0$$

l'équation en u ; on a

$$-d_1 = \Sigma u = \Sigma [(\Sigma \zeta_1 \zeta_2 \dots \zeta_i) (\Sigma \eta_1 \eta_2 \dots \eta_k)].$$

Le second membre est une fonction symétrique des ξ_i , où les ξ_i figurent tous au premier degré chacun; donc, d'après la proposition qui vient d'être énoncée, d_1 est un polynôme d'ordre un par rapport à l'ensemble des $\gamma_i : \gamma_0$. De même d_2 est d'ordre deux, d_3 est d'ordre trois, etc.

On peut donc écrire l'équation en u :

$$u^M + \frac{P_1}{\gamma_0} u^{M-1} + \frac{P_2}{\gamma_0} u^{M-2} + \dots + \frac{P_M}{\gamma_0^M} = 0,$$

P_i étant un polynôme entier à coefficients entiers ordinaires d'ordre i par rapport à $\gamma_0, \gamma_1, \gamma_2, \dots$, et *homogène*, puisque d_i était un polynôme d'ordre i en $\gamma_1 : \gamma_0, \gamma_2 : \gamma_0$, etc. D'ailleurs, $\alpha_i \beta_k : \alpha_0 \beta_0$ est l'un des u ; donc, en posant $\alpha_i \beta_k = v$ et observant que $\alpha_0 \beta_0 = \gamma_0$, on a pour v l'équation

$$\left(\frac{v}{\gamma_0} \right)^M + \frac{P_1}{\gamma_0} \left(\frac{v}{\gamma_0} \right)^{M-1} + \dots + \frac{P_M}{\gamma_0^M} = 0,$$

c'est-à-dire

$$v^M + P_1 v^{M-1} + P_2 v^{M-2} + \dots + P_M = 0.$$

Supposons maintenant que les γ_i soient tous divisibles par ω ; je dis que v l'est aussi, ou que $\frac{v}{\omega}$ est un entier algébrique. On écrit en effet

$$\left(\frac{v}{\omega}\right)^M + \frac{P_1}{\omega} \cdot \left(\frac{v}{\omega}\right)^{M-1} + \frac{P_2}{\omega^2} \cdot \left(\frac{v}{\omega}\right)^{M-2} + \dots + \frac{P_M}{\omega^M} = 0.$$

Or, d'après l'hypothèse $\frac{P_1}{\omega}, \frac{P_2}{\omega^2}, \dots$ sont des entiers algébriques, car P_i étant *homogène*, à coefficients entiers ordinaires, d'ordre i par rapport aux γ et ceux-ci divisibles par ω , $\frac{P_i}{\omega^i}$ est un polynôme entier à coefficients entiers ordinaires par rapport aux entiers algébriques $\frac{\gamma}{\omega}$; donc entier algébrique aussi, par un théorème connu. Donc, également d'après un théorème connu, $\frac{v}{\omega}$, racine d'une équation de premier coefficient 1 et à coefficients entiers algébriques, est entier algébrique; ou encore $\alpha_i \beta_k$ est divisible par ω , c'est-à-dire que le quotient $\alpha_i \beta_k : \omega$ est entier algébrique.

C. q. f. d.

NOTE II (ANNEXE AU § 5),

PAR G. HUMBERT.

Démonstration du théorème fondamental 8 par la méthode de Hurwitz mentionnée au paragraphe 6.

LEMME 1. — Soit α un nombre fractionnaire du corps de base $(\omega_1, \dots, \omega_m)$:

$$\alpha = m_1 \omega_1 + \dots + m_m \omega_m,$$

les m_i entiers ou fractionnaires ordinaires. Prenons successivement pour μ les quantités

$$\mu = 0, 1, \dots, K^m,$$

K entier ordinaire positif plus grand que 1; considérons les quantités $\mu \alpha$ et en particulier les parties entières et fractionnaires des μm_i , c'est-à-dire écrivons $\mu m_i = E_i + \varphi_i$, E_i entier positif, nul ou négatif et $0 \leq \varphi_i < 1$. On appellera E_i la partie entière, φ_i la partie fractionnaire de μm_i .

Si on divise l'intervalle $0 - 1$ en K parties égales, d'amplitude $\frac{1}{K}$ (avec la conven-

tion que α appartient au premier intervalle partiel, $\frac{1}{K}$ au second, et ainsi de suite), chacune des m parties fractionnaires tombe dans l'une de ces K parties égales; or, on peut répartir *a priori* m quantités dont l'ordre est donné, dans K intervalles, de K^m manières différentes (évident en passant de m à $m+1$). D'autre part, en faisant varier μ , ($\mu=0, 1, \dots, K^m$), on a K^m+1 systèmes de m parties fractionnaires à répartir successivement dans les K intervalles. Comme K^m+1 est plus grand que K^m , les K^m+1 répartitions ne seront pas toutes distinctes, c'est-à-dire que deux *au moins* d'entre elles seront identiques.

Soient μ' et μ'' les valeurs correspondantes de μ ($\mu'' > \mu'$); les parties fractionnaires de $\mu'm_1, \mu''m_1$ tombent dans un même intervalle de $\frac{1}{K}$; de même celles de $\mu'm_2, \mu''m_2$, etc. On a ainsi

$$\mu''m_i = e_i'' + \varphi_i'', \quad \mu'm_i = e_i' + \varphi_i', \quad (i = 1, 2, \dots, m);$$

φ_i'' et $\varphi_i' \geq 0$ et compris dans le même intervalle de $\frac{1}{K}$; $|\varphi_i'' - \varphi_i'|$ est donc sûrement $< \frac{1}{K}$.

Si donc on pose $\mu = \mu'' - \mu'$ (μ est *positif et non nul*, puisque $\mu'' > \mu'$), on aura

$$\mu m_i = e_i'' - e_i' + \varphi_i'' - \varphi_i',$$

c'est-à-dire

$$\mu m_i = E_i + \varphi_i,$$

E_i entier positif, nul ou négatif et φ_i positif, nul ou négatif, mais inférieur à $\frac{1}{K}$ en valeur absolue.

Par suite, étant données m quantités m_1, m_2, \dots, m_m , on peut trouver dans la série $1, 2, \dots, K^m$ un entier μ (non nul) tel que, pour $i = 1, 2, \dots, m$, on ait

$$\mu m_i = E_i + \varphi_i; \quad E_i \text{ entier et } |\varphi_i| < \frac{1}{K}.$$

LEMME 2. — L'entier μ étant ainsi déterminé, on a

$$\begin{aligned} \mu \alpha &= \mu m_1 \omega_1 + \mu m_2 \omega_2 + \dots \\ &= (E_1 + \varphi_1) \omega_1 + (E_2 + \varphi_2) \omega_2 + \dots \end{aligned}$$

E_i entier ordinaire, φ_i fractionnaire, $|\varphi_i| < \frac{1}{K}$, ou

$$\mu \alpha = (E_1 \omega_1 + E_2 \omega_2 + \dots) + \varphi_1 \omega_1 + \varphi_2 \omega_2 + \dots$$

Il résulte de là que

$$|\mu \alpha - E_1 \omega_1 - E_2 \omega_2 - \dots| \leq |\varphi_1| \cdot |\omega_1| + |\varphi_2| \cdot |\omega_2| + \dots;$$

donc, si Ω est le maximum du module des ω (c'est-à-dire le plus grand des $|\omega_i|$), on a

$$|\mu \alpha - A| < \frac{m \Omega}{K},$$

μ étant un entier du corps ω . Passant aux conjugués, on a de même, pour le même μ :

$$|\mu \alpha' - A'| < \frac{m \Omega'}{K}.$$

.

On a le même μ parce que ce μ ne dépend que de m_1, m_2, \dots, m_m , qui restent les mêmes quand on passe de α à ses conjugués α', α'', \dots ; de même A' est le conjugué de A , parce que les E_i ne dépendent que des m_i . Maintenant observons que si β est un nombre d'un corps ω , sa norme est $\beta \beta' \beta'' \dots$; si l'équation en ω a des racines imaginaires, elles sont deux à deux imaginaires conjuguées et il en est de même pour les β correspondants, de sorte qu'on a dans tous les cas

$$|\text{Norme } \beta| = |\beta| \cdot |\beta'| \dots$$

Donc, en multipliant membre à membre les inégalités ci-dessus, on a

$$|\text{Norme } (\mu \alpha - A)| < \frac{m^m \Omega \Omega' \dots}{K^m} < \frac{C^m}{K^m},$$

C étant un entier fixe qui ne dépend que du corps et non du nombre α .

Prenons $K = C$; il en résulte le lemme suivant :

Etant donné dans un corps d'ordre m un nombre entier ou fractionnaire α , on peut trouver un entier ordinaire μ positif, au plus égal à C^m , (C étant un entier positif ne dépendant que du corps) et un entier A du corps tels que

$$|\text{Norme } (\mu \alpha - A)| < 1.$$

COROLLAIRE. — Soit I un idéal quelconque, α un de ses entiers autre que 0 et de norme minimum en valeur absolue (autre que 0 nécessairement, car la norme étant $\alpha \alpha' \dots$ ne peut être nulle qui si un des α , donc évidemment tous, sont nuls). Soit α_i un autre entier de I ; appliquons le lemme 2 au nombre du corps $\frac{\alpha_i}{\alpha}$. On aura, pour μ entier ordinaire positif et $\leq C^m$,

$$|\text{Norme } (\mu \frac{\alpha_i}{\alpha} - \beta)| < 1,$$

β entier du corps, d'où

$$|\text{Norme } (\mu \alpha_i - \beta \alpha)| < |\text{Norme } \alpha|.$$

Mais $|\text{Norme } \alpha|$ étant en valeur absolue la norme minimum autre que 0 dans l'idéal et $\mu \alpha_i - \beta \alpha$ étant un entier de l'idéal, puisque α_i et α en sont et que μ et β sont entiers du corps, on a nécessairement

$$\text{Norme } (\mu \alpha_i - \beta \alpha) = 0,$$

d'où

$$\mu \alpha_i = \beta \alpha$$

par une remarque qu'on vient de faire.

Donc μz_i est divisible par z ; *a fortiori*, puisque μ est un des entiers $1, 2, \dots, C^m$, il en sera de même de $C^m! z_i$.

Posant $C^m! = M$, on voit que, z_i étant un entier quelconque d'un idéal I , Mz_i est divisible par z , ou encore que tous les entiers de l'idéal MI sont divisibles par z , ce qui entraîne

$$(M)I = (z)J,$$

J étant un idéal.

Je dis que J contient M . En effet, $(M)I = (z)J$ montre que le produit d'un nombre de I par M , divisé ensuite par z , est un nombre de J ; or, z étant de I , l'entier $\frac{z \cdot M}{z} = M$ est de J .

Si donc on dit que deux idéaux I et J sont *équivalents* lorsqu'il existe deux entiers du corps λ et μ tels que $(\lambda)I = (\mu)J$, on peut dire que

Tout idéal équivaut à un idéal qui contient un nombre fixe M dépendant seulement du corps.

REMARQUE. — *Deux idéaux équivalents à un troisième le sont entre eux.* Car si

$$(z)I = (\beta)K,$$

$$(z_i)I_i = (\beta_i)K,$$

on en conclut

$$(\beta)(\beta_i)K = (z\beta_i)I = (z_i\beta_i)I_i.$$

THÉORÈME. — *Si on range dans une même classe les idéaux équivalents, le nombre des classes d'idéaux est fini.*

Car tout idéal équivaut à un idéal contenant M , donc contenant (M) . Or, un idéal donné, ici (M) , n'est contenu que dans un nombre limité d'idéaux (lemme 1 du paragraphe 4); donc le nombre des classes d'idéaux est fini.

THÉORÈME. — *Une puissance convenable d'un idéal quelconque I est un idéal principal.*

Formons, en effet, I, I^2, I^3, \dots en nombre illimité; il faut, par le théorème précédent, que deux de ces idéaux soient équivalents, c'est-à-dire

$$(z)I^r = (\beta)I^{r+s} = (\beta)I^r \cdot I^s.$$

On n'a pas le droit de diviser par I^r , parce qu'on ne suppose pas établi le théorème fondamental qu'on peut trouver, pour tout idéal I , un autre idéal J tel que IJ soit principal. Mais on sait que si un idéal quelconque $J = KL$, tout nombre de J appartient à K , car si ρ_1, ρ_2, \dots sont les nombres de K et $\sigma_1, \sigma_2, \dots$ ceux de L , ceux de KL sont $\sum \lambda \rho_i \sigma_k$, et ce sont évidemment des nombres de K ; ainsi tout nombre de $KL = J$ est de K .

Soient $\alpha_1, \dots, \alpha_m$ et β_1, \dots, β_m des bases de I^r et I^s ; il résulte de la relation précédente que $\alpha \alpha_i$ est divisible par β et que le quotient est un nombre de $I^r \cdot I^s$, donc de I^r ; c'est-à-dire $\frac{\alpha}{\beta} \alpha_i = \lambda_i \alpha_i + \mu_i \alpha_i + \dots$, les λ_i, μ_i , etc., entiers ordinaires. On a ainsi, pour $i = 1, 2, \dots, m$, m relations linéaires et homogènes entre les α_i . Eliminant ces quantités, on a

$$\begin{vmatrix} \lambda_1 - \frac{\alpha}{\beta}, \mu_1, \dots, \\ \lambda_2, \mu_2 - \frac{\alpha}{\beta}, \dots, \\ \dots \dots \dots \dots \end{vmatrix} = 0,$$

équation à coefficients entiers ordinaires en $\frac{\alpha}{\beta}$, d'ordre m , de premier coefficient ± 1 .

Donc $\frac{\alpha}{\beta}$ est un entier (du corps), soit γ , et l'on peut écrire

$$(\gamma) I^r = I^r \cdot I^s.$$

Les nombres $\alpha_1 \beta_1, \alpha_2 \beta_1, \dots, \alpha_m \beta_1$ sont des nombres de $I^r I^s$ (car les α_i sont une base de I^r , les β_i de I^s); donc, divisés par γ , ce sont des nombres de I^r , c'est-à-dire que

$$\alpha_i \frac{\beta_i}{\gamma} = \lambda_i \alpha_i + \mu_i \alpha_i + \dots, \quad (i = 1, 2, \dots, m)$$

d'où on conclut encore que $\frac{\beta_1}{\gamma}, \dots, \frac{\beta_m}{\gamma}$, sont entiers du corps.

Donc $I^s = (\gamma) J$, J étant un nouvel idéal, et $(\gamma) I^r = I^r I^s$ donne $(\gamma) I^r = (\gamma) I^r J$, c'est-à-dire évidemment

$$I^r = I^r J$$

(car ici on peut manifestement diviser par l'idéal *principal* (γ)).

Si δ_1, δ_2 , etc., est une base de J , la relation $I^r = I^r J$ montre que α_i est un nombre de $I^r J$; or, un nombre de I^r étant $x_1 \alpha_1 + x_2 \alpha_2 + \dots$, un de J étant $y_1 \delta_1 + y_2 \delta_2 + \dots$, un nombre de $I^r J$ est manifestement du type $\sum \Theta_{j,k} \alpha_j \delta_k$, les $\Theta_{j,k}$ étant entiers du corps.

On a ainsi :

$$\begin{aligned} \alpha_1 &= x_1 \sum \lambda_i \delta_i + x_2 \sum \mu_i \delta_i + \dots + x_m \sum \rho_i \delta_i, \\ \alpha_2 &= x_1 \sum \lambda'_i \delta_i + x_2 \sum \mu'_i \delta_i + \dots + x_m \sum \rho'_i \delta_i, \\ &\dots \dots \dots \dots \dots \dots \dots \end{aligned}$$

les $\lambda_i, \mu_i, \dots, \lambda'_i, \mu'_i$, etc., étant entiers du corps. Eliminant les α_i entre ces m relations linéaires et homogènes, il vient

$$\begin{vmatrix} -1 + \sum \lambda_i \delta_i, & \sum \mu_i \delta_i, \dots, \\ \sum \lambda'_i \delta_i, & -1 + \sum \mu'_i \delta_i, \dots, \\ \dots \dots \dots \dots \dots \dots \dots \end{vmatrix} = 0;$$

d'où ± 1 = polynôme entier par rapport aux δ_i à coefficients entiers du corps, *sans terme indépendant*. Or, les δ_i étant des entiers de J , il en est de même de tout polynôme en δ_i à coefficients entiers quelconques du corps et *sans terme indépendant*, d'après la définition même d'un idéal; donc ± 1 est de J , c'est-à-dire 1 est de J et $J = 1$. L'égalité $I^s = (\gamma)J$ donne donc

$$I^s = (\gamma).$$

C. q. f. d.

THÉORÈME. — *Cela s'écrit $I \cdot I^{s-1} = (\gamma)$, c'est-à-dire que tout idéal multiplié par un autre idéal convenable donne un idéal principal.*

C'est le théorème FONDAMENTAL d'où se déduit la décomposition unique en idéaux premiers, comme on l'a vu au paragraphe 5.

NOTE III (ANNEXE AU § 17),

PAR G. HUMBERT.

Démonstration des inégalités fondamentales de Minkowski pour n formes linéaires à n variables.

Il existe trois démonstrations différentes du théorème de Minkowski, énoncé dans le paragraphe 17 sous les deux formes équivalentes des lemmes 6 et 7 : la première, celle de Minkowski, se trouve dans la *Geometrie der Zahlen*; une autre, de M. Hilbert, a été reprise par Minkowski dans ses *Diophantische Approximationen*; on la trouvera aussi dans les *Vorlesungen über Zahlentheorie*, de M. Sommer, traduction française de M. A. Lévy; une troisième a été donnée par M. Hurwitz dans les *Göttinger Nachrichten*, Math.-phys. kl. 1897 : c'est celle qui va être exposée.

Les raisonnements restant les mêmes quel que soit le nombre des variables, on le supposera, pour fixer les idées, égal à trois.

Soient les trois formes linéaires

$$f_i = a_i x + b_i y + c_i z$$

de déterminant Δ . En divisant les a_i , b_i , c_i par $\sqrt[3]{|\Delta|}$, on ramène le déterminant à ± 1 ; si c'est -1 , on changera les signes de a_i , b_i , c_i , et on aura, dans tous les cas,

trois formes f'_i de déterminant ± 1 . Dire qu'on peut donner à x, y, z des valeurs entières non toutes nulles, telles que l'on ait

$$|f'_i| \leq 1$$

revient donc à dire que, pour ces valeurs, on a

$$|f_i| \leq \sqrt[3]{\Delta}$$

($\sqrt[n]{\Delta}$ dans le cas de n formes à n variables).

C'est sous cette dernière forme que M. Hurwitz établit la proposition.

Sa démonstration se divise en quatre parties.

PREMIÈRE PARTIE. — On supposera d'abord les coefficients des f_i entiers.

Réduction du système des f_i . — On opérera sur x, y, z une suite de substitutions à coefficients entiers de déterminant ± 1 , de manière à simplifier les f_i .

Soit $f_i = a_i x + b_i y + c_i z$; si c_i est le plus petit (non nul) en valeur absolue des coefficients a_i, b_i, c_i , on peut faire en sorte que le coefficient de x soit, en valeur absolue, inférieur ou au plus égal à $|c_i|$: il suffit d'opérer la substitution $(z; z + \lambda x)$, λ entier; le coefficient de x devient $a_i + \lambda c_i$ et peut, dès lors, par choix de λ , être > 0 et $\leq |c_i|$; ceux de y et de z n'ont pas varié. Si $|a_i| < |b_i|$ et $|c_i|$, on changera, s'il y a lieu, x en $-x$. On peut donc supposer le coefficient de x positif et non nul, inférieur en valeur absolue à ceux de y et z .

Faisons maintenant la substitution $(x, x + \lambda y)$: nous pouvons rendre le coefficient de y positif ou nul et $< |a_i|$; puis, par $(y, y + \lambda x)$, diminuer de nouveau celui de x en le laissant toujours positif et non nul; puis, par $(x, x + \lambda y)$, diminuer de nouveau celui de y en le laissant positif ou nul, etc. On arrive ainsi à annuler le coefficient de y et de même celui de z .

f_i se réduit ainsi à Ax , A entier et positif. Opérant de même sur f_2 et f_3 , on peut, par des substitutions opérées successivement sur y et z , faire disparaître le terme en z , en sorte que $f_3 = b'x + By$, $B > 0$. Faisant $(y, y + \lambda x)$, on a

$$f_3 = b'x + By, \quad \text{avec } 0 \leq b < B, \quad B > 0.$$

Et alors $f_3 = c'x + c''y + Cz$, où C est $\neq 0$, à cause du déterminant qui est resté le même et est ABC . Par $(z, z + \lambda x)$ et $(z, z + \mu y)$, on peut faire en sorte que l'on ait $0 \leq c' < |C|$, $0 \leq c'' < |C|$.

Finalement, le système est

$$\begin{aligned} f_1 &= Ax, & A > 0, \\ f_2 &= bx + By, & B > 0, \quad 0 \leq b < B, \\ f_3 &= c_1 x + c_2 y + Cz, & 0 \leq (c_1, c_2) < |C|. \end{aligned}$$

Et les substitutions opérées étant de déterminant ± 1 , les anciennes variables sont entières en même temps que les nouvelles et réciproquement.

Pour établir le théorème de Minkowski dans le cas où les f_i ont leurs coefficients entiers, il suffira donc de l'établir pour le système réduit. On peut le faire directement, mais c'est compliqué à cause des cas et sous-cas à distinguer. Mieux vaut raisonner autrement.

DEUXIÈME PARTIE. — Disons que deux formes linéaires et homogènes en x, y, z à coefficients entiers sont *équivalentes* ou *congrues* (modd f_i) si leur différence est du type $\lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3$, les λ entiers.

Si φ est une telle forme, les $\varphi + \lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3$, sont donc congrues à φ (modd f_i).

Soit $\psi = \varphi + \lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3$, φ étant donnée; on peut choisir les λ_i de manière que, dans ψ (on dira que ψ est réduite) :

1° Le coefficient de z (qui est celui de z dans φ , augmenté de $C\lambda_3$), soit compris entre 0 inclus et $|C|$ exclus;

2° λ_3 étant ainsi déterminé, on peut choisir λ_2 ; de manière que le coefficient de y soit entre 0 inclus et B exclus;

3° Choisir λ_1 , de manière que le coefficient de x soit entre 0 inclus et A exclus.

Alors les formes ψ réduites sont au nombre de $|C|BA$ distinctes. $|C|BA$ est Δ , déterminant des f_i , et, d'après le calcul précédent, toute forme équivaut (modd f_i) à une et une seule réduite. Donc il y a $|\Delta|$ formes et $|\Delta|$ seulement non congrues deux à deux, modd f_i ; parmi elles, celle dont les trois coefficients sont nuls.

Ce résultat obtenu par la réduction des f_i est évidemment vrai pour des f_i non réduites, puisque deux formes congrues (modd f_i) le restent si on opère sur les x, y, z une substitution de déterminant ± 1 .

Reprendons alors les f_i initiales. Le théorème du nombre des classes de formes linéaires modd f_i s'applique dès lors aux formes de déterminant Δ :

$$F_1 = a_1 x + a_2 y + a_3 z,$$

$$F_2 = b_1 x + b_2 y + b_3 z,$$

$$F_3 = c_1 x + c_2 y + c_3 z.$$

Soient r^3 et $(r+1)^3$ les cubes positifs d'entiers consécutifs qui comprennent $|\Delta|$, de sorte que $r^3 \leq |\Delta| < (r+1)^3$; considérons les formes $\varphi = l_1 x + l_2 y + l_3 z$, où l'on a $0 \leq (l_1, l_2, l_3) \leq r$. Elles sont $(r+1)^3$, y compris la forme nulle. Comme $(r+1)^3 > |\Delta|$, deux des φ sont congrues entre elles modd F_i , leur différence est donc $\lambda_1 F_1 + \lambda_2 F_2 + \lambda_3 F_3$, les λ n'étant pas nuls à la fois, car les deux φ sont distinctes. On a donc pour des valeurs des l_i entières non nulles à la fois, — car les deux φ sont distinctes, — et comprises entre $-r$ et $+r$ inclus :

$$\lambda_1(a_1 x + a_2 y + a_3 z) + \lambda_2(b_1 x + \dots) + \lambda_3(c_1 x + \dots) = l_1 x + l_2 y + l_3 z,$$

d'où

$$\begin{aligned} a_1\lambda_1 + b_1\lambda_2 + c_1\lambda_3 &= l_1, \\ a_2\lambda_1 + b_2\lambda_2 + c_2\lambda_3 &= l_2, \\ a_3\lambda_1 + b_3\lambda_2 + c_3\lambda_3 &= l_3, \end{aligned}$$

les $|l_i|$ étant $\ll r$, c'est-à-dire $\ll |\Delta|^{\frac{1}{3}}$ et les λ_i non nuls à la fois. Le théorème de Minkowski est donc démontré pour des f_i à coefficients entiers.

TROISIÈME PARTIE. — Il est vrai pour des f_i à coefficients fractionnaires, car si S est le dénominateur commun des coefficients, posons $f_i = \frac{F_i}{S}$, le déterminant des F_i est $S^3\Delta$. Le théorème étant vrai pour les F_i (dont les coefficients sont entiers), on peut trouver x, y, z entiers de telle sorte que $|F_i| \leq S|\Delta|^{\frac{1}{3}}$; donc, pour ces valeurs de x, y, z , on a $|f_i| \leq |\Delta|^{\frac{1}{3}}$. C. q. f. d.

QUATRIÈME PARTIE. — Soient les f_i à coefficients quelconques et de déterminant + 1. Nous allons obtenir la démonstration en suivant maintenant un procédé d'Hilbert, qui consiste à comparer les formes f_i à des formes φ_i à coefficients rationnels, suffisamment voisins des premiers. [Voir, par exemple, Sommer.] Soient

$$f_i = a_i x + b_i y + c_i z, \quad (i = 1, 2, 3).$$

Je dis qu'étant donné un nombre positif δ aussi petit que l'on voudra, il est possible de trouver un nombre ε positif et inférieur à δ , tel que, en faisant varier tous les coefficients, sauf un, de quantités inférieures ou égales à ε en valeur absolue, on n'aura à faire varier le dernier en valeur absolue que de moins de δ pour que le déterminant des formes reste égal à + 1.

