RÉSULTATS ET PROBLÈMES DE LA THÉORIE DES CORPS DE CLASSES

par P. RIBENBOIM

(Instituto de Matemática Pura e Aplicada do Conselho
Nacional de Pesquisas, Rio de Janeiro)

§ 1. Introduction, cas particuliers.

Un des problèmes fondamentaux de la théorie arithmétique des nombres algébriques c'est la détermination de la décomposition des idéaux premiers d'un corps de nombres algébriques lorsqu'on passe à une extension algébrique finie.

Dans le cas d'une *extension quadratique* du corps des nombres rationnels, par exemple $K = \mathbb{R}_0(\sqrt{a})$, nous savons exprimer la condition pour qu'un nombre premier p se décompose, se ramifie ou reste premier en K par l'intermédiaire du *symbole de Kronecker*. En effet, le discriminant de K étant égal à $d = a$ lorsque $a \equiv 1 \pmod{4}$, ou bien $d = 4a$ lorsque $a \equiv 2$ ou $3 \pmod{4}$, si le premier p est impaire alors on a :

$$\left\{ \begin{array}{l} \left(\frac{d}{p}\right) = +1 \text{ équivaut à } p = \mathbf{P}_1 \cdot \mathbf{P}_2 \text{ (idéaux premiers dis-} \\ \qquad \qquad \qquad \text{tincts)} \\ \left(\frac{d}{p}\right) = 0 \text{ équivaut à } p|d \text{ ou encore à } p = \mathbf{P}^2 \\ \left(\frac{d}{p}\right) = -1 \text{ équivaut à que } p \text{ soit un idéal premier de } K \\ \qquad \qquad \qquad \text{ayant degré } 2 \end{array} \right.$$

Si par contre $p = 2$ alors :

$$\left\{ \begin{array}{l} d \text{ impaire, } \left(\frac{d}{8}\right) = +1, \text{ équivaut à } 2 = \mathbf{P}_1 \cdot \mathbf{P}_2 \text{ (idéaux} \\ \qquad \qquad \qquad \text{premiers distincts)} \\ d \text{ pair équivaut à } 2 = \mathbf{P}^2 \\ d \text{ impair, } \left(\frac{d}{8}\right) = -1, \text{ équivaut à que } 2 \text{ soit un idéal} \\ \qquad \qquad \qquad \text{premier de } K \text{ ayant degré } 2. \end{array} \right.$$

Dans le cas des *corps circulaires*, obtenus par l'adjonction d'une racine primitive de l'unité, nous allons indiquer les lois de décomposition des premiers dans les différents cas possibles.

Premier cas: Supposons d'abord que $K = R_0(\xi)$, où ξ est une racine primitive p -ième de l'unité, p étant un premier impaire. Alors l'équation minimale de ξ est $(X^p - 1)/(X - 1) = X^{p-1} + \dots + X + 1 = 0$, $[K : R_0] = p - 1$, K possède une base d'intégrité égale à $\{1, \xi, \xi^2, \dots, \xi^{p-1}\}$, le discriminant de $K|R_0$ est $d_{K|R_0} = (-1)^{\frac{p-1}{2}} p^{p-2}$. Dans ce cas, on a $p = \mathbf{P}^{p-1}$, où $\mathbf{P} = (1 - \xi)$ (idéal principal engendré par $1 - \xi$). Si q est un premier distinct de p , si f est le plus petit entier tel que $q^f \equiv 1 \pmod{p}$ alors f divise $p - 1$, donc $p - 1 = f \cdot g$ et q se décompose de la façon suivante: $q = Q_1 \cdot Q_2 \dots Q_g$, où chaque idéal premier Q_i possède degré f .

Deuxième cas: Supposons maintenant que $K = R_0(\xi)$, où ξ est une racine primitive p^h -ième de l'unité, p étant un premier. Alors l'équation minimale de ξ est

$$(X^{p^h} - 1)/(X^{p^{h-1}} - 1) = X^{p^{h-1}(p-1)} + X^{p^{h-1}(p-2)} + \dots + X^{p^{h-1}} + 1 = 0, [K : R_0] = \varphi(p^h) = p^{h-1}(p-1)$$

(indicateur de Euler de p^h), K possède une base d'intégrité égale à $\{1, \xi, \xi^2, \dots, \xi^{p^{h-1}(p-1)-1}\}$, le discriminant de $K|R_0$ est $d_{K|R_0} = p^{p^{h-1}(p^h-h-1)}$ lorsque $p^h \neq 4$ et $p \equiv 1$ ou $2 \pmod{4}$, ou bien $d_{K|R_0} = -p^{p^{h-1}(p^h-h-1)}$ lorsque $p^h = 4$ ou $p \equiv 3 \pmod{4}$. Dans ce cas, on a $p = \mathbf{P}^{p^{h-1}(p-1)}$ où $\mathbf{P} = (1 - \xi)$. Si q est un premier distinct de p , si f est le plus petit entier tel que $q^f \equiv 1 \pmod{p}$ alors f divise $p^{h-1}(p-1)$, donc $p^{h-1}(p-1) = f \cdot g$ et q se décompose de la façon suivante: $q = Q_1 \cdot Q_2 \dots Q_g$, où chaque idéal premier Q_i possède degré g .

Troisième cas (général): Supposons maintenant que $K = R_0(\xi)$, où ξ est une racine primitive m -ième de l'unité, m étant un entier positif distinct de 2. Soit $m = p_1^{h_1} \cdot p_2^{h_2} \dots p_r^{h_r}$ la décomposition de m en facteurs premiers; soit ξ_i une racine primitive $p_i^{h_i}$ -ième de l'unité; alors $\xi = \xi_1^{a_1} \cdot \xi_2^{a_2} \dots \xi_r^{a_r}$, où a_i sont les entiers déterminés par la relation $1/m = a_1/p_1^{h_1} + \dots + a_r/p_r^{h_r}$. Alors, si $K_i = R_0(\xi_i)$ ($i = 1, \dots, r$) on a $K = K_1 \dots K_r$ (corps composé). L'équation minimale de ξ est $\Phi_m(X) = 0$ (équation cyclotomique),

$[K : R_0] = \varphi(m) = \prod p_i^{h_i-1} (p_i - 1)$ (indicateur de Euler de m), K possède une base d'intégrité égale à $\{1, \xi, \dots, \xi^{\varphi(m)}\}$, le discriminant de $K | R_0$ est $d_{K|R_0} = \pm \prod p_i^{h_i-1} (p_i^{h_i} - 1)$.

Chacun des premiers p_i qui divise m se décompose de la façon suivante: $p_i = (\mathbf{P}_{i1} \dots \mathbf{P}_{i g_i})^{f_i}$, où f_i est le plus petit entier tel que $p_i^{f_i} \equiv 1 \pmod{m/p_i^{h_i}}$ et $g_i \cdot f_i = \varphi(m/p_i^{h_i})$. Si q est un premier qui ne divise pas m , alors $q = \mathbf{Q}_1 \dots \mathbf{Q}_g$, où f est le plus petit entier tel que $q^f \equiv 1 \pmod{m}$ et $f \cdot g = \varphi(m)$, et chaque idéal premier $\mathbf{Q}_i$ possède degré f .

On voit ainsi que pour un corps circulaire $R_0(\xi)$, où ξ est une racine m -ième primitive de l'unité, à un nombre fini d'exceptions près, la décomposition de deux nombres premiers congrus modulo m est du même type, et ainsi la décomposition de p dépend exclusivement de sa classe modulo m . Par cette raison, nous disons que le corps circulaire $K = R_0(\xi)$ est un *corps de classes*.

Nous allons montrer que cela est aussi vrai pour les extensions quadratiques; pour cela il faut d'abord montrer que toute extension quadratique de R_0 est contenue dans un corps circulaire; il en résultera que la loi de décomposition des nombres premiers dans ce corps circulaire induira la loi de décomposition dans le corps quadratique contenu; par comparaison des lois de décomposition obtenue directement et induite par celle du corps circulaire, on arrivera à la loi de réciprocité quadratique.

Soit p un premier impaire, ξ une racine primitive p -ième de l'unité. La somme $\tau_a = \sum \left(\frac{x}{p}\right) \cdot \xi^{ax}$ (pour x non congruent à 0 modulo p) est appelée la *somme de Gauss* définie par la racine primitive p -ième de l'unité ξ^a (où a n'est pas congruent à 0 (mod. p)). La somme de Gauss τ_1 sera notée simplement τ ; on a $\tau_a = \left(\frac{a}{p}\right) \cdot \tau$, la vérification étant simple.

