SÉMINAIRE N. BOURBAKI

CLAUDE CHEVALLEY

Le théorème fondamental de la multiplication complexe

Séminaire N. Bourbaki, 1958, exp. n° 138, p. 19-31

<http://www.numdam.org/item?id=SB_1956-1958__4__19_0>

Séminaire BOURBAKI
(Décembre 1956)

LE THÉORÈME FONDAMENTAL DE LA MULTIPLICATION COMPLEXE.

(Démonstration de EICHLER [1])

par Claude CHEVALLEY

1. L'invariant j . Correspondances modulaires.

Soit E le demi-plan supérieur ; le groupe modulaire Γ opère dans E, et y définit par suite une relation d'équivalence R (la relation $R(\tau, \tau')$ est : il existe un $s \in \Gamma$ tel que $\tau' = s.\tau$). Soit $Q = E/R$; appelons holomorphes celles des fonctions g sur Q à valeurs complexes qui possèdent la propriété suivante : f étant l'application canonique de E sur Q, $g \circ f$ est une fonction holomorphe sur E ; les fonctions holomorphes sur Q sont donc déterminées par les fonctions holomorphes sur E qui sont invariantes par Γ. Nous admettrons les faits suivants : il existe une fonction holomorphe $\overline{j}$ sur Q qui est une bijection de Q sur le plan complexe, et toute fonction holomorphe sur Q se met sous la forme d'une fonction entière de $\overline{j}$; si $j = \overline{j} \circ f$, j admet un développement de Fourier de la forme

$$j(\tau) = \sum_{\nu=-1}^{\infty} c_\nu e^{2i\pi\nu\tau}$$

où les c_ν sont des nombres rationnels dont les dénominateurs ne font intervenir qu'un nombre fini de nombres premiers (dits dans la suite exceptionnels) : on a $c_{-1} = 1$.

Si n est un entier >0, nous désignerons par Γ_n l'ensemble des substitutions homographiques $\tau \to (a\tau - b)(c\tau - d)^{-1}$, où a, b, c, d sont des entiers et $ad - bc = n$. Il y a un nombre fini d'éléments s_i $(1 \leqslant i \leqslant r)$ de Γ_n tels que $\Gamma_n = \bigcup_{i=1}^{r} \Gamma s_i$, $\Gamma s_i \cap \Gamma s_j = \emptyset$ si $i \neq j$. Si $x \in E/R$, l'ensemble $S(x)$ des $f(s\tau)$, pour $s \in \Gamma_n$ et $\tau \in f^{-1}(x)$, est fini. Introduisons une indéterminée X et posons

$$F_n'(X ; \tau) = \prod_{i=1}^{r} (X - j(s_i \tau)) ;$$

ce polynôme en X à coefficients fonctions holomorphes sur E ne dépend pas du choix des représentants s_i ; ses coefficients sont invariants par Γ. On peut donc écrire

$$F'_n(X\,;\,\tau) = X^r + \sum_{k=1}^{r} (-1)^k H_{n,k}(j(\tau))X^{r-k}$$

où les $H_{n,k}$ sont des fonctions entières : on a

$$H_{n,k}(j(\tau)) = \sum_{\{i_1,\dots,i_k\}} j(s_{i_1}\tau)\dots j(s_{i_k}\tau)$$

$$= (k!)^{-1} \sum_{(i_1,\dots,i_k)} j(s_{i_1}\tau)\dots j(s_{i_k}\tau) \qquad (1)$$

où la première sommation est étendue aux ensembles, et la seconde aux suites de k entiers distincts $i_1, \dots, i_k$ entre 1 et r.

THÉORÈME 1. - Les $H_{n;k}$ sont des polynômes à coefficients rationnels : les dénominateurs de ces coefficients ne font intervenir que des nombres premiers exceptionnels.

Soit E_0 l'ensemble des τ tels que $|\mathrm{Re}\,\tau| \leq 1/2$, $\mathrm{Im}\,\tau > \varepsilon$; si ε est assez petit, on a $f(E_0) = E/R$. On sait qu'on peut prendre comme représentants s_i les substitutions homographiques $\tau \longrightarrow w^{-1}(u\tau + v)$, où u, v, w sont des entiers $\geqslant 0$, $uw = n$ et $0 \leq v < w$. Dans ces conditions, si τ tend vers l'infini dans E_0, $s_i\tau$ garde une partie réelle bornée, et sa partie imaginaire vaut $w^{-1}u\,\mathrm{Im}\,\tau$. Or, si τ augmente indéfiniment en gardant une partie réelle bornée, $j(\tau)$ est asymptotique à $e^{-2i\pi\tau}$; on conclut alors immédiatement des expressions (1) que $H(z)$ reste borné par une puissance de $|z|$ quand $|z|$ augmente indéfiniment, ce qui montre que $H_{n,k}$ est un polynôme. Nous allons utiliser la seconde expression (1) pour montrer que les coefficients de $H_{n,k}$ sont rationnels. Supposons que s_i soit la substitution $\tau \longrightarrow w_i^{-1}(u_i\tau + v_i)$; nous ferons d'abord la sommation par rapport aux suites $(i_1, \dots, i_k)$ pour lesquelles $w_{i_1}, \dots, w_{i_k}$ ont des valeurs données $a_1, \dots, a_k$ (d'où $u_{i_q} = na_q^{-1}$). Cette somme partielle s'écrit