En effet, ce déterminant n'étant pas nul, l'un au moins de ses mineurs d'ordre deux n'est pas nul, soit, par exemple, $a_1 b_2 - a_2 b_1 \neq 0$. Soient $\alpha_i, \beta_i, \gamma_i$ les quantités dont nous faisons varier a_i, b_i, c_i . En écrivant que le déterminant reste égal à 1, on a

$$\gamma_3 [(a_1 + \alpha_1)(b_2 + \beta_2) - (a_2 + \alpha_2)(b_1 + \beta_1)] = \Sigma \alpha_i A_i,$$

le second membre contenant toutes les variations $\alpha_i, \beta_i, \gamma_i$, sauf γ_3 et les A_i, B_i, C_i dépendant des a_i, b_i, c_i et de leurs variations (sauf toujours γ_3). Il est clair qu'en prenant pour la plus grande valeur absolue de ces variations (sauf γ_3) un nombre ε suffisamment petit, on aura $|\gamma_3| < \varepsilon K$, K étant un nombre positif ne dépendant que des a_i, b_i, c_i . Ecrivant $\varepsilon K < \delta$, c'est-à-dire $\varepsilon < \frac{\delta}{K}$, on voit que les variations (sauf γ_3) restant inférieures à ε , $|\gamma_3|$ restera inférieur à δ , et on peut supposer $\varepsilon < \delta$, parce que si $\frac{\varepsilon}{K} > \delta$, on ne prendra que les valeurs de ε inférieures à δ , lesquelles conviennent *a fortiori*.

Faisons de plus les modifications de manière à rendre rationnels tous les coefficients, sauf c_3 , et modifions c_3 de manière que le déterminant reste $+1 : c_3$ deviendra rationnel par le fait même que les autres coefficients le sont, ainsi que le déterminant. On aura alors trois formes $\varphi_1, \varphi_2, \varphi_3$, dont les coefficients diffèrent de moins de δ de ceux des f_1, f_2, f_3 , et telles, d'après la troisième partie, que pour des valeurs des x, y, z , non nulles à la fois, on ait $|\varphi_i| \leq 1$, ($i = 1, 2, 3$).

Observons maintenant que les systèmes de valeurs entières des x, y, z , qui peuvent rendre les $|f_i| \leq 1$, sont en nombre limité. Car si l'on pose $f_i = w_i$, ($i = 1, 2, 3$), les w_i étant compris entre -1 et $+1$, et si on résout ce système en x, y, z , on trouve des fonctions linéaires et homogènes des w_i dont les coefficients dépendent des a_i, b_i, c_i . Donc, les $|w_i| \leq 1$, les x, y, z sont en valeur absolue inférieurs ou égaux à une limite finie G : les systèmes des x, y, z entiers sont donc en nombre limité.

De même si les φ_i se déduisent des f_i par des variations des coefficients inférieures à δ (le déterminant étant $+1$, comme celui des f_i), on trouve que les systèmes des x, y, z entiers, rendant les $|\varphi_i| \leq 1$, sont tels que les x, y, z soient en valeur absolue inférieurs ou égaux à une limite G' voisine de G .

Considérons les f_i et tous les systèmes de trois formes de déterminant $+1$ qui s'en déduisent par des variations des coefficients inférieures en valeur absolue à δ , et soit G_0 un nombre tel que les x, y, z , qui peuvent rendre un quelconque de ces systèmes ≤ 1 en valeur absolue, soient inférieurs à G_0 en valeur absolue.

Je dis que parmi les systèmes des x, y, z entiers, tels que $(x, y, z) \leq G_0$, il en est pour lesquels les $|f_i|$ sont ≤ 1 .

Supposons qu'il n'y en ait aucun, c'est-à-dire que pour chaque système considéré il y ait au moins une f_K telle que $|f_K| = 1 + \lambda$, ($\lambda > 0$), K pouvant varier ($K = 1, 2, 3$) d'un système à l'autre. Soit λ_0 le plus petit des λ .

La différence entre f_i et φ_i pour un même système de valeurs des variables considérées (c'est-à-dire inférieures ou égales à G_0 en valeur absolue) est inférieure en valeur absolue à $3\delta G_0$; si donc on choisit δ de telle sorte que $3\delta G_0 < \lambda_0$, la valeur de φ_K différera de celle de f_K de moins de λ_0 , et comme $|f_K| = 1 + \lambda \geq 1 + \lambda_0$, $|\varphi_K|$ sera > 1 .

Donc, si, pour chacun des systèmes x_i considérés, un au moins des $|f_i|$ est > 1 , on pourra choisir δ de manière que l'un des $|\varphi_i|$ soit également > 1 : c'est en contradiction avec ce qui précède, car on a vu qu'on pouvait faire varier les coefficients des f_i de moins de δ de telle façon que, pour un système de x, y, z au moins, les $|\varphi_i|$ soient ≤ 1 . Donc, il faut conclure que, pour un système x_i , au moins les trois f_i sont ≤ 1 .

C. q. f. d.

NOTE IV (ANNEXE AU § 59),

PAR G. HUMBERT.

Questions diverses concernant les bases des idéaux d'un corps quadratique.

En raison des fréquentes applications des corps quadratiques, il ne paraîtra pas inutile de rappeler ici les principaux résultats classiques relatifs aux bases des idéaux de ces corps. C'est d'ailleurs une occasion de montrer, dans un cas particulier, la façon d'utiliser les principes généraux du paragraphe 4.

THÉORÈME. — Un idéal quelconque du corps $k(\sqrt{m})$ est un module de ce corps, *déduit de deux nombres fondamentaux*, c'est-à-dire que l'on peut trouver deux entiers du corps e_1 et e_2 , tels que tout nombre de l'idéal soit du type $l_1 e_1 + l_2 e_2$, l_1 et l_2 étant des entiers ordinaires et *réciproquement*.

En effet, soient $a + b\omega$, $a_1 + b_1\omega$ deux entiers de l'idéal I ⁽¹⁾; l'entier $x(a + b\omega) + y(a_1 + b_1\omega)$, où x et y sont entiers ordinaires, appartient à I . On peut déterminer x et y de manière que $bx + b_1y$ soit le plus grand commun diviseur de b et b_1 , soit b' .

Si $a_2 + b_2\omega$ est un autre nombre de I , il y a de même dans I un nombre où le coefficient de ω est le plus grand diviseur de b' et de b_2 , et ainsi de suite.

On arrive ainsi à un nombre $A + h\omega$, où h est le plus grand commun diviseur (positif si l'on veut, car $-A - h\omega$ appartient aussi à I , comme produit d'un nombre de I par -1) de tous les nombres b, b_1, b_2, \dots .

Maintenant $\frac{b}{h}, \frac{b'}{h}, \dots$, étant entiers, les nombres tels que $a + b\omega - \frac{b}{h}(A + h\omega)$, c'est-à-dire $a - \frac{b}{h}A$, qui sont entiers ordinaires (puisque $\frac{b}{h}$ l'est), appartiennent à I .

I renferme donc les entiers ordinaires en nombre infini : $a - \frac{b}{h}A; a_1 - \frac{b_1}{h}A; \dots$.

(Que I renferme un nombre infini d'entiers ordinaires, c'est évident, car si α est de I , son conjugué α' appartenant au corps, le produit $\alpha'\alpha$, qui est entier ordinaire, est de I .)

Soit q le plus grand commun diviseur positif des nombres entiers ordinaires ci-dessus : $a - \frac{b}{h}A$, etc., de I : il est clair que q appartient à I .

(1) On désigne par ω , selon la notation du paragraphe 59, un nombre qui forme avec 1 une base du corps $k(\sqrt{m})$.

Alors un nombre quelconque $a + b\omega$ de \mathbf{I} s'écrit :

$$\begin{aligned} a + b\omega &= \frac{b}{h}(\mathbf{A} + h\omega) + \frac{a - \frac{b}{h}\mathbf{A}}{q} \cdot q, \\ &= x(\mathbf{A} + h\omega) + y \cdot q, \end{aligned}$$

x et y étant des entiers ordinaires, puisque h est le plus grand commun diviseur des b et q celui des $a - \frac{b}{h}\mathbf{A}$.

Réiproquement, tout nombre $x(\mathbf{A} + h\omega) + y \cdot q$, où x, y sont entiers ordinaires, appartient à \mathbf{I} ; car q et $\mathbf{A} + h\omega$ lui appartiennent.

Donc, \mathbf{I} est le *module* de *base* $\mathbf{A} + h\omega$ et q .

On peut simplifier en prenant pour base q et $\mathbf{A} + h\omega + \theta q$ (θ étant un entier ordinaire quelconque), et choisissant θ de manière que l'on ait

$$0 \leqslant \mathbf{A} + \theta q < q.$$

On a ainsi la base q et $g + h\omega$, où q et h sont positifs (*non nuls, comme plus grands communs diviseurs d'entiers ordinaires*) et où l'on a

$$0 \leqslant g < q.$$

RÉCIPROQUE. — Le module de base q et $g + h\omega$ est-il un idéal?

Pour cela, il faut et il suffit que

$$q(x + y\omega) + (g + h\omega)(z + t\omega),$$

où x, y, z, t sont entiers ordinaires quelconques, appartenne au module. Comme la somme de deux nombres du module lui appartient aussi, il faut et il suffit que $q, q\omega, g + h\omega, \omega(g + h\omega)$ appartiennent au module; q et $g + h\omega$ lui appartiennent. Pour que $q\omega$ lui appartenne aussi, il faut

$$q\omega = xq + y(g + h\omega);$$

d'où

$$q = yh, \quad 0 = xq + yg.$$

Donc : 1° h divise q ; $q = hq_i$, et, par suite, $y = q_i$; et $xq = -yg$ donne alors $xhq_i = -q_i g$ ou $xh = -g$; d'où, 2° h divise g ; $g = hg_i$.

Enfin, pour que $\omega(g + h\omega)$ appartenne au module, il faut

$$\omega(g + h\omega) = xq + y(g + h\omega).$$

ce qui, en distinguant $m \equiv 1$ et $m \equiv 1 \pmod{4}$, donne

$$1^{\circ} \quad m \equiv 1, \quad \omega^2 = m;$$

d'où

$$g = hy, \quad hm = xq + yg;$$

h divisant g , y est un entier g_i ; ensuite $hm = xhq_i + g_i^2h$ montre que $\frac{m-g_i^2}{q_i}$ doit être entier.

$$2^o \quad m \equiv 1, \quad \omega^2 - \omega = \frac{m-1}{4};$$

d'où

$$\omega g + h \left(\omega + \frac{m-1}{4} \right) = xq + y(g + h\omega),$$

et

$$g + h = hy, \quad h \frac{m-1}{4} = xq + yg,$$

c'est-à-dire, puisque $g = hg_i$:

$$g_i + 1 = y, \quad h \cdot \frac{m-1}{4} = xhq_i + hg_i(g_i + 1),$$

et donc

$$\frac{1}{q_i} \left[\frac{m-1}{4} - g_i(g_i + 1) \right]$$

doit être entier.

Donc, pour que le module de base q , $g + h\omega$, soit un idéal, il faut et il suffit que $q = hq_i$; $g = hg_i$ et que

$$\text{si } m \equiv 1 \pmod{4}, \quad g_i^2 - m \text{ soit multiple de } q_i,$$

$$\text{si } m \equiv 1 \pmod{4}, \quad g_i^2 + g_i - \frac{m-1}{4} \text{ soit multiple de } q_i.$$

Dans tous les cas, m est résidu quadratique de q (et même de $4q_i$, si m est $\equiv 1 \pmod{4}$).

L'idéal $(q, g + h\omega)$ ou $(q_i h, g_i h + h\omega)$ a tous ses nombres divisibles par h ; il s'écrit évidemment

$$(q, g + h\omega) = (h)(q_i, g_i + \omega),$$

c'est-à-dire est le produit de l'idéal principal (h) par l'idéal $(q_i, g_i + \omega)$, dont les nombres ne sont plus divisibles évidemment par un même entier ORDINAIRE.

Ce dernier idéal sera dit *idéal NORMAL*.

BASE CANONIQUE. — Une base de l'idéal I : $q, g + h\omega$ où q et g sont divisibles par h , où q, h sont > 0 et où g est ≥ 0 et $< q$, est dite *base canonique* de cet idéal.

Il n'y a qu'une base canonique.

Car si $q', g' + h'\omega$ en est une autre, on a d'abord $h' = h$, car, d'après ce qui précède, h est le plus grand diviseur commun entier ordinaire de tous les nombres de l'idéal, et de même h' .

Ensuite, tous les entiers ordinaires de I sont q et les multiples entiers ordinaires

de q (par $qx + (g + h\omega)y$), de même ce sont q' et ses multiples; donc $q' = q$, puisque q et q' sont positifs. Enfin, $g' + h\omega$ étant de I, on a : $g' + h\omega = qx + y(g + h\omega)$, d'où $y = 1$, c'est-à-dire $g' = qx + g$, et comme on a

$$0 \leq g' < q \quad \text{et} \quad 0 \leq g < q,$$

il faut $x = 0$ et $g' = g$.

C. q. f. d.

Mais il y a une infinité de *bases non canoniques*, c'est-à-dire de couples $\alpha + \beta\omega$, $\alpha' + \beta'\omega$, tels que tout entier de I soit $x(\alpha + \beta\omega) + y(\alpha' + \beta'\omega)$ avec x, y , entiers ordinaires.

Il suffit en effet de prendre

$$\begin{aligned} \alpha + \beta\omega &= x_1 q + y_1(g + h\omega), \\ \alpha' + \beta'\omega &= x_2 q + y_2(g + h\omega), \end{aligned}$$

x_1, y_1, x_2, y_2 entiers ordinaires tels que l'on ait

$$x_1 y_2 - x_2 y_1 = \pm 1.$$

Alors, q et $g + h\omega$ sont de la forme

$$n(\alpha + \beta\omega) + n'(\alpha' + \beta'\omega),$$

n et n' entiers ordinaires, et tout entier de I étant $q\xi + (g + h\omega)\eta$, ξ et η entiers ordinaires, la proposition est établie. La réciproque est évidente, toute base s'obtient ainsi.

PROBLÈME. — Le module de base $\alpha + \beta\omega$, $\alpha' + \beta'\omega$ est-il un idéal?

Il faut chercher dans ce module une base canonique et voir si elle satisfait aux relations voulues pour être base d'idéal. *On va prouver qu'un module a une base canonique et une seule.*

D'abord $\alpha\beta' - \beta\alpha'$ ne peut être nul. Car soit δ le plus grand commun diviseur des entiers ordinaires α et β , δ' celui de α' et β' , on a

$$\alpha + \beta\omega = \delta(a + b\omega), \quad \alpha' + \beta'\omega = \delta'(a' + b'\omega),$$

et on a

$$ab' - ba' = 0, \quad \text{si} \quad \alpha\beta' - \beta\alpha' = 0.$$

On en conclut, a et b étant premiers entre eux ainsi que a' et b' :

$$a' = \varepsilon a, \quad b' = \varepsilon b, \quad \varepsilon = \pm 1.$$

Alors on peut écrire

$$\alpha + \beta\omega = \delta(a + b\omega), \quad \alpha' + \beta'\omega = \delta_1(a + b\omega).$$

On peut supposer δ et δ_1 premiers entre eux, en faisant au besoin rentrer leur plus grand commun diviseur dans $a + b\omega$. Alors $a + b\omega$ est un nombre du module, qui ne comprend dès lors que les multiples entiers ordinaires de $a + b\omega$. Un tel module ne peut être un idéal, car celui-ci, comprenant $a + b\omega$, comprendrait aussi $\omega(a + b\omega)$, et ω n'est pas entier ordinaire.

Cela posé, on aura une base canonique par

$$\begin{aligned} x(x + \beta\omega) + y(x' + \beta'\omega) &= \text{quantité réelle positive } q, \\ x'(x + \beta\omega) + y'(x' + \beta'\omega) &= g + h\omega, \quad \text{avec } h > 0, \\ 0 &\leq g < q, \\ xy' - yx' &= \pm 1. \end{aligned}$$

Cela donne $\beta x + \beta' y = 0$, d'où x et y , puisqu'ils sont premiers entre eux ; quant au signe, il est déterminé par la condition $\alpha x + \alpha' y > 0$.

Ensuite, $xy' - yx' = \pm 1$ donne

$$x' = \varepsilon(x_0 + \theta x), \quad y' = \varepsilon(y_0 + \theta y), \quad \varepsilon = \pm 1,$$

θ entier ordinaire quelconque, x_0, y_0 solution particulière. Alors, $\beta x' + \beta' y' > 0$ donne, puisque $\beta x + \beta' y = 0$,

$$\varepsilon(\beta x_0 + \beta' y_0) > 0,$$

d'où le signe de ε . Et enfin

$$0 \leq \varepsilon[\alpha(x_0 + \theta x) + \alpha'(y_0 + \theta y)] < q$$

ou

$$0 \leq \varepsilon(M + \theta q) < q \quad (\text{car } \alpha x + \alpha' y = q)$$

donne θ sans ambiguïté.

On trouve ainsi une et une seule base canonique pour le module considéré.

NOTE V (ANNEXE AU § 118),

PAR TH. GOT.

Détail de la démonstration de la seconde expression du nombre de classes d'idéaux du corps circulaire des racines l èmes de l'unité, l étant premier.

On part de la première expression, transformée à l'aide de l'identité d'Euler :

$$\chi_h = \prod_{(u)} \lim_{s \rightarrow 1} \prod_{(p)} \left(1 - \left[\frac{p}{l} \right]^u p^{-s} \right)^{-1} = \prod_{(u)} \lim_{s \rightarrow 1} \sum \left[\frac{n}{l} \right]^u \frac{1}{n^s}$$

(u = 1, 2, ..., l-2)

On a, pour n non divisible par l :

$$\left[\frac{n}{l} \right] = e^{\frac{2i\pi\nu}{l-1}},$$

ν désignant l'indice de n par rapport au module l et à une racine primitive $r (r^\nu \equiv n, \pmod{l})$; et, pour n divisible par l , on pose :

$$\left[\frac{n}{l} \right] = 0.$$

Si $n' \equiv n, (l)$, on a $\nu' \equiv \nu, (l-1)$; donc

$$\left[\frac{n'}{l} \right] = \left[\frac{n}{l} \right],$$

et l'on a, par suite,

$$\Sigma = \sum_{k=1}^{k=l-1} \left[\frac{k}{l} \right]^n \left(\frac{1}{k^s} + \frac{1}{(k+l)^s} + \frac{1}{(k+2l)^s} + \dots \right).$$

Mais

$$\frac{1}{n^s} = \frac{1}{\Gamma(s)} \int_0^\infty e^{-nt} t^{s-1} dt$$

$$\frac{1}{k^s} + \frac{1}{(k+l)^s} + \dots = \frac{1}{\Gamma(s)} \int_0^\infty t^{s-1} dt (e^{-kt} + e^{-(k+l)t} + \dots) = \frac{1}{\Gamma(s)} \int_0^\infty \frac{e^{-kt}}{1-e^{-lt}} t^{s-1} dt.$$

Donc, comme $\Gamma(1) = 1$,

$$\chi h = \prod_u \lim_{s \rightarrow 1} \int_0^\infty \frac{t^{s-1} dt}{1-e^{-lt}} \sum_{n=1}^{n=l-1} e^{-nt} e^{\frac{2i\pi\nu n}{l-1}}.$$

Posons

$$F_u(e^{-t}) = \sum_{n=1}^{n=l-1} e^{-nt} e^{\frac{2i\pi\nu n}{l-1}},$$

$$\chi h = \prod_u \lim_{s \rightarrow 1} \int_0^\infty \frac{t^{s-1} F_u(e^{-t})}{1-e^{-lt}} dt.$$

$F_u(e^{-t}) = 0$ pour $t = 0$, car $\sum_{n=1}^{n=l-1} e^{\frac{2i\pi\nu n}{l-1}} = 0$. Donc, $F_u(e^{-t})$ est divisible par $1-e^{-lt}$, comme $1-e^{-lt}$, et la fraction $\frac{F_u(e^{-t})}{1-e^{-lt}}$ reste finie pour $t=0$; on a donc :

$$\lim_{s \rightarrow 1} \int_0^\infty \frac{F_u(e^{-t}) t^{s-1} dt}{1-e^{-lt}} = \int_0^\infty \frac{F_u(e^{-t}) dt}{1-e^{-lt}}.$$

Posons $e^{-t} = x$, $e^{-t} dt = -dx$. L'intégrale devient

$$\int_0^1 \frac{F_u(x) dx}{x(1-x^l)}.$$

En décomposant en fractions simples, on a :

$$\frac{F_u(x)}{x(1-x^l)} = -\frac{1}{l} \sum_{q=1}^{l-1} \frac{F_u(e^{\frac{2q\pi i}{l}})}{x^s - e^{\frac{2q\pi i}{l}}},$$

$$F_u(e^{\frac{2q\pi i}{l}}) = \sum_{k=1}^{k=l-1} \zeta^{qk} \theta^{u \text{ ind } k}$$

en posant $\theta = e^{\frac{2i\pi}{l-1}}$.

Soit u impair. — On a :

$$F_u(e^{\frac{2q\pi i}{l}}) = \theta^{-u \text{ ind } q} F_u(e^{\frac{2i\pi}{l}}).$$

D'ailleurs,

$$\int_0^1 \frac{dx}{x - e^{\frac{2q\pi i}{l}}} = L\left(2 \sin \frac{q\pi}{l}\right) + \frac{\pi}{2} \left(1 - \frac{2q}{l}\right) i,$$

L désignant la partie réelle du logarithme.

Pour deux valeurs q, q' complémentaires à l , le L a même valeur, et

$$\text{ind } q' = \text{ind } q + \frac{l-1}{2}, \quad \theta^{-u \text{ ind } q'} = -\theta^{-u \text{ ind } q},$$

car u est impair.

Les termes logarithmiques se détruisent donc dans la somme.

Puis $\frac{\pi}{2} \sum \theta^{-u \text{ ind } q} = 0$, car $u \equiv 0 \pmod{l-1}$.

Reste $-\frac{\pi i}{l} \sum q \theta^{-u \text{ ind } q}$;

et par suite le produit relatif aux valeurs impaires de u se réduit à

$$\left(\frac{\pi i}{l^2}\right)^{\frac{l-1}{2}} \prod_u F_u(e^{\frac{2i\pi}{l}}) \prod_{u=1,3,\dots,l-2} q \theta^{u \text{ ind } q}.$$

(On a changé θ en θ^{-1} dans le second produit, ce qui est permis, les valeurs de u étant deux à deux complémentaires à $l-1$.)

Quant au premier produit $\prod_u F_u(e^{\frac{2i\pi}{l}})$, on remarque que, d'après des formules de la division du cercle,

$$F_u(e^{\frac{2i\pi}{l}}) \times F_{l-1-u}(e^{\frac{2i\pi}{l}}) = \pm l,$$

suivant que u est pair ou impair, et que

$$F_{\frac{l-1}{2}}(e^{\frac{2i\pi}{l}}) = \pm \sqrt{\pm l}.$$

Donc $\prod_{u=1}^{u=l-2} F_u(e^{\frac{2i\pi}{l}}) = \pm i l^{\frac{l-2}{2}}$.

Soit u pair. — Les termes non logarithmiques se détruisent. En posant

$$\text{LA}_q = L \sqrt{\left(1 - e^{\frac{2qi\pi}{l}}\right) \left(1 - e^{-\frac{2qi\pi}{l}}\right)} = L_2 \sin \frac{q\pi}{l},$$

le produit étendu aux $\frac{l-3}{2}$, valeurs paires de u , s'écrit

$$\frac{1}{l^2} \prod_{u=2, 4, \dots, l-3} \sum_{q} \theta^{-u \text{ ind } q} \text{LA}_q,$$

à $\frac{l}{2}$ près (q ne prenant plus dans la somme que les valeurs inférieures à $\frac{l}{2}$).

Donc, puisque

$$\chi = \frac{2^{r_1+r_2} \pi^{r_2} R}{w |\sqrt{d}|}$$

est ici

$$\frac{(2\pi)^{\frac{l-1}{2}} R}{2l \times \frac{l-2}{2}}$$

on a

$$\frac{(2\pi)^{\frac{l-1}{2}} R h}{2l^2} = \pm i \frac{l^{\frac{l-2}{2}}}{l^{\frac{l-3}{2}}} \left(\frac{\pi}{l^2}\right)^{\frac{l-1}{2}} \prod_{u=1, 3, \dots, l-2} \sum_q q \theta^{u \text{ ind } q} \prod_{u=2, 4, \dots, l-3} \sum_{q \neq 0} \theta^{-u \text{ ind } q} \text{LA}_q,$$

$$h = \frac{1}{(2l)^{\frac{l-3}{2}}} \prod_4 \prod_2,$$

en désignant par \prod_4 et \prod_2 , pour abréger les deux produits du second membre.

Enfin, pour obtenir la forme plus simple du théorème 142 :

$$h = \frac{\prod_4}{(2l)^{\frac{l-3}{2}}} \frac{\Delta}{R},$$

remarquons qu'en changeant un peu les notations et posant

$$A_g = \sqrt{(1 - \zeta^{rg})(1 - \zeta^{-rg})},$$

on a $\varepsilon_g = \frac{A_g}{A_{g-1}}$, et, par suite, $\log \varepsilon_g = \text{LA}_g - \text{LA}_{g-1}$, et l'on trouve alors

$$\prod_u \theta^{-ug} \text{LA}_g (1 - \theta^{-u}) = \log \varepsilon_4 + \theta^u \log \varepsilon_2 + \dots + \theta^{\frac{l-3}{2}u} \log \varepsilon_{\frac{l-1}{2}}.$$

Comme

$$\prod_{u=2, 4, \dots, l-3} (1 - \theta^{-u}) = \frac{l-1}{2},$$

et que

$$\prod_u \theta^{ku} \log \varepsilon_{k-1} = \frac{l-1}{2} \Delta,$$

la formule est démontrée.

NOTE VI (ANNEXE AU § 172),

PAR TH. GOT.

Recherches sur le théorème de Fermat, faites par Kummer et divers auteurs, postérieurement à la démonstration de l'impossibilité en nombres entiers de l'équation

$$(1) \quad x^l + y^l + z^l = 0,$$

donnée par Kummer pour les exposants l premiers réguliers.