Théorème de Gauss. Tout corps quadratique sur le corps des rationnels est contenu dans un corps $R_0(\xi)$ (corps circulaire), engendré par une racine primitive de l'unité.

En effet, d'abord $\tau^2 = p^*$, où $p^* = p$ lorsque $p \equiv 1 \pmod{4}$ ou $p^* = -p$ lorsque $p \equiv -1 \pmod{4}$. En effet,

$$\tau^2 = \sum \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \xi^x \cdot \xi^y = \sum \left(\frac{x \cdot y}{p}\right) \xi^{x+y}$$

(somme pour x, y non congruents à 0, modulo p); en posant

$$y \equiv x \cdot t \pmod{p},$$

x fixe, on a

$$\tau^2 = \sum_{t, x} \left(\frac{x^2 \cdot t}{p} \right) \xi_{x(1+t)} = \sum_t \left(\frac{t}{p} \right) \sum_x \xi_{x(1+t)}$$

(sommées pour t, x non congruents à 0, modulo p). D'autre part, on a

$$\xi^a + \xi^{2a} + \dots + \xi^{(p-1)a} = \begin{cases} p-1 & \text{lorsque } a \equiv 0 \pmod{p} \\ -1 & \text{dans le cas contraire.} \end{cases}$$

Il résulte que

$$\tau^2 = - \left[\left(\frac{1}{p} \right) + \left(\frac{2}{p} \right) + \dots + \left(\frac{p-2}{p} \right) \right] + \left(\frac{-1}{p} \right) \cdot (p-1) = p \left(\frac{-1}{p} \right) - \sum \left(\frac{t}{p} \right) = p \cdot (-1)^{\frac{p-1}{2}} = p^*$$

(somme étendue aux t non congruents à 0, modulo p). Cela montre que $R_0(\sqrt{p^*}) \subseteq R_0(\xi)$.

Généralement, soit $K = R_0(\sqrt{a})$ un corps quadratique absolu; puisque $\sqrt{a} = (\sqrt{-1})^\alpha \cdot (\sqrt{2})^\beta \cdot \prod_i (\sqrt{p_i})^{\gamma_i}$, avec $\alpha, \beta = 0$ ou 1, p_i les facteurs premiers impaires de la décomposition de a , et en remarquant que $\sqrt{-1} = i$ avec $i^4 = 1$, et que $\sqrt{2}$ s'exprime avec des racines 8-ièmes de l'unité, et enfin que $\sqrt{p_i} = \pm \tau$, on conclut que $K = R_0(\sqrt{a}) \subseteq R_0(\xi)$.

Il résulte de ce théorème que la loi de décomposition des premiers dans l'extension quadratique peut être obtenue à partir de la loi de décomposition dans une extension circulaire contenant l'extension quadratique. Par comparaison avec la loi obtenue directement, on a arrive à la loi de réciprocité quadratique (sur le corps des rationnels) et aux lois complémentaires: si p, q sont des premiers distincts et impaires, alors

$$\left(\frac{p}{q} \right) \left(\frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$$

et aussi

$$\left(\frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}}.$$

En généralisant le symbole de Legendre, on peut considérer des expressions du type $\left(\frac{a}{b}\right)$ avec a, b entiers impairs, et on obtient les formules suivantes:

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2} \frac{b-1}{2} + \frac{\text{sgn}(a)-1}{2} \frac{\text{sgn}(b)-1}{2}}$$

$$\frac{-1}{b} = (-1)^{\frac{b-1}{2} + \frac{\text{sgn}(b)-1}{2}}, \quad \left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$$

Enfin, ces formules sont encore valables lorsqu'on permet que b soit un possible discriminant d'un corps quadratique.

De l'examen de ces formules on déduit que si $p \equiv p' \pmod{d}$ (avec p, p' non diviseurs du discriminant d du corps quadratique $K = R_0(\sqrt{a})$) alors $\left(\frac{p}{d}\right) = \left(\frac{p'}{d}\right)$, donc la décomposition d'un premier p dépend exclusivement de sa classe modulo d (à l'exception d'un nombre fini de premiers). Par cette raison, nous disons que le corps quadratique $K = R_0(\sqrt{a})$ est un *corps de classes*.

§ 2. La théorie de Hilbert.

Hilbert a cherché à établir une relation entre la décomposition d'idéaux premiers et une généralisation de la loi de réciprocité quadratique. Tout d'abord il a considéré le cas des corps quadratiques relatifs à un corps de nombres algébriques (non nécessairement égal à celui des nombres rationnels); ensuite, il a considéré aussi le cas des corps relativement abéliens, en énonçant des théorèmes qui ont été démontrés plus tard par Fürtwangler. Toutefois, dans la théorie de Hilbert il restait toujours une lacune qui a seulement été comblée plus tard par Takagi.

Dans cette théorie d'extensions de corps de nombres algébriques distincts de celui des nombres rationnels, il y a un fait qui joue un rôle essentiel et est responsable des difficultés nouvelles, à savoir, l'existence, découverte par Kronecker, de corps contenant strictement le corps de base et ayant discriminant relatif égal à 1; ce sont les corps non ramifiés, qui seront exactement les sous-corps du corps de classes absolu associé au corps de base.

Nous allons maintenant décrire, en lignes générales, les définitions et théorèmes énoncés par Hilbert.

Soit R un corps de nombres algébriques (de degré fini sur le corps des rationnels) et K une extension galoisienne finie de R .

Définition. K est dit un *corps de classes* de R lorsque les seuls idéaux de R qui se décomposent en K en idéaux premiers distincts ayant degré absolu égal à 1, sont les idéaux premiers principaux ayant degré absolu égal à 1.

Si $R = R_0$ alors le seul corps de classes (au sens de Hilbert) pour R_0 est R_0 lui-même, car le corps de classes possède discriminant égal à 1.

THÉORÈME H 1. (existence et unicité). Pour tout corps de nombres algébriques R il existe un et un seul corps de classes K .

THÉORÈME H 2 (isomorphisme). Le corps de classes K est une extension abélienne de R ; plus précisément, $\text{Gal}(K|R) \cong \mathcal{I}/\mathcal{P}$ (groupe multiplicatif des classes d'idéaux fractionnaires modulo les idéaux fractionnaires principaux), don $[K : R] = h$, nombre de classes d'idéaux de R .

THÉORÈME H 3 (discriminant). Le corps de classes K est une extension non ramifiée de R , c. a. d le discriminant relatif $d_{K|R}$ est égal à l'idéal unité de R .

THÉORÈME H 4 (décomposition). Tout idéal premier $\mathbf{P}$ de R se décompose en K selon la règle suivante: si f est le plus petit entier tel que $\mathbf{P}^f$ soit un idéal principal (c. a. d. f est l'ordre de $\mathbf{P}$ mod. $\mathcal{P}$ dans le groupe $\mathcal{I}/\mathcal{P}$) alors $\mathbf{P}$ est un produit de h/f idéaux premiers distincts de K , ayant degré f .

Du théorème H 4 il résulte aussitôt que la décomposition en K d'un idéal premier de R dépend uniquement de sa classe dans le groupe $\mathcal{I}/\mathcal{P}$; cela justifie la dénomination de corps de classes qu'il a donné au corps K .

§ 3. La théorie de Takagi.

Takagi a généralisé la théorie de Hilbert en utilisant la notion de groupe admissible d'idéaux, introduite auparavant par Weber.

Définition. Soit R un corps de nombres algébriques; pour tout idéal entier $\mathbf{M}$ de R soit $\mathcal{I}^{(\mathbf{M})}$ le groupe multiplicatif des idéaux fractionnaires de R premiers avec $\mathbf{M}$, et soit $\mathcal{R}^{(\mathbf{M})}$ le groupe multiplicatif des idéaux principaux fractionnaires (a) , avec $a \equiv 1$

(mod. $\mathbf{M}$) et a totalement positif. $\mathcal{R}^{(\mathbf{M})}$ s'appelle le *rayon* défini par $\mathbf{M}$, tout groupe multiplicatif $\mathcal{H}$ d'idéaux de $\mathbf{R}$ tel que $\mathcal{R}^{(\mathbf{M})} \subseteq \mathcal{H} \subseteq \mathcal{I}^{(\mathbf{M})}$ s'appelle un *groupe admissible* d'idéaux de $\mathbf{R}$, associé à $\mathbf{M}$.