$$\sum_{(\nu_1,\dots,\nu_k)} c_{\nu_1}\dots c_{\nu_k}\, e^{2i\pi\rho(\nu)\tau} \sum_{(b_1,\dots,b_k)} e^{2i\pi \sum^{i} b_q a_q^{-1} \nu_q}$$

où la seconde sommation est étendue aux suites $(b_1, \dots, b_k)$ d'entiers vérifiant les conditions suivantes : on a $0 \leq b_q < a_q$ et $b_q \neq b_{q'}$, si $a_q = a_{q'}$;

la première sommation est étendue à toutes les suites $(\nu_1 , \dots , \nu_k)$ de k entiers $\geqslant -1$, et $\rho(\nu) = \sum_{q=1}^{k} n a_q^{-2} \nu_q$. Or le nombre

$$\sum_{(b_1,\dots,b_k)} e^{2i\pi \sum b_q a_q^{-1} \nu_q}$$

est un nombre rationnel ; en effet, si h est un entier premier à n , l'application qui, à toute suite $(b_1 , \dots , b_k)$ fait correspondre la suite $(b'_1 , \dots , b'_k)$, où b'_q est le reste de la division de hb_q par n , permute entre elles les suites satisfaisant aux conditions imposées, ce qui montre que le nombre en question est invariant par les automorphismes du corps engendré par $e^{2i\pi n^{-1}}$. On en conclut que $H_{n;k}(j(\tau))$ admet un développement de Fourier de la forme

$$\sum_{-m}^{\infty} d_\nu e^{2i\pi n^{-1} \nu \tau}$$

où m est un entier >0 et où les d_ν sont des nombres rationnels : comme $H_{n,k}$ est un polynôme, on sait d'ailleurs que $d_\nu = 0$ si $\nu \not\equiv 0 \pmod{n}$. Utilisons maintenant la première expression (1) de $H_{n,k}(j(\tau))$; on voit alors que les d_ν s'expriment comme polynômes en les c_ν à coefficients entiers dans le corps Z engendré par $e^{2i\pi n^{-1}}$; si donc p est un nombre premier non exceptionnel, et si $\mathfrak{p}$ est un idéal premier de Z au-dessus de p , les d_ν sont entiers pour $\mathfrak{p}$ dans le corps Z : comme ce sont des nombres rationnels, leurs dénominateurs ne sont pas divisibles par p . Le théorème 1 se déduit facilement de là.

On peut donc écrire $F'_n(X ; \tau) = F_n(X , j(\tau))$, où F_n est un polynôme en 2 lettres à coefficients rationnels, les dénominateurs de ces coefficients ne faisant intervenir que les nombres premiers execptionnels.

THÉORÈME 2. - Soit p un nombre premier non exceptionnel ; on a alors

$$F_p(X , Y) \equiv (X^p - Y)(X - Y^p) \pmod{p} .$$

Soit $\mathfrak{p}$ l'unique idéal premier du corps Z engendré par $e^{2i\pi p^{-1}}$ qui divise p ; si A , A' sont deux fonctions holomorphes sur E qui peuvent se développer en séries de Fourier en $e^{2i\pi p^{-1}\tau}$ à coefficients $\mathfrak{p}$-entiers dans Z , nous écrirons $A \equiv A' \pmod{\mathfrak{p}}$ si les coefficients de $A' - A$ sont divisibles par $\mathfrak{p}$ (ou, plus exactement, par l'idéal premier maximal de l'anneau des éléments $\mathfrak{p}$-entiers). On sait que $e^{2i\pi p^{-1}} - 1$ appartient à $\mathfrak{p}$; si donc s est la

substitution $\tau \to w^{-1}(u\tau + v)$ (avec $uw = p$, $0 \leq v < w$), on a $j(s\tau) \equiv j(w^{-1} u \tau)$ (mod $\wp$). On a ici $r = p + 1$; utilisant les mêmes notations que dans la démonstration du théorème 1, nous supposerons que $u_i = 1$, $w_i = p$, $v_i = i - 1$, si $1 \leq i \leq p$, $u_r = p$, $w_r = 1$, $v_r = 0$. Soit σ un ensemble $\{i_1, \cdots, i_k\}$ de k entiers distincts entre 1 et $p + 1$; si cet ensemble contient $p + 1$, on a $j(s_{i_1} \tau) \cdots j(s_{i_k} \tau) \equiv (j(p^{-1} \tau))^{k-1} j(p \tau)$; dans le cas contraire, on a $j(s_{i_1} \tau) \cdots j(s_{i_k} \tau) \equiv (j(p^{-1} \tau))^k$. Le nombre des σ qui contiennent $p + 1$ est le coefficient binomial $\binom{p}{k-1}$, qui est divisible par p si $k \neq 1$, $p + 1$; le nombre des σ qui ne contient pas $p + 1$ est $\binom{p}{k}$, qui est divisible par p si $k \neq 0$, p. Par ailleurs, on a en vertu du premier théorème de Fermat, $j(p \tau) \equiv (j\tau))^p$, $(j(p^{-1} \tau))^p \equiv j(\tau)$. Il vient donc