La fondation récente du prix Wolfskehl a donné un renouveau d'actualité à la question du théorème de Fermat et a suscité un grand nombre de travaux s'y rapportant. Il nous a paru intéressant d'indiquer l'état de la question à la fin de 1911. Mais pour comprendre la portée des travaux actuels et même les méthodes qui ont inspiré certains d'entre eux, il est indispensable de se reporter aux résultats obtenus déjà par Kummer il y a cinquante ou soixante ans : il a d'abord démontré l'impossibilité de l'équation de Fermat pour les exposants l premiers réguliers (c'est-à-dire ne divisant le numérateur d'aucun des $\frac{l-3}{2}$ premiers nombres de Bernoulli) : c'est à ce théorème que le dernier chapitre du Rapport de M. Hilbert est consacré; Kummer a ensuite, dans un Mémoire de 1857 (*Abhandlungen der Königl. Akad. der Wissenschaften zu Berlin*), étendu la démonstration à la classe particulière suivante d'exposants l premiers non réguliers :

1° l divise un seul, B_v , des $\frac{l-3}{2}$ premiers nombres de Bernoulli et une seule fois;

2° il existe un module pour lequel une certaine unité E_v n'est pas reste de $l^{\text{ième}}$ puissance;

3° $B_v l$ n'est pas divisible par l^3 .

C'est à l'exposé de ce résultat que la plus grande partie de la présente note est consacrée : tout en suivant la marche de Kummer, j'ai apporté à ses démonstrations les changements nécessaires pour les faire cadrer avec la conception actuelle des idéaux (d'après la définition de Dedekind) et avec les procédés et les notations du Rapport de M. Hilbert. A part deux exceptions relatives à des questions très simples, pour lesquelles je renvoie le lecteur aux Mémoires de Kummer, je me suis

d'ailleurs astreint à réunir dans ma Note, lorsqu'elles ne se trouvaient pas déjà dans le Rapport, les démonstrations de toutes les propositions utilisées : on n'aura pas ainsi à les chercher dans plusieurs longs Mémoires de Kummer où elles sont disséminées ; j'ai, du reste, pu, sur quelques points, abréger notablement les calculs, soit en traitant d'une manière unique les cas des idéaux premiers du premier degré et de ceux de degré quelconque, soit en utilisant les résultats du Rapport. Exception faite des deux exceptions mentionnées, la lecture de notre Note n'exige donc, en dehors de l'étude de ce Rapport, aucune étude supplémentaire. J'ai conservé, pour les renvois aux théorèmes ou paragraphes, et pour les références bibliographiques, les abréviations de cet Ouvrage, et j'ai distingué par des chiffres romains les divisions et les théorèmes de la Note.

Parmi les travaux récents, nous nous contenterons — renvoyant pour les démonstrations aux Mémoires originaux — d'indiquer les plus importants des résultats obtenus, soit en partant de ceux de Kummer [Mirimanoff, Wieferich, Frobenius], soit dans un autre ordre d'idées, voisin de celui de Legendre [Dickson, Hurwitz].

L'étude de l'équation (1) est entièrement différente suivant que l'un des nombres x, y, z est ou n'est pas divisible par l ; nous examinerons donc les deux cas successivement.

I. — ÉTUDE DU CAS OU xyz N'EST PAS DIVISIBLE PAR l .

§ I. — Étude d'un produit particulier d'idéaux conjugués.

THÉORÈME I. — Soit r une racine primitive, module l , et désignons par r_a le plus petit reste positif de r^a , module l , et par s la substitution (ζ, ζ') . \mathbf{j} désignant un idéal quelconque, le produit $\prod_k s^k \mathbf{j}$ est toujours un idéal principal, lorsqu'on l'étend soit aux $\frac{l-1}{2}$ valeurs de k vérifiant l'inégalité

$$(3) \quad r_{-k} + r_{-k+\text{ind } q} < l,$$

soit aux $\frac{l-1}{2}$ valeurs de k vérifiant l'inégalité inverse. q désigne un entier quelconque non divisible par l ; l'indice est relatif à la racine primitive r , module l . [Kummer⁶].

Démonstration. — Nous allons démontrer d'abord (lemme I) que le théorème est vrai pour tout idéal premier du premier degré. Nous établirons ensuite (lemme II) que tout idéal premier de degré quelconque est équivalent à un produit d'idéaux premiers du premier degré, ce qui achèvera la démonstration.

LEMME I. — \mathfrak{p} étant un idéal premier du premier degré, le produit $\prod_k s^k \mathfrak{p}$, étendu aux mêmes valeurs de k que ci-dessus, est un idéal principal⁽¹⁾.

Soit, en effet, p le nombre premier rationnel divisible par \mathfrak{p} ; il est de la forme $ml + 1$, puisque \mathfrak{p} est du premier degré, et il se décompose en $l - 1$ facteurs conjugués :

$$p = \prod_{i=0}^{i=l-2} s^i \mathfrak{p}.$$

D'autre part, on a la formule suivante, de la division du cercle :

$$p = \psi_q(\zeta) \psi_q(\zeta^{-1}),$$

dans laquelle $\psi_q(\zeta)$ désigne la somme

$$\psi_q(\zeta) = \sum_{t=1}^{t=p-2} \zeta^{\text{ind} t + q \text{ind}(t+1)},$$

où les indices sont pris par rapport à une racine primitive g , module p . (Voir, par exemple, Weber, *Algèbre supérieure*.)

Soit, d'autre part,

$$\mathfrak{p} = (p, \zeta - g^m).$$

(Voir note du § 93.)

Cherchons à quelle condition l'idéal

$$s^k \mathfrak{p} = (p, \zeta^{r^k} - g^m)$$

est un diviseur de $\psi_q(\zeta)$. Il faut et il suffit pour cela que la division de $\psi_q(\zeta)$ par $\zeta^{r^k} - g^m$ donne un reste divisible par p . Pour avoir ce reste R , (mod p), nous remplaçons ζ^{r^k} par g^m , c'est-à-dire ζ par $g^{mr^{-k}}$, et nous avons

$$R \equiv \sum_{t=1}^{t=p-2} g^{mr^{-k}(\text{ind} t + q \text{ind} t + 1)} \equiv \sum_{t=1}^{t=p-2} t^{mr^{-k}} (t+1)^{qmr^{-k}} \equiv \sum_{t=1}^{t=p-1} t^{mr^{-k}} (t+1)^{qmr^{-k}}, \pmod{p},$$

ou encore, en remplaçant mr^{-k} et mr^{-k} par mr_{-k} et mr_{-k+q} , ce qui ne modifie pas les exposants pour le module $ml = p - 1$:

$$R \equiv \sum_{t=1}^{t=p-1} t^{mr_{-k}} (t+1)^{mr_{-k+q}}.$$

⁽¹⁾ Ce lemme est identique au théorème 136, si l'on prend $q = r - 1$; en raison de son importance, nous en donnons une autre démonstration, d'après les procédés de Kummer.

En développant par la formule du binôme, nous aurons

$$R \equiv \sum_u a_u \sum_{t=1}^{t=p-1} t^u,$$

expression dans laquelle les a_u sont des coefficients binomiaux, dont aucun n'est divisible par p , puisque l'on a

$$mr_{-k+\text{ind}q} < p-1.$$

Les sommes $\sum_{t=1}^{t=p-1} t^u$ sont divisibles par p , sauf si t^u est congru à 1, module p ,

c'est-à-dire, — u étant compris entre zéro et $2p-2$, — si u est égal à $p-1$. La condition nécessaire et suffisante pour que R soit divisible par p , et que, par suite, $s^k p$ divise $\psi_q(\zeta)$, est donc que la plus grande valeur de u soit inférieure à $p-1$:

$$mr_{-k} + mr_{-k+\text{ind}q} < p-1,$$

ou, en divisant par m :

$$r_{-k} + r_{-k+\text{ind}q} < l.$$

Or, de deux nombres k et $\mu+k$ ⁽¹⁾, l'un vérifie l'inégalité ci-dessus et l'autre l'inégalité inverse (car $r_{\mu+k} = l - r_{-k}$); par suite, la moitié des $l-1$ idéaux premiers de p divisent $\psi_q(\zeta)$ et l'autre moitié $\psi_q(\zeta^{-1})$, — comme on le voit d'ailleurs *a priori* en changeant ζ en ζ^{-1} ; — et comme $\psi_q(\zeta)\psi_q(\zeta^{-1})$, qui est égal à p , ne contient que $l-1$ facteurs idéaux, on a nécessairement ⁽²⁾

$$\prod_k s^k p = \pm \zeta^a \psi_q(\zeta),$$

et

$$\prod_{\mu-k} s^{\mu-k} p = \pm \zeta^{-a} \psi_q(\zeta^{-1}),$$

k prenant, dans ces deux produits, les valeurs vérifiant l'inégalité (3) ou l'inégalité équivalente :

$$(4) \quad r_{\mu-k} + r_{\mu-k+\text{ind}q} > l.$$

Ces produits sont donc des idéaux principaux.

C. q. f. d.

(1) $\mu = \frac{l-1}{2}$.

(2) $E(\zeta)$, unité à introduire dans le produit, est nécessairement de la forme $\pm \zeta^a$, car $E(\zeta) \cdot E(\zeta)^{-1} = 1$. (Théorème 48.)

LEMME II. — Tout idéal premier \mathfrak{p} de degré quelconque f est équivalent à un produit d'idéaux premiers du premier degré.

Il suffit évidemment de démontrer que tout idéal premier de degré supérieur à 1 est équivalent à un produit d'idéaux premiers de degré inférieur. Nous allons pour cela déterminer un nombre $F(\zeta)$, divisible par \mathfrak{p} une fois et une seule, et dont tous les autres facteurs idéaux premiers \mathfrak{q} soient de degré inférieur. On aura donc

$$F(\zeta) = \mathfrak{p} \prod \mathfrak{q},$$

et comme la norme de $\prod \mathfrak{q}$ est un entier N ,

$$N = \prod \mathfrak{q} \cdot s \prod \mathfrak{q} \cdot s^2 \prod \mathfrak{q} \cdot \dots \cdot s^{l-2} \prod \mathfrak{q},$$

on aura ainsi montré l'équivalence de \mathfrak{p} au produit $s \prod \mathfrak{q} \cdot s^2 \prod \mathfrak{q} \cdot \dots \cdot s^{l-2} \prod \mathfrak{q}$, dont tous les idéaux sont de degré moindre.

Pour le nombre $F(\zeta)$, il suffit de prendre $P(\zeta) + p$, en désignant par $P(x)$ le facteur correspondant à \mathfrak{p} dans l'équation fondamentale décomposée, modulo p , en ses $e = \frac{l-1}{f}$ facteurs irréductibles :

$$x^{l-1} + x^{l-2} + \dots + 1 \equiv P(x) \cdot P_1(x) \dots P_{e-1}(x), \pmod{p},$$

de sorte que l'on a

$$\mathfrak{p} = (p, P(\zeta))$$

(voir théorème 119).

Pour démontrer que $F(\zeta)$ remplit bien les conditions indiquées, remarquons que le premier coefficient de P peut être pris égal à 1 et démontrons que le dernier est alors égal, modulo p , à $(-1)^f$. Considérons pour cela l'équation

$$\Phi_k(x) = x^f + A_1(\eta_k)x^{f-1} + \dots + A_f(\eta_k) = 0$$

dont les racines sont les racines de l'unité formant la période η_k ($\eta_k = \zeta^{r^k} + \zeta^{r^{k+e}} + \dots + \zeta^{r^{k+(f-1)e}}$). Le produit de ces racines de l'unité étant égal à 1, on a

$$A_f(\eta_k) = (-1)^f.$$

Le produit $\prod_{k=0}^{e-1} \Phi_k(x)$ est un polynôme à coefficients entiers, — car ces coefficients

sont des fonctions symétriques des périodes, — et il est identique au premier membre de l'équation fondamentale, — car il a même degré, mêmes racines et même premier coefficient. Soit, d'autre part,

$$\varphi(y) = 0$$

l'équation de degré e , à coefficients entiers, dont les racines sont les e périodes à f termes : cette équation, considérée comme congruence, modulo p , a e racines u_k . [Kummer³.] Faisons correspondre, d'une façon quelconque, ces dernières aux périodes

et substituons dans les Φ_k les u_k aux τ_k . Puisque les fonctions symétriques élémentaires des u_k sont congrues, pour le module p , aux mêmes fonctions des périodes, on a la congruence

$$x^{l-1} + x^{l-2} + \dots + 1 \equiv \prod_{k=0}^{k=e-1} \Phi_k(x, u_k), \pmod{p}.$$

Comme le polynôme $x^{l-1} + x^{l-2} + \dots + 1$ ne peut être décomposé de deux manières différentes en facteurs irréductibles, modulo p , les $P_j(x)$ ne sont autres, à l'ordre près, que les $\Phi_k(x, u_k)$, ce qui démontre notre assertion sur la valeur du dernier coefficient de $P(x)$.

Dès lors, $P(\zeta) + p$ est :

- 1° Divisible par \mathfrak{p} ;
- 2° Non divisible par \mathfrak{p}^2 , car tout nombre divisible par \mathfrak{p}^2 doit, après division par $P(\zeta)$, donner un reste divisible par p^2 , et ici le reste est p ;
- 3° Non divisible par un autre facteur \mathfrak{p}_k de p , égal à $(p, P_k(\zeta))$, car le polynôme $P(x)$ n'est pas divisible par $P_k(x)$, mod p ;
- 4° Non divisible par un idéal premier de degré supérieur à f , car $P(\zeta)$ est de degré f et le premier coefficient est 1;
- 5° Non divisible par un idéal premier de degré f autre que \mathfrak{p} , car, soit \mathfrak{q} , égal à $(q, Q(\zeta))$, un tel idéal; le reste de la division de $P(x) + p$ par $Q(x)$ est $P(x) - Q(x) + p$, et il n'est pas divisible par q , puisque les derniers termes de P et Q étant égaux (à $(-1)^f$), le dernier terme du reste est p .

Le nombre $F(\zeta) = P(\zeta) + p$ remplit donc les conditions que nous avons utilisées et le lemme II se trouve ainsi démontré, ce qui achève la démonstration du théorème I⁽¹⁾.

§ II. — *Le critérium de Kummer.*

THÉORÈME II. — Si trois entiers rationnels x, y, z , premiers entre eux et à l , vérifient l'équation

$$x^l + y^l + z^l = 0,$$

chaque couple de deux quelconques d'entre eux, x, y , vérifie le système des $\frac{l-3}{2} = \mu - 1$ congruences suivantes⁽²⁾ :

$$(5) \quad B_n \frac{d_{\mathfrak{o}}^{l-2n} \log(x + e^u y)}{du^{l-2n}} \equiv 0, \pmod{l},$$

$(n = 1, 2, \dots, \mu-1).$

⁽¹⁾ Le lemme II est vrai pour un corps de Galois quelconque (théorème 89), il nous a paru utile d'en reproduire la démonstration particulière au corps circulaire.

⁽²⁾ $\frac{d_{\mathfrak{o}}^{l-2n}}{du^{l-2n}}$ désigne la valeur de la dérivée $(l-2n)$ ème pour $u=0$.

En effet, l'équation peut s'écrire

$$(x + y)(x + \zeta y) \dots (x + \zeta^{l-1} y) = -z^l.$$

Les facteurs du premier membre sont premiers entre eux deux à deux, puisque x et y sont premiers entre eux et que z est premier à l (voir § 172) : donc, leur produit étant une puissance $l^{\text{ème}}$, chacun d'eux est, à un facteur unité près, la puissance $l^{\text{ème}}$ d'un idéal. On a donc

$$x + \zeta y = \varepsilon \mathbf{j}^l,$$

et, par suite,

$$x + \zeta^{r^k} y = s^k \varepsilon (s^k \mathbf{j})^l,$$

(s désignant toujours la substitution (ζ, ζ^r)).

Donnons à k les $\frac{l-1}{2}$ valeurs vérifiant l'inégalité (4) :

$$r_{\mu-k} + r_{\mu-k+\text{ind } q} > l,$$

et formons le produit des $x + \zeta^{r^k} y$ étendu à ces valeurs de k : on sait (théorème I) que le produit $\prod_k s^k \mathbf{j}$ correspondant est un idéal principal (α) . Quant au produit $\prod_k s^k \varepsilon$, il se réduit, au signe près, à une racine $l^{\text{ème}}$ de l'unité (théorème 48), car son module est égal à ± 1 , puisque l'on a pour la norme :

$$n(\varepsilon) = \prod_k s^k \varepsilon \cdot \prod_{\mu+k} s^{\mu+k} \varepsilon = \pm 1$$

et que \prod_k et $\prod_{\mu+k}^k$ qui se déduisent l'un de l'autre par le changement de ζ en ζ^{-1} sont imaginaires conjugués. On a donc

$$\prod_k (x + \zeta^{r^k} y) = \pm \zeta^l \alpha^l.$$

On en déduit (voir § 131, note), les congruences

$$(6) \quad \sum_k \frac{d_{\alpha}^{l-2n} \log(x + e^{ur^k} y)}{du^{l-2n}} \equiv 0, \pmod{l},$$

pour $n = 1, 2, \dots, \mu - 1$, c'est-à-dire encore

$$\frac{d_{\alpha}^{l-2n} \log(x + e^u y)}{du^{l-2n}} \sum_k r^{k(l-2n)} \equiv 0, \pmod{l}.$$

Transformons \sum_k , de manière à étendre la sommation à toutes les valeurs de k de 1 à $l-1$, en multipliant chaque terme de $\sum_{k=1}^{l-1} r^{k(l-2n)}$ par la fraction

$$\frac{r_{\mu-k} + r_{\mu-k+\text{ind } q} - r_{\mu-k+\text{ind } (q+1)}}{l}$$

égale à 1 lorsque la valeur de k est à conserver, égale à 0 dans le cas contraire. On aura

$$\sum_k r^{k(l-2n)} \equiv \sum_{k=1}^{l-1} \frac{r_{\mu-k} + r_{\mu-k+\text{ind } q} - r_{\mu-k+\text{ind } (q+1)}}{l} r^{k(l-2n)},$$

ou, en multipliant par l et remplaçant $r^{k(l-2n)}$ par $r^{kl(l-2n)}$ qui lui est congru, mod l ,

$$l \sum_k r^{k(l-2n)} \equiv \sum_{k=1}^{l-1} [r_{\mu-k} + r_{\mu-k+\text{ind } q} - r_{\mu-k+\text{ind } (q+1)}] r^{kl(l-2n)}, \pmod{l^2}.$$

Il suffit d'évaluer la seconde somme

$$\sum_{k=1}^{l-1} r_{\mu-k+\text{ind } q} r^{kl(l-2n)},$$

les deux autres s'en déduiront en effet par le changement de q en 1 et en $q+1$. Posons dans cette somme

$$r_{\mu-k+\text{ind } q} = i,$$

i prendra toutes les valeurs : $1, 2, \dots, l-1$, comme k ; on a d'ailleurs

$$r_{\mu-k+\text{ind } q} \equiv i, \pmod{l},$$

d'où on tire

$$r^k \equiv -\frac{q}{i}, \pmod{l},$$

et par suite

$$r^{kl(l-2n)} \equiv -\frac{q^{l(l-2n)}}{i^{l(l-2n)}}, \pmod{l^2},$$

ou encore

$$r^{kl(l-2n)} \equiv -q^{l(l-2n)} i^{l(2n-1)}, \pmod{l^2},$$

car $i^{l(l-1)}$ est congru à 1 pour le même module.

On a dès lors

$$l \sum_k r^{k(l-2n)} \equiv -[1 + q^{l(l-2n)} - (q+1)^{l(l-2n)}] \sum_{i=1}^{l-1} i^{l(2n-1)+1}, \pmod{l^2}.$$

Mais on a, d'après la formule sommatoire de Bernoulli (voir la note du § 137) :

$$\sum i^{l(2n-1)+1} \equiv (-1)^{\frac{l(2n-1)-1}{2}} B_{\frac{l(2n-1)+1}{2}} \cdot l, \pmod{l^2};$$

d'où en divisant par l , revenant au module l , et tenant compte de ce que l'on a

$$\frac{l(2n-1)+1}{2} = n + (2n-1) \left(\frac{l-1}{2} \right)$$

et que l'on a⁽¹⁾

$$\frac{B_{n+s\mu}}{n+s\mu} \equiv (-1)^{s\mu} \frac{B_n}{n}, \pmod{l}.$$

la congruence

$$\sum_k r^{k(l-2n)} \equiv (-1)^n [1 + q^{l-2n} - (q+1)^{l-2n}] \frac{B_n}{2n}, \pmod{l}.$$

Or, q peut toujours être choisi de manière à ce que le crochet ne soit pas divisible par l ; on a donc bien, en portant l'expression de $\sum_k r^{k(l-2n)}$ dans les congruences (6) les conditions

$$B_n \frac{d^{l-2n} \log(x + e^u y)}{du^{l-2n}} \equiv 0, \pmod{l},$$

qu'il s'agissait de démontrer.

§ III. — *Impossibilité de l'équation (1) en nombres entiers x, y, z premiers à l , quand l ne divise qu'un des $\frac{l-3}{2}$ premiers nombres de Bernoulli.*

THÉORÈME III. — Si le nombre premier l ne divise que l'un des $\frac{l-3}{2}$ premiers nombres de Bernoulli et qu'une seule fois, l'équation (1) est impossible en nombres entiers x, y, z premiers à l . [Kummer¹⁶.]

Soit ν le rang du nombre de Bernoulli B_ν qui est divisible par l .

Si ν n'est pas $\frac{l-3}{2}$, on doit avoir, d'après le théorème II, la congruence

$$\frac{d^3 \log(x + e^u y)}{du^3} \equiv 0, \pmod{l},$$

c'est-à-dire

$$\frac{xy(x-y)}{(x+y)^3} \equiv 0, \pmod{l},$$

⁽¹⁾ KUMMER, *Ueber eine allgemeine Eigenschaft der rationalem Entwicklungs-coefficienten einer bestimmten Gattung analytischen Functionen.* (J. de Crelle, t. XLI.) — On pourra se contenter de voir P. BACHMANN : *Niedere Zahlentheorie. Zweiter Teil. Erstes Kapitel.*

ainsi que les congruences analogues, relatives aux autres combinaisons de x, y, z . On doit donc avoir $x \equiv y$ et, par suite, $x \equiv y \equiv z$; mais comme on doit avoir, d'après le théorème de Fermat,

$$x + y + z \equiv 0, \pmod{l},$$

il en résulterait $3x \equiv 0$, ce qui est impossible, l n'étant pas égal à 3.

Il ne pourrait donc être égal qu'à $\frac{l-3}{2}$; mais alors on aurait, d'après le critérium,

$$\frac{d_0^5 \log(x + e^u y)}{du^5} \equiv 0, \pmod{l},$$

c'est-à-dire

$$\frac{xy(x-y)(x^2 - 10xy + y^2)}{(x+y)^5} \equiv 0, \pmod{l},$$

ou

$$(x-y)(x^2 - 10xy + y^2) \equiv 0, \pmod{l},$$

et par suite aussi

$$(x-z)(x^2 - 10xz + z^2) \equiv 0, \pmod{l}.$$

On ne peut avoir $x \equiv y$, car alors on aurait $z \equiv -2x$ et la deuxième congruence deviendrait

$$3 \cdot 25 \cdot x^3 \equiv 0, \pmod{l},$$

qui est impossible, l n'étant ni 3 ni 5.

Enfin, on ne peut avoir non plus

$$x^2 - 10xy + y^2 \equiv x^2 - 10xz + z^2 \equiv 0, \pmod{l},$$

car, avec $x + y + z \equiv 0$, on en déduirait

$$11x(x+2y) \equiv 0, \pmod{l},$$

ce qui est impossible, car on ne peut avoir $x \equiv -2y$, l n'étant ni 3 ni 5, et d'autre part l n'est pas non plus égal à 11, qui est régulier comme 3 et 5. C. q. f. d.

§ IV. — *Recherches récentes sur l'équation (1) dans le cas où xyz n'est pas divisible par l .*

Les recherches récentes relatives à l'équation (1), dans le cas où xyz n'est pas divisible par l , ont presque toutes leur origine soit dans les travaux de Kummer, soit dans ceux, plus anciens, de Sophie Germain et de Legendre.

Mirimanoff s'est placé au premier point de vue dans son Mémoire : *L'équation indéterminée $x^l + y^l + z^l = 0$ et le critérium de Kummer.* (J. f. d. r. u. a. Mathematik, tome CXXVIII). En discutant les congruences (5) il a établi le théorème suivant :

THÉORÈME IV. — L'équation (1) est impossible en nombres entiers premiers à l , si les nombres de Bernoulli $B_{\frac{l-3}{2}}, B_{\frac{l-5}{2}}, B_{\frac{l-7}{2}}, B_{\frac{l-9}{2}}$ ne sont pas tous divisibles par l .

D'autre part, il montre qu'on peut éliminer de la façon suivante les nombres de Bernoulli des congruences de Kummer : en désignant par $\varphi_i(t)$, pour $i=2, 3, \dots, l-1$, le polynôme

$$\varphi_i(t) = t - 2^{i-1}t^2 + 3^{i-1}t^3 - \dots + (-1)^{l-2}(l-1)^{i-1}t^{l-1}$$

et par $\varphi_1(t)$ le quotient

$$\varphi_1(t) = \frac{t(1 - t^{l-1})}{1 + t};$$

t représentant l'un quelconque des rapports des trois nombres x, y, z , ces congruences équivalent au système

$$\begin{aligned} \varphi_i \varphi_{l-i} &\equiv 0, & (i=2, 3, \dots, l-2), \\ \varphi_{l-1} &\equiv 0. \end{aligned}$$

Wieferich (*Zum letzten Fermatschen Theorem*. J. f. d. Mathematik, tome CXXXVI) a déduit des congruences de Mirimanoff le critérium suivant :

THÉORÈME V. — Pour que l'équation (1) puisse avoir une solution, x, y, z étant premiers à l , il faut que le quotient de Fermat

$$q(2) = \frac{2^{l-1} - 1}{l}$$

soit divisible par l .

De nouvelles démonstrations, plus simples, de ce critérium ont été données par Frobenius (*Sitzungsberichte der K. Ak. d. Wiss. zu Berlin*, 2 décembre 1909, et *J. f. d. Mathematik*, tome CXXXVII), et par Mirimanoff (*Sur le dernier théorème de Fermat*. J. f. d. Mathematik, tome CXXXIX).

Mirimanoff a montré en outre que :

THÉORÈME VI. — Pour que l'équation (1) puisse avoir une solution, x, y, z étant premiers à l , il faut que le quotient de Fermat

$$q(3) = \frac{3^{l-1} - 1}{l}$$

soit divisible par l . (C. R., 24 janvier 1910.)

Dans l'ordre d'idées de Legendre, Dickson part du théorème de Sophie Germain que nous reproduisons :

THÉORÈME VII. — S'il existe un nombre premier impair p tel que la congruence

$$x^n + y^n + z^n \equiv 0, \pmod{p},$$

soit impossible en nombres entiers premiers à p et tel de plus que n ne soit pas

résidu de puissance $n^{\text{ème}}$, module p , l'équation $x^n + y^n + z^n = 0$ n'a pas de solution en nombres entiers x, y, z premiers à n .