Tout d'abord il est utile de remarquer que pour tout idéal entier $\mathbf{M}$, le rayon $\mathcal{R}^{(\mathbf{M})}$ possède indice fini dans $\mathcal{I}^{(\mathbf{M})}$.

Il se peut très bien qu'un groupe multiplicatif d'idéaux $\mathcal{H}$ soit admissible associé à des idéaux distincts $\mathbf{M}, \mathbf{M}'$. On est conduit aux considérations suivantes. Soit, dans l'ensemble des groupes admissibles d'idéaux de $\mathbf{R}$, la relation d'équivalence suivante: si $\mathcal{H}, \mathcal{H}'$ sont des groupes admissibles associés à $\mathbf{M}, \mathbf{M}'$, posons $\mathcal{H} \sim \mathcal{H}'$ lorsqu'il existe un idéal entier $\mathbf{A}$ tel que $\mathcal{H} \cap \mathcal{I}^{(\mathbf{A})} = \mathcal{H}' \cap \mathcal{I}^{(\mathbf{A})}$. On démontre alors que dans chaque classe de groupes admissibles équivalents il existe un groupe admissible $\mathcal{H}$ associé à un idéal $\mathbf{F}$, de façon que si $\mathcal{H}'$ est équivalent à $\mathcal{H}$ et associé à $\mathbf{M}$, alors $\mathbf{F} | \mathbf{M}$. L'idéal entier $\mathbf{F}$, univoquement défini de cette façon, s'appelle le *conducteur* (de la classe d'équivalence) du groupe admissible $\mathcal{H}$; alors si $\mathcal{H}$ est un groupe admissible ayant conducteur $\mathbf{F}$, $\mathcal{R}^{(\mathbf{F})} \subseteq \mathcal{H} \subseteq \mathcal{I}^{(\mathbf{F})}$, si $\mathcal{H}'$ est équivalent à $\mathcal{H}$, $\mathcal{R}^{(\mathbf{A}\mathbf{F})} \subseteq \mathcal{H}' \subseteq \mathcal{I}^{(\mathbf{A}\mathbf{F})}$ avec $\mathbf{A}$ idéal entier, alors $\mathcal{H}' = \mathcal{H} \cap \mathcal{I}^{(\mathbf{F})}$; de cette remarque il résulte un isomorphisme canonique entre les groupes quotients $\mathcal{I}^{(\mathbf{F})}/\mathcal{H}$ et $\mathcal{I}^{(\mathbf{A}\mathbf{F})}/\mathcal{H}'$. De même, si $\mathcal{H}, \mathcal{H}'$ sont deux groupes admissibles d'idéaux ayant conducteurs $\mathbf{F}, \mathbf{F}'$ resp., s'il existe un idéal multiple commun $\mathbf{A} \cdot \mathbf{F} = \mathbf{A}' \cdot \mathbf{F}'$ des conducteurs, de façon que $\mathcal{H}_1 \subseteq \mathcal{H}_1'$ où $\mathcal{H}_1$ est le groupe admissible associé à $\mathbf{A} \cdot \mathbf{F}$, $\mathcal{H}_1 \sim \mathcal{H}$, et $\mathcal{H}_1'$ est le groupe admissible associé à $\mathbf{A}' \cdot \mathbf{F}'$, $\mathcal{H}_1' \sim \mathcal{H}'$, alors nécessairement $\mathbf{F}' | \mathbf{F}$ et pour tout idéal $\mathbf{M}$ multiple de $\mathbf{F}$, si $\mathcal{H}^{(\mathbf{M})}, \mathcal{H}'^{(\mathbf{M})}$ sont des groupes admissibles associés à $\mathbf{M}$, respectivement équivalents à $\mathcal{H}, \mathcal{H}'$, alors $\mathcal{H}^{(\mathbf{M})} \subseteq \mathcal{H}'^{(\mathbf{M})}$; s'il en est ainsi on peut écrire $\{\mathcal{H}\} \subseteq \{\mathcal{H}'\}$.

Les groupes admissibles ayant conducteur $\mathbf{F} = (1)$ sont tous les groupes admissibles équivalents à des groupes $\mathcal{H}$ tels que $\mathcal{P}_0 = \mathcal{R}^{(1)} \subseteq \mathcal{H} \subseteq \mathcal{I}$, où $\mathcal{P}_0$ désigne le groupe multiplicatif des idéaux principaux restreints, c. a. d. engendrés par les éléments totalement positifs, $\mathcal{I}$ le groupe multiplicatif des idéaux fractionnaires non nuls de $\mathbf{R}$. Dans ce cas, l'indice de $\mathcal{P}_0$ dans $\mathcal{I}$ est le nombre h_0 de classes restreintes d'idéaux ($h_0 \geq h =$ nombre de classes d'idéaux).

Définition. Soit R un corps de nombres algébriques, $\mathcal{H}$ un groupe admissible d'idéaux de R associé à l'idéal entier M . On dit qu'une extension galoisienne K de R est un *corps de classes* de R associé à $\mathcal{H}$ lorsqu'un idéal premier P de degré absolu 1 appartient à $\mathcal{H}$ si et seulement si P est premier avec M et il se décompose en K en idéaux premiers distincts ayant degré absolu égal à 1.

Dans le cas particulier où $\mathcal{H} = \mathcal{P}$ (ayant conducteur (1)) cette définition se réduit à celle de Hilbert. Si $\mathcal{H} = \mathcal{P}_0$ (ayant conducteur (1)) le corps de classes défini ci-dessus s'appelle *corps de classes absolu*.

Avec ces définitions, Takagi a réussi à démontrer, par un chemin indirect, les théorèmes suivants:

THÉORÈME T 1 (existence et unicité). Pour toute classe d'équivalence de groupes admissibles $\mathcal{H}$ d'idéaux de R , il existe un et un seul corps de classes K de R associé à $\mathcal{H}$.

THÉORÈME T 2 (isomorphisme). Le corps de classes K de R associé à $\mathcal{H}$ est une extension abélienne; plus précisément, si F est le conducteur de $\mathcal{H}$ alors $\text{Gal}(K|R) \cong \mathcal{I}^{(F)}/\mathcal{H}^{(F)}$ (groupe multiplicatif quotient du groupe des idéaux fractionnaires premiers à F , par le groupe admissible $\mathcal{H}^{(F)}$ où $\mathcal{H}^{(F)} \sim \mathcal{H}$, $\mathcal{R}^{(F)} \subseteq \mathcal{H}^{(F)} \subseteq \mathcal{I}^{(F)}$); donc $[K : R] = (\mathcal{I}^{(F)} : \mathcal{H}^{(F)})$.

THÉORÈME T 3 (discriminant). Tout idéal premier qui divise le discriminant relatif $d_{K|R}$ divise aussi le conducteur F du groupe admissible $\mathcal{H}$ auquel est associé le corps des classes K .

THÉORÈME T 4 (décomposition). Tout idéal premier P de R qui ne divise par le conducteur F de $\mathcal{H}$ se décompose en K selon la règle suivante: si f est le plus petit entier tel que $P^f \in \mathcal{H}^{(F)}$ (c. a. d. f est l'ordre de P mod. $\mathcal{H}^{(F)}$ dans le groupe $\mathcal{I}^{(F)}/\mathcal{H}^{(F)}$) où $\mathcal{H}^{(F)} \sim \mathcal{H}$, $\mathcal{R}^{(F)} \subseteq \mathcal{H}^{(F)} \subseteq \mathcal{I}^{(F)}$, alors p est un produit de $[K : R]/f$ idéaux premiers distincts de K , ayant degré f .

En plus de ces résultats qui généralisent ceux de Hilbert, Takagi a aussi démontré:

THÉORÈME T 5 (inclusion inverses). Soient $\mathcal{H}, \mathcal{H}'$ deux groupes admissibles d'idéaux de R , et soient K, K' leurs respectifs corps de classes. Alors $K \subseteq K'$ si et seulement si $\{\mathcal{H}\} \supseteq \{\mathcal{H}'\}$.

Enfin, Takagi a démontré l'important théorème réciproque qui établit une correspondance parfaite entre les extension abélien-

nes relatives et les groupes admissibles d'idéaux, ou bien les corps de classes:

THÉORÈME T 6 (réciproque). Si K est une extension abélienne finie du corps de nombres algébriques R , il existe une classe d'équivalence de groupes admissibles d'idéaux $\mathcal{H}$, univoquement déterminée avec la propriété que K soit le corps de classes associé.