$$H_{p,1}(j(\tau)) \equiv (j(\tau))^p \; ; \; H_{p,k}(j(\tau)) \equiv 0 \quad \text{si} \quad 1 \leq k \leq p$$

$$H_{p,p}(j(\tau)) \equiv j(\tau) \; ; \; H_{p,p+1} \equiv (j(\tau))^{p+1}$$

d'où le résultat.

Les polynômes F_n définissent des correspondances sur la droite projective, qu'on appelle <u>les correspondances modulaires</u>. Il est clair que $F_n(X, X) = 0$ si n est carré ; par contre, si n n'est pas un carré, on a $F_n(X, X) \neq 0$. Les notations étant les mêmes que plus haut, il suffit de montrer que si $s \in \Gamma_n$, la fonction $j(\tau) - j(s\tau)$ n'est pas identiquement nulle. Or, si τ est tel que $j(\tau) = j(s\tau)$, il y a un $s' \in \Gamma$ tel que $s'^{-1} s \tau = \tau$; comme $s \in \Gamma_n$ et comme n n'est pas un carré, $s'^{-1} s$ ne peut être l'identité ; comme Γ est dénombrable, $j(\tau) - j(s\tau)$ n'a qu'un ensemble dénombrable de zéros dans E.

2. Classes d'isomorphismes.

Nous désignerons dans ce qui suit par K un corps imaginaire quadratique, par o un sous-anneau des entiers de K admettant K comme corps des fractions, par $\mathfrak{M}$ l'algèbre des matrices de degré 2 à coefficients rationnels, par $\mathcal{O}$ l'anneau des matrices de $\mathfrak{M}$ qui sont à coefficients entiers.

Pour tout élément inversible α

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{2}$$

de $\mathfrak{M}$, nous désignerons par $S(\alpha)$ la substitution homographique $\tau \to (a\tau + b)(c\tau + d)^{-1}$.

THÉORÈME 3. - Soit φ un isomorphisme de K sur un sous-corps de $\mathfrak{M}$; soit K^* l'ensemble des éléments $\neq 0$ de K . Il existe alors un nombre τ et un seul du demi-plan supérieur qui est invariant par toutes les opérations $S(\varphi(x))$, $x \in K^*$; $\varphi(K^*)$ est l'ensemble des éléments inversibles, α de $\mathfrak{M}$ tels que τ soit laissé fixe par $S(\alpha)$.

Soit x_0 un générateur du corps K : le polynôme caractéristique de $\varphi(x_0)$ qui est de degré 2, est égal au polynôme minimal de x_0 ; ses racines sont donc imaginaires, ce qui montre que les points fixes de $S(\varphi(x_0))$ sont imaginaires ; $S(\varphi(x_0))$ a donc un point fixe et un seul dans le demi-plan supérieur, soit τ . Si a est un élément inversible de $\mathfrak{M}$ donné par (2), une condition nécessaire et suffisante pour que $S(\alpha)$ laisse τ fixe est que l'on ait $c\tau^2 + (d - a)\tau - b = 0$.

L'ensemble des matrices dont les coefficients satisfont à cette relation est un sous-espace vectoriel de dimension 2, soit V , de $\mathfrak{M}$. Comme $\{1 , x_0\}$ est une base de K , on a $\varphi(K^*) \subset V$; comme $\varphi(K)$ est un espace vectoriel de dimension 2, on a $\varphi(K) = V$.

Le nombre τ du théorème 3 sera désigné par $\tau(\varphi)$.

Si α est un élément inversible de $\mathfrak{M}$, nous désignerons par $J(\alpha)$ l'automorphisme intérieur $u \to \alpha u \alpha^{-1}$ de $\mathfrak{M}$. Si $\det \alpha > 0$, l'opération $S(\alpha)$ transforme le demi-plan supérieur en lui-même : on a donc alors :

$$\tau(J(\alpha) \circ \varphi) = S(\alpha).\tau(\varphi) . \tag{3}$$

La relation "il existe un $\varepsilon \in \mathcal{O}$ tel que $\det \varepsilon = 1$ et $\varphi' = J(\varepsilon) \circ \varphi$" est une relation d'équivalence entre isomorphismes φ et φ' de K sur des sous-corps de $\mathfrak{M}$. Nous appellerons classes d'isomorphismes les classes relativement à cette relation d'équivalence. Soit Φ une classe d'équivalence ; les nombres $\tau(\varphi)$ pour tous les $\varphi \in \Phi$ sont transformés les uns des autres par les opérations du groupe modulaire Γ ; les nombres $j(\tau(\varphi))$ pour tous les $\varphi \in \Phi$ sont donc égaux ; nous désignerons leur valeur commune par $j(\Phi)$; $j(\Phi)$ s'appelle l'invariant de la classe Φ .