Il en déduit par des méthodes nouvelles l'impossibilité de l'équation (1) avec $xyz \equiv 0 \pmod{l}$, pour tout nombre premier l inférieur à 6857. (Dickson, *On the last theorem of Fermat*, février 1908. *Messenger of Mathematics*, tome XXXVIII, et deuxième note, mai 1908, *Quarterly Journal of P. a A. Mathematics*, tome XL.)

II. — ÉTUDE DU CAS où xyz EST DIVISIBLE PAR l .

§ V.

Nous allons, avec Kummer, examiner le cas particulier où l remplit les trois conditions suivantes :

- 1° l divise un seul B_r des $l-3$ premiers nombres de Bernoulli et une seule fois;
- 2° il existe un module pour lequel l'unité

$$E_r = \varepsilon(s\varepsilon)^{r-2} \cdots (s^{\mu-1}\varepsilon)^{r-2(\mu-1)},$$

où ε désigne l'unité circulaire définie au paragraphe 138 :

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

n'est pas résidu de $l^{\text{ème}}$ puissance ;

- 3° B_{rl} n'est pas divisible par l^3 .

Dans ces conditions, l'équation (1) est impossible, même avec l'un des nombres x, y, z divisible par l . [Kummer¹⁶.]

Pour arriver à la démonstration, un certain nombre de théorèmes préliminaires sont nécessaires : ils feront l'objet des paragraphes VI, VII, VIII, IX et X. Auparavant, démontrons d'abord le

THÉORÈME VIII. — Les deux premières hypothèses faites entraînent que le second facteur du nombre des classes n'est pas divisible par l .

Pour cela, nous allons montrer que, dans la première hypothèse, *ce second facteur $\frac{\Delta}{R}$ ne peut être divisible par l que si l'unité E_r est la $l^{\text{ème}}$ puissance d'une unité.*

Reprendons en effet les notations du paragraphe 139 : si $\frac{\Delta}{R}$ est divisible par l , le déterminant du système (117) :

$$\log \varepsilon_t = \sum_{i=1}^{i=\mu-1} M_{i,t} \log |\gamma_i|, \quad (t=1, 2, \dots, \mu-1),$$

l'est aussi ; d'où l'existence de $p-1$ nombres N_t , non tous divisibles par l , et tels que toutes les sommes $\sum_t N_t M_{it}$ le soient : l'unité $\prod_t \varepsilon_t^{N_t}$ est donc la $l^{\text{ème}}$ puissance d'une unité E et on en déduit, comme au paragraphe 139 :

$$B_t N_t \equiv 0 \pmod{l}, \quad (t=1, 2, \dots, p-1).$$

Or, les B_t sont tous $\equiv 0 \pmod{l}$, excepté B_v ; il faut donc que tous les N_t soient $\equiv 0$, excepté N_v . On a, par suite, E' désignant une unité :

$$E^l = E'^l \varepsilon_v^{N_v}.$$

Exprimons ε_v avec les unités circulaires selon la formule (109)

$$\varepsilon_v \equiv \varepsilon^{(l-1)F(s)} \equiv \varepsilon^{n_0} (s\varepsilon)^{n_1} \dots (s^{p-2}\varepsilon)^{n_{p-2}},$$

où l'exposant symbolique $F(s)$ est égal à $\frac{1-s^p}{(1-s)(r^{2v}-s)}$, de sorte qu'on a les congruences

$$n_i \equiv \frac{1-r^{-2(i+1)v}}{1-r^{2v}}, \quad (mod \ l), \quad (i=0, 1, \dots, p-2).$$

Posant alors

$$N_v \equiv -mr^{2v}(1-r^{2v}), \quad (mod \ l),$$

on aura pour l'exposant de $s^i\varepsilon$ dans E' :

$$N_v n_i \equiv mr^{2v}(r^{-2(i+1)v}-1), \quad (mod \ l), \quad (i=0, 1, \dots, p-2).$$

On introduit aisément l'unité $s^{p-1}\varepsilon$ en tenant compte de ce que la norme est 1, et on arrive à la formule

$$E''^l = E'^m,$$

E'' désignant une unité et E' étant $\varepsilon(s\varepsilon)^{r^{-2v}} \dots (s^{p-1}\varepsilon)^{r^{-2(p-1)v}}$.

Enfin, m n'étant pas divisible par l , on peut déterminer deux entiers a et b , tels que $am = 1 + bl$, de sorte qu'en élevant $E''^l = E'^m$ à la puissance $a^{\text{ème}}$ et remplaçant am par $1 + bl$, on a

$$E' = E'''^l,$$

E''' désignant une unité.

Dans ce cas, l'unité E' est donc résidu de $l^{\text{ème}}$ puissance pour tous les modules.

Si donc nous supposons qu'il existe un module pour lequel l'unité E' n'est pas résidu de $l^{\text{ème}}$ puissance, le second facteur du nombre de classes n'est pas divisible par l . C. q. f. d.

§ VI. — *Définition et propriétés des logarithmes pour le module l^{n+1} .*

Soit $f(\zeta)$ un nombre non divisible par l , c'est-à-dire tel que $f(1)$ ne soit pas divisible par l . Posons, pour abréger,

$$x = 1 - \frac{f(\zeta)}{f(1)},$$

et considérons le développement purement formel

$$x = \frac{1}{2}x^2 + \frac{1}{3}x^3 - \dots + \frac{(-1)^{i+1}}{i}x^i + \dots,$$

qui serait égal à $\log(1 - x)$, si l'on avait $|x| < 1$.

Nous allons montrer que le nombre des termes de ce développement non divisibles par l^{n+1} est limité, et nous *conviendrons* de dire que cet ensemble de termes est congru pour le module l^{n+1} au logarithme de $\frac{f(\zeta)}{f(1)}$; nous écrirons

$$(7) \quad \log \left[\frac{f(\zeta)}{f(1)} \right] \equiv x - \frac{1}{2}x^2 + \frac{1}{3}x^3 - \dots, \pmod{l^{n+1}},$$

en employant le même signe \log que pour les logarithmes népériens, mais uniquement comme notation abrégée. [Kummer¹⁷].

x est divisible par $1 - \zeta$, c'est-à-dire par l'idéal l , et l est égal à l^{n+1} ; un terme quelconque du développement est divisible par une puissance de l , — par l^m , si le rang m de ce terme n'est pas divisible par l , et, si ce rang est ml^n , m n'étant pas divisible par l , par $\frac{l^{ml^n}}{l^{(l-1)m}}$, où l'exposant du numérateur est toujours supérieur à celui du dénominateur; l'exposant de cette puissance de l augmente indéfiniment dans les deux cas avec m , il finira donc par être supérieur à $(n+1)(l-1)$, ce qui montre qu'à partir d'un certain rang tous les termes sont divisibles par l^{n+1} .

THÉORÈME IX. — On a, au sens qui vient d'être défini, la congruence

$$(8) \quad (l-1) \log \left[\frac{f(\zeta)}{f(1)} \right] \equiv \log \left[\frac{Nf(\zeta)}{f(1)^{l-1}} \right] + \sum_{k=1}^{k=l-2} \frac{d_o^{kl^n} \log f(e^u)}{du^{kl^n}} X_k(\zeta), \pmod{l^{n+1}},$$

$Nf(\zeta)$ désignant la norme, l'indice o indiquant que l'on fait $u=o$ dans les dérivées kl^n èmes de $\log f(e^u)$, et $X_k(\zeta)$ désignant le polynôme

$$(9) \quad X_k(\zeta) = \zeta + r^{-kl^n}\zeta r + r^{-2kl^n}\zeta r^2 + \dots + r^{-(l-2)l^n}\zeta r^{l-2},$$

où r est une racine primitive pour le module l . [Kummer¹².]

Ordonnons, en effet, la différence $f(1) - f(\zeta)$ suivant les puissances de $1 - \zeta$, de sorte que l'on ait

$$f(1) - f(\zeta) = A_1(1 - \zeta) + A_2(1 - \zeta)^2 + \dots + A_{l-1}(1 - \zeta)^{l-1},$$

les A_i étant des entiers rationnels. On en déduit

$$(10) \quad \log \left[\frac{f(\zeta)}{f(1)} \right] \equiv \sum_i \frac{C_i(1 - \zeta)^i}{i f(1)^i} \pmod{l^{n+1}}.$$

Remplaçons ζ successivement par tous ses conjugués $\zeta^r, \zeta^{r^2}, \dots, \zeta^{r^h}, \dots, \zeta^{r^{l-2}}$, puis ajoutons toutes ces égalités multipliées respectivement par r^{-hkl^n} ; on a

$$\sum_{h=0}^{h=l-2} r^{-hkl^n} \log \left[\frac{f(\zeta^r)}{f(1)} \right] \equiv \sum_{h=0}^{h=l-2} \sum_i \frac{C_i r^{-hkl^n} (1 - \zeta^r)^i}{i (f(1))^i}.$$

On a, en développant $(1 - \zeta^r)^i$ et sommant d'abord par rapport à h ,

$$\sum_{h=0}^{h=l-2} \frac{r^{-hkl^n} (1 - \zeta^r)^i}{i} = \sum_{h=0}^{h=l-2} \sum_{s=0}^{s=i} (-1)^s \frac{i!}{i \cdot s! (i-s)!} r^{-hkl^n} \zeta^{sr^h} = \sum_{s=0}^{s=i} (-1)^s \frac{i!}{i \cdot s! (i-s)!} X_k(\zeta^s).$$

En désignant alors par P_t la somme

$$P_t = (-1)^t \left[\frac{i!}{t! (i-t)!} - \frac{i!}{(t+1)! (i-t-1)!} + \frac{i!}{(t+2)! (i-t-2)!} - \dots \right]_{s=i}$$

et en partageant la somme \sum en l sommes partielles, correspondant respectivement à $s \equiv 0, s \equiv 1, \dots, s \equiv l-1 \pmod{l}$, on obtient

$$\sum_{h=0}^{h=l-2} \frac{r^{-hkl^n} (1 - \zeta^r)^i}{i} = \frac{1}{i} [P_0 X_k(1) + P_1 X_k(\zeta) + \dots + P_{l-1} X_k(\zeta^{l-1})].$$

Pour transformer cette égalité en congruence relative au module l^{n+1} , démontrons d'abord que P_t contient toujours autant de facteurs l que i . Si t n'est pas nul, chaque terme de P_t contient l autant de fois que i : c'est ce qu'il est aisément de voir, à l'aide du théorème suivant, facile à démontrer :

« Si p est un nombre premier et que le nombre A soit représenté dans le système de numération de base p par

$$A = a + a_1 p + \dots + a_{m-1} p^{m-1},$$

l'exposant de la plus haute puissance de p qui divise $A!$ est

$$\frac{A - (a + a_1 + \dots + a_{m-1})}{p - 1}.$$

[Kummer^{12.}]

Quant à P_0 , il contient de même autant de facteurs l que i , car la somme $P_0 + P_1 + \dots + P_{l-1}$ étant la somme des coefficients binômaux alternativement changés de signe est égale à $(1 - 1)^i = 0$.

Les $\frac{P_i}{i}$ peuvent donc être considérés comme des entiers pour le module l^{n+1} , et l'on a, pour toute valeur de i , en tenant compte des congruences $X_k(\zeta^s) \equiv s^{kl^n} X_k(\zeta)$ et $X_k(1) \equiv 0$, (mod l^{n+1}) :

$$\sum_{h=0}^{h=l-2} \frac{r^{-hkl^n}(1 - \zeta^{rh})^i}{i} \equiv \frac{1}{i} [1^{kl^n} P_1 + 2^{kl^n} P_2 + \dots + (l-1)^{kl^n} P_{l-1}] X_k(\zeta), \pmod{l^{n+1}}.$$

Si l'on développe, d'autre part, $(1 - e^u)^i$ par la formule du binôme et que l'on prenne la kl^n ème dérivée pour $u = 0$, on a

$$\frac{d_0^{kl^n}(1 - e^u)^i}{du^{kl^n}} = \sum_{s=0}^{s=i} (-1)^i \frac{i!}{s!(i-s)!} s^{kl^n};$$

d'où, en décomposant cette somme comme plus haut et tenant compte de la congruence

$$(s + ml)^{kl^n} \equiv s^{kl^n}, \pmod{l^{n+1}},$$

on déduit la congruence

$$\frac{d_0^{kl^n}(1 - e^u)^i}{du^{kl^n}} \equiv [1^{kl^n} P_1 + 2^{kl^n} P_2 + \dots + (l-1)^{kl^n} P_{l-1}], \pmod{l^{n+1}}.$$

On a, par suite,

$$\sum_{h=0}^{h=l-2} \frac{r^{-hkl^n}(1 - \zeta^{rh})^i}{i} \equiv \frac{1}{i} \frac{d_0^{kl^n}(1 - e^u)^i}{du^{kl^n}} \cdot X_k(\zeta), \pmod{l^{n+1}},$$

et

$$\sum_{h=0}^{h=l-2} r^{-hkl^n} \log \left[\frac{f(\zeta^{rh})}{f(1)} \right] \equiv \sum_i \frac{C_i}{i f(1)^i} \cdot \frac{d_0^{kl^n}(1 - e^u)^i}{du^{kl^n}} \cdot X_k(\zeta), \pmod{l^{n+1}}.$$

Or, d'après (10), la somme $\sum_i \frac{C_i (1 - e^u)^i}{i f(1)^i}$ n'est autre chose que le développement, ordonné suivant les puissances de $1 - e^u$, de $\log \left[\frac{f(e^u)}{f(1)} \right]$, c'est-à-dire de $\log f(e^u) - \log f(1)$ (1).

(1) \log désigne ici le logarithme népérien, car e^u étant égal à 1 pour $u = 0$, le développement par la série de Mac Laurin est convergent dans le voisinage de $u = 0$.

On a donc

$$(11) \quad \sum_{h=0}^{h=l-2} r^{-hkl^n} \log \left[\frac{f(\zeta^{r^h})}{f(1)} \right] \equiv \frac{d_o^{kl^n} \log f(e^u)}{du^{kl^n}} \cdot X_k(\zeta), \pmod{l^{n+1}}.$$

Donnant alors à k les valeurs $1, 2, \dots, l-2$, faisant la somme, et mettant à part la valeur $h=0$, on obtient, en remarquant que $r^{-hl^n} + r^{-2hl^n} + \dots + r^{-(l-2)hl^n}$ est congru à -1 pour le module l^{n+1} ,

$$(l-1) \log \left[\frac{f(\zeta)}{f(1)} \right] \equiv \log \left[\frac{Nf(\zeta)}{f(1)^{l-1}} \right] + \frac{d_o^{l^n} \log f(e^u)}{du^{l^n}} X_1(\zeta) + \dots, \pmod{l^{n+1}},$$

c'est-à-dire la formule (8) qu'il s'agissait de démontrer.

CAS PARTICULIER. — Dans le cas particulier de $n=0$, on a simplement, comme $Nf(\zeta)$ est congru à 1 , ainsi que $f(1)^{l-1}$, pour le module l :

$$(12) \quad - \log \left[\frac{f(\zeta)}{f(1)} \right] \equiv \frac{d_o \log f(e^u)}{du} X_1(\zeta) + \frac{d_o^2 \log f(e^u)}{du^2} X_2(\zeta) + \dots + \frac{d_o^{l-2} \log f(e^u)}{du^{l-2}} X_{l-2}(\zeta), \pmod{l},$$

car on a $\log \left[\frac{Nf(\zeta)}{f(1)^{l-1}} \right] \equiv 0, \pmod{l}$, vu le théorème X qui va être démontré.

APPLICATION. — Comme application, nous calculerons le logarithme, pour le module l , de l'unité fréquemment employée

$$E_n(\zeta) = \varepsilon(\zeta) \cdot \varepsilon(\zeta^r)^{r-2n} \cdot \varepsilon(\zeta^{r^2})^{r-4n} \dots \varepsilon(\zeta^{r^{n-1}})^{r-2(n-1)n},$$

expression où $\varepsilon(\zeta)$ désigne l'*unité circulaire* (§§ 98 et 138)

$$\varepsilon(\zeta) = \sqrt{\frac{\zeta^r - 1}{\zeta - 1} \cdot \frac{\zeta^{-r} - 1}{\zeta^{-1} - 1}}.$$

On a

$$\log \left[\frac{E_n(\zeta)}{E_n(1)} \right] = \sum_{h=0}^{h=\mu-1} r^{-2hn} \log \left[\frac{\varepsilon(\zeta^{r^h})}{\varepsilon(1)} \right] \equiv \frac{1}{2} \sum_{h=0}^{h=2\mu-1} r^{-2hn} \log \left[\frac{\varepsilon(\zeta^{r^h})}{\varepsilon(1)} \right], \pmod{l};$$

la congruence des deux derniers membres résulte des relations

$$r^{h+\mu} \equiv -r^h, \quad \text{et} \quad r^{-2(h+\mu)n} \equiv r^{-2hn}, \pmod{l},$$

et de ce que $\varepsilon(\zeta^{r^{h+\mu}}) = \varepsilon(\zeta^{-r^h}) = \varepsilon(\zeta^{r^h})$.

On a donc, d'après la formule (9), où l'on prend $n=0$ et $f(\zeta) = \varepsilon(\zeta)$, la congruence

$$\log \left[\frac{E_n(\zeta)}{E_n(1)} \right] \equiv \frac{1}{2} \frac{d_o^{2n} \log \varepsilon(e^u)}{du^{2n}} X_{2n}(\zeta), \pmod{l}.$$

Pour calculer la dérivée qui figure dans le second membre, partons du développement connu

$$\frac{1}{e^u - 1} = \frac{1}{u} - \frac{1}{2} + \frac{B_1 u}{2!} - \frac{B_2 u^2}{4!} + \frac{B_3 u^3}{6!} - \dots$$

qui donne, si l'on change u en ru et qu'on retranche le développement ci-dessus du nouveau multiplié par r :

$$\frac{r}{e^{ru} - 1} - \frac{1}{e^u - 1} = -\frac{1}{2}(r-1) + \frac{(r^2-1)B_1 u}{2!} - \frac{(r^4-1)B_2 u^3}{4!} + \dots,$$

et en intégrant :

$$\log \left[\frac{e^{ru} - 1}{e^u - 1} \right] - (r-1)u = \log r - \frac{1}{2}(r-1)u + \frac{(r^2-1)B_1 u^2}{2 \cdot 2!} - \dots,$$

la constante d'intégration étant égale à $\log r$, comme on le voit en faisant $u=0$; on a, par suite,

$$\log \varepsilon(e^u) = \log \left(\frac{e^{ru} - 1}{e^u - 1} \cdot \frac{e^{-\frac{1}{2}ru}}{e^{-\frac{1}{2}u}} \right) = \log r + \frac{(r^2-1)B_1 u^2}{2 \cdot 2!} - \frac{(r^4-1)B_2 u^4}{4 \cdot 4!} + \dots.$$

On a, dès lors,

$$(13) \quad \frac{d_{\vartheta}^{2n} \log \varepsilon(e^u)}{du^{2n}} = (-1)^{n+1} (r^{2n} - 1) \frac{B_n}{2n},$$

et enfin

$$(14) \quad \log \left[\frac{E_n(\zeta)}{E_n(1)} \right] \equiv (-1)^{n+1} (r^{2n} - 1) \frac{B_n}{4n} X_{2n}(\zeta), \quad (\text{mod } l).$$

REMARQUE. — L'utilité des logarithmes pour le module l^{n+1} tient, d'une part, à ce que, évidemment, ces développements ont la propriété fondamentale qui correspond à celle des logarithmes eux-mêmes : le logarithme d'un produit est congru à la somme des logarithmes des facteurs; — et, d'autre part, au théorème suivant :

THÉORÈME X. — Deux nombres congrus pour le module l^{n+1} , ainsi que les entiers qu'on en déduit par la substitution de 1 à ζ , ont aussi leurs logarithmes congrus pour le même module. [Kummer¹².]

Démonstration. — Si, en effet, $f(\zeta)$ et $\varphi(\zeta)$ sont ces deux nombres et qu'on pose

$$x = \frac{f(\zeta) - f(1)}{f'(1)}, \quad y = \frac{\varphi(\zeta) - \varphi(1)}{\varphi'(1)},$$

on aura

$$\left. \begin{aligned} \log \left[\frac{f(\zeta)}{f(1)} \right] &\equiv x - \frac{1}{2}x^2 + \frac{1}{3}x^3 - \dots, \\ \log \left[\frac{\varphi(\zeta)}{\varphi(1)} \right] &\equiv y - \frac{1}{2}y^2 + \frac{1}{3}y^3 - \dots, \end{aligned} \right\} \quad (\text{mod } l^{n+1}).$$

On a, vu les hypothèses,

$$x \equiv y \pmod{l^{n+1}},$$

d'où évidemment

$$\frac{x^k}{k} \equiv \frac{y^k}{k} \pmod{l^{n+1}},$$

au moins si k n'est pas divisible par l . Mais cette congruence est vraie même si k est un multiple de l , soit cl^a , l^a étant la plus haute puissance de l qui entre dans k : car en posant

$$y = x + l^{n+1}z,$$

la formule du binôme donne

$$y^{cl^a} \equiv x^{cl^a} + cl^{n+a+1}x^{cl^a-1}z \pmod{l^{n+a+2}},$$

et, par suite,

$$\frac{y^{cl^a}}{cl^a} \equiv \frac{x^{cl^a}}{cl^a} \pmod{l^{n+1}}.$$

Les deux développements $\log \left[\frac{f(\zeta)}{f(1)} \right]$ et $\log \left[\frac{\varphi(\zeta)}{\varphi(1)} \right]$ étant congrus terme à terme, le théorème est démontré.

§ VII. — Expression de l'indice de l'unité $E_n(\zeta)$.

Étant donné un idéal premier quelconque \mathfrak{p} , de degré f , il est possible de déterminer une racine primitive $\varphi^{(1)}$ de cet idéal, telle que l'on ait

$$\zeta \equiv \varphi^{\frac{p^f-1}{l}}.$$

p désignant le nombre premier divisible par \mathfrak{p} . Cette racine étant ainsi déterminée, l'indice d'un nombre quelconque α du corps $c(\zeta)$ est le même, soit qu'on le prenne par rapport à la racine φ , soit qu'on le définisse comme au paragraphe 113. En d'autres termes, si l'on pose

$$\alpha \equiv \varphi^l, \quad (\mathfrak{p}), \quad \left\{ \frac{\alpha}{\mathfrak{p}} \right\} = \zeta^l \equiv \alpha^{\frac{p^f-1}{l}}, \quad (\mathfrak{p}),$$

on a toujours

$$I \equiv l', \quad (l).$$

Pour déterminer l'indice de l'unité $E_n(\zeta)$, nous allons d'abord établir les propriétés fondamentales du nombre

$$\Psi_q(\zeta) = \sum \zeta^{-(q+1)h + \text{Ind}(\varphi^h + 1)}$$

(¹) Voir Hilbert, paragraphe 9.

où l'indice a la signification qu'on vient de rappeler et où la sommation s'étend à toutes les valeurs

$$h = 0, 1, 2, \dots, p^f - 2,$$

à l'exception de

$$h = \frac{1}{2}(p^f - 1),$$

valeur pour laquelle $\rho^h + 1$ serait congru à zéro, et pour laquelle l'indice n'aurait pas de sens. [Kummer¹².]

Première propriété fondamentale : Ψ_q ne dépend que des périodes à f termes. En effet, on a

$$(\rho^h + 1)^p = \rho^{hp} + 1, \quad (\text{mod } p) \text{ et par suite } (\text{mod } \mathfrak{p});$$

donc, on a

$$\Psi_q(\zeta^p) = \sum \zeta^{-(q+1)hp + p \text{Ind}(\zeta^h + 1)} = \sum \zeta^{-(q+1)hp + \text{Ind}(\zeta^h + 1)^p} = \sum \zeta^{-(q+1)hp + \text{Ind}(\zeta^{hp} + 1)} = \Psi_q(\zeta),$$

car les hp reproduisent les h à l'ordre près, $(\text{mod } p^f - 1)$. Comme p est congru à r^e , $(\text{mod } l)$, r étant une racine primitive $(\text{mod } l)$, puisqu'il appartient à l'exposant f , Ψ_q admet la substitution (ζ, ζ^{r^e}) et ses puissances, et ne dépend, par suite, que des périodes à f termes⁽¹⁾.

Deuxième propriété fondamentale. On a

$$\Psi_q(\zeta) \Psi_q(\zeta^{-1}) = p^f, \quad (q \equiv 0 \text{ et } \equiv -1 \pmod{l}).$$

En effet,

$$\Psi_q(\zeta) \Psi_q(\zeta^{-1}) = \sum \sum \zeta^{-(q+1)(h-k) + \text{Ind}(\zeta^h + 1) - \text{Ind}(\zeta^k + 1)} = p^f - 2 + \sum \sum \zeta^{-(q+1)(h-k) + \text{Ind}(\zeta^h + 1) - \text{Ind}(\zeta^k + 1)},$$

le dernier membre étant obtenu en prenant d'abord $h = k$, ce qui donne $p^f - 2$ termes égaux à 1, et la somme double s'étendant ensuite à toutes les valeurs inégales de h et k .

Posons

$$\rho^{h-k} \equiv \rho^{k'}, \quad \frac{\rho^h + 1}{\rho^k + 1} \equiv \rho^{h'}, \quad (\mathfrak{p});$$

il vient

$$\Psi_q(\zeta) \Psi_q(\zeta^{-1}) = p^f - 2 + \sum \sum \zeta^{q+k'-h'}, \quad (h', k' = 1, 2, \dots, p^f - 2, h' \equiv k'),$$

ou encore

$$\Psi_q(\zeta) \Psi_q(\zeta^{-1}) = p^f - 2 - \sum \zeta^{qk'} + \sum \sum \zeta^{(q+1)k'-h'},$$

(1) $ef = l - 1$.

h' et k' pouvant alors être égaux dans la somme double. En sommant par rapport à h' , on trouve $\Sigma \zeta^{-h'} = -1$, donc

$$\Psi_q(\zeta) \Psi_q(\zeta^{-1}) = p^f - 2 - \Sigma \zeta^{qk'} - \Sigma \zeta^{(q+1)k'},$$

et, par suite, si q est $\equiv 0$ ou $\equiv -1 \pmod{l}$, on a

$$\Psi_q(\zeta) \Psi_q(\zeta^{-1}) = p^f.$$

Si $q \equiv 0$ ou $\equiv -1 \pmod{l}$, la relation donne $\Psi_q(\zeta) \Psi_q(\zeta^{-1}) = +1$, comme cela résulte de $\Psi_0 = \Psi_{-1} = -1$, et de $\Psi_{q+l} = \Psi_q$.