Il résulte alors le complément au théorème du discriminant:

THÉORÈME T 3' (discriminant et conducteur). Si K est le corps de classes associé au groupe admissible $\mathcal{H}$ ayant conducteur F , alors les facteurs premiers de $d_{K|R}$ (discriminant relatif) et F sont les mêmes.

De ces théorèmes on déduit aussitôt que le type de décomposition d'un idéal premier P de R lorsqu'on passe à une extension abélienne K , associée au groupe admissible $\mathcal{H}$ d'idéaux de R ayant conducteur F , $\mathcal{R}^{(F)} \subseteq \mathcal{H} \subseteq \mathcal{I}^{(F)}$, est déterminé uniquement à partir de la classe de P mod. $\mathcal{H}$ dans le groupe multiplicatif $\mathcal{I}^{(F)}/\mathcal{H}$ (lorsque P est distinct des idéaux premiers en nombre fini qui divisent Φ , et qui sont les seuls idéaux premiers qui se ramifient en passant à K).

Enfin, pour la décomposition des idéaux premiers exceptionnels, qui divisent le conducteur F de $\mathcal{H}$, c. a. d.; qui se ramifient en passant à K , corps de classes associé à $\mathcal{H}$, Takagi a démontré:

THÉORÈME T 4' (décomposition des idéaux premiers ramifiés). Soit K une extension abélienne finie d'un corps de nombres algébriques R , $\mathcal{H}$ le groupe admissible d'idéaux de R déterminé par K , F son conducteur, $\mathcal{R}^{(F)} \subseteq \mathcal{H} \subseteq \mathcal{I}^{(F)}$. Si P est un idéal premier de R qui divise F , si $\mathcal{H}'$ est le plus petit groupe admissible d'idéaux de R contenant $\mathcal{H}$ et dont le conducteur F' n'est pas multiple de P , si f est le plus petit entier tel que $P^f \in \mathcal{H}'$, alors P se décompose en $[K : R]/f \cdot (\mathcal{H}' : \mathcal{H})$ idéaux premiers distincts de K , ayant ramification $(\mathcal{H}' : \mathcal{H})$ et degré f .

Le théorème classique de Kronecker-Weber peut se déduire facilement comme cas particulier des résultats de Takagi:

THÉORÈME DE KRONECKER-WEBER. Tout corps de nombres algébriques abélien absolu (c. a. d. extension abélienne de R_0) est un corps circulaire (c. a. d. contenu dans un corps du type $R_0(\xi)$, où ξ est une racine de l'unité).

En effet, si K est un corps de nombres algébriques abélien absolu, par le théorème réciproque, K est le corps de classes (sur R_0) associé à un groupe admissible $\mathcal{H}$ d'idéaux, dont le conducteur sera noté (f) , et $\mathcal{R}^{(f)} \subseteq \mathcal{H} \subseteq \mathcal{I}^{(f)}$. Le corps de classes sur R_0 associé au rayon $\mathcal{R}^{(f)}$ est $R_0(\xi)$, où ξ est une racine primitive f -ième de l'unité; en effet, par la théorie des corps circulaires, tout premier $p \equiv 1 \pmod{f}$ se décompose en $R_0(\xi)$ en facteurs premiers distincts ayant degré 1, d'autre part, si p est un premier avec une telle décomposition en $R_0(\xi)$ alors il est faux que p divise le discriminant et nécessairement p est premier avec f et enfin, on a $p \equiv 1 \pmod{f}$ car il se décompose en idéaux premiers ayant degré 1. Il en résulte, par l'unicité du corps de classes, que $R_0(\xi)$ est le corps de classes associé au rayon $\mathcal{R}^{(f)}$. Enfin, de $\mathcal{R}^{(f)} \subseteq \mathcal{H}$, on déduit que $K \supseteq R_0(\xi)$.

Il est encore important de signaler le résultat difficile obtenu par Fürtwangler en 1930 (démontrant un théorème énoncé auparavant par Hilbert):

THÉORÈME DE L'IDÉAL PRINCIPAL. Si K est le corps de classes absolu de R (défini par le rayon $\mathcal{P}_0 = \mathcal{R}^{(h)}$) tout idéal de R engendre un idéal principal de K .

§ 4. *Loi de réciprocité de Artin et des restes de puissances.*

Dans ce paragraphe nous voulons préciser le théorème d'isomorphisme (th. T 2) en montrant que l'isomorphisme indiqué entre $\text{Gal}(K|R)$ et $\mathcal{I}^{(\mathbb{F})}/\mathcal{H}$ est *canonique*. Précisément, cet isomorphisme est donné par la *loi de réciprocité générale de Artin*, dont la formulation se fait plus commodément avec la notion d'*idèle* de Chevalley.

Définition. Soit R un corps de nombres algébriques et pour chacun de ses idéaux premiers ou places à l'infini $\mathbf{P}$, soit $R_{\mathbf{P}}$ le corps complété de R par la valuation $w_{\mathbf{P}}$ définie par $\mathbf{P}$ c. a. d. le corps des nombres $\mathbf{P}$ -adiques de Hensel ou le corps des réels ou complexes). On appelle *idèle* de R à tout élément $(z_{\mathbf{P}})_{\mathbf{P}} \in \prod_{\mathbf{P}} R_{\mathbf{P}}^*$ de façon que $z_{\mathbf{P}}$ soit une unité $\mathbf{P}$ -adique sauf pour un nombre fini d'idéaux premiers $\mathbf{P}$ de R .

L'ensemble des idèles de R est un groupe multiplicatif, noté $\mathbf{J}_R$; le groupe multiplicatif R^* peut être plongé isomorphiquement de façon naturelle dans $\mathbf{J}_R$, donc on peut écrire $R^* \subseteq \mathbf{J}_R$ (à chaque $z \in R^*$ on associe la famille $(z_{\mathbf{P}})_{\mathbf{P}}$ avec $z_{\mathbf{P}} = z$ pour tout $\mathbf{P}$).

Si $K | R$ est une extension algébrique, si $(z_Q)_Q \in J_K$ alors on définit la norme $N(z_Q)_Q$ comme étant l'idèle $(y_P)_P y_P = \prod N_{Q|P}(z_Q)$ (produit étendu aux places Q qui divisent P) où $N_{Q|P}$ désigne la norme relative à l'extension $K_Q | R_P$.

Avant d'établir la loi de réciprocité de Artin, nous allons faire quelques considérations préliminaires.

Soit P un idéal premier ou place à l'infini de R , $K | R$ une extension abélienne, $Q_1, \dots, Q_g$ les idéaux premiers ou places à l'infini de K qui divisent P ; alors les corps de décomposition des Q_i coïncident; notons $Z(P)$ le corps de décomposition, $Z(P) = \text{Gal}(K | Z(P))$ le groupe de décomposition d'un quelconque Q_i qui divise P . Chacun des corps locaux K_{Q_i} est R_P -isomorphe à $K \cdot R_P$; on obtient tous les R_P -isomorphismes de K_{Q_i} sur $K \cdot R_P$ à partir d'un isomorphisme quelconque, en le composant avec les éléments de $Z(P)$. On en déduit que $N_{Q_i|P}(K_{Q_i}) = R_P \cap N(J_K)$.

A ce point, il est convenable d'étudier en détail les extensions abéliennes des corps du type R_P , qui sont des corps munis d'une valuation discrète et tels qu'ils soient complets et possèdent corps des restes fini. La *théorie locale des corps des classes* est exactement l'étude des extensions abéliennes des corps du type R_P .

Dans la théorie locale, Artin a défini l'*isomorphisme principal* du groupe $R_P / (R_P \cap N(J_K)) = R_P / N_{Q_i|P}(K_{Q_i})$ sur le groupe de Galois $Z(P) = \text{Gal}(K | Z(P))$.