Soit σ l'automorphisme distinct de l'identité du corps K : pour tout isomorphisme φ de K sur un sous-corps de $\mathfrak{M}$, nous désignerons par $\bar{\varphi}$ l'isomorphisme $\varphi \circ \sigma$. Si Φ est une classe d'isomorphismes, les isomorphismes $\bar{\varphi}$ pour $\varphi \in \Phi$ forment évidemment une classe, que nous désignerons par $\bar{\Phi}$.

LEMME 1. - Soient Φ et Φ' deux classes d'isomorphismes de K sur des sous-corps de Ω ; pour que l'on ait $j(\Phi) = j(\Phi')$, il faut et il suffit que l'on ait ou bien $\Phi' = \Phi$ ou bien $\Phi' = \overline{\Phi}$.

Soient φ et φ' des représentations de Φ et Φ respectivement. Si $\Phi' = \Phi$ (resp. $\Phi' = \overline{\Phi}$), on peut prendre $\varphi' = \varphi$ (resp. $\varphi' = \overline{\varphi}$) ; dans les deux cas, on a $\varphi(K) = \varphi'(K)$, d'où il résulte que $\tau(\varphi) = \tau(\varphi')$, $j(\Phi) = j(\Phi')$. Supposons réciproquement que $j(\Phi) = j(\Phi')$. Alors $\tau(\varphi')$ est transformé de $\tau(\varphi)$ par une opération du groupe modulaire, donc par une opération $S(\varepsilon)$, où ε est un élément de déterminant 1 de $\mathfrak{o}$. Remplaçant φ par $J(\varepsilon) \circ \varphi$, on peut supposer que $\tau(\varphi) = \tau(\varphi')$; il résulte alors du théorème 3 que $\varphi'(K) = \varphi(K)$, donc que $\varphi' = \varphi \circ s$, où s est un automorphisme de K, ce qui achève la démonstration du lemme.

On observera que, si φ est un isomorphisme de K sur un sous-corps de Ω et x un élément de K tel que $\varphi(x) \in \mathfrak{o}$, on a encore $\varphi'(x) \in \mathfrak{o}$ pour tout φ' de la classe de φ. Nous désignerons par $\mathfrak{F}$ l'ensemble des classes Φ d'isomorphismes telles que la condition $\varphi \in \Phi$ entraîne $\varphi(o) \subset \mathfrak{o}$.

Soient Φ un élément de $\mathfrak{F}$, φ un représentant de la classe Φ et α un idéal de o. L'ensemble $\varphi(\alpha)$ engendre un idéal à gauche $\mathfrak{o}\varphi(\alpha)$ dans $\mathfrak{o}$. Or, on sait que les idéaux à gauche de $\mathfrak{o}$ sont principaux ; de plus, $\mathfrak{o}$ contient un élément inversible de déterminant -1 ; il y a donc un élément $\alpha \in \mathfrak{o}$ tel que $\mathfrak{o}\varphi(\alpha) = \mathfrak{o}\alpha$ et $\det \alpha > 0$; comme $\Omega\varphi(\alpha) = \Omega$, α est inversible dans Ω, et on a $\det \alpha > 0$; α est déterminé à la multiplication à gauche près par un élément de déterminant 1 de $\mathfrak{o}$. Posons $\varphi' = J(\alpha) \circ \varphi$: on a alors $\varphi'(o) \subset \mathfrak{o}$; en effet, $\alpha^{-1}\mathfrak{o}\alpha$ est l'ensemble des $v \in \Omega$ tels que $\mathfrak{o}\varphi(\alpha)v = \mathfrak{o}\alpha v \subset \mathfrak{o}$; or, cet ensemble contient $\varphi(o)$, puisque $\varphi(\alpha)\varphi(o) = \varphi(\alpha)$. Une fois φ et α donnés, φ' n'est pas entièrement déterminé, mais sa classe l'est : en effet, si on remplace α par $\varepsilon\alpha$, où $\varepsilon \in \mathfrak{o}$, $\det \varepsilon = 1$, φ' est remplacé par $J(\varepsilon) \circ \varphi'$. De plus, pour α donné, la classe de φ' ne dépend que de Φ. Posons en effet, $\varphi_1 = J(\varepsilon_1) \circ \varphi$ où $\varepsilon_1 \in \mathfrak{o}$, $\det \varepsilon_1 = 1$; on a $\varphi_1(\alpha) = \varepsilon_1 \varphi(\alpha) \varepsilon_1^{-1}$; on a donc $\mathfrak{o}\varphi_1(\alpha) = \mathfrak{o}\alpha\,\varepsilon_1^{-1}$; or on a $J(\alpha\,\varepsilon_1^{-1}) \circ \varphi_1 = \varphi'$, ce qui démontre notre assertion. Nous désignerons la classe de φ' par $\theta(\alpha).\Phi$.