Troisième propriété fondamentale. Si f est pair, on a

$$\Psi_q(\zeta) = p^{\frac{f}{2}};$$

si f est impair, on a

$$\Psi_q(\zeta) = \pm \mathfrak{p}^{m_0} (s \mathfrak{p})^{m_1} \dots (s^{e-1} \mathfrak{p})^{m_{e-1}},$$

expression où les exposants m_i ont les valeurs suivantes (1) :

$$m_i = S_{\mu-i} + S_{\mu-i+\text{ind } q} - S_{\mu-i+\text{ind}(q+1)},$$

S_h désignant la somme

$$S_h = \frac{1}{l} (r_h + r_{h+e} + \dots + r_{h+(f-1)e}).$$

La première partie de l'énoncé résulte immédiatement de ce que l'on a $p^{\frac{f}{2}} \equiv -1 \pmod{l}$, et, par suite, $\Psi_q(\zeta^{-1}) = \Psi_q(\zeta^{\frac{f}{2}}) = \Psi_q(\zeta)$, et de la relation $\Psi_q(\zeta) \Psi_q(\zeta^{-1}) = p^f$.

En vertu de cette même relation, il est clair aussi, pour f impair, que Ψ_q ne peut contenir que l'idéal premier \mathfrak{p} et ses conjugués, et il ne reste qu'à déterminer leurs exposants et l'unité dont le produit est affecté.

Pour cela, nous allons substituer à ζ une puissance de ρ qui lui soit congrue $\pmod{\mathfrak{p}^n}$. Posons pour abréger

$$l' = \frac{p^f - 1}{l};$$

on a successivement

$$\begin{aligned} \zeta^p &\equiv \rho^{l'p}, & (\mathfrak{p}^2), \\ \zeta^{p^k} &\equiv \rho^{l'p^k}, & (\mathfrak{p}^{k+1}), \\ \zeta^{p^{nf}} &= \zeta \equiv \rho^{l'p^{nf}}, & (\mathfrak{p}^{nf+1}). \end{aligned}$$

(1) Ind désigne l'indice par rapport au module \mathfrak{p} et à la racine primitive ρ , ind l'indice par rapport au module l et à la racine primitive r .

Evaluons maintenant $\Psi_q(\zeta^{r-i})$; en posant $q+i \equiv r^s$, (mod l), prenant $\text{Ind}(\varphi^{hp^{nf}} + 1)$ au lieu de $\text{Ind}(\varphi^h + 1)$, on a

$$\Psi_q(\zeta^{r-i}) = \Sigma \zeta^{-hr_{s-i} + r-i} \text{Ind}(\varphi^h + 1),$$

d'où la congruence

$$\Psi_q(\zeta^{r-i}) \equiv \Sigma \zeta^{-l'p^{nf}hr_{s-i}} (\varphi^{hp^{nf}} + 1)^{l'p^{nf}r_{s-i}}, \quad (\mathfrak{p}^{nf+1}),$$

h prenant cette fois dans la somme toutes les valeurs $0, 1, \dots, q^t - 2$, la valeur exclue précédemment $h = \frac{1}{2}(p^f - 1)$ donnant ici un terme $\equiv 0$.

Si l'on développe par la formule du binôme, et qu'on effectue la sommation par rapport à h , il ne reste que les termes où l'exposant de φ est un multiple de $p^f - 1 = ll'$; soient sll' ces exposants, on a

$$\Psi_q(\zeta^{r-i}) \equiv \Sigma \frac{(p^f - 1) \cdot (l'p^{nf}r_{s-i})!}{(l'r_{s-i} + sll')! (l'p^{nf}r_{s-i} - l'r_{s-i} - sll')!}, \quad (\mathfrak{p}^{nf+1}),$$

ou, en posant

$$s = r_{s-i} \frac{(p^{nf} - 1)}{l} - z$$

et remplaçant ζ^{r-i} par ζ :

$$\Psi_q(\zeta) \equiv \Sigma \frac{(p^f - 1) (l'p^{nf}r_{s-i})!}{(l'p^{nf}r_{s-i} - ll'z)! [(r_{s-i} - r_{s-i})l'p^{nf} + ll'z]!}$$

pour le module $(s^i \mathfrak{p})^{nf+1}$.

La somme doit être étendue à toutes les valeurs de z qui ne rendent négatifs aucun des deux facteurs du dénominateur. Comme c'est un entier rationnel, tout revient, pour trouver l'exposant de $s^i \mathfrak{p}$ dans $\Psi_q(\zeta)$, à trouver quelle est la plus haute puissance de p qui divise la somme Σ .

En s'appuyant sur le théorème relatif aux factorielles énoncé dans le paragraphe V, on trouve aisément, en supposant $r_{s-i} - r_{s-i} > 0$, que c'est le terme où $z=0$ qui contient p avec le plus petit exposant, et nous avons à calculer le nombre de facteurs p contenus dans

$$N = \frac{(l'p^{nf}r_{s-i})!}{(l'p^{nf}r_{s-i})! [(r_{s-i} - r_{s-i})l'p^{nf}]!}.$$

Pour cela, cherchons d'une manière générale le nombre de facteurs p contenus dans $(l'p^{nf}r_h)!$ Soit

$$l'r_h = a + a_1 p + \dots + a_{f-1} p^{f-1},$$

les a étant inférieurs à p et non négatifs : le nombre des facteurs p de la factorielle sera, d'après le théorème rappelé ci-dessus :

$$\frac{l'p^{nf}r_h - (a + a_1 + \dots + a_{f-1})}{p - 1}.$$

Multiplions $l'r_h$ par l et remplaçons ll' par $p^f - 1$, nous avons

$$p^f r_h = r_h + la + la_1 p + \dots + la_{f-1} p^{f-1},$$

d'où, le second membre devant être divisible par p^f :

$$\begin{aligned} r_h + la &= \alpha p, \\ \alpha + la_1 &= \alpha_1 p, \\ \dots & \dots \dots \dots \\ \alpha_{f-2} + la_{f-1} &= \alpha_{f-1} p, \end{aligned}$$

les α étant positifs et inférieurs à l ; et comme on a $p \equiv r^{me}$, ($\text{mod } l$), m premier à f , puisque p appartient à l'exposant f , on a les congruences

$$r^h \equiv \alpha r^{me}, \quad \alpha \equiv \alpha_1 r^{me}, \quad \dots, \quad \alpha_{f-2} \equiv \alpha_{f-1} r^{me}, \quad (\text{mod } l),$$

d'où

$$\alpha \equiv r^{h-me}, \quad \alpha_1 \equiv r^{h-2me}, \quad \dots, \quad \alpha_{f-1} \equiv r^h, \quad (\text{mod } l);$$

et comme tous les α sont restes positifs, mod l , on a

$$\alpha = r_{h-me}, \quad \alpha_1 = r_{h-2me}, \quad \dots, \quad \alpha_{f-1} = r_h.$$

Puis, en ajoutant membre à membre les égalités $r_h + la = ap$, etc., on a :

$$l(a + a_1 + \dots + a_{f-1}) = (p - 1)(r_{h-me} + r_{h-2me} + \dots + r_h).$$

D'ailleurs, le dernier facteur du second membre est égal, à l'ordre des termes près, à

$$r_h + r_{h+e} + \dots + r_{h+(f-1)e},$$

parce que m est premier à f . Désignons par lS_h cette somme, qui est en effet divisible par l (1); on aura pour le nombre de facteurs p de la factorielle :

$$\frac{l'p^{nf}r_h}{p-1} - S_h.$$

Posant pour abréger $r_{-i} - r_{-i} = \hat{z}$, entier positif et inférieur à l , on aura pour le nombre de facteurs p de N , c'est-à-dire pour l'exposant m_i :

$$m_i = S_{-i} + S_{\hat{z}} - S_{-i}.$$

Et pour obtenir l'expression de l'énoncé, il suffit de remarquer que l'on a

$$S_{h+\mu} = f - S_h$$

et que de l'expression de S résulte la congruence

$$r^{-i} - r^{z-i} \equiv \hat{z} \equiv r^{-i} - (q+1)r^{-i} \equiv -qr^{-i} \equiv r^u r^{-i} r^{\text{ind } q},$$

d'où l'on déduit $\hat{z} = r_{\mu-i+\text{ind } q}$.

(1) Excepté pour $f=1$, cas déjà traité paragraphe 1.

Il reste, pour achever la démonstration, à lever la restriction relative au signe de $r_{-i} - r_{\star-i}$. Or, de $r_{\star+h} = l - r_h$ on déduit

$$r_{-i} - r_{\star-i} = -(r_{-i-\mu} - r_{\star-i-\mu}),$$

de sorte que si i ne vérifie pas la condition $r_{-i} - r_{\star-i} > 0$, $\mu - i$ la vérifie. D'autre part, si l'on fait le produit $\Psi_q(\zeta)\Psi_q(\zeta^{-1})$, qui est égal à p^f , il en résulte $m_i + m_{i+\mu} = f$. On a donc $m_i = f - m_{i+\mu}$, et comme on a aussi $S_h = f - S_{h+\mu}$, on retombe sur la même expression de m_i que dans la première hypothèse.

Enfin l'unité $E(\zeta)$, qui affecte le produit des idéaux premiers, est égale à ± 1 , car, d'une part, elle ne doit dépendre que des périodes à f termes ($f > 1$), et, d'autre part, on doit avoir $E(\zeta)E(\zeta^{-1}) = 1$ à cause de l'égalité $\Psi_q(\zeta)\Psi_q(\zeta^{-1}) = p^f$; ceci exige $E(\zeta) = \pm \zeta_k$, et k doit être nul d'après la première condition.

REMARQUE. — La démonstration précédente s'applique encore aux idéaux du premier degré. Si l'on fait, en effet, $f = 1$,

$$lS_h \text{ se réduit à } r_h, \text{ et } m_i \text{ à } \frac{1}{l}(r_{\mu-i} + r_{\mu-i+\text{ind } q} - r_{\mu-i+\text{ind } (q+1)}),$$

expression prenant la valeur 1 ou la valeur 0, suivant que $s^i p$ figure dans $\Psi_q(\zeta)$ avec l'exposant 1 ou l'exposant 0; — c'est le résultat du théorème 1.

Cette remarque permet de donner une expression unique pour $\Psi_q(\zeta)$, que f soit égal ou supérieur à 1; on a

$$\Psi_q(\zeta) = \pm \prod_{k=0}^{k=l-2} (s^k p)^{m_k},$$

l'exposant m_k égal à 0 ou 1 étant donné par la formule

$$m_k = \frac{1}{l}(r_{\mu-k} + r_{\mu-k+\text{ind } q} - r_{\mu-k+\text{ind } (q+1)}).$$

La formule s'applique aussi pour f pair; elle est donc générale.

INDICE DE $E_n(\zeta)$. — L'identité des propriétés de $\Psi_q(\zeta)$ ⁽¹⁾, quel que soit l'exposant auquel appartient le nombre p correspondant, va nous permettre de trouver, par un calcul unique, s'appliquant à tous les cas, une expression de l'indice de $E_n(\zeta)$ à l'aide de ce nombre.

Cette expression est la suivante :

$$(15) \quad \text{Ind } E_n(\zeta) \equiv \frac{r^{2n} - 1}{2} \cdot \frac{1}{1 + q^{l-2n} - (q+1)^{l-2n}} \cdot \frac{d_0^{l-2n} \log \Psi_q(e^u)}{du^{l-2n}}, \quad (\text{mod } l).$$

[Kummer¹².]

⁽¹⁾ Nous avons utilisé dans le paragraphe 1 et le paragraphe actuel deux formes différentes de $\Psi_q(\zeta)$, mais on passe aisément de l'une à l'autre. (Voir Weber, *Alg. sup.*)

Pour la démontrer, calculons d'abord la dérivée, en partant du développement

$$\Psi_q(e^u) = \Sigma e^{u(-(q+1)h + \text{Ind}(\varphi^h + 1))}.$$

On a, en posant pour abréger,

$$m = l - 2n - 1, \quad \mathbf{U} = \frac{\mathbf{I}}{\Psi_q(e^u)},$$

$$\frac{d^{l-2n} \log \Psi_q(e^u)}{du^{l-2n}} = \frac{d^m \left(\frac{d\Psi_q(e^u)}{du} \cdot \mathbf{U} \right)}{du^m};$$

d'où, par la formule de Leibnitz :

$$\frac{d^{l-2n} \log \Psi_q(e^u)}{du^{l-2n}} = \frac{d^{m+1} \Psi_q}{du^{m+1}} \cdot \mathbf{U} + \frac{m}{1} \cdot \frac{d^m \Psi_q}{du^m} \cdot \frac{d\mathbf{U}}{du} + \dots$$

Comme

$$\Psi_q(\zeta) \Psi_q(\zeta^{-1}) = p^f,$$

on a

$$\Psi_q(e^u) \Psi_q(e^{-u}) = p^f + \mathbf{V} \mathbf{W},$$

où \mathbf{W} désigne un polynôme en e^u à coefficients entiers et où

$$\mathbf{V} = 1 + e^u + e^{2u} + \dots + e^{(l-1)u}$$

(parce que la différence $\Psi_q(x) \Psi_q(x^{-1}) - \Psi_q(\zeta) \Psi_q(\zeta^{-1})$, admettant la racine ζ , admet toutes les racines de $1 + x + \dots + x^{l-1}$).

On a donc

$$\Psi_q(e^{-u}) = \mathbf{U}(p^f + \mathbf{V} \mathbf{W}),$$

$$\frac{d^i \Psi_q(e^{-u})}{du^i} = \frac{d^i \mathbf{U}}{du^i} (p^f + \mathbf{V} \mathbf{W}) + \frac{1}{i} \cdot \frac{d^{i-1} \mathbf{U}}{du^{i-1}} \cdot \frac{d \mathbf{V} \mathbf{W}}{du} + \dots$$

Pour $u=0$, \mathbf{V} et ses $l-2$ premières dérivées s'annulent, mod l , et comme on a $p^f \equiv 1$, pour ce même module, on déduit du développement précédent

$$\frac{d_0^i \Psi_q(e^{-u})}{du^i} \equiv \frac{d_0^i \mathbf{U}}{du^i}, \quad (\text{mod } l),$$

pour $i=0, 1, 2, \dots, l-2$.

On peut encore écrire

$$\frac{d_0^i \mathbf{U}}{du^i} \equiv (-1)^i \frac{d_0^i \Psi_q(e^u)}{du^i} \equiv (-1)^i \mathbf{D}_i, \quad (\text{mod } l).$$

Donc, on a

$$\frac{d_0^{l-2n} \log \Psi_q(e^u)}{du^{l-2n}} \equiv \mathbf{D}_{m+1} \mathbf{D}_0 - \frac{m}{1} \mathbf{D}_m \mathbf{D}_1 + \frac{m(m-1)}{1 \cdot 2} \cdot \mathbf{D}_{m-1} \mathbf{D}_2 - \dots, \quad (\text{mod } l).$$

Mais

$$\mathbf{D}_i = \Sigma [-(q+1)h + \text{Ind}(\varphi^h + 1)]^i$$

$$\left(h = 0, 1, \dots, p^f-2, \text{ except } \frac{p^f-1}{2} \right).$$

Désignons le crochet par C_h , nous aurons

$$d = \frac{d_0^{l-2n} \log \Psi_q(e^u)}{du^{l-2n}} \equiv \Sigma \Sigma (C_h^{m+1} C_k^0 - \frac{m}{1} \cdot C_h^m C_k^1 + \dots), \pmod{l},$$

les valeurs $h = \frac{1}{2}(p^f - 1)$, $k = \frac{1}{2}(p^f - 1)$ étant exclues de la sommation, c'est-à-dire

$$\begin{aligned} d &\equiv \Sigma \Sigma C_h (C_h - C_k)^m \\ &\equiv \Sigma \Sigma [-(q+1)h + \text{Ind}(\zeta^h + 1)] [-(q+1)(h-k) + \text{Ind}(\zeta^h + 1) - \text{Ind}(\zeta^k + 1)]^m. \end{aligned}$$

Comme tous les termes sont congrus à zéro pour $h = k$, employons la transformation déjà utilisée

$$\zeta^{k-h} \equiv \zeta^{k'}, \quad \frac{\zeta^k + 1}{\zeta^h + 1} \equiv \zeta^{h'}, \pmod{p};$$

nous avons

$$\begin{aligned} \Sigma \Sigma [-(q+1) \text{Ind}(\zeta^{h'} - 1) + \text{Ind}(\zeta^{k'} - 1) + q \text{Ind}(\zeta^{k'} - \zeta^{h'})] [(q+1)k' - h']^m, \pmod{l}. \\ (h', k' = 1, 2, \dots, p^f - 1, h' \neq k'). \end{aligned}$$

Évaluons séparément les trois sommes correspondant aux termes du premier crochet, en sommant d'abord par rapport à k' ; pour plus de facilité, on ajoute dans la somme double les termes où $h' = k'$, en les retranchant d'autre part. La première somme, comme $p^f - 1$ est $\equiv 0 \pmod{l}$, que $\Sigma k'^i$ est $\equiv 0$ pour $i = 1, 2, \dots, l-2$, et que l'on a

$$\sum_{k'} [(q+1)k' - h']^{l-2n-1} \equiv (p^f - 2)h'^{l-2n-1} \equiv -h'^{l-2n-1},$$

devient

$$(q+1)(1 + q^{l-2n-1}) \Sigma h'^{l-2n-1} \text{Ind}(\zeta^{h'} - 1).$$

On trouve de même pour la seconde :

$$- [q^{l-2n-1} + (q+1)^{l-2n-1}] \Sigma h'^{l-2n-1} \text{Ind}(\zeta^{h'} - 1).$$

Pour évaluer la troisième, ajoutons et retranchons les termes relatifs à $h' = 0$ et à $k' = 0$:

$$- q[1 + (q+1)^{l-2n-1}] \Sigma h'^{l-2n-1} \text{Ind}(\zeta^{h'} - 1);$$

le reste de la somme

$$q \Sigma \Sigma [\text{Ind}(\zeta^{h'} - 1) + k'] (rk' - h')^{l-2n-1} \quad \begin{pmatrix} h' = 1, 2, \dots, p^f - 2 \\ k' = 0, 1, 2, \dots, p^f - 2 \end{pmatrix}$$

est congru à zéro.

On a donc en réunissant les trois sommes

$$\frac{d_0^{l-2n} \log \Psi_q(e^u)}{du^{l-2n}} = [1 + q^{l-n} - (q+1)^{l-2n}] \Sigma h'^{l-2n-1} \text{Ind}(\zeta^{h'} - 1), \pmod{l}.$$

Dans la somme, tous les termes pour lesquels h' est $\equiv 0 \pmod{l}$, disparaissent, et si l'on pose $h' = i + lk \left(\begin{smallmatrix} i=1, 2, \dots, l-1 \\ k=0, 1, 2, \dots, l'-1 \end{smallmatrix} \right)$, on a

$$\Sigma \equiv \Sigma \Sigma i^{l-2n-1} \text{ind} (\zeta^{i+kl} - 1).$$

Mais on a évidemment toujours la congruence

$$(\zeta^i - 1)(\zeta^{i+l} - 1)(\zeta^{i+2l} - 1) \dots (\zeta^{i+(l'-1)l} - 1) \equiv 1 - \zeta^{l'i} \pmod{\mathfrak{p}},$$

et, par suite,

$$\Sigma \text{ind} (\zeta^{i+kl} - 1) \equiv \text{ind} (1 - \zeta^{l'i}) \equiv \text{ind} (1 - \zeta^i) \pmod{l}.$$

Donc, on a

$$\Sigma \equiv \Sigma i^{l-2n-1} \text{ind} (1 - \zeta^i) \pmod{l}.$$

En remplaçant i par ir , ce qui ne change pas Σ , multipliant par r^{2n} et retranchant l'égalité primitive de la nouvelle, on obtient

$$(r^{2n} - 1) \Sigma \equiv \Sigma i^{l-2n-1} \text{ind} \left(\frac{1 - \zeta^{ri}}{1 - \zeta^i} \right).$$

Si l'on change enfin i en r^h , on a

$$(r^{2n} - 1) \Sigma \equiv \Sigma r^{-2nh} \text{ind} \left(\frac{1 - \zeta^{r^{h+1}}}{1 - \zeta^h} \right) \equiv 2 \text{ind} E_n(\zeta),$$

puisque

$$E_n(\zeta) = \varepsilon(\zeta) \varepsilon(\zeta^r)^{r-2n} \dots \varepsilon(\zeta^{r^{l-1}})^{r-2(l-1)n}$$

et que l'on a

$$\varepsilon(\zeta^{r^h}) = \frac{1 - \zeta^{r^{h+1}}}{1 - \zeta^h} \cdot \zeta^{\frac{r^h(l-r)}{2}}.$$

Par conséquent, on a pour expression de l'indice de $E_n(\zeta)$, $(\text{mod } \mathfrak{p})$:

$$\text{ind } E_n(\zeta) \equiv \frac{r^{2n} - 1}{2} \cdot \frac{1}{1 + q^{l-2n} - (q + 1)^{l-2n}} \cdot \frac{d_0^{l-2n} \log \Psi_q(e^u)}{du^{l-2n}}, \pmod{l}. \quad \text{C. q. f. d.}$$

REMARQUE. — L'indice est $\equiv 0$ pour toute unité E_n , telle que $l - 2n$ ne soit pas divisible par f .

En effet, d'après la première propriété fondamentale de Ψ_q , on a

$$\Psi_q(\zeta) = \Psi_q(\zeta^{r^e}),$$

et, par suite,

$$\Psi_q(e^u) = \Psi_q(e^{ur^e}) + \text{V.W.}$$

et

$$\frac{d_0^{l-2n} \log \Psi_q(e^u)}{du^{l-2n}} \equiv \frac{d_0^{l-2n} \log \Psi_q(e^{ur^e})}{du^{l-2n}} \equiv r^{(l-2n)e} \frac{d_0^{l-2n} \log \Psi_q(e^u)}{du^{l-2n}}, \pmod{l}.$$

Si donc l'on n'a pas

$$r^{(l-2n)e} - 1 \equiv 0, \pmod{l},$$

c'est-à-dire si $l - 2n$ n'est pas divisible par l , il faut que $\frac{d_0^{l-2n} \log \Psi_q(e^u)}{du^{l-2n}}$ soit $\equiv 0$, c'est-à-dire que $\text{ind } E_n(\zeta) = 0$.

§ VIII. — *Étude des idéaux dont la $l^{\text{ème}}$ puissance est un idéal principal.*

Le résultat final de cette étude est le

THÉORÈME XI. — Moyennant les hypothèses du paragraphe V, la condition nécessaire et suffisante pour qu'un idéal \mathfrak{i} , dont la $l^{\text{ème}}$ puissance est idéal principal, soit lui-même principal, est que l'on ait

$$(16) \quad \frac{d_{\mathfrak{o}}^{l-2} \log \mathfrak{i}^l(e^u)}{du^{l-2}} \equiv 0, \pmod{l}.$$

[Kummer^{46.}]

La démonstration nécessite quelques développements, qui font l'objet des deux lemmes suivants :

LEMME III. — Si le nombre de classes h est divisible une seule fois par l et qu'un idéal \mathfrak{i} appartienne à l'exposant l , c'est-à-dire si \mathfrak{i}^l est la première puissance de \mathfrak{i} qui soit un idéal principal, les idéaux $1, \mathfrak{i}, \mathfrak{i}^2, \dots, \mathfrak{i}^{l-1}$ représentent *toutes* les classes d'idéaux appartenant à l'exposant l .

Ces l classes sont évidemment distinctes, puisque \mathfrak{i} appartient à l'exposant l ; si l'existait un autre idéal \mathfrak{i}' appartenant à l'exposant l et non équivalent à l'un des précédents, les produits $\mathfrak{i}^m \mathfrak{i}'^m$ représenteraient pour m et m' égaux à $0, 1, 2, \dots, l-1$, l^2 classes d'idéaux non équivalentes; ensuite \mathfrak{i}'' désignant un idéal non équivalent à l'un des idéaux représentés par $\mathfrak{i}^m \mathfrak{i}'^m$, les idéaux $\mathfrak{i}^m \mathfrak{i}'^m \mathfrak{i}''^m$ seraient tous non équivalents pour m et m' égaux à $0, 1, \dots, l-1$, et m'' égal à $0, 1, \dots, h''-1$, en désignant par $\mathfrak{i}^{h''}$ la première puissance de \mathfrak{i}'' qui soit équivalente à $\mathfrak{i}^m \mathfrak{i}'^m$. En continuant ainsi on arrive à épuiser le nombre h de toutes les classes, et l'on aurait $h = l^2 h'' h''' \dots$, ce qui est impossible si h n'est divisible par l qu'une fois.

LEMME IV. — Si les deux premières hypothèses du paragraphe V sont vérifiées, l'indice de l'unité E_n , par rapport à un module premier \mathfrak{p} , est

$$(17) \quad \text{Ind } E_n \equiv \frac{(-1)^{r+u} (r^{2u} - 1) B_{l-2} - u}{2h} \cdot \frac{d_{\mathfrak{o}}^{l-2} \log \mathfrak{p}^h(e^u)}{du^{l-2}}, \pmod{l}.$$

[Kummer^{46.}]

En effet, on a démontré la formule générale (15)

$$\text{Ind } E_n \equiv \frac{r^{2n} - 1}{2} \cdot \frac{1}{1 + q^{l-2n} - (q+1)^{l-2n}} \cdot \frac{d_{\mathfrak{o}}^{l-2} \log \Psi_q(e^u)}{du^{l-2}}, \pmod{l},$$

où l'on a

$$\Psi_q(\zeta) = \pm \prod_{k=0}^{k=l-2} (s^k \mathfrak{p})^{m_k},$$

les exposants m_k étant donnés par la formule

$$m_k = \frac{1}{l} (r_{\mu-k} + r_{\mu-k+\text{ind } q} - r_{\mu-k+\text{ind } (q+1)}).$$

En éllevant à la puissance $h_1 l = h$, de manière à n'avoir que des idéaux principaux, on a

$$\Psi_q(\zeta)^{h_1 l} = \pm \prod_{k=0}^{k=l-2} (s^k \mathfrak{p})^{h_1 m_k}.$$

On en déduit

$$h_1 l \frac{d_0^{(l-2n)l} \log \Psi_q(e^u)}{du^{l-2n}} \equiv \sum_{k=0}^{k=l-2} m_k \frac{d_0^{(l-2n)l} \log s^k \mathfrak{p}^h(e^u)}{du^{l-2n}}, \pmod{l^3},$$

car si deux nombres α et β sont égaux, ou même simplement congrus, mod l^{i+1} , on a pour toute valeur de t non divisible par $l-1$

$$\frac{d_0^{tl^i} \alpha(e^u)}{du^{tl^i}} \equiv \frac{d_0^{tl^i} \beta(e^u)}{du^{tl^i}}, \pmod{l^{i+1}}.$$

On a donc, vu l'expression donnée plus haut de $\text{Ind } E_n$,

$$h_1 l \text{Ind } E_n \equiv \frac{r^{2n} - 1}{2[1 + q^{l-2n} - (q+1)^{l-2n}]} \cdot \frac{d_0^{(l-2n)l} \log \mathfrak{p}^h(e^u)}{du^{(l-2n)l}} \cdot \sum_{k=0}^{k=l-2} m_k r^{(l-2n)lk}, \pmod{l^3},$$

en remarquant que $s^k \mathfrak{p}^h(e^u) = \mathfrak{p}^h(e^{ur^k})$, et qu'on peut remplacer la dérivée $(l-2n)^{\text{ème}}$ par la $(l-2n)^{\text{ème}}$ qui lui est congrue, mod l .