La définition de l'isomorphisme principal de Artin se fait en lignes générales de la façon suivante: 1) on considère d'abord l'ensemble H , formé des groupes extensions de K_{Q_i} par $Z(P)$, lequel est un groupe multiplicatif en définissant l'opération de produit à partir de la multiplication des classes d'équivalence des systèmes de facteurs qui servent à définir les extensions de K_{Q_i} par $Z(P)$ (en langage moderne, H est isomorphe au 2^e groupe de cohomologie construit sur K_{Q_i} et $Z(P)$); 2) un théorème fondamental est celui qui affirme que le groupe multiplicatif H est cyclique ayant ordre égal à l'ordre du groupe $Z(P)$; 3) plus précisément, avec l'automorphisme de Frobenius défini par le corps des restes $\overline{K}_{Q_i}$ de K_{Q_i} , il est possible déterminer un *générateur principal* du groupe H . Notons $(a_{\sigma, \tau})_{\sigma, \tau \in Z(P)}$ un système de facteurs représentant de la classe d'équivalence de systèmes de facteurs qui est le générateur principal de H ; soit $f(\sigma) = \prod a_{\sigma, \tau} \in R_P$ (produit étendu aux $\tau \in Z(P)$) pour tout $\sigma \in Z(P)$; si $(a'_{\sigma, \tau})_{\sigma, \tau \in Z(P)}$ est un autre

système de facteurs de la même classe, alors

$$\frac{f'(\sigma)}{f(\sigma)} = \prod_{c_{\sigma, \tau}} \frac{a'_{\sigma, \tau}}{c_{\sigma, \tau}}$$

$\in N_{\mathbf{Q}_j | \mathbf{P}}(K \cdot \mathbf{Q}_j)$ (produit étendu aux $\tau \in Z(\mathbf{P})$)

Posons $\varphi_{K | \mathbf{R}, \mathbf{P}}(\sigma)$ égal à la classe de $f(\sigma)$ modulo $N_{\mathbf{Q}_j | \mathbf{P}}(K \cdot \mathbf{Q}_j)$, donc $\varphi_{K | \mathbf{R}, \mathbf{P}}$ est un isomorphisme de $Z(\mathbf{P})$ sur le groupe multiplicatif $R \cdot \mathbf{P} / N_{\mathbf{Q}_j | \mathbf{P}}(K \cdot \mathbf{Q}_j)$. Soit $\psi_{K | \mathbf{R}, \mathbf{P}} : R \cdot \mathbf{P} \rightarrow Z(\mathbf{P})$ l'homomorphisme canonique ayant noyau $N_{\mathbf{Q}_j | \mathbf{P}}(K \cdot \mathbf{Q}_j) = R \cdot \mathbf{P} \cap N(\mathbf{J}_K)$ et déduit de l'application $\bar{\varphi}_{K | \mathbf{R}, \mathbf{P}}$. Alors, $\psi_{K | \mathbf{R}, \mathbf{P}}$ est l'homomorphisme principal et l'isomorphisme déduit de $\psi_{K | \mathbf{R}, \mathbf{P}}$ est l'isomorphisme principal de Artin.

Enfin, soit $\psi_{K | \mathbf{R}} : \mathbf{J}_K \rightarrow G = \text{Gal}(K | \mathbf{R})$ l'application définie par $\psi_{K | \mathbf{R}}(z_{\mathbf{P}})_{\mathbf{P}} = \prod \psi_{K | \mathbf{R}, \mathbf{P}}(z_{\mathbf{P}})$ (ce produit est fini car $(z_{\mathbf{P}})_{\mathbf{P}}$ est un idéal).

THÉORÈME DE ARTIN (loi de réciprocité générale). L'application $\psi_{K | \mathbf{R}}$ est un homomorphisme de $\mathbf{J}_K$ sur le groupe de Galois $G = \text{Gal}(K | \mathbf{R})$ ayant noyau $R \cdot N(\mathbf{J}_K)$.

La démonstration se fait en plusieurs parties: a) si $a \in R$ alors $\psi_{K | \mathbf{R}}(a) = 1$; b) $\psi_{K | \mathbf{R}}$ est un homomorphisme sur le groupe de Galois G ; c) l'ordre de G est égal à l'indice $(\mathbf{J}_R : R \cdot N(\mathbf{J}_R))$. La démonstration de (c) se fait en deux étapes; tout d'abord on montre que l'ordre de G divise $(\mathbf{J}_K : R \cdot N(\mathbf{J}_K))$ (*première inégalité fondamentale*), ensuite on montre que l'ordre de G est un multiple de l'indice ci-dessus (*deuxième inégalité fondamentale*).

Nous allons maintenant indiquer comment est-il possible déduire la loi de réciprocité des restes de puissances m -ièmes à partir de la loi de réciprocité de Artin.

Soit $\mathbf{R}$ un corps contenant toutes les racines m -ièmes de l'unité. Un élément $a \in \mathbf{R}$ est dit un *reste de puissance m -ième modulo l'idéal premier $\mathbf{P}$* de $\mathbf{R}$ (où $\mathbf{P}$ ne divise pas a , m) lorsqu'il existe $b \in \mathbf{R}$ tel que $a \equiv b^m \pmod{\mathbf{P}}$.

Pour l'étude des restes de puissances m -ièmes mod. $\mathbf{P}$, on est naturellement conduit à considérer les extensions binômes $K | \mathbf{R}$, c. a. d. les corps des racines des binômes $X^m - a \in \mathbf{R}[X]$; rappelons que ce sont des extensions cycliques, ayant degré d égal au plus petit entier tel que a^d soit puissance m -ième d'un élément de $\mathbf{R}$, et en outre K est engendré par une quelconque racine $\sqrt[m]{a}$ de l'équa-

tion $X^m - a$, c. a. d. $K = \mathbf{R}(\sqrt[m]{a})$. Les idéaux premiers $\mathbf{P}$ de $\mathbf{R}$ qui se ramifient dans l'extension $\mathbf{R}(\sqrt[m]{a}) | \mathbf{R}$ sont exactement ceux tels que $\mathbf{P} | m$ ou bien $\mathbf{P} | a$; donc les seuls facteurs premiers du discriminant et du conducteur $\mathbf{F}$ de $K | \mathbf{R}$ sont les idéaux premiers qui divisent m ou a . En outre, si $\sigma \in G = \text{Gal}(K | \mathbf{R})$ alors $\sigma(\sqrt[m]{a}) = \omega_\sigma \cdot \sqrt[m]{a}$, où $\omega_\sigma \in \mathbf{R}$ est une racine m -ième de l'unité; l'application $\sigma \in G \rightarrow \omega_\sigma$ est un isomorphisme du groupe de Galois G sur un groupe de racines m -ièmes de l'unité.

Pour tout idéal $\zeta = (z_{\mathbf{P}})_{\mathbf{P}} \in \mathbf{J}_{\mathbf{R}}$ on a $\psi_{K|\mathbf{R}}(\zeta) \in G$ donc il existe une racine m -ième de l'unité, qui dépend de a , ζ , et qui sera notée $\left(\frac{a}{\zeta}\right)$ telle que $\psi_{K|\mathbf{R}}(\zeta)(\sqrt[m]{a}) = \left(\frac{a}{\zeta}\right) \sqrt[m]{a}$. Si $\mathbf{P}$ est un idéal premier non ramifié, si $t \in \mathbf{R}$ est un élément primitif selon $\mathbf{P}$, soit l'idéal $\tau = (z_{\mathbf{P}})_{\mathbf{P}}$, avec $z_{\mathbf{P}} = t$, $z_{\mathbf{P}'} = 1$ lorsque $\mathbf{P}' \neq \mathbf{P}$; on peut alors définir $\left(\frac{a}{\tau}\right)$ et cette définition ne dépend pas du particulier élément primitif t choisi, ce qui permet de noter $\left(\frac{a}{\mathbf{P}}\right)$ la racine m -ième de l'unité définie par la relation:

$$\psi_{K|\mathbf{R}}(\tau)(\sqrt[m]{a}) = \left(\frac{a}{\mathbf{P}}\right) \sqrt[m]{a}.$$

$\left(\frac{a}{\mathbf{P}}\right)$ s'appelle le *symbole de restes de puissances m -ièmes modulo $\mathbf{P}$* , et possède les propriétés suivantes:

$$1. \quad \left(\frac{a_1 a_2}{\mathbf{P}}\right) = \left(\frac{a_1}{\mathbf{P}}\right) \left(\frac{a_2}{\mathbf{P}}\right)$$

lorsque P divise m , P ne divise pas $a_1 a_2$

$$2. \quad \left(\frac{a}{\mathbf{P}}\right) = 1$$

(lorsque P ne divise pas a) si et seulement si a est une puissance m -ième de $\mathbf{R}_{\mathbf{P}}$, ou équivalamment a est congru modulo $\mathbf{P}$ à une puissance m -ième d'un élément de $\mathbf{R}$, c. a. d. a est un reste de puissance m -ième modulo $\mathbf{P}$

$$3. \quad \left(\frac{a}{\mathbf{P}}\right) \cdot a^{-\frac{NP-1}{m}} \equiv 1 \pmod{\mathbf{P}}$$

Dans le cas particulier où $R = R_0$ (corps des rationnels), $m = 2$ alors $\left(\frac{a}{\mathbf{P}}\right)$ devient le symbole de Legendre et la propriété (3) est la formule de Euler.