Il est clair que $\theta(\alpha).\overline{\Phi} = \overline{\theta(\alpha).\Phi}$.

LEMME 2. - On a $\theta(\alpha).\Phi \neq \bar{\Phi}$.

En effet, soit φ un représentant de la classe Φ. Si on avait $\theta(\alpha).\Phi = \bar{\Phi}$, il y aurait un élément inversible α de $\mathfrak{M}$ tel que $\bar{\varphi}(x) = \alpha\varphi(x)\alpha^{-1}$ pour $x \in K$; or c'est impossible, car il est bien connu que les représentations φ et $\bar{\varphi}$ de l'algèbre K sont inéquivalentes.

THÉORÈME 4. - Soient Φ un élément de $\mathfrak{R}$ et $\mathfrak{a}$ un idéal de $\mathfrak{o}$; si $\mathfrak{a} = \mathfrak{o}u$ (avec $u \in \mathfrak{o}$), on a $\theta(\mathfrak{a}).\Phi = \Phi$; supposons maintenant que l'on ait $\varphi(\mathfrak{o}) = \varphi(K) \cap \mathfrak{O}$ si $\varphi \in \Phi$; alors, si $\theta(\mathfrak{a}).\Phi = \Phi$, $\mathfrak{a}$ est engendré par un élément de $\mathfrak{o}$.

Soit φ un élément de Φ. Si $\mathfrak{a} = \mathfrak{o}u$, $u \in \mathfrak{o}$, on a $\mathfrak{O}\varphi(\mathfrak{a}) = \mathfrak{O}\varphi(u)$, det $\varphi(u) > 0$. Comme $\varphi(u)$ commute avec les éléments de $\varphi(K)$, il en résulte que $\theta(\mathfrak{a}).\Phi = \Phi$. Supposons maintenant que l'on ait $\varphi(\mathfrak{o}) = \varphi(K) \cap \mathfrak{O}$ et que $\theta(\mathfrak{a}).\Phi = \Phi$. Soit α un élément de $\mathfrak{O}$ tel que $\mathfrak{O}\varphi(\alpha) = \mathfrak{O}\alpha$, det $\alpha > 0$. Il existe par hypothèse un élément ε de $\mathfrak{O}$ tel que det $\varepsilon = 1$ et $J(\varepsilon) \circ \varphi = J(\alpha) \circ \varphi$. Remplaçant α par $\varepsilon^{-1}\alpha$, on peut supposer que l'on a $J(\alpha) \circ \varphi = \varphi$. Cela signifie que α commute avec tous les éléments de $\varphi(K)$, comme $\varphi(K)$ est une sous-algèbre commutative maximale de $\mathfrak{M}$, on a $\alpha \in \varphi(K)$; soit $\alpha = \varphi(u)$, avec $u \in K$, d'où $\varphi(u) \in \varphi(K) \cap \mathfrak{O}$ et par suite $u \in \mathfrak{o}$; on a $\mathfrak{O}\varphi(\alpha) = \mathfrak{O}u$. Nous allons en déduire que $\mathfrak{a} = \mathfrak{o}u$. Si $x \in \mathfrak{a}$, on a $\varphi(x) = \lambda\varphi(u)$ avec $\lambda \in \mathfrak{O}$; il en résulte que $\lambda \in \varphi(K)$, d'où $\lambda = \varphi(v)$, $v \in \mathfrak{o}$, et $x = vu$; on a donc $\mathfrak{a} = \mathfrak{b}u$, où $\mathfrak{b}$ est un idéal de $\mathfrak{o}$; on a $\mathfrak{O}\varphi(\mathfrak{b}) = \mathfrak{O}$. Posons $\mathfrak{o}' = \varphi(\mathfrak{o})$, $\mathfrak{b} = \varphi(\mathfrak{b})$; alors, $\mathfrak{O}$ est un $\mathfrak{o}'$-module fini ; soit $\mathfrak{O} = \mathfrak{o}'\xi_1 + \ldots + \mathfrak{o}'\xi_r$, avec $\xi_1 = 1$. On a par hypothèse des relations de la forme $\xi_i = \sum_{j=1}^{r} b'_{ij}\xi_j$, $b'_{ij} \in \mathfrak{b}'$; soit B la matrice (b'_{ij}), et soit I la matrice unité de degré r ; on a donc $\det(I - B).\xi_i = 0$ $(1 \leq i \leq r)$, et, en particulier, $\det(I - B) = 0$. Mais il est clair que $\det(I - B)$ est un élément de $\mathfrak{o}'$ qui est $\equiv 1 \pmod{\mathfrak{b}'}$; on a donc $1 \in \mathfrak{b}$, d'où $1 \in \mathfrak{b}$.