Désignant pour abréger par K la somme \sum_k et remplaçant m_k par sa valeur, on a

$$lK \equiv \sum_{k=0}^{k=l-2} r^{(l-2n)lk} [r_{\mu-k} + r_{\mu-k+\text{ind } q} - r_{\mu-k+\text{ind } (q+1)}], \pmod{l^3}.$$

Remplaçons maintenant $r^{(l-2n)lk}$ par $r^{(l-2n)l^2k}$ qui lui est congru pour le module l^3 , nous aurons

$$lK \equiv \sum_{k=0}^{k=l-2} r_{\mu-k} r^{(l-2n)l^2k} + \sum_{k=0}^{k=l-2} r_{\mu-k+\text{ind } q} r^{(l-2n)l^2k} - \sum_{k=0}^{k=l-2} r_{\mu-k+\text{ind } (q+1)} r^{(l-2n)l^2k}, \pmod{l^3}.$$

Il suffit d'évaluer la seconde somme, dont les deux autres se déduisent par le changement de q en 1 ou en $q + 1$. Posons

$$r_{\mu-k+\text{ind } q} = i;$$

i prendra toutes les valeurs $1, 2, \dots, l-1$ quand k prendra les valeurs $0, 1, \dots, l-2$; puis, de

$$r_{\mu-k+\text{ind } q} \equiv i, \quad \text{ou} \quad r^k \equiv -\frac{q}{i} \pmod{l},$$

on tire

$$r^{(l-2n)l^2k} \equiv -\frac{q^{(l-2n)l^2}}{i^{(l-2n)l^2}} \pmod{l^3},$$

ou encore

$$r^{(l-2n)l^2k} \equiv -q^{(l-2n)l^2} i^{(2n-1)l^2} \pmod{l^3},$$

parce que l'on a $i^{(l-1)l^2} \equiv 1 \pmod{l^3}$.

La seconde somme est donc congrue à

$$-q^{(l-2n)l^2} \sum_{i=1}^{l-1} i^{(2n-1)l^2+1} \pmod{l^3},$$

et l'on a

$$lK \equiv -[1 + q^{(l-2n)l^2} - (q+1)^{(l-2n)l^2}] \sum_{i=1}^{l-1} i^{(2n-1)l^2+1} \pmod{l^3}.$$

Or, on a

$$\sum_{i=1}^{l-1} i^{(2n-1)l^2+1} \equiv (-1)^{n+1} B_{\frac{(2n-1)l^2+1}{2}} \cdot l \pmod{l^3}.$$

En posant, pour abréger,

$$Q = 1 + q^{l-2n} - (q+1)^{l-2n}, \quad Q' = 1 + q^{(l-2n)l} - (q+1)^{(l-2n)l},$$

et revenant au module l^3 , en divisant par l , on a donc, pour l'expression de l'indice :

$$h_1 l \text{ Ind } E_n(\zeta) \equiv (-1)^n \frac{(r^{2n} - 1)Q'}{Q} \cdot B_{\frac{(2n-1)l^2+1}{2}} \cdot \frac{d_{\mu}^{(l-2n)l} \log p^h(e^u)}{du^{(l-2n)l}} \pmod{l^3}.$$

En utilisant la congruence

$$\frac{B_m}{m} \equiv (-1)^{s\mu} \frac{B_{m+sl\mu}}{m+sl\mu} \pmod{l^3},$$

(démontrée dans le Mémoire de Kummer, cité en note au § II), on a, si l'on y fait

$$m = \frac{(2n-1)l+1}{2} = nl - \mu \text{ et } s = 2n-1 :$$

$$B_{\frac{(2n-1)l^2+1}{2}} \equiv \frac{(-1)^\mu B_{nl-\mu}}{2(nl-\mu)} \pmod{l^3}.$$

Si l'on fait enfin $n = v$, $B_{v,l-\mu}$ est divisible par l , car B_v l'est: on peut alors diviser par l les deux membres de la congruence qui donne l'indice, et comme on a $Q' \equiv Q$, $(\text{mod } l)$, et aussi

$$\frac{d_{\alpha}^{(l-2v)l} \log \mathfrak{p}^h(e^u)}{du^{(l-2v)l}} \equiv \frac{d_{\alpha}^{l-2v} \log \mathfrak{p}^h(e^u)}{du^{l-2v}}, \quad (\text{mod } l),$$

on a finalement

$$\text{Ind } E_v(\zeta) \equiv \frac{(-1)^{n+\mu}(r^{2v}-1)B_{v,l-\mu}}{2h_1l} \cdot \frac{d_{\alpha}^{l-2v} \log \mathfrak{p}^h(e^u)}{du^{l-2v}}, \quad (\text{mod } l).$$

C. q. f. d.

DÉFINITION. — La formule précédente s'applique encore dans le cas d'un module composé, moyennant une généralisation de la notion d'indice, analogue à celle que Jacobi a donnée du symbole de Legendre. D'après la définition du symbole $\left\{ \frac{\alpha}{\mathfrak{p}} \right\}$ (voir § 113), on a

$$\zeta^{\text{Ind } \alpha} = \left\{ \frac{\alpha}{\mathfrak{p}} \right\}.$$

On définira le symbole $\left\{ \frac{\alpha}{\mathfrak{i}} \right\}$, dans le cas d'un idéal \mathfrak{i} composé, par la relation

$$\left\{ \frac{\alpha}{\mathfrak{i}} \right\} = \left\{ \frac{\alpha}{\mathfrak{p}} \right\} \left\{ \frac{\alpha}{\mathfrak{q}} \right\} \left\{ \frac{\alpha}{\mathfrak{r}} \right\} \dots,$$

$\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$, etc., étant les idéaux premiers distincts ou non dont le produit est égal à \mathfrak{i} : l'indice par rapport à \mathfrak{i} est la somme des indices pour $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$, etc. Le logarithme d'un produit de facteurs étant égal à la somme des logarithmes des facteurs, et l'indice ayant la même propriété, on voit que l'on a encore dans le cas d'un module \mathfrak{i} composé :

$$\text{Ind } E_v(\zeta) \equiv \frac{(-1)^{n+\mu}(r^{2v}-1)B_{v,l-\mu}}{2h_1l} \cdot \frac{d_{\alpha}^{l-2v} \log \mathfrak{i}^h(e^u)}{du^{l-2v}}, \quad (\text{mod } l).$$

REMARQUE I. — Il résulte de là que si l'idéal \mathfrak{i} est principal ou s'il appartient à un exposant non divisible par l , l'indice de $E_v(\zeta)$, par rapport à ce module, est divisible par l , c'est-à-dire que

$$\left\{ \frac{E_v(\zeta)}{\mathfrak{i}} \right\} = 1,$$

car l'exposant a , auquel appartient \mathfrak{i}^a , étant un diviseur de $h = h_1l$, et n'étant pas divisible par l , doit diviser h_1 ; soit $h_1 = ah_2$, on aura $\mathfrak{i}^h = (\mathfrak{i}^a)^{h_2}l$, et, par suite,

$$\log \mathfrak{i}^h(e^u) = h_2l \log \mathfrak{i}^a(e^u),$$

d'où

$$\frac{d_{\alpha}^{l-2v} \log \mathfrak{i}^h(e^u)}{du^{l-2v}} \equiv 0 \quad \text{et} \quad \text{Ind } E_v(\zeta) \equiv 0, \quad (\text{mod } l).$$

REMARQUE II. — Il résulte de là que $E_v(\zeta)$ a même indice par rapport à deux idéaux équivalents \mathfrak{a} et \mathfrak{b} .

Car dans ce cas il existe un idéal \mathfrak{c} , tel que $\mathfrak{a}\mathfrak{c}$ et $\mathfrak{b}\mathfrak{c}$ soient tous deux principaux, et alors

$$\left\{ \frac{E_v}{\mathfrak{a}\mathfrak{c}} \right\} = 1 = \left\{ \frac{E_v}{\mathfrak{b}\mathfrak{c}} \right\},$$

ou en supprimant le facteur commun $\left\{ \frac{E_v}{\mathfrak{c}} \right\}$:

$$\left\{ \frac{E_v}{\mathfrak{a}} \right\} = \left\{ \frac{E_v}{\mathfrak{b}} \right\}.$$

Passons maintenant à la *démonstration du théorème XI*.

Par hypothèse, il existe un module \mathfrak{a} pour lequel $E_v(\zeta)$ n'est pas reste de $l^{\text{ème}}$ puissance et, par conséquent, $i = \text{Ind } E_v(\zeta)$ est $\equiv 0 \pmod{l}$, ou encore

$$\left\{ \frac{E_v(\zeta)}{\mathfrak{a}} \right\} = \zeta^i.$$

Il résulte alors de la remarque I précédente que \mathfrak{a} appartient à un exposant divisible par l , soit al , et a n'est pas divisible par l , car autrement le nombre des classes serait divisible par l^l . Ensuite $\mathfrak{b} = \mathfrak{a}^a$ appartient à l'exposant l , et l'on a

$$\left\{ \frac{E_v(\zeta)}{\mathfrak{b}} \right\} = \zeta^{ai}, \quad \left\{ \frac{E_v(\zeta)}{\mathfrak{b}^m} \right\} = \zeta^{aim}.$$

Si maintenant \mathfrak{i} est un idéal dont la $l^{\text{ème}}$ puissance est idéal principal, il est (d'après le lemme IV) équivalent à l'un \mathfrak{b}^m des idéaux

$$1, \mathfrak{b}, \mathfrak{b}^2, \dots, \mathfrak{b}^{l-1}.$$

On a donc

$$\left\{ \frac{E_v(\zeta)}{\mathfrak{i}} \right\} = \left\{ \frac{E_v(\zeta)}{\mathfrak{b}^m} \right\} = \zeta^{aim}$$

ou

$$\text{Ind } E_v(\zeta) \equiv aim, \quad (\text{mod } l).$$

l'indice se rapportant au module \mathfrak{i} . Comme ai n'est pas divisible par l , l'indice est ou n'est pas divisible par l , en même temps que m , c'est-à-dire à cause de l'équivalence

$$\mathfrak{i} \sim \mathfrak{b}^m,$$

suivant que \mathfrak{i} est ou n'est pas principal.

Mais puisqu'on suppose que \mathfrak{i}^l est principal, l'expression de l'indice de $E_v(\zeta)$ devient (après suppression du facteur h_i dans les deux termes de la fraction)

$$\text{Ind } E_v(\zeta) \equiv \frac{(-1)^{v+\mu}(r^{2v}-1)B_{v,l-\mu}}{2l} \cdot \frac{d_{\mathfrak{o}}^{l-2v} \log \mathfrak{i}^l(e^u)}{du^{l-2v}}, \quad (\text{mod } l),$$

et si l'on observe que le premier facteur du second membre est indépendant de i et qu'il n'est certainement pas divisible par l , car autrement $E_v(\zeta)$ serait reste de puissance $l^{\text{ème}}$ pour le module i , contrairement à l'hypothèse, on voit que l'indice de E_v est ou n'est pas divisible par l , en même temps que $\frac{d_o^{l-2v} \log i(e^u)}{du^{l-2v}}$, ce qui achève la démonstration du théorème.

COROLLAIRE. — Dans le cas d'un idéal i du corps $c(\zeta + \zeta^{-1})$, on a $i^l(\zeta) = i^l(\zeta^{-1})$, et, par suite, toutes les dérivées d'ordre impair du logarithme sont congrues à zéro pour $u=0$, en particulier la $(l-2v)^{\text{ème}}$.

Donc, tout idéal du corps $c(\zeta + \zeta^{-1})$, dont la $l^{\text{ème}}$ puissance est un idéal principal, est lui-même idéal principal.

§ IX. — *Condition moyennant laquelle un nombre du corps $c(\zeta + \zeta^{-1})$, multiplié par une unité convenable, est congru, mod l , à un entier rationnel.*

THÉORÈME XII. — Si l ne divise qu'un seul B , des $\frac{l-3}{2}$ premiers nombres de Bernoulli et qu'une seule fois, tout nombre $F(\zeta)$ du corps $c(\zeta + \zeta^{-1})$, qui vérifie la congruence

$$\frac{d^{2v} \log F(e^u)}{du^{2v}} \equiv 0, \pmod{l}.$$

peut, après multiplication par une unité convenable, devenir congru, mod l , à un entier rationnel. [Kummer¹⁶.]

On a, en effet, dans ce cas, en appliquant la formule (12) :

$$-\log \left[\frac{F(\zeta)}{F(1)} \right] \equiv \frac{d_o^2 \log F(e^u)}{du^2} X_2(\zeta) + \dots + \frac{d_o^{l-3} \log F(e^u)}{du^{l-3}} X_{l-3}(\zeta), \pmod{l}.$$

les dérivées d'ordres impairs disparaissant à cause de $F(e^u) = F(e^{-u})$.

Employons maintenant les unités $E_n(\zeta)$, pour lesquelles on a, d'après la formule (14) :

$$\log \left[\frac{E_n(\zeta)}{E_n(1)} \right] \equiv (-1)^{n+1} (r^{2n} - 1) \frac{B_n}{4n} X_{2n}(\zeta), \pmod{l}.$$

Déterminons les entiers N_n pour $n=1, 2, \dots, p-1$, à l'exception de $n=v$ par les congruences

$$(-1)^{n+1} (r^{2n} - 1) \frac{B_n}{4n} \cdot N_n \equiv \frac{d_o^{2n} \log F(e^u)}{du^{2n}}, \pmod{l},$$

nous aurons

$$N_n \log \left[\frac{E_n(\zeta)}{E_n(1)} \right] \equiv \frac{d_o^{2n} \log F(e^u)}{du^{2n}} \cdot X_{2n}(\zeta), \pmod{l},$$

et, pour $n = v$, on a, quel que soit N_v , puisque B_v est supposé divisible par l :

$$N_v \log \left[\frac{E_v(\zeta)}{E_v(1)} \right] \equiv 0, \pmod{l}.$$

Par suite, si l'on suppose

$$\frac{d^{2v} \log F(e^u)}{du^{2v}} \equiv 0, \pmod{l},$$

on a

$$-\log \left[\frac{F(\zeta)}{F(1)} \right] \equiv N_1 \log \left[\frac{E_1(\zeta)}{E_1(1)} \right] + N_2 \log \left[\frac{E_2(\zeta)}{E_2(1)} \right] + \dots + N_{p-1} \log \left[\frac{E_{p-1}(\zeta)}{E_{p-1}(1)} \right], \pmod{l},$$

c'est-à-dire en posant

$$E = E_1^{N_1} E_2^{N_2} \dots E_{p-1}^{N_{p-1}}$$

$$\log \left[\frac{F(\zeta)E(\zeta)}{F(1)E(1)} \right] \equiv 0, \pmod{l}.$$

ou

$$F(\zeta)E(\zeta) \equiv F(1)E(1), \pmod{l}.$$

C. q. f. d.

§ X. — Propriété des unités congrues, mod l^p , à un entier rationnel.

THÉORÈME XIII. — Si l satisfait aux trois conditions suivantes :

1° il divise un seul B_v des $\frac{l-3}{2}$ premiers nombres de Bernoulli,

2° il ne divise pas le second facteur du nombre de classes,

3° $B_{v,l}$ n'est pas divisible par l^p ,

toute unité du corps $c(e^{\frac{2i\pi}{l}})$ congrue, mod l^p , à un entier rationnel, est la $l^{\text{ème}}$ puissance d'une unité du corps. [Kummer^{16.}] (Théorème correspondant au théorème 156 pour les corps réguliers.)

Démonstration. — Soit

$$E(\zeta) = \pm \zeta^s \gamma_1^{N_1} \gamma_2^{N_2} \dots \gamma_{p-1}^{N_{p-1}}$$

l'expression d'une unité quelconque $E(\zeta)$ à l'aide d'un système de $p-1 = \frac{l-3}{2}$ unités fondamentales $\gamma_1, \dots, \gamma_{p-1}$, et soit

$$\varepsilon(\zeta^{r^k}) = \gamma_1^{n_{k,1}} \gamma_2^{n_{k,2}} \dots \gamma_{p-1}^{n_{k,p-1}}, \quad (k = 0, 1, 2, \dots, p-2),$$

celle des unités circulaires.

On en déduit pour $E(\zeta)$, en éliminant les γ , — ce qui est aisément démontré en prenant les logarithmes, — l'expression

$$E(\zeta) = \pm \zeta^s \varepsilon(\zeta)^{\frac{m_0}{t}} \varepsilon(\zeta^r)^{\frac{m_1}{t}} \cdots \varepsilon(\zeta^{r^{\mu-2}})^{\frac{m_{\mu-2}}{t}},$$

où nous supposons que t représente le plus petit dénominateur commun des fractions en exposant. Ce dénominateur t n'est pas divisible par l , car c'est un diviseur du déterminant des $n_{k,i}$, et ce dernier est égal au quotient $\frac{\Delta}{R}$ des déterminants des systèmes de logarithmes des unités circulaires et des unités fondamentales, c'est-à-dire (théorème 142) au second facteur du nombre de classes, facteur non divisible par l , d'après l'hypothèse.

Supposons $E(\zeta)$ congrue, mod l^s , à un entier rationnel a . Il en résulte d'abord $s=0$, car de $E(\zeta) \equiv a$, mod l^s , résulte $E(\zeta^{-1}) \equiv E(\zeta)$, mod l^s , ce qui exige, comme les unités circulaires sont réelles, $\zeta^s \equiv \zeta^{-s}$, mod l^s , et, par suite, $s=0$.

Ensuite, comme $E(1)$ est congru à a , et, par suite, à $E(\zeta)$, mod l^s , on a, en prenant les logarithmes, mod l^s (voir § VI) :

$$\log \left[\frac{E(\zeta)}{E(1)} \right] \equiv 0, \pmod{l^s}.$$

ce qui donne, en développant d'après la seconde expression de $E(\zeta)$ et supprimant le diviseur t , non divisible par l :

$$m_0 \log \left[\frac{\varepsilon(\zeta)}{\varepsilon(1)} \right] + m_1 \log \left[\frac{\varepsilon(\zeta^r)}{\varepsilon(1)} \right] + \cdots + m_{\mu-2} \log \left[\frac{\varepsilon(\zeta^{r^{\mu-2}})}{\varepsilon(1)} \right] \equiv 0, \pmod{l^s}.$$

Appliquons à $\varepsilon(\zeta^{r^k})$ la formule (8), paragraphe VI, en remarquant que toutes les dérivées d'ordre impair sont nulles pour $u=0$, parce que ces unités sont réelles, et tenant compte de ce que la norme est égale à un ; nous avons

$$(l-1) \log \left[\frac{\varepsilon(\zeta^{r^k})}{\varepsilon(1)} \right] \equiv - \log \varepsilon(1)^{l-1} + \sum_{n=1}^{n=\mu-1} r^{2nk} \frac{d_0^{2nl} \log \varepsilon(e^u)}{du^{2nl}} \cdot X_{2n}(\zeta), \pmod{l^s}.$$

Multiplions par m_k et faisons la somme pour $k=0, 1, 2, \dots, \mu-2$, en posant pour abréger

$$M_n = \sum_{k=0}^{k=\mu-2} m_k r^{2nk},$$

nous aurons

$$- M_0 \log \varepsilon(1)^{l-1} + \sum_{n=1}^{n=\mu-1} M_n \frac{d_0^{2nl} \log \varepsilon(e^u)}{du^{2nl}} \cdot X_{2n}(\zeta) \equiv 0, \pmod{l^s}.$$

On trouve aisément $\varepsilon(1) = r$, et si l'on suppose, ce qui est possible, r choisi de manière que r^{l-1} soit congru à 1, mod l^2 , on aura $\log \varepsilon(1)^{l-1} \equiv 0$, (mod l^2). En exprimant ensuite que les coefficients de ζ, ζ^r, \dots , sont tous divisibles par l^2 , on a un système de $l-1$ congruences linéaires et homogènes indépendantes par rapport aux $\mu - 1 = \frac{l-3}{2}$ produits $M_n \frac{d_0^{2nl} \log \varepsilon(e^u)}{du^{2nl}}$, ce qui entraîne, pour $n = 1, 2, \dots, \mu - 1$:

$$M_n \frac{d_0^{2nl} \log \varepsilon(e^u)}{du^{2nl}} \equiv 0, \pmod{l^2}.$$

Mais on a, d'après la formule (13),

$$\frac{d_0^{2nl} \log \varepsilon(e^u)}{du^{2nl}} = (-1)^{n+1} (r^{2nl} - 1) \frac{B_{nl}}{2nl},$$

$$\frac{d_0^{2n} \log \varepsilon(e^u)}{du^{2n}} = (-1)^{n+1} (r^{2n} - 1) \frac{B_n}{2n}.$$

D'ailleurs, on a toujours

$$\frac{d_0^{kl} \log \Phi(e^u)}{du^{kl}} \equiv \frac{d_0^k \log \Phi(e^u)}{du^k}, \pmod{l},$$

comme on le voit en comparant les développements de $\log \left[\frac{\Phi(\zeta)}{\Phi(1)} \right]$, mod l^2 , et mod l (les $X_k(\zeta)$ étant congrus dans les deux développements, d'après le théorème de Fermat). Donc $\frac{d_0^{2nl} \log \varepsilon(e^u)}{du^{2nl}}$ ne peut être divisible par l que si B_n l'est; dans le cas actuel, c'est seulement pour $n = \nu$. On a, par suite, $M_n \equiv 0$, (mod l^2), sauf pour $n = \nu$; si on suppose $\frac{B_\nu l}{\nu l} \equiv 0$, (mod l^2), c'est-à-dire $B_\nu l \equiv 0$, (mod l^2), on aura nécessairement $M_\nu \equiv 0$, (mod l). Posons alors $M_\nu \equiv \mu b l$, $M_0 \equiv \mu c$, (mod l^2), nous aurons, en multipliant M_n par $r^{-2nk\ell}$ et ajoutant pour $n = 0, 1, \dots, \nu - 1$:

$$\mu m_k \equiv \mu c + \mu b l r^{-2\nu k\ell}, \pmod{l^2}.$$

$$m_k = c + b l r^{-2\nu k\ell} + s_k l^2. \quad (k = 0, 1, \dots, \nu - 2.)$$

En portant ces valeurs dans l'expression de $E(\zeta)$, tenant compte de ce que la norme de $\varepsilon(\zeta)$ est 1 et que, l étant premier à l , on peut déterminer deux entiers d et e tels que $td = 1 + le$, on trouve aisément

$$E(\zeta) = \left[\frac{E_1(\zeta)^d}{E(\zeta)^e} \right]^l.$$

expression où E_1 est une autre unité, ce qui démontre le théorème.

§ XI. — *Théorème sur l'impossibilité de l'équation (1), dans le cas de x, y ou z divisible par l, lorsque l vérifie les trois conditions du paragraphe V.*

THÉORÈME XIV. — Si l satisfait aux trois conditions suivantes :

1° il divise un seul B_l des $\frac{l-3}{2}$ premiers nombres de Bernoulli, et une seule fois,

2° il existe un module pour lequel E_l n'est pas reste de $l^{\text{ème}}$ puissance,

3° $B_{\sqrt{l}}$ n'est pas divisible par l^k ,

l'équation (1) est impossible en nombres entiers x, y, z premiers entre eux deux à deux, l'un d'entre eux étant divisible par une puissance quelconque de l . [Kummer¹⁶.]

Soit z celui des trois nombres qui est divisible par l , et soit l^k la plus haute puissance de l qu'il contient, de sorte que $z = l^k z_i$. Considérons, au lieu de l'équation (1), l'équation plus générale

$$(1)' \quad U^l + V^l = E(z - \zeta - \zeta^{-1})^{ml} W^l,$$

U, V, W désignant des entiers premiers à l du corps $c(\zeta + \zeta^{-1})$, E une unité quelconque du corps; $z - \zeta - \zeta^{-1}$, c'est-à-dire $(1 - \zeta)(1 - \zeta^{-1})$, est l'un des $\frac{l-1}{2}$ facteurs égaux réels de l dans le corps $c(\zeta + \zeta^{-1})$; enfin m est supposé plus grand que un. L'équation (1) n'en est qu'un cas particulier, correspondant à

$$U = x, \quad V = y, \quad W = -z_i, \quad m = k \frac{(l-1)}{2}, \quad E = \frac{l^k}{(z - \zeta - \zeta^{-1})^{k(\frac{l-1}{2})} l}.$$

Nous allons déduire de l'équation (1)' une série d'équations de même forme :

$$U_i^l + V_i^l = E_i(z - \zeta - \zeta^{-1})^{ml} W_i^l,$$

dans laquelle W_i contiendra moins de facteurs idéaux premiers que W_{i-1} . Ceci conduit à une contradiction qui entraîne l'impossibilité de l'équation (1)'; car W ne contenant qu'un nombre limité de facteurs premiers, on sera forcément arrêté dans la série des transformations précédentes.