Comme dans le cas de la loi de réciprocité sur le corps des rationnels, il faut aussi étendre le domaine de définition du symbole de restes de puissances, en considérant le cas où $\mathbf{P}$ ne divise pas m et $\mathbf{P}$ divise a avec $w_{\mathbf{P}}(a) \equiv 0 \pmod{m}$; on dit que a est primaire pour l'idéal premier $\mathbf{P}$ (relativement à l'exposant m). Dans ce cas $w_{\mathbf{P}}(a)/m$ est entier et il existe $b \in R$ tel que $w_{\mathbf{P}}(b) = w_{\mathbf{P}}(a)/m$, donc P ne divise pas ab^{-m} ; de $R(\sqrt[m]{ab^{-m}}) = R(\sqrt[m]{a})$ et puisque $\mathbf{P}$ ne se ramifie pas dans $R(\sqrt[m]{a})$, on pose

$$\left(\frac{a}{\mathbf{P}}\right) = \left(\frac{ab^{-m}}{\mathbf{P}}\right) \text{ (symbole déjà défini);}$$

de même, la formule (1) reste valable. Enfin, pour tout diviseur $\mathbf{B} = \prod \mathbf{P}^{\beta_{\mathbf{P}}}$ du corps R , tel que si $\beta_{\mathbf{P}} \neq 0$ alors a est primaire pour $\mathbf{P}$, on peut poser: $\left(\frac{a}{\mathbf{B}}\right) = \prod \left(\frac{a}{\mathbf{P}}\right)^{\beta_{\mathbf{P}}}$; remarquons que pour chaque $a \in R$ l'ensemble de tels diviseurs est un groupe multiplicatif M_a . L'application $\mathbf{B} \rightarrow \left(\frac{a}{\mathbf{B}}\right)$ est un homomorphisme du groupe M_a dans le groupe des racines m -ièmes de l'unité, c. a. d. $\left(\frac{a}{\mathbf{B}_1 \mathbf{B}_2}\right) = \left(\frac{a}{\mathbf{B}_1}\right) \left(\frac{a}{\mathbf{B}_2}\right)$. Pour déterminer le noyau de cet homomorphisme, associons à chaque diviseur $\mathbf{B} \in M_a$ un idèle $\beta = \prod \tau_{\mathbf{P}}^{\beta_{\mathbf{P}}}$ avec $\tau_{\mathbf{P}} = (z_{\mathbf{P}'})_{\mathbf{P}'}$, $z_{\mathbf{P}} = t_{\mathbf{P}}$ élément primitif de $\mathbf{P}$, $z_{\mathbf{P}'} = 1$ lorsque $\mathbf{P}' \neq \mathbf{P}$; le noyau est formé des diviseurs $\mathbf{B}$ tels que l'idèle associé β appartienne à $R \cdot N(J_K)$. Cela découle aussitôt en appliquant la loi de réciprocité de Artin.

En particulier, si b est un élément de R appartenant au rayon $\mathcal{R}^{(\mathbf{F})}$, où $\mathbf{F}$ est le conducteur de $R(\sqrt[m]{a}) \mid R$, alors nécessairement $\left(\frac{a}{b}\right) = 1$ (par abus de notation on a écrit $\left(\frac{a}{b}\right)$ au lieu de $\left(\frac{a}{\text{div}(b)}\right)$, $\text{div}(b)$ étant le diviseur principal engendré par l'élément b).

Si on veut avoir la loi de réciprocité des restes de puissances sous une forme classique, et plus ressemblante à la loi de réciprocité quadratique, il faut travailler avec le *symbole normique de Hilbert* $\left(\frac{b, a}{\mathbf{P}}\right)$.

Pour tout élément $b \in \mathbf{R}$ et tout idéal premier ou place infinie $\mathbf{P}$ de $\mathbf{R}$, soit $\left(\frac{b, a}{\mathbf{P}}\right)$ la racine m -ième de l'unité définie par la relation $\psi_{K|\mathbf{R}, \mathbf{P}}(b) (\sqrt[m]{a}) = \left(\frac{b, a}{\mathbf{P}}\right)^m \sqrt[m]{a}$, où $\psi_{K|\mathbf{R}, \mathbf{P}}$ est l'homomorphisme principal défini pour l'extension $K|\mathbf{R}$ et associé à $\mathbf{P}$. La loi de réciprocité de Artin pour l'extension $\mathbf{R}(\sqrt[m]{a})|\mathbf{R}$ équivaut à $\left(\frac{b, a}{\mathbf{P}}\right) = 1$ (formule du produit) et la relation $\left(\frac{b, a}{\mathbf{P}}\right) = 1$ signifie que $b \in \mathbf{R} \subseteq \mathbf{R}_{\mathbf{P}}$ est la norme d'un élément de $\mathbf{R}_{\mathbf{P}}(\sqrt[m]{a})$. Ce symbole a les propriétés suivantes:

- 1) $\left(\frac{b, a}{\mathbf{P}}\right) = \left(\frac{a}{\mathbf{P}}\right)^{w_{\mathbf{P}}(b)}$ lorsque $\mathbf{P}$ est premier et ne divise pas le conducteur $\mathbf{F}$ de $K|\mathbf{R}$
- 2) $\left(\frac{b_1 b_2, a}{\mathbf{P}}\right) = \left(\frac{b_1, a}{\mathbf{P}}\right) \left(\frac{b_2, a}{\mathbf{P}}\right)$ quelques soient $b_1, b_2 \in \mathbf{R}$.
- 3) $\left(\frac{b, a_1 a_2}{\mathbf{P}}\right) = \left(\frac{b, a_1}{\mathbf{P}}\right) \left(\frac{b, a_2}{\mathbf{P}}\right)$ quelques soient $a_1, a_2 \in \mathbf{R}$.
- 4) $\left(\frac{b, a}{\mathbf{P}}\right) \left(\frac{a, b}{\mathbf{P}}\right) = 1$ quelques soient $a, b \in \mathbf{R}$.

Loi de réciprocité de restes de puissances m -ièmes. Soient $a, b \in \mathbf{R}$ (où $\mathbf{R}$ contient toutes les racines m -ièmes de l'unité), soient $\mathbf{F}_a, \mathbf{F}_b$ resp. les conducteurs des extensions $\mathbf{R}(\sqrt[m]{a})|\mathbf{R}, \mathbf{R}(\sqrt[m]{b})|\mathbf{R}$; posons $\text{div.}(a) = \mathbf{A} \cdot \mathbf{A}'$, où $\mathbf{A}$ est le produit des diviseurs premiers $\mathbf{P}$ tels que $\mathbf{P}$ divise $\text{div.}(a)$, $\mathbf{P}$ ne divise pas $\mathbf{F}_b$ et des plus grandes puissances m -ièmes possibles des diviseurs premiers $\mathbf{P}$ tels que $\mathbf{P}|\mathbf{F}_b$; de même, posons $\text{div.}(b) = \mathbf{B} \cdot \mathbf{B}'$ où $\mathbf{B}$ est le produit des diviseurs premiers $\mathbf{P}$ tels que $\mathbf{P}$ divise $\text{div.}(b)$, $\mathbf{P}$ ne divise pas $\mathbf{F}_a$, et des plus grandes puissances m -ièmes possibles de diviseurs premiers $\mathbf{P}$ tels que $\mathbf{P}|\mathbf{F}_a$. Notons $\Phi_{a,b}$ l'ensemble des places à infini

de $\mathbb{R}$ ou des premiers $\mathbf{P}$ tels que $\mathbf{P}$ divise le plus grand commun diviseur de $\mathbf{F}_a, \mathbf{F}_b$. Alors

$$\left(\frac{b}{\mathbf{A}}\right)\left(\frac{a}{\mathbf{B}}\right)^{-1} = \prod \left(\frac{b, a}{\mathbf{P}}\right),$$

produit étendu aux $\mathbf{P} \in \Phi_{a,b}$. En particulier, si $a, b \in \mathbb{R}$ et m sont deux à deux étrangers, alors

$$\left(\frac{b}{\mathbf{A}}\right)\left(\frac{a}{\mathbf{B}}\right)^{-1} = \prod \left(\frac{b, a}{\mathbf{P}}\right),$$

produit étendu aux $\mathbf{P} \in \Phi_m$, où Φ_m désigne l'ensemble des places à l'infini de $\mathbb{R}$ ou des diviseurs premiers $\mathbf{P}$ tels que $\mathbf{P} \mid m$. Enfin, si $\mathbb{R} = \mathbb{R}_0$ (corps des nombres rationnels), $m = 2$, si $a, b \in \mathbb{R}_0$ sont des nombres premiers impaires, alors on a

$$\left(\frac{b}{a}\right)\left(\frac{a}{b}\right)^{-1} = \left(\frac{b, a}{2}\right) \text{ avec } \left(\frac{b, a}{2}\right) = \pm 1,$$

selon qu'il existe ou non des solutions de $X^2 - aY^2 = b$ dans le corps premier de caractéristique 2.