Soit $\mathfrak{o}_0$ l'anneau des entiers de K. Alors $\mathfrak{o}_0$ possède une base sur $\mathbb{Z}$ de la forme $(1, x_0)$; il en résulte tout de suite qu'il existe un entier $f > 0$ et un seul tel que $(1, fx_0)$ soit une base de $\mathfrak{o}$; l'idéal $\mathfrak{f} = f\mathfrak{o}_0$ s'appelle le conducteur de $\mathfrak{o}$; c'est l'ensemble des $x \in \mathfrak{o}_0$ tels que $x\mathfrak{o}_0 \subset \mathfrak{o}$. En effet, il est clair que $f\mathfrak{o}_0 \subset \mathfrak{o}$; soit réciproquement $x = a + bx_0$ tel $x\mathfrak{o}_0 \subset \mathfrak{o}$: comme $x \in \mathfrak{o}_0$, on a $b \equiv 0 \pmod{f}$, d'où $bx \in \mathfrak{f}$ et $a\mathfrak{o}_0 \subset \mathfrak{o}$, d'où $ax_0 \in \mathfrak{o}$ et $a \equiv 0 \pmod{f}$. Si p est un nombre premier, nous désignerons par

$\mathbb{Z}_{(p)}$ l'anneau des nombres rationnels dont les dénominateurs ne sont pas divisibles par p : il est bien connu que $\mathbb{Z}_{(p)}[o_0]$ est un anneau à idéaux principaux. Si p ne divise pas f, on a $f^{-1} \in \mathbb{Z}_{(p)}$, d'où $\mathbb{Z}_{(p)}[o_0] = \mathbb{Z}_{(p)}[o]$. Nous poserons $o_p = \mathbb{Z}_{(p)}[o]$, $(o_0)_p = \mathbb{Z}_{(p)}[\alpha_0]$. Si α (resp. α_0) est un idéal de o (resp. o_0), α (resp. α_0) est l'intersection des idéaux αo_p (resp. $\alpha_0 (o_0)_p$) qu'il engendre dans les divers anneaux o_p (resp. $(o_0)_p$) si α (resp. α_0) est premier à f, on peut dans l'assertion précédente se limiter aux nombres premiers p qui ne divisent pas f. Il en résulte que, si α est un idéal de o premier à f, et α_0 l'idéal de o_0 qu'il engendre, on a $\alpha = o \cap \alpha_0$; de même, si α_0 est un idéal de o_0 premier à f, α_0 est l'idéal engendré par $\alpha_0 \cap o$. Si α est un idéal de o premier à f, nous appellerons norme de α la norme de l'idéal α_0 qu'il engendre dans o_0 ; c'est un entier $N(\alpha)$ premier à f. Si p est un nombre premier ne divisant pas f, la contribution $N_p(\alpha)$ de p à $N(\alpha)$ peut se calculer comme suit : αo_p est un idéal principal $a o_p$, et $N_p(\alpha)$ est la contribution de p au nombre rationnel $N(a)$. Si φ est un isomorphisme quelconque de K sur un sous-corps de $\mathfrak{M}$, $N(a)$ est égal à $\det \varphi(a)$. Supposons que $\varphi(o) \subset \mathfrak{o}$, et soit $\mathfrak{o}\varphi(\alpha) = \mathfrak{o}\alpha$, $\det \alpha > 0$; soit $\mathfrak{o}_p$ l'anneau engendré par $\mathbb{Z}_{(p)}$ et $\mathfrak{o}$; utilisant les mêmes notations que ci-dessus, on a $\mathfrak{o}_p a = \mathfrak{o}_p \alpha$; il en résulte que $N_p(\alpha)$ est aussi la contribution de p à $\det \alpha$. Par ailleurs, si p divise f, on a $\mathfrak{o}_p \alpha = \mathfrak{o}_p$, et $\det \alpha$ est premier à p. Puisque $\det \alpha > 0$, on a $N(\alpha) = \det \alpha$.

THÉOREME 5. - *Soit Φ une classe appartenant à $\mathfrak{f}$, et soit α un idéal de o premier au conducteur f ; si $n = N(\alpha)$, on a $F_n(j(\theta(\alpha).\Phi), j(\Phi)) = 0$.*

Soit φ un représentant de la classe Φ ; posons $\tau = \tau(\varphi)$. Soit α un élément de $\mathfrak{o}$ tel que $\det \alpha > 0$, $\mathfrak{o}\varphi(\alpha) = \mathfrak{o}\alpha$, et soit $\varphi' = J(\alpha) \circ \varphi$; φ' appartient donc à la classe $\theta(\alpha).\Phi$. Par ailleurs, on a $\tau(\varphi') = S(\alpha).\tau$ (formule (3)) ; comme $\det \alpha = n$, $S(\alpha)$ appartient à Γ_n et $F_n(X, j(\tau))$ est par suite divisible par $X - J(S(\alpha).\tau)$, ce qui démontre le théorème 5.