Ecrivons l'équation (1)'

$$(U + V)(U + \zeta V) \dots (U + \zeta^{l-1} V) = E(z - \zeta - \zeta^{-1})^{ml} \cdot W^l.$$

Le plus grand commun diviseur des facteurs du premier membre est $1 - \zeta$, et ce facteur $1 - \zeta$ ne peut diviser plusieurs fois que le seul facteur $U + V$, car si $U + \zeta^r V$ était divisible par $(1 - \zeta)^2$, il en serait de même, comme on le voit en changeant

ζ en ζ^{-1} , de $U + \zeta^{-r}V$, et, par suite, de $(\zeta^r - \zeta^{-r})V$, ce qui est impossible, si r n'est pas nul, V étant premier à l . On a donc, le nombre total des facteurs $1 - \zeta$ étant $2ml$,

$$(A) \quad U + \zeta^r V = \varepsilon_r(1 - \zeta^r)I_r^l, \quad (r=1, 2, \dots, l-1),$$

$$(B) \quad U + V = \varepsilon(2 - \zeta - \zeta^{-1})^{ml - \frac{l-1}{2}} J^l,$$

les ε_r et ε étant des unités⁽¹⁾, les I_r des idéaux du corps $c(\zeta)$ et J un idéal du corps $c(\zeta + \zeta^{-1})$, car il ne change pas par la substitution (ζ, ζ^{-1}) , vu l'équation (B).

Ces idéaux I_r et J sont des idéaux principaux.

Car on a, en éliminant U :

$$V = -\varepsilon_r \cdot I_r^l + \varepsilon \cdot \frac{(2 - \zeta - \zeta^{-1})^{ml - \frac{l-1}{2}}}{1 - \zeta^r} \cdot J^l.$$

V et $\varepsilon_r I_r^l$ sont donc congrus mod l , et il en est alors de même de leurs dérivées logarithmiques (voir § 131, note)

$$\frac{d_{0}^{l-2v} \log V(e^u)}{du^{l-2v}} \equiv \frac{d_{1}^{l-2v} \log \varepsilon_r(e^u)}{du^{l-2v}} + \frac{d_{0}^{l-2v} \log I_r(e^u)^l}{du^{l-2v}}, \quad (\text{mod } l);$$

mais comme $V(e^u) = V(e^{-u})$ et que $l - 2v$ est impair, on a

$$\frac{d_{0}^{l-2v} \log V(e^u)}{du^{l-2v}} \equiv 0, \quad (\text{mod } l),$$

et de même, parce que l'on a $\varepsilon_r(\zeta) = \zeta^l \varepsilon_r(\zeta^{-1})$, d'après une propriété générale des unités (théorème 48) :

$$\frac{d_{0}^{l-2v} \log \varepsilon_r(e^u)}{du^{l-2v}} \equiv 0, \quad (\text{mod } l);$$

par conséquent on a aussi

$$\frac{d_{0}^{l-2v} \log I_r(e^u)^l}{du^{l-2v}} \equiv 0, \quad (\text{mod } l),$$

et il en résulte (théorème XI) que I_r est un idéal principal.

D'ailleurs, J est aussi principal d'après le corollaire du même théorème.

Le produit de $I_r(\zeta)I_r(\zeta^{-1})$ par une unité convenable est congru, mod l , à un entier rationnel.

En effet, en observant que V , ε et J ne changent pas par la substitution (ζ, ζ^{-1}) , on a

$$\varepsilon_r(\zeta)I_r(\zeta)^l - \varepsilon_r(\zeta^{-1})I_r(\zeta^{-1})^l = \frac{\varepsilon(2 - \zeta - \zeta^{-1})^{ml - \frac{l-1}{2}}(1 + \zeta^r)J^l}{1 - \zeta^r},$$

(1) Dans ce paragraphe, ε désigne une unité quelconque et non l'unité circulaire.

d'où, comme $I_r(\zeta)^l$ est congru, mod l , à un entier rationnel, et par suite à $I_r(\zeta^{-1})^l$, la congruence

$$\varepsilon_r(\zeta) \equiv \varepsilon_r(\zeta^{-1}), \pmod{l},$$

ce qui exige, vu la propriété générale des unités $(\varepsilon(\zeta) = \zeta^t \varepsilon(\zeta^{-1}))$,

$$\varepsilon_r(\zeta) = \varepsilon_r(\zeta^{-1}).$$

En divisant alors par $\varepsilon_r(\zeta)$ et remplaçant $2 - \zeta - \zeta^{-1}$ par $-\zeta^{-1}(1 - \zeta)^2$, on a

$$(C) \quad I_r(\zeta)^l - I_r(\zeta^{-1})^l = \varepsilon'(1 - \zeta)^{(2m-1)l} J^l,$$

où ε' désigne une unité.

I_r ne figure dans toutes nos équations qu'à la puissance $l^{\text{ème}}$; on peut donc le supposer semi-primaire, c'est-à-dire congru, mod $(1 - \zeta)^2$, à un entier rationnel, en le multipliant au besoin par une puissance convenable de ζ (§ 115). En décomposant alors le premier membre de (C) en ses l facteurs linéaires de la forme $I_r(\zeta) - \zeta^t I_r(\zeta^{-1})$, on voit, comme plus haut, qu'ils ont pour plus grand commun diviseur $1 - \zeta$, et que le seul facteur $I_r(\zeta) - I_r(\zeta^{-1})$ est divisible plusieurs fois par $1 - \zeta$ (un facteur $I_r(\zeta) - \zeta^t I_r(\zeta^{-1})$ ne peut l'être si t n'est pas nul, puisque $I_r(\zeta)$ congru, mod $(1 - \zeta)^2$, à une entier rationnel, est congru à $I_r(\zeta^{-1})$). On a donc, les I'_t et J' étant des idéaux :

$$\begin{aligned} I_r(\zeta) - \zeta^t I_r(\zeta^{-1}) &= \varepsilon_t''(\zeta) \cdot (1 - \zeta^t) \cdot I'_t(\zeta)^l, & (t=1, 2, \dots, l-1). \\ I_r(\zeta) - I_r(\zeta^{-1}) &= \varepsilon''(\zeta) (1 - \zeta)^{(2m-2)l+1} \cdot I'(\zeta)^l. \end{aligned}$$

En résolvant par rapport à $I_r(\zeta)$ et $I_r(\zeta^{-1})$, on en tire les congruences

$$\begin{aligned} I_r(\zeta) &\equiv \varepsilon_t''(\zeta) I'_t(\zeta)^l, \\ I_r(\zeta^{-1}) &\equiv \varepsilon_t''(\zeta^{-1}) I'_t(\zeta^{-1})^l, \end{aligned} \quad \left\{ \pmod{(1 - \zeta)^{(2m-1)l}},\right.$$

d'où, comme m est > 1 ,

$$I_r(\zeta) I_r(\zeta^{-1}) \equiv \varepsilon_t''(\zeta) \cdot \varepsilon_t''(\zeta^{-1}) \cdot [I'_t(\zeta) \cdot I'_t(\zeta^{-1})]^l, \pmod{l},$$

$I'_t(\zeta) \cdot I'_t(\zeta^{-1})$, idéal du corps $c(\zeta + \zeta^{-1})$, dont la $l^{\text{ème}}$ puissance est un idéal principal, est lui-même principal (corollaire du théorème XI); de sorte, qu'en tenant compte de la congruence ci-dessus, on a

$$\frac{d_{\phi}^{2y} \log [I_r(e^u) \cdot I_r(e^{-u})]}{du^{2y}} \equiv \frac{d_{\phi}^{2y} \log [\varepsilon_t''(e^u) \cdot \varepsilon_t''(e^{-u})]}{du^{2y}}, \pmod{l},$$

c'est-à-dire, vu la propriété générale des unités,

$$\frac{d_{\phi}^{2y} \log [I_r(e^u) \cdot I_r(e^{-u})]}{du^{2y}} \equiv 0, \pmod{l},$$

ce qui prouve, vu le théorème XII, qu'en multipliant $I_r(\zeta) \cdot I_r(\zeta^{-1})$ par une unité convenable $A_r(\zeta)$, on rend ce produit congru, mod l , à un entier rationnel. On démontrerait de plus, comme pour ε_r , que A_r est une unité du corps $c(\zeta + \zeta^{-1})$.

On déduit de (1)' une équation de même forme.

Multiplions l'équation (A) par celle qu'on obtient par la substitution (ζ, ζ^{-1}) , on a

$$U^2 + (\zeta^r + \zeta^{-r})UV + V^2 = \varepsilon_r(\zeta) \cdot \varepsilon_r(\zeta^{-1}) \cdot (2 - \zeta^r - \zeta^{-r}) \cdot [I_r(\zeta) \cdot I_r(\zeta^{-1})]^l;$$

de même,

$$U^2 + (\zeta^s + \zeta^{-s})UV + V^2 = \varepsilon_s(\zeta) \cdot \varepsilon_s(\zeta^{-1}) \cdot (2 - \zeta^s - \zeta^{-s}) \cdot [I_s(\zeta) \cdot I_s(\zeta^{-1})]^l,$$

et en éllevant (B) au carré, on a

$$U^2 + 2UV + V^2 = \varepsilon(\zeta)^2 \cdot (2 - \zeta - \zeta^{-1})^{2ml-l+1} \cdot J(\zeta)^{2l}.$$

Si on élimine $U^2 + V^2$ et UV entre ces trois équations, on a

$$\begin{aligned} \varepsilon_r(\zeta) \cdot \varepsilon_r(\zeta^{-1}) \cdot [I_r(\zeta) \cdot I_r(\zeta^{-1})]^l - \varepsilon_s(\zeta) \cdot \varepsilon_s(\zeta^{-1}) \cdot [I_s(\zeta) \cdot I_s(\zeta^{-1})]^l \\ = \frac{\varepsilon(\zeta)^2 \cdot (2 - \zeta - \zeta^{-1})^k \cdot (\zeta^r + \zeta^{-r} - \zeta^s - \zeta^{-s}) J(\zeta)^{2l}}{(2 - \zeta^r - \zeta^{-r})(2 - \zeta^s - \zeta^{-s})}. \end{aligned}$$

En posant, pour abréger,

$$\begin{aligned} A_r(\zeta) \cdot I_r(\zeta) \cdot I_r(\zeta^{-1}) &= U'(\zeta), & A_s(\zeta) \cdot I_s(\zeta) \cdot I_s(\zeta^{-1}) &= V'(\zeta), \\ \frac{\varepsilon_r(\zeta) \cdot \varepsilon_r(\zeta^{-1})}{A_r(\zeta)^2} &= \mathbf{e}_r(\zeta), & \frac{\varepsilon_s(\zeta) \cdot \varepsilon_s(\zeta^{-1})}{A_s(\zeta)^2} &= \mathbf{e}_s(\zeta), \end{aligned}$$

on a

$$\mathbf{e}_r(\zeta) \cdot U'(\zeta)^l - \mathbf{e}_s(\zeta) \cdot V'(\zeta)^l = \frac{\varepsilon(\zeta)^2 \cdot (2 - \zeta - \zeta^{-1})^k \cdot (\zeta^r + \zeta^{-r} - \zeta^s - \zeta^{-s}) \cdot J(\zeta)^{2l}}{(2 - \zeta^r - \zeta^{-r})(2 - \zeta^s - \zeta^{-s})}$$

et en observant que $\zeta^r + \zeta^{-r} - \zeta^s - \zeta^{-s}$ est divisible une fois par $2 - \zeta - \zeta^{-1}$, et de même $2 - \zeta^r - \zeta^{-r}$ et $2 - \zeta^s - \zeta^{-s}$, on a, en remplaçant k par sa valeur $2ml - l + 1$, et désignant par E_1 une unité :

$$U'' - \frac{\mathbf{e}_s}{\mathbf{e}_r} V'' = E_1 \cdot (2 - \zeta - \zeta^{-1})^{(2m-1)l} J^{2l},$$

ce qui donne la congruence

$$U'' \equiv \frac{\mathbf{e}_s}{\mathbf{e}_r} V'' \pmod{l^2}.$$

Mais U' et V' étant congrus, mod l , à des entiers rationnels, U'' et V'' sont congrus, mod l^2 , à des entiers rationnels; donc, l'unité $\frac{\mathbf{e}_s}{\mathbf{e}_r}$ est congrue, mod l^2 , à un entier rationnel, et elle est, d'après le théorème (XIII), la $l^{\text{ème}}$ puissance d'une unité $\mathbf{G}(\zeta)$. En posant alors

$$U' = U_1, \quad -\mathbf{G}V' = V_1, \quad J^2 = W_1,$$

on a l'équation

$$U_1^l + V_1^l = E_1 (2 - \zeta - \zeta^{-1})^{(2m-1)l} W_1^l,$$

de même forme que celle dont on est parti et qui doit encore être vérifiée par des entiers U_1, V_1, W_1 du corps $c(\zeta + \zeta^{-1})$ premiers entre eux et à l . Par le même pro-

cédé on en déduirait une troisième et ainsi de suite indéfiniment; mais c'est impossible, car *le nombre des facteurs idéaux de W va en diminuant*.

En effet, on a d'abord :

$$W = I_1 I_2 \dots I_{l-1} J.$$

Comme tous les facteurs du second membre sont premiers entre eux deux à deux, W_1 , qui est égal à J^2 , ne pourrait donc contenir tous les facteurs idéaux de W que si tous les I étaient des unités, c'est-à-dire, d'après (A), que si $\frac{U + \zeta^r V}{1 - \zeta^r}$ était, pour toute valeur de r , une unité; en changeant alors ζ en ζ^{-1} on devrait avoir (propriété générale des unités) :

$$\frac{U + \zeta^r V}{1 - \zeta^r} = \zeta^k \frac{U + \zeta^{-r} V}{1 - \zeta^{-r}},$$

c'est-à-dire

$$U(1 + \zeta^{r+k}) + V(\zeta^r + \zeta^k) = 0.$$

Mais comme, d'après (B), on a

$$U + V \equiv 0, \pmod{l},$$

il en résulterait

$$1 + \zeta^{r+k} - \zeta^r - \zeta^k \equiv 0, \pmod{l},$$

c'est-à-dire

$$(1 - \zeta^r)(1 - \zeta^k) \equiv 0, \pmod{l},$$

ce qui est impossible en dehors de l égal à 3, cas exclu, ou de k égal à 0, ce qui ne peut avoir lieu, car alors on aurait $U + V = 0$, $W = 0$.

Le théorème est ainsi complètement démontré.

D'après l'expression du premier facteur du nombre de classes pour les nombres premiers inférieurs à 100, expression donnée par Kummer (*Journal de Liouville*, tome XVI), 37, 59 et 67 sont les seuls nombres premiers non réguliers inférieurs à 100. Ils entrent une fois et une seule dans ce premier facteur. Relativement aux deux autres conditions, on a $v_{37} = 16$, $v_{59} = 22$, $v_{67} = 29$, et Kummer a trouvé $\text{Ind } E_{16} \equiv 24 \pmod{37}$, pour le facteur idéal de 149 correspondant à $\zeta - 17$, $\text{Ind } E_{22} \equiv 50 \pmod{59}$, pour l'idéal de 709 correspondant à $\zeta - 385$, $\text{Ind } E_{29} \equiv 4 \pmod{67}$, pour l'idéal de 269 correspondant à $\zeta - 47$ (2 étant choisi dans les trois cas pour la racine primitive, \pmod{l} , qui figure dans E_v). Enfin, les nombres $B_{v,l}$ sont congrus respectivement à $35 \times 37^2 \pmod{37^3}$, $41 \times 59^2 \pmod{59^3}$, et $49 \times 67^2 \pmod{67^3}$. Les trois conditions requises pour la démonstration sont donc remplies, de sorte que l'impossibilité de l'équation (1) est établie pour tous les exposants premiers l inférieurs à 100.

En dehors du résultat de Kummer, il a été obtenu peu de résultats nouveaux, dans le cas où xyz est $\equiv 0$, (mod l).

Signalons seulement un résultat négatif, qui conduit à abandonner une méthode qui paraissait s'appliquer aussi bien aux deux cas de $xyz \equiv 0$ ou $\not\equiv 0$, (mod l).

Il paraissait naturel de chercher si la congruence $x^n + y^n + z^n \equiv 0$, mod p , ne serait pas impossible en nombres entiers premiers à p , pourvu seulement qu'on prît le module p suffisamment grand : car, dans le cas de l'affirmative, l'impossibilité de l'équation (1) se trouverait complètement démontrée. Mais Dickson a montré que cette méthode devait être abandonnée, car :

THÉORÈME XV. — La congruence $x^n + y^n + z^n \equiv 0$, mod p , a toujours des solutions x, y, z , premières à p , dès que p dépasse une certaine limite. (Dickson, *On the congruence $x^n + y^n + z^n \equiv 0$, mod p ; et Lower limit for the number of sets of solutions of $x^e + y^e + z^e \equiv 0$, mod p .* J. f. d. Mathematik, Band 135.)

Hurwitz a donné de cette proposition une démonstration plus élémentaire tout en la généralisant. (*Ueber die Congruenz $ax^e + by^e + cz^e \equiv 0$, mod p .* J. f. d. Mathematik, Band 136.)



ERRATA ET RECTIFICATIONS

Tome I^{er}. — 1909

Page 265, ligne 12. *Au lieu de* au domaine, lire : ou domaine.

266, 13. *Au lieu de* α_m , lire : α^m .

» 15. Dans l'énoncé du théorème 2, l'expression *fonction entière* est synonyme de *polynôme entier* (et non de *série entière*); il en est de même dans tout l'ouvrage.

» 15 et 21. *Après* coefficients entiers, *ajouter* : rationnels.

268. *Remplacer la ligne 18 par :*

$$r_s = \frac{|1, \alpha, \dots, \omega, \dots, \alpha^{m-1}|}{|1, \alpha, \dots, \alpha^{s-1}, \dots, \alpha^{m-1}|} = \frac{|1, \alpha, \dots, \omega, \dots, \alpha^{m-1}| \times |1, \alpha, \dots, \alpha^{s-1}, \dots, \alpha^{m-1}|}{|1, \alpha, \dots, \alpha^{s-1}, \dots, \alpha^{m-1}|^2} = \frac{A_s}{d(\alpha)}.$$

Page 268. Dans l'avant-dernière ligne, *remplacer* $O_2^{(2)}, \dots, O_s^{(2)}$ *par* : $O_2^{(1)}, \dots, O_s^{(1)}$.

269, ligne 5. *Après* nombre, *ajouter* : entier.

270. *Intervertir la ligne 19 et la ligne de points suivante.*

271, ligne 1. *Ajouter à la fin* : ou module α .

» 3. *Au lieu de* d'après, lire : suivant.

» 10. *Après* coefficients, *ajouter* : entiers.

» 22. *Après* restes, *ajouter* : positifs.

». Dans l'antépénultième ligne, *après* premiers, *ajouter* : entre eux.

272, ligne 15. *Au lieu de* entier ω , lire : entier algébrique ω .

» 25. *Au lieu de* puissance, lire : forme.

» 28. *Remplacer le point-virgule* après n *par une virgule.*

273, 3. *Après* (α) , *ajouter un point-virgule.*

» 23. *Ajouter un point-virgule avant* : par hypothèse.

275, 1. *Au lieu de* claire, lire : clair.

» 14. *Au lieu de* puissances de a , lire : puissances de u .

» 17. *Au lieu de* b , lire : G .

- Page 275, ligne 29. *Au lieu de* égal, *lire* : équivalent.
 » 31. *Après première, ajouter* : P.
276. Dans l'énoncé du théorème 17, *après nombre, ajouter* : premier.
- 277, ligne 22. *Au lieu de* incongrus à, *lire* : incongrus suivant.
 » Dans l'antépénultième ligne, *remplacer* les formes *par* : des formes.
- 278, ligne 2. *Au lieu de* exciterait, *lire* : existerait.
- 279, 17. *Au lieu de* premier, *lire* : premiers.
- 280, 8. *Au lieu de* d'après, *lire* : suivant.
 » 11. *Remplacer les coefficients* α , α_i , etc., *par* : a , a_i , etc.
- » 14. *Au lieu de* Fx , *lire* : $F(x)$.
- 281, 8 et 9. *Au lieu de* d'après, *lire* : suivant.
 » 12. *Mettre des virgules* *après* alors, *et après* suivant \mathfrak{p} .
 » 13. *Au lieu de* (\mathfrak{p}) , *lire* (\mathfrak{p}^e) .
 » 14. *Au lieu de* α_i , *lire* : α_i .
 » 16. *Au lieu de* α_e , *lire* : α_e .
 » Dans l'antépénultième ligne, *mettre une virgule entre* ρ *et* $P(\rho)$.
- 282, ligne 6. *Mettre* : $d =$, *devant le carré du déterminant*.
283. Dans la dernière ligne, *après et, ajouter* : est.
284. *Ajouter à la fin* :
 « Toutefois, si (p) n'est divisible que par \mathfrak{p} et non par \mathfrak{p}^e , ces coefficients peuvent être tous divisibles par \mathfrak{p}^e . S'il en est ainsi, il suffit, pour obtenir une fonction Π_i satisfaisant aux conditions de l'énoncé, de prendre $\Pi_i = \Pi(x; u_1, \dots, u_m) + kp$, k étant un entier quelconque premier à p ». (G. H. et T. G.)
- 285, ligne 6. *Au lieu de* suites, *lire* : seules.
 » 12. *Au lieu de* \mathfrak{p}^e , *lire* : \mathfrak{p}^e .
 » 13. *Au lieu de* où $e' < e$ et F , *lire* : où l'on a $e' < e$ et où F est.
 » Dans l'antépénultième ligne, *remplacer* nombre *par* : membre.
- 286, ligne 16. *Au lieu de* précédentes, *lire* : précédents.
- 287, 1. *Au lieu de* des U_{ik} , *lire* : les U_{ik} .
- 288, 15. *Supprimer les points* *après* : $\Pi^{e'}$.
 » 6, à partir du bas. *Au lieu de* nombre, *lire* : membre.
- 290, 7. *Au lieu de* choisis, *lire* : choisi.
- 292, 1. *Au lieu de* de, *lire* : le.
- 293, 7, à partir du bas. *Après degré, ajouter* : r .
- » 4, à partir du bas. *Au lieu de* M , *lire* : m .
- 294, 7. *Remplacer le troisième terme écrit par* : $(\Xi^{(r-1)})^{r-1}$.
 » 15. *Remplacer* Ω_i , *par* : Ω'_i .
 » 22. *Au lieu de* déterminantes, *lire* : déterminants.
 » Dans la dernière ligne, *au lieu de* déterminant, *lire* : discriminant.

Page 296, ligne 5. *Après et, ajouter : de.*

297, 4. *Au lieu de conjuguées, lire : conjugués.*

» 19. *Remplacer f_s par : f_s .*

» 20. *Rectifier la seconde égalité (8) de la façon suivante :*

$$f_s = \frac{1}{i\sqrt{2}} [(\omega_1^{(s)} - \omega_1^{(s')})u_1 + \dots + (\omega_m^{(s)} - \omega_m^{(s')})u_m].$$

299, 6, à partir du bas. *Après formons, ajouter : au moyen de ces nombres.*

302, 6. *Remplacer $\Lambda^{\frac{1}{2}\lambda_r t}$ par : $\Lambda_r = e^{\frac{1}{2}\lambda_r t}$.*

303, 7. Dans le dernier crochet, *remplacer $l_i(\alpha)$ par : $l_r(\alpha)$.*

305, 1 et 2. *Remplacer deux quelconques de ces puissances par : il y aura deux de ces puissances qui.*

» 6. *Supprimer : chaque fois.*

» 7. *Au lieu de H^T , lire : H_T .*

» 8. *Au lieu de $M_T^{M_T}$, lire : $H_T^{M_T}$.*

» 9. *Au lieu de composants, lire : exposants de.*

» Dans l'avant-dernière ligne, *au lieu de ρ^H , lire : ρ^M .*

308, ligne 10, à partir du bas. *Au lieu de (j), lire : n(j).*

309, 5, à partir du bas. *Au lieu de déterminantes, lire : déterminants.*

310, 4. *Au lieu de déterminants, lire : déterminant.*

311, 8. *Mettre une virgule après et, et remplacer le point-virgule après = o par une virgule.*

» 10. *Au lieu de $|\xi^{(t)}(\xi)|$, lire : $|\xi^{(t)}(\varphi)|$.*

313, 6. *Remplacer $l_{r-1}(\eta)$ par : $l_{r-1}(\bar{\eta})$.*

» 8. *Remplacer $l_{r+1}(\eta) = l_{r+1}(\xi)$ par : $l_{r+1}(\eta) = l_{r+1}(\bar{\xi})$.*

314, 17. *Après norme, ajouter : n.*

316, 8. *Après nombres premiers, ajouter : p.*

» 9. *Supprimer : du corps.*

» 17. *Au lieu de h_{q-1} , lire : $h_q - 1$, et au lieu de $A_q^{h_q}$, lire : $A_1^{h_1}$.*

» 9, à partir du bas. *Au lieu de puissance de H_s , lire : puissance de H_t .*

317. Dernière ligne, *remplacer la dernière égalité par : $\gamma_q(A) = e^{\frac{2i\pi x_q}{h_q}}$.*

318, ligne 4, à partir du bas. *Après entiers, ajouter : des coefficients.*

319. Au bas de la page, *supprimer les accents des α dans la première ligne du déterminant.*

320. *L'anneau est ce que Dedekind a appelé ordre.*

» ligne 5, à partir du bas. *Après discriminant, supprimer : de.*

322, 3. *Au lieu de $\mathfrak{z} = \mathfrak{f}\theta$, lire : $\mathfrak{z} = \mathfrak{f}\mathfrak{d}$.*

» 2, à partir du bas. *Au lieu de déterminant, lire : discriminant.*

327. Dans la formule au bas de la page, *faire passer wR_r au dénominateur, et w_rR au numérateur.*

Tome II. — 1910

Page 225. *Au lieu de* corps des nombres de Galois, *lire* : corps de nombres de Galois.

- 244, ligne 3. *Au lieu de* engendrent des classes, *lire* : engendrent les classes.
 260, 13. *Après* est congru, *ajouter* : mod w .
 » 14. *Au lieu de* dans $k(\sqrt{m})$ un nombre entier, *lire* : un nombre entier dans $k(\sqrt{m})$.
 290, 17. *Au lieu de* Si le corps K , *lire* : Le corps K qui.
 298, 1 et 4. *Au lieu de* différent, *lire* : différent.
 312, 15, à partir du bas. *Au lieu de* mod (j) , *lire* : mod j .
 313, 2. *Au lieu de* $(\zeta\lambda - 1)^u$, *lire* : $(\zeta\lambda - 1)^u$.
 332, 4, à partir du bas. *Au lieu de* $\prod_{(e)}(1 - s^e)$, *lire* : $\prod_{(e)}(1 - s^e)$.
 337. A la dernière ligne, *au lieu de* note I, *lire* : note V.
 351, ligne 2, à partir du bas. *Lire à la fin* : ζM^* , *au lieu de* : M^* .
 355, 16 et 18. *Au lieu de* S^{-1} , *lire* : S^{l-1} .
 » 25. *Au lieu de* différent, *lire* : différent.
 360, 19, à partir du bas. *Au lieu de* $\mu^*(1 - \lambda^{k+1})^l \equiv 1 - \lambda^{ly}$, *lire* : $\mu^*(1 - \lambda^{k+1})^{ly} \equiv 1 - \lambda^l$.
 374, 11, à partir du haut et ligne 2 à partir du bas. *Au lieu de* x , *lire* : x .
 375, 12, à partir du bas. *Au lieu de* i_4 , *lire* : i .
 415, 5. *Au lieu de* paragraphes, *lire* : paragraphe.