Il est important de remarquer que seulement pour des corps particuliers on a déjà calculé explicitement la valeur du produit

$$\prod \left(\frac{b, a}{\mathbf{P}}\right) \text{ (produit étendu aux } \mathbf{P} \in \Phi_m)$$

§ 5. Relations avec le théorème de Dirichlet et les séries-L.

Dans ce paragraphe nous allons indiquer en lignes générales comment est-il possible déduire le théorème de Dirichlet (existence d'une infinité de nombres premiers dans toute progression arithmétique avec premier terme et différence relativement premiers) à partir de la théorie des corps de classes.

Soit $\mathcal{H}$ un groupe admissible d'idéaux de M , ayant conducteur $\mathbf{F}$, $\mathcal{R}^{(\mathbf{F})} \subseteq \mathcal{H} \subseteq \mathcal{I}^{(\mathbf{F})}$. A chacun des $(\mathcal{I}^{(\mathbf{F})} : \mathcal{H})$ caractères $\bar{\chi}$ du groupe abélien fini $\mathcal{I}^{(\mathbf{F})}/\mathcal{H}$ associons une application χ définie sur $\mathcal{I}$, en posant: $\chi(\mathbf{A}) = \bar{\chi}(\bar{\mathbf{A}})$ lorsque $\mathbf{A} \in \mathcal{I}^{(\mathbf{F})}$ et $\bar{\mathbf{A}}$ est la classe latérale de $\mathcal{I}^{(\mathbf{F})}/\mathcal{H}$ définie par $\mathbf{A}$; $\chi(\mathbf{A}) = 0$ lorsque $\mathbf{A} \in \mathcal{I}$, $\mathbf{A} \notin \mathcal{I}^{(\mathbf{F})}$. On définit alors les séries-L de $\mathbb{R}$ associées au groupe admissible d'idéaux $\mathcal{H}$, en écrivant pour tout paramètre complexe s tel que $\text{Re}(s) > 1$:

$$L(s | \chi) = \sum_{\mathbf{A}} \frac{\chi(\mathbf{A})}{N(\mathbf{A})^s}$$

(ces séries sont convergentes dans cette région). Comme dans le cas particulier où R est le corps des rationnels, on détermine les abscisses de convergence des séries- L . Dans le cas du caractère principal χ_0 ($\chi_0(\mathbf{A}) = 1$ pour tout $\mathbf{A} \in \mathcal{J}^{(\mathbb{F})}$) l'abscisse de convergence est 1 et on a $\lim (s-1) \cdot L(s|\chi_0) = c \cdot (\mathcal{J}^{(\mathbb{F})} : \mathcal{H})$, $c \neq 0$ constante, où la limite est prise lorsque s tend vers 1 par valeurs réelles à droite; le calcul de cette limite dépend de propriétés particulières des séries de Dirichlet. Dans le cas d'un caractère non principal $\chi \neq \chi_0$, l'abscisse de convergence est < 1 et $\lim L(s|\chi) = L(1|\chi)$ (fini). D'autre part, par l'identité de Euler, on peut exprimer les séries- L dans la région de convergence ($Re(s) > 1$) comme produit infini absolument convergent:

$$L(s|\chi) = \sum \frac{\chi(\mathbf{A})}{N(\mathbf{A})^s} = \prod \frac{1}{1 - \frac{\chi(\mathbf{P})}{N(\mathbf{P})^s}}$$

(somme étendue aux idéaux $\mathbf{A} \in \mathcal{J}$, produit étendu aux idéaux premiers $\mathbf{P} \in \mathcal{J}$).

En prenant les logarithmes, on obtient

$$\begin{aligned} \log L(s|\chi) &= \sum \frac{\chi(\mathbf{P})}{N(\mathbf{P})^s} + g(s|\chi) = \\ &= \sum_{\mathcal{C}} \chi(\mathcal{C}) \sum_{\mathbf{P} \in \mathcal{C}} \frac{1}{N(\mathbf{P})^s} + g(s|\chi) \end{aligned}$$

(la première somme étant étendue aux idéaux premiers $\mathbf{P} \in \mathcal{J}^{(\mathbb{F})}$, où $g(s|\chi)$ est une fonction qui reste bornée lorsque s tend vers 1, où $\mathcal{C}$ parcourt les classes latérales du groupe $\mathcal{J}^{(\mathbb{F})}/\mathcal{H}$ et où $\chi(\mathcal{C}) = \chi(\mathbf{P})$ quelque soit $\mathbf{P} \in \mathcal{C}$. En multipliant les expressions ci-dessus par $\chi(\mathcal{C}^{-1})$, en additionnant pour les différents caractères et en prenant compte des relations d'orthogonalité des caractères, on obtient:

$$\begin{aligned} (\mathcal{J}^{(\mathbb{F})} : \mathcal{H}) \cdot \sum_{\mathbf{P} \in \mathcal{C}} \frac{1}{N(\mathbf{P})^s} + \sum_{\chi} g(s|\chi) &= \log L(s|\chi_0) + \\ &+ \sum_{\chi \neq \chi_0} \log L(s|\chi) \end{aligned}$$

donc

$$\sum_{\mathbf{P} \in \mathcal{C}} \frac{1}{N(\mathbf{P})^s} = \frac{1}{(\mathcal{J}^{(\mathbb{F})} : \mathcal{H})} \cdot \log \frac{1}{s-1} + f(s) \quad [1]$$

où $f(s)$ est une fonction qui reste bornée ou tend vers $-\infty$ lorsque s tend vers 1.

D'autre part, soit $K|R$ une extension galoisienne et considérons la série- ζ de Dedekind du corps K , à savoir

$$\zeta_K(s) = \sum \frac{1}{N(\mathbf{B})^s} = \prod \frac{1}{1 - \frac{1}{N(\mathbf{Q})^s}}$$

pour $Re(s) > 1$ (sommes étendues aux idéaux $\mathbf{B}$ de K et aux idéaux premiers $\mathbf{Q}$ de K). Si on sépare les idéaux premiers de K selon leurs degrés absolus, en remarquant que le produit

$$\prod \frac{1}{1 - \frac{1}{N(\mathbf{Q})^s}}$$

étendu aux idéaux premiers $\mathbf{Q}$ ayant degré $f \geq 2$ reste borné (lorsque $s \rightarrow 1$), alors en prenant les logarithmes, on a

$$\begin{aligned} \log \zeta_K(s) &= \log \prod \frac{1}{1 - \frac{1}{N(\mathbf{Q})^s}} = \\ &= \sum \log \frac{1}{1 - \frac{1}{N(\mathbf{Q})^s}} = \sum \frac{1}{N(\mathbf{Q})^s} + g(s) \end{aligned}$$

(sommes et produits étendus aux idéaux premiers $\mathbf{Q}$ ayant degré absolu égal à 1), où $g(s)$ reste bornée (lorsque $s \rightarrow 1$). Or, $\lim_{s \rightarrow 1} (s-1) \cdot \zeta_K(s)$ est une constante non nulle; d'autre part, si $\mathbf{P}$ est un idéal premier de R (ayant degré 1) et qui se décompose en $[K:R] = n$ idéaux premiers distincts ayant degré 1 de K , $\mathbf{P} = \mathbf{Q}_1 \dots \mathbf{Q}_n$, alors $N_{K|R_0} \mathbf{Q}_i = N_{R|R_0} \mathbf{P}$, donc

$$\sum \frac{1}{N(\mathbf{Q})^s} = \log \frac{1}{s-1} + g(s)$$

(somme étendue aux idéaux premiers $\mathbf{Q}$ de K ayant degré absolu 1),

$$n \sum \frac{1}{N(\mathbf{P}_1)^s} = \sum \frac{1}{N(\mathbf{Q})^s}$$

(la première somme étant étendue aux idéaux premiers $\mathbf{P}_1$ de $\mathbf{R}$ ayant degré 1 et se décomposant en n idéaux premiers distincts de $\mathbf{K}$ ayant degré 1, tandis que la seconde somme est étendue aux idéaux premiers $\mathbf{Q}$ de $\mathbf{K}$ ayant degré absolu 1), donc enfin

$$\sum \frac{1}{N(\mathbf{P}_1)^s} = \frac{1}{n} \log \frac{1}{s-1} + g(s). \quad [2]$$