COROLLAIRE. - *Pour toute classe Φ d'isomorphismes de K sur des sous-corps de $\mathfrak{M}$, $j(\Phi)$ est un nombre algébrique*

Soit φ un représentant de Φ, et soit $\mathfrak{o}$ l'anneau des $x \in K$ tels que $\varphi(x) \in \mathfrak{O}$; il admet K comme corps des fractions. Soit $f\mathfrak{o}$ son conducteur ; il résulte du théorème de la progression arithmétique qu'il y a une infinité d'idéaux premiers $\mathfrak{p}_0$ du premier degré de l'anneau $\mathfrak{o}_0$ des entiers de K qui sont représentés par des nombres $\equiv 1 \pmod{f\,\mathfrak{o}_0}$. Soient $\mathfrak{p}_0$ l'un de ces idéaux premiers, $\mathfrak{p}_0 = \mathfrak{o}_0 x$, avec $x \equiv 1 \pmod{f\,\mathfrak{o}_0}$, p le nombre premier divisible par $\mathfrak{p}_0$ et $\mathfrak{p} = \mathfrak{o} \cap \mathfrak{p}_0 = \mathfrak{o} x$; on a $p = N(\mathfrak{p})$ et $\theta(\mathfrak{p}).\Phi = \Phi$. Il en résulte que $F_p(j(\Phi), j(\Phi)) = 0$; or $F_p(X, X)$ est un polynôme $\neq 0$ à coefficients rationnels (cf. n° 1).

La même démonstration montre que l'ensemble des $j(\Phi)$, pour $\Phi \in \mathfrak{R}$, est fini, et par suite (en vertu du lemme 1) que $\mathfrak{R}$ est fini.

3. Démonstration du théorème fondamental.

Nous emploierons les mêmes notations que ci-dessus ; on désignera notamment par $\mathfrak{o}_0$ l'anneau des entiers de K et par f le nombre entier >0 tel que le conducteur de $\mathfrak{o}$ soit $f\,\mathfrak{o}_0$.

Si L est un corps de nombres algébriques, on désignera par E(L) l'anneau des entiers de L : si p est un nombre premier, on désignera par $E_p(L)$ l'anneau engendré par $\mathbb{Z}_{(p)}$ et par E(L). Rappelons qu'un idéal premier $\mathfrak{P}$ de E(L) est dit être du premier degré si tout élément de E(L) est congru modulo $\mathfrak{P}$ à un entier rationnel : si p est le nombre premier appartenant à $\mathfrak{P}$, les assertions suivantes sont équivalentes : $\mathfrak{P}$ est du premier degré : la norme (absolue) de $\mathfrak{P}$ est p ; pour tout $\eta \in E_p(L)$, on a $\eta^p \equiv \eta \pmod{\mathfrak{P}\,E_p(L)}$.

Soit L'/L une extension de degré n de L, et soit $\mathfrak{P}$ un idéal premier de E(L). Un idéal premier $\mathfrak{P}'$ de E(L') est dit être "au-dessus" de $\mathfrak{P}$ si $\mathfrak{P}$ est contenu dans $\mathfrak{P}'$. On dit que $\mathfrak{P}$ est complètement décomposé dans L' s'il y a n idéaux premiers distincts de E(L') au-desssus de $\mathfrak{P}$; pour qu'il en soit ainsi il faut et suffit que, pour tout idéal premier $\mathfrak{P}'$ de E(L') au-dessus de $\mathfrak{P}$, tout élément de E(L') soit congru (mod $\mathfrak{P}'$) à un élément de E(L) et que, de plus, $\mathfrak{P}$ ne soit pas ramifié dans E(L') (i.e. $\mathfrak{P}\,E(L')$ n'est divisible par le carré d'aucun d'idéal premier). Il n'y a qu'un nombre fini d'idéaux premiers de E(L) qui soient ramifiés dans E(L') ; si $\mathfrak{P}$ est un idéal premier du premier degré de E(L) non ramifié dans E(L'), pour qu'il soit complètement décomposé, il faut et il suffit que tout idéal premier de E(L') au-dessus de $\mathfrak{P}$ soit du premier degré. Soit $\mathfrak{P}$ un idéal premier quelconque de L ; désignons par $L^{\mathfrak{P}}$

la complétion $\mathfrak{P}$-adique de L ; pour que $\mathfrak{P}$ soit complètement décomposé dans L', il faut et suffit que l'algèbre $L^{\mathfrak{P}} \otimes_L L'$ soit somme directe de corps isomorphes à $L^{\mathfrak{P}}$; il résulte immédiatement de ce critère que, pour que $\mathfrak{P}$ soit complètement décomposé dans L', il faut et suffit qu'il le soit dans la plus petite extension normale de L contenant L'.