Tome III. — 1911

Page 19, ligne 3, à partir du bas. *Au lieu de* et que, *lire* : et.

INDEX ALPHABÉTIQUE DES DÉFINITIONS⁽¹⁾

Abélien (corps).....	238 **	Conjugués (corps)	265 *
» relatif (corps).....	239 **	» (idéaux)	278 *
Ambige (idéal) dans un corps de Galois ..	252 **	» (nombres)	266 *
» » quadratique.	275 **	» relatifs (nombres)	290 *
» » kummerien.	394 **	Contenu (d'une forme).....	275 *
Anneau.....	320 *	Corps algébriques	265 *
Base (d'un anneau).....	320 *	» abéliens	238 **
» (d'un idéal d'anneau).....	321 *	» biquadratique.....	290 **
» (d'un corps).....	269 *	» de classes	254 **
» (d'un idéal).....	270 *	» conjugués.....	265 *
» (d'une famille d'unités).....	393 **	» » relatifs.....	290 *
» (d'une famille de classes).....	395 **	» circulaires.....	295 et 299 **
» normale.....	316 **	» » (généralisés)	307 **
» de Lagrange	324 **	» » réguliers.....	381 **
Caractères d'un nombre du second degré.	265 **	» cycliques.....	238 **
» d'un idéal d'un corps quadra-		» de décomposition.....	228 **
tique.....	266 **	» de Galois.....	225 **
» d'une classe	319 *	» » relatifs.....	239 **
Caractère de puissance	327 **	» d'inertie	228 **
Caractères d'un nombre kummerien	408 **	» kummeriens.....	349 **
» d'un idéal ».....	409 **	» » réguliers.....	381 **
Coefficients d'une forme.....	319 *	» quadratiques	255 **
Classe ambiguë (d'idéaux).....	275 **	» de ramification.....	231 **
» (d'idéaux d'un corps kum- merien	395 **	» » soulignés.....	233 **
Classes d'un anneau.....	328 *	» relatifs	290 *
» conjuguées relatives.....	395 **	» supérieurs	290 *
» fondamentales.....	318 *	Degré (d'un corps).....	265 *
» de formes.....	320 *	» (d'un idéal premier).....	276 *
» d'idéaux.....	308 *	» relatif	290 *
Classe principale.....	308 *	Densité des idéaux.....	240 **
Classes réciproques	309 *	Différente (d'un nombre)	267 *
» de modules	329 *	» (d'un corps)	288 *
Complexes.....	411 **	» relative	291 *
Conducteur (d'un anneau).....	322 *	Discriminant (d'un nombre)	267 *
Congru.....	271 *	» (d'un corps)	282 *
Conjuguées (formes)	274 *	» (d'un anneau)	321 *
		» (d'une classe de modules)	329 *

(1) Un seul * renvoie aux pages du tome Ier, 1909. — ** renvoient aux pages du tome II, 1910.

Discriminant (d'une forme)	319 *	Idéal invariant (corps de Galois)	226 **
» relatif.....	292 *	» » (corps kummeriens)	394 **
Dirichlet (corps biquadratique de).....	395 *	» premier	271 *
Divisible (forme)	274 *	Incongru	271 *
» (fonction).....	282 *	Indépendantes (classes).....	276 **
» (idéal)	271 *	» (unités).....	307 *
Domaine d'intégrité.....	321 *	Irréductibles module p (fonctions).....	283 *
Éléments	288 *	Invariant (complexe)	411 **
Entiers algébriques	266 *	Kummerien	349 **
Équation fondamentale	282 *	» régulier.....	381 **
Équivalence (des idéaux).....	308 *	Lagrange (base normale de).....	324 **
» (des formes).....	274 *	» (résolvante de).....	324 **
» (des modules).....	329 *	Logarithmes d'une forme.....	301 *
» au sens restreint.....	316 *	» d'un nombre	301 *
Facteurs du nombre de classes	336 **	Modules	329 *
Familles d'unités	393 **	Nombre primitif	280 *
Fonction à coefficients entiers	282 *	Normale (base)	316 **
Formes du corps..	274 *	Norme d'une forme	274 *
» conjuguées	274 *	» d'un idéal	276 *
» composées.....	321 *	» » d'anneau.....	327 *
» décomposables	319 *	» » d'un nombre.....	267 *
» » d'un corps.....	320 *	» » relative	291 *
Forme fondamentale	282 *	Polynôme adjoint	366 **
» première.....	274 *	Primaire (nombre)	391 **
» primitive.....	318 *	» » de \mathfrak{p} (nombre)	413 **
» unité	274 *	Première (fonction)	283 *
» » rationnelle.....	274 *	Premiers entre eux	271 *
Galois (corps de)	225 **	Produit de deux idéaux.....	271 *
Genres (dans les corps quadratiques)...	266 **	» » classes	309 *
» » kummeriens) ...	410 **	» » complexes	411 **
» (d'un complexe).....	411 **	» » genres.....	410 **
Groupe d'un corps de Galois.....	226 **	Régulier	381 **
» de décomposition	228 **	Régulateur	307 *
» d'inertie	228 **	Résidu de puissance	318 **
» de ramification	231 **	» » de norme	357 **
» » souligné.....	233 **	Résolvante de Lagrange	324 **
Idéal.....	270 *	Semi-primaire (nombre)	330 **
» ambige (corps de Galois).....	252 **	Unités	300 *
» » (corps quadratiques).....	275 **	» indépendantes.....	307 *
» » (corps kummeriens).....	395 **	» fondamentales.....	307 *
» d'anneau.....	321 *	» relatives.....	248 **
» » régulier.....	326 *	» circulaires.....	305 **
» conjugué	278 *	» (familles).....	393 **
» » relatif	291 *		

TABLE DES MATIÈRES

PRÉFACE PAR M. G. HUMBERT	I
AVERTISSEMENT	II
PRÉFACE DE L'AUTEUR	III
Tome I^{er}. — 1909	
Table des ouvrages cités dans le texte	257
PREMIÈRE PARTIE. — Théorie générale.	
CHAPITRE I. — <i>Nombres algébriques et corps algébriques.</i>	
§ 1. — Les corps et les corps conjugués	265
§ 2. — Entiers algébriques	266
§ 3. — Norme, différente, discriminant d'un nombre. Base d'un corps	267
CHAPITRE II. — <i>Idéaux du corps.</i>	
§ 4. — Multiplication et division des idéaux. Idéaux premiers	269
§ 5. — Décomposition unique d'un idéal en idéaux premiers	272
§ 6. — Les formes du corps et leur contenu	274
CHAPITRE III. — <i>Congruences par rapport aux idéaux.</i>	
§ 7. — La norme d'un idéal et ses propriétés	276
§ 8. — Théorème de Fermat pour les idéaux. Fonction $\varphi(\mathfrak{a})$	279
§ 9. — Nombres primitifs suivant un idéal premier	280
CHAPITRE IV. — <i>Le discriminant du corps et ses diviseurs.</i>	
§ 10. — Diviseurs du discriminant. Lemmes sur les polynômes	282
§ 11. — Équation fondamentale : décomposition et discriminant	285
§ 12. — Éléments et différente du corps. Théorème sur les diviseurs du discriminant du corps	287
§ 13. — Détermination des idéaux premiers. Diviseur fixe de la forme unité rationnelle U	288
CHAPITRE V. — <i>Corps relatifs.</i>	
§ 14. — Norme, différente et discriminant relatifs	290
§ 15. — Propriétés de la différente et du discriminant relatifs	292
§ 16. — Décomposition d'un élément du corps k dans le corps supérieur K . Théorème sur la différente de K	295

CHAPITRE VI. — *Unités du corps.*

§ 17. — Existence de nombres conjugués vérifiant en valeur absolue certaines inégalités.	296
§ 18. — Théorèmes sur la valeur absolue du discriminant.....	298
§ 19. — Existence des unités. Lemme sur l'existence d'une unité de nature particulière..	300
§ 20. — Démonstration de l'existence des unités.....	303
§ 21. — Unités fondamentales. Régulateur. Système d'unités indépendantes.....	306

CHAPITRE VII. — *Classes d'idéaux.*

§ 22. — Classes d'idéaux. Le nombre des classes est fini.....	307
§ 23. — Applications.....	308
§ 24. — Détermination des classes. Sens plus restreint de la notion de classe	310
§ 25. — Lemme sur la valeur asymptotique du nombre de tous les idéaux principaux divisibles par un idéal donné.....	310
§ 26. — Détermination du nombre de classes par le résidu de $\zeta(s)$ pour $s = 1$	313
§ 27. — Autres développements de $\zeta(s)$	316
§ 28. — Composition des classes d'idéaux.....	316
§ 29. — Caractères d'une classe. Généralisation de $\zeta(s)$	317

CHAPITRE VIII. — *Les formes décomposables du corps.*

§ 30. — Formes décomposables. Les classes de formes et leur composition.....	317
------------------------------------------------------------------------------	-----

CHAPITRE IX. — *Les anneaux du corps.*

§ 31. — Anneaux. Idéaux d'anneaux.....	320
§ 32. — Anneaux définis par un seul entier algébrique. Théorème sur la différente d'un entier du corps.....	321
§ 33. — Idéaux d'anneaux réguliers. Leur divisibilité.....	325
§ 34. — Unités d'un anneau. Classes d'un anneau.....	327
§ 35. — Modules et classes de modules.....	328

DEUXIÈME PARTIE. — *Corps de Galois.*CHAPITRE X. — *Idéaux premiers du corps de Galois et de ses sous-corps.*Tome II. — 1910

§ 36. — Décomposition unique en idéaux premiers des idéaux d'un corps de Galois.....	225
§ 37. — Éléments, différente et discriminant d'un corps de Galois.....	227
§ 38. — Sous-corps d'un corps de Galois.	228
§ 39. — Corps de décomposition, corps d'inertie d'un idéal premier.....	228
§ 40. — Théorème sur le corps de décomposition.....	230
§ 41. — Corps de ramification d'un idéal premier.....	231
§ 42. — Théorème sur le corps d'inertie.....	232
§ 43. — Théorèmes sur les groupes et corps de ramification.....	232
§ 44. — Groupes et corps de ramification soulignés.....	233
§ 45. — Résumé des théorèmes sur la décomposition d'un nombre premier p dans le corps de Galois.	234

CHAPITRE XI. — <i>Différents et discriminants du corps de Galois.</i>	
§ 46. — Différentes du corps d'inertie et des corps de ramification.....	236
§ 47. — Les diviseurs du discriminant du corps de Galois.....	237
CHAPITRE XII. — <i>Rapports entre les propriétés arithmétiques et algébriques d'un corps de Galois.</i>	
§ 48. — Le corps de Galois relatif, corps abélien relatif, corps cyclique relatif.....	238
§ 49. — Propriétés algébriques des corps d'inertie et de ramification. Représentation des nombres d'un corps de Galois par des radicaux dans le domaine du corps de décomposition.....	239
§ 50. — Densité des idéaux premiers du premier degré; relation de cette densité avec les propriétés algébriques du corps.....	240
CHAPITRE XIII. — <i>Composition des corps.</i>	
§ 51. — Corps de Galois composé d'un corps et de ses conjugués.....	242
§ 52. — Composition de deux corps dont les discriminants sont premiers entre eux.....	242
CHAPITRE XIV. — <i>Idéaux premiers du premier degré. Notion de classe.</i>	
§ 53. — Les classes d'idéaux peuvent être engendrées par les idéaux premiers du premier degré.....	244
CHAPITRE XV. — <i>Corps cyclique relatif de degré premier.</i>	
§ 54. — Puissance symbolique. Théorème sur les nombres de norme relative égale à 1	246
§ 55. — Système d'unités relatives fondamentales.....	248
§ 56. — Existence dans le corps d'une unité de norme relative égale à 1 et qui n'est pourtant pas le quotient de deux unités conjuguées relatives.....	250
§ 57. — Idéaux ambiges et différente relative du corps cyclique relatif.....	252
§ 58. — Théorème fondamental sur les corps cycliques relatifs dont la différente relative est égale à 1. Définition de ce corps comme corps de classes.....	253
TROISIÈME PARTIE. — <i>Les corps quadratiques.</i>	
CHAPITRE XVI. — <i>Décomposition des nombres dans un corps quadratique.</i>	
§ 59. — Base et discriminant d'un corps quadratique.....	255
§ 60. — Idéaux premiers d'un corps quadratique.....	256
§ 61. — Symbole $\left(\frac{a}{w}\right)$	258
§ 62. — Unités du corps quadratique.....	259
§ 63. — Classes d'idéaux.....	260
CHAPITRE XVII. — <i>Genres dans un corps quadratique et leurs caractères.</i>	
§ 64. — Symbole $\left(\frac{n, m}{w}\right)$	260
§ 65. — Caractères d'un idéal.....	265
§ 66. — Caractères d'une classe d'idéaux. Genre.....	266

§ 67. — Théorème fondamental sur les genres.....	267
§ 68. — Lemme sur les corps quadratiques dont les discriminants ne sont divisibles que par un seul nombre premier.....	267
§ 69. — Loi de réciprocité des restes quadratiques. Lemme sur le symbole $(\frac{n, m}{w})$	268
§ 70. — Démonstration de la relation fondamentale du théorème 100 entre tous les caractères d'un genre.....	271

CHAPITRE XVIII. — *Existence des genres.*

§ 71. — Théorème sur les normes des nombres d'un corps quadratique.....	272
§ 72. — Classes du genre principal.....	274
§ 73. — Idéaux ambiges.....	275
§ 74. — Classes d'idéaux ambiges.....	275
§ 75. — Classes ambiges déterminées par des idéaux ambiges.....	276
§ 76. — Classes ambiges sans idéal ambige.....	277
§ 77. — Nombre des classes ambiges.....	278
§ 78. — Démonstration arithmétique de l'existence des genres.....	279
§ 79. — Expression transcendante du nombre de classes et application à la démonstration de l'existence d'une limite positive pour un certain produit infini.....	279
§ 80. — Existence d'une infinité de nombres premiers pour lesquels des nombres donnés ont des caractères de résidus quadratiques donnés.....	281
§ 81. — Existence d'une infinité d'idéaux premiers ayant des caractères donnés à l'avance dans le corps c	283
§ 82. — Démonstration transcendante de l'existence des genres et des autres résultats des paragraphes 71 à 77.....	285
§ 83. — Conception plus étroite de l'équivalence et de la classe.....	285
§ 84. — Le théorème fondamental avec cette nouvelle conception.....	286

CHAPITRE XIX. — *Nombre des classes d'un corps quadratique.*

§ 85. — Symbole $(\frac{a}{w})$ pour un nombre composé.....	287
§ 86. — Expression finie du nombre de classes.....	287
§ 87. — Corps biquadratique de Dirichlet.....	290

CHAPITRE XX. — *Anneaux et modules d'un corps quadratique.*

§ 88. — Anneaux d'un corps quadratique.....	291
§ 89. — Théorème sur les classes de modules d'un corps quadratique. Formes quadratiques binaires.....	291
§ 90. — Théories élémentaire et supérieure des corps quadratiques.....	292

QUATRIÈME PARTIE. — *Les corps circulaires.*CHAPITRE XXI. — *Les racines de l'unité d'indice premier l et le corps circulaire qu'elles définissent.*

§ 91. — Degré du corps circulaire des $l^{\text{èmes}}$ racines de l'unité et décomposition du nombre premier l dans ce corps.....	295
§ 92. — Base et discriminant du corps circulaire.....	297
§ 93. — Décomposition des nombres premiers.....	298

CHAPITRE XXII. — Racines mèmes de l'unité, m étant composé et corps circulaire correspondant.	
§ 94. — Le corps des racines m èmes de l'unité.....	299
§ 95. — Degré du corps circulaire des l èmes racines de l'unité et décomposition du nombre premier l dans ce corps.....	300
§ 96. — Base et discriminant du corps circulaire des l èmes racines de l'unité.....	301
§ 97. — Le corps circulaire général. Degré, discriminant, idéaux premiers.....	301
§ 98. — Unités du corps $c(e^{\frac{2i\pi}{m}})$. Définition des « unités circulaires ».....	303
CHAPITRE XXIII. — Propriétés du corps circulaire comme corps abélien.	
§ 99. — Le groupe du corps circulaire des racines l èmes de l'unité.....	306
§ 100. — Généralisation. Théorème fondamental sur les corps abéliens.....	307
§ 101. — Lemme général sur les corps cycliques.....	308
§ 102. — Sur certains facteurs premiers du discriminant d'un corps cyclique de degré l^h	309
§ 103. — Le corps cyclique de degré u , dont le discriminant ne contient que u et les corps cycliques de degré u^h et 2^h qui contiennent U_4 et Π_4 comme sous-corps.....	312
§ 104. — Démonstration du théorème fondamental sur les corps abéliens.....	314
CHAPITRE XXIV. — Les résolvantes d'un corps circulaire des racines lèmes de l'unité.	
§ 105. — Définition et existence de la base normale.....	316
§ 106. — Les corps abéliens de degré premier l et de discriminant p^{l-1}	317
§ 107. — Propriétés caractéristiques des résolvantes.....	318
§ 108. — Décomposition de la l ème puissance d'une résolvante dans le corps des racines l èmes de l'unité.....	321
§ 109. — Une équivalence relative aux idéaux du premier degré du corps des racines l èmes de l'unité.....	322
§ 110. — Détermination de toutes les bases normales et de toutes les résolvantes.....	323
§ 111. — La base normale et la résolvante de Lagrange.....	324
§ 112. — Propriétés caractéristiques de la résolvante de Lagrange.....	324
CHAPITRE XXV. — Loi de réciprocité pour les résidus de lèmes puissances entre un nombre rationnel et un nombre du corps des racines lèmes de l'unité.	
§ 113. — Caractère de puissance d'un nombre et symbole $\left\{ \frac{\alpha}{\mathfrak{p}} \right\}$	327
§ 114. — Lemme sur le caractère de puissance de la l ème puissance de la résolvante de Lagrange.....	329
§ 115. — Démonstration de la loi de réciprocité entre un nombre rationnel et un nombre quelconque de $c(\zeta)$	330
CHAPITRE XXVI. — Détermination du nombre de classes d'idéaux.	
§ 116. — Le symbole $\left[\frac{a}{l} \right]$	334
§ 117. — Expression du nombre des classes dans le corps circulaire des racines m èmes de l'unité.....	335
§ 118. — Démonstration des formules du nombre des classes de $c(e^{\frac{2i\pi}{m}})$	338

§ 119. — Existence d'une infinité de nombres premiers qui ont pour un nombre donné un reste donné premier à ce dernier.....	340
§ 120. — Représentation de toutes les unités du corps circulaire au moyen d'unités circulaires.....	342

CHAPITRE XXVII. — *Applications aux corps quadratiques.*

§ 121. — Expression des unités d'un corps quadratique réel au moyen d'unités circulaires.....	342
§ 122. — Loi de réciprocité des résidus quadratiques.....	343
§ 123. — Les corps quadratiques imaginaires de discriminant premier.....	345
§ 124. — Détermination du signe de la somme de Gauss.....	346

CINQUIÈME PARTIE. — **Les corps kummeriens.**CHAPITRE XXVIII. — *Décomposition des nombres d'un corps circulaire dans un corps kummerien.*

§ 125. — Définition d'un corps kummerien.....	349
§ 126. — Discriminant relatif d'un corps kummerien.....	350
§ 127. — Le symbole $\left\{ \frac{v, \mu}{w} \right\}$	353
§ 128. — Idéaux premiers d'un corps kummerien.....	354

CHAPITRE XXIX. — *Résidus et non-résidus de normes d'un corps kummerien.*

§ 129. — Définition des résidus de normes et des non-résidus.....	357
§ 130. — Théorème sur le nombre des résidus de normes. Idéaux de ramification.....	357
§ 131. — Le symbole $\left\{ \frac{v, \mu}{w} \right\}$	365
§ 132. — Lemmes sur le symbole $\left\{ \frac{v, \mu}{w} \right\}$ et les résidus de normes mod 1.....	368
§ 133. — Distinction des résidus et non-résidus avec le symbole $\left\{ \frac{v, \mu}{w} \right\}$	373

CHAPITRE XXX. — *Existence d'une infinité d'idéaux premiers ayant des caractères de puissances donnés dans un corps kummerien.*

§ 134. — Valeur limite d'un produit infini.....	377
§ 135. — Idéaux premiers de $c(\zeta)$ ayant des caractères de puissance donnés.....	378

CHAPITRE XXXI. — *Corps circulaires réguliers.*

§ 136. — Définition des corps circulaires réguliers, des nombres premiers réguliers et des corps kummeriens réguliers.....	381
§ 137. — Lemme sur la divisibilité par l du premier facteur du nombre de classes de $c\left(e^{\frac{2i\pi}{l}}\right)$	381
§ 138. — Lemme sur les unités du corps circulaire $c\left(e^{\frac{2i\pi}{l}}\right)$ dans le cas où l ne divise le numérateur d'aucun des $\frac{l-3}{2}$ premiers nombres de Bernoulli.....	384

TABLE DES MATIÈRES.

62 m

139. — Critère pour les nombres premiers réguliers.....	387
§ 140. — Système particulier d'unités indépendantes d'un corps circulaire régulier.....	389
§ 141. — Propriété caractéristique des unités d'un corps circulaire régulier.....	390
§ 142. — Nombres primaires d'un corps circulaire régulier.....	391

CHAPITRE XXXII. — *Classes d'idéaux invariantes et genres d'un corps kummerien régulier.*

§ 143. — Familles d'unités d'un corps circulaire régulier.....	393
§ 144. — Idéaux invariants, classes d'idéaux invariantes d'un corps kummerien régulier.....	394
§ 145. — Familles de classes dans un corps kummerien régulier.....	395
§ 146. — Deux lemmes généraux sur les unités fondamentales relatives d'un corps cyclique relatif de degré premier impair.....	396
§ 147. — Les classes d'idéaux déterminées par les idéaux invariants.....	398
§ 148. — La totalité des classes d'idéaux invariantes.....	405
§ 149. — Caractères d'un nombre et d'un idéal dans un corps kummerien régulier.....	407
§ 150. — Caractères d'une classe et notion de genre.....	409
§ 151. — Limites supérieures du degré de la famille issue de toutes les classes invariantes.....	410
§ 152. — Complexes d'un corps kummerien régulier.....	411
§ 153. — Limites supérieures du nombre des genres d'un corps kummerien régulier.....	412

CHAPITRE XXXIII. — *Loi de réciprocité des résidus de l'ièmes puissances dans un corps circulaire régulier.*

§ 154. — La loi de réciprocité des résidus de l'ièmes puissances et les lois complémentaires.....	413
§ 155. — Idéaux premiers de première et de seconde espèce dans un corps circulaire régulier.....	414
§ 156. — Lemmes sur les idéaux premiers de première espèce.....	417
§ 157. — Cas particulier de la loi de réciprocité pour deux idéaux premiers.....	420
§ 158. — Existence d'idéaux premiers auxiliaires pour lesquels la loi de réciprocité se vérifie.....	422
§ 159. — Démonstration de la première loi complémentaire.....	424
§ 160. — Démonstration de la loi de réciprocité entre deux idéaux premiers quelconques.....	424
§ 161. — Démonstration de la deuxième loi complémentaire.....	427

CHAPITRE XXXIV. — *Nombre des genres d'un corps kummerien régulier.*

§ 162. — Théorème sur le symbole $\left\{ \frac{v, \mu}{w} \right\}$	428
§ 163. — Théorème fondamental sur les genres d'un corps kummerien régulier.....	429
§ 164. — Les classes du genre principal dans un corps kummerien régulier.....	431
§ 165. — Sur les normes relatives des nombres d'un corps kummerien régulier.....	432

CHAPITRE XXXV. — *Nouvelle méthode pour la théorie d'un corps kummerien régulier.*

§ 166. — Propriétés essentielles des unités d'un corps circulaire régulier.....	435
§ 167. — Démonstration d'une propriété des nombres primaires d'idéaux premiers de seconde espèce	437
§ 168. — Démonstration de la loi de réciprocité pour les cas où l'un des deux idéaux premiers est de seconde espèce	439

§ 169. — Lemme sur le produit $\Pi' \left\{ \frac{v, \mu}{w} \right\}$ étendu à tous les idéaux premiers w autres que 1 .	443
§ 170. — Le symbole $\{v, \mu\}$ et la loi de réciprocité entre deux idéaux premiers quelconques.	445
§ 171. — Coïncidence des symboles $\{v, \mu\}$ et $\left\{ \frac{v, \mu}{1} \right\}$.	447

CHAPITRE XXXVI. — *L'équation diophantine $\alpha^m + \beta^m + \gamma^m = 0$.*

§ 172. — Impossibilité de l'équation $\alpha^l + \beta^l + \gamma^l = 0$ pour les exposants premiers réguliers l .	448
§ 173. — Autres recherches sur l'impossibilité de $\alpha^m + \beta^m + \gamma^m = 0$	454

NOTES DE M. G. HUMBERT

Tome III. — 1911
(présent volume).

NOTE I. — Démonstration du lemme 2 (théorème d'Hurwitz)	1
NOTE II. — Démonstration du théorème fondamental 8 par la méthode d'Hurwitz mentionnée au paragraphe 6	3
NOTE III. — Démonstration des inégalités fondamentales de Minkowski pour n formes linéaires à n variables	8
NOTE IV. — Questions diverses concernant les bases des idéaux d'un corps quadratique.	13

NOTES DE M. TH. GOT

NOTE V. — Détail de la démonstration de la seconde expression du nombre de classes d'idéaux du corps circulaire des racines $l^{\text{èmes}}$ de l'unité, l étant premier.	17
NOTE VI. — Recherches sur le théorème de Fermat faites par Kummer et divers auteurs, postérieurement à la démonstration de l'impossibilité en nombres entiers de l'équation $x^l + y^l + z^l = 0$, donnée par Kummer pour les exposants l premiers réguliers.	21
<i>Errata et rectifications</i>	62 a
<i>Index alphabétique des définitions</i>	62 e
<i>Table des matières</i>	62 g

—25—