Or, en utilisant le théorème d'existence de corps de classes et en prenant pour $\mathbf{K}$ exactement le corps des classes sur $\mathbf{R}$ associé au groupe admissible d'idéaux $\mathcal{H}$, alors un idéal premier $\mathbf{P}$ est dans $\mathcal{H}$ si et seulement si $\mathbf{P}$ est un idéal premier de degré absolu 1 et qui se décompose en $\mathbf{K}$ en idéaux premiers distincts de degré 1; donc les premiers membres des relations [1] (pour la classe d'idéaux $\mathcal{C} = \mathcal{H}$) et [2] coïncident et alors nécessairement il de même des seconds membres; donc $f(s)$ reste bornée lorsque s tend vers 1, et ceci implique l'existence d'une infinité d'idéaux premiers $\mathbf{P} \in \mathcal{H}$, d'où nécessairement $L(1|\chi) \neq 0$ pour tout $\chi \neq \chi_0$ et on déduit l'existence dans chaque classe d'idéaux $\mathcal{C}$ modulo $\mathcal{H}$ d'une infinité d'idéaux premiers, même de degré 1.

En particulier, dans tout rayon $\mathcal{R}^{(\mathbf{F})}$ du corps $\mathbf{R}$ il existe une infinité d'idéaux premiers de degré 1. Si $\mathbf{R} = \mathbf{R}_0$, si f est un entier positif, alors on obtient le théorème classique de Dirichlet.

Ces considérations montrent que le cadre naturel du théorème de Dirichlet se trouve dans la théorie des corps de classes.

§ 6. Extensions abéliennes de corps imaginaires quadratiques et le 12^e problème de Hilbert.

Le théorème de Kronecker-Weber a permis de connaître toutes les extensions abéliennes $\mathbf{K}$ du corps des rationnels: ce sont les sous-corps des corps obtenus par adjonction de racines de l'unité; en d'autres termes, les éléments de $\mathbf{K}$ sont obtenus comme valeurs d'une fonction exponentielle $\exp(2\pi ix/m)$ lorsque x prend des valeurs rationnelles (ces valeurs, lorsque x appartient au corps de base, sont appelées les valeurs *singulières de la fonction exponentielle*).

Kronecker avait cru —et c'est cela le fameux "Kroneckerschen Jugendtraum"— que les éléments de toute extension abélienne $\mathbf{K}$ d'un corps imaginaire quadratique $\mathbf{R} = \mathbf{R}_0(\sqrt{-d})$ (avec $d > 0$) pouvaient être obtenus comme valeurs singulières d'une fonction

exponentielle et de la fonction elliptique modulaire $J(\tau)$. Plus tard, Fueter a démontré que sa conjecture était fautive et que pour certaines extensions abéliennes K de R il était nécessaire de considérer aussi les valeurs singulières de certaines fonctions elliptiques pour obtenir tous les éléments de K .

Le manque d'espace nous empêche de considérer plus longuement cette question. Nous voulons seulement signaler que ces recherches ont amené à la théorie de la *multiplication complexe*.

La question posée par Kronecker pour le cas d'un corps de base quadratique imaginaire a été plus tard considérée à nouveau par Hilbert et déjà sous une forme plus ample. C'est le 12^e problème de Hilbert; étant donné un corps de nombres algébriques R , déterminer des fonctions telles que chaque extension abélienne K de R puisse être obtenue en prenant des valeurs singulières de ces fonctions. Par l'étude de cette question on arrivera à comprendre pourquoi la théorie des fonctions analytiques joue un rôle aussi important en théorie des nombres.

§ 7. Théories du type des corps de classes.

Un des aspects les plus intéressants des résultats de la théorie des corps des classes est le suivant: la donnée des classes d'équivalence de groupes admissibles d'idéaux du corps de base R permet d'obtenir toutes les extensions abéliennes K de R , en vertu du théorème réciproque de Takagi. On peut ainsi dire, grossièrement, que les extensions abéliennes de R sont déjà en germe dans le corps R lui-même, ou plus précisément, peuvent être caractérisées par des objets définis uniquement en termes de R .

Il y a d'autres théories d'Algèbre qui partagent cet aspect avec la théorie des corps de classes et qui nous pouvons classer comme des théories *du type* des corps de classes, et dont le problème fondamental est le suivant: étant donné un corps de base R et un ensemble $\mathcal{E}$ de corps extensions de R , définir uniquement à partir de R , un ensemble $\mathfrak{D}$ d'objets (d'une nature qui dépend de chaque cas), et une application $\psi : \mathcal{E} \rightarrow \mathfrak{D}$, de façon qu'on ait: 1) ψ est une application *biunivoque* (c'est le théorème de caractérisation pour cette théorie), 2) ψ est une application *surjective* (c'est le théorème d'existence pour cette théorie). Il va sans dire qu'il y a dans cette formulation du problème un grand arbitraire; il faut donc limiter convenablement la nature du corps R ainsi que l'espèce d'extensions de R qui appartiennent à l'ensemble $\mathcal{E}$.

De même, pour que la théorie présente un intérêt, il faut que les objets de $\mathfrak{E}$ soient assez simples, en tout cas maniables. On dit alors que $\mathfrak{E}$ est une *famille d'invariants* pour les extensions de l'ensemble $\mathcal{E}$ et que ψ est une *classification* des extensions de $\mathcal{E}$ par les éléments de $\mathfrak{E}$.

Il est convenable d'illustrer avec quelques exemples ce qui nous venons de dire.

Exemple 1: la théorie locale des corps de classes. Dans ce cas, R est un corps valué discret complet ayant corps de restes fini, $\mathcal{E}$ est l'ensemble des extensions abéliennes (de degré fini) de R ; $\mathfrak{E}$ est l'ensemble des sous-groupes d'indice fini du groupe multiplicatif R ; ψ est l'application $N_{K|R}$.

Exemples 2: la théorie des extensions galoisiennes (de degré fini) d'un corps R , qui a été abordée par Hasse, Witt et leurs élèves. Dans un cas particulier important, Witt a obtenu des résultats plus complets: la théorie des extensions $p^{(g_1, g_2, \dots, g_r)}$ abéliennes d'un corps R de caractéristique $p > 0$, c. a. d. les extensions galoisiennes K de R , ayant groupe de Galois abélien qui admet une décomposition en produit direct de groupes cycliques ayant ordres $p^{g_1}, p^{g_2}, \dots, p^{g_r}$; $\mathfrak{E}$ est alors un certain ensemble de groupes additifs W de vecteurs de Witt de longueur finie construits sur le corps de base R .

BIBLIOGRAPHIE

- [1] ARTIN, *Algebraic Numbers and Algebraic Functions*, Princeton, 1950.
- [2] BOURBAKI, *Notes polycopiées sur la Théorie des Corps de Classes*, Paris.
- [3] DEURING, *Algebraische Begründung der komplexen Multiplikation*. Abh. Math. Sem. Hamburg, 16, 1949.
- [4] FÜRTWÄGLER, *Beweis des Hauptidealsatzes*. Abh. Math. Sem. Hamburg, 7, 1930.
- [5] HASSE, *Vorlesungen über Zahlentheorie*. Springer Verlag, Berlin, 1950.
- [6] *Bericht über neuere untersuchungen und Probleme aus der Theorie des algebraischen Zahlkörper. I - Klassenkörpertheorie*. Bericht D. Math. Ver., 35, 1926.
- [7] HASSE, *Neue Begründung der komplexen Multiplikation. I - Cralle J.*, 157, 1927 et 165, 1931.
- [8] HECKE, *Algebraischen Zahlen*, Chelsea Publ. Co. New York, 1948.
- [9] HILBERT, *Über die Theorie des relativ-quadratischen Zahlkörpers*. Math. Annalen, 51, 1898.
- [10] HILBERT, *Über die Theorie der relativ-Abelschen Zahlkörper*. Göttinger Nachrichten, 1898.
- [11] TAKAGI, *Über eine Theorie des relativ-Abelschen Zahlkörpers*. Journal Coll. Sci. Tokyo, 41, 1920.
- [12] TAKAGI, *Über das Reziprozitätsgesetz in einem beliebigen algebraischen Zahlkörper*. Journal Coll. Sci., Tokyo, 44, 1920.