La théorie transcendante des corps de nombres algébriques permet d'établir que, si L'/L est une extension de degré $n > 1$, il y a une infinité d'idéaux premiers du premier degré de L qui ne sont pas complètement décomposés dans L'. Indiquons rapidement comment on procède. La fonction $\zeta_{L'}$ du sur-corps est donnée par $\zeta_{L'}(s) = \prod(1 - (N(\mathfrak{P}'))^{-s})^{-1}$, le produit étant étendu à tous les idéaux premiers $\mathfrak{P}'$ de L'. Si on étend seulement le produit aux idéaux premiers du premier degré de L' qui ne sont pas ramifiéspar rapport à L, on obtient une fonction $\zeta'_{L'}$ qui ne diffère de $\zeta_{L'}$ que par un facteur qui reste holomorphe pour $s = 1$, or il est clair que $\zeta'_{L'}(s) = (\prod(1 - N(\mathfrak{P}))^{-s})^{-n}$, où le produit est ici étendu aux idéaux premiers du premier degré $\mathfrak{P}$ de L qui sont complètement décomposés dans L'. Or, $\zeta_{L'}$ a un pôle d'ordre 1 en $s = 1$; il en est donc de même de $\zeta'_{L'}$; par ailleurs, la fonction $\prod(1-(N(\mathfrak{P})^{-s})^{-1}$, où le produit est maintenant étendu à tous les idéaux premiers du premier degré de L, admet également un pôle d'ordre 1 en $s = 1$: il en résulte immédiatement qu'il y a une infinité d'idéaux premiers du premier degré de L qui ne sont pas complètement décomposés dans L'.

Il résulte de là que, si L' et L'' sont des extensions finies de L, L'' étant de plus galoisienne, si presque tous (i.e. tous sauf un nombre fini) les idéaux premiers du premier degré de L qui se décomposent complètement dans L'' se décomposent complètement dans L', on a $L' \subset L''$; en effet, dans le cas contraire, il y aurait une infinité d'idéaux premiers du premier degré de L'' qui ne se décomposeraient pas complètement dans le corps L''_1 engendré par L'' et L' ; il y aurait donc une infinité d'idéaux premiers du premier degré de L qui se décomposeraient complètement dans L'' mais non dans L''_1 (car, si un idéal premier $\mathfrak{P}''$ de L'' est du premier degré, il en est de même de tous ceux qui sont au-dessus du même idéal de L que $\mathfrak{P}''$, car ils sont conjugués de $\mathfrak{P}''$ par rapport à L). Or, c'est impossible, car ces idéaux premiers ne se décomposeraient pas complètement dans L' (un idéal premier $\mathfrak{P}$ qui se décompose complètement dans L' et dans L'', se décompose aussi complètement dans L''_1 puisque $L'' \otimes_L L^{\mathfrak{P}}$ et $L' \otimes_L L^{\mathfrak{P}}$ sont tous deux des sommes directes de corps isomorphes à $L^{\mathfrak{P}}$, d'où il résulte qu'il en est de même de $L''_1 \otimes_L L^{\mathfrak{P}}$).

Rappelons que deux éléments a , a' de K sont dits être congrus l'un à l'autre modulo $\mathfrak{f}$ si leur différence peut se mettre sous la forme bc^{-1} où b , c sont des entiers tels que $b \in \mathfrak{f}$ et que c soit premier à $\mathfrak{f}$. Les idéaux principaux fractionnaires de K qui sont représentables par un nombre u qui est congru à un entier rationnel modulo $\mathfrak{f}$ et qui sont premiers à $\mathfrak{f}$ forment un groupe multiplicatif que nous désignerons par H . Il résulte de la théorie du corps de classes qu'il existe une extension abélienne Z de K et une seule, telle que les idéaux premiers, premiers à $\mathfrak{f}$, qui sont complètement décomposés dans Z soient exactement ceux qui appartiennent à l'ensemble H ; Z s'appelle le corps de classes pour le groupe H . On notera que les idéaux premiers de H sont les idéaux premiers, premiers à $\mathfrak{f}$, qui sont engendrés par des éléments de l'anneau o (o se compose en effet, de deux des entiers de K qui sont congrus à des entiers rationnels modulo $\mathfrak{f}$). Ceci étant, le théorème fondamental de la multiplication complexe est le suivant :

THÉORÈME 6. - *Le corps de classes Z pour le groupe H défini ci-dessus est le corps engendré par adjonction à K des nombres $j(\Phi)$, pour toutes les classes Φ d'isomorphismes de K sur des sous-corps de $\mathfrak{M}$ telles que la condition $\varphi \in \Phi$ entraîne $\varphi(o) \subset \mathfrak{p}$.*

Soient ξ_1 , ... , ξ_m les nombres distincts de la forme $j(\Phi)$, où $\Phi \in \mathfrak{F}$; on a donc $L = K(\xi_1 , \dots , \xi_m)$. Soit A l'anneau $o_0[\xi_1 , \dots , \xi_m]$; il a même corps des fractions que L , d'où il résulte qu'il y a un entier $a > 0$ tel que $aA \subset E(L)$, $aE(L) \subset A$; si p est un nombre premier ne divisant pas a , on a $Z_{\mathfrak{p}}(A) = Z_{\mathfrak{p}}[E(L)]$. Soient $\mathfrak{P}$ un idéal premier de $E(L)$ contenant p , et soit $\mathfrak{P}$ l'idéal qu'il engendre dans $E_p(L) = Z_{\mathfrak{p}}[E(L)]$; supposons de plus que l'idéal premier $\mathfrak{p}_0$ de o_0 contenu dans $\mathfrak{P}$ soit du premier degré. Il est alors clair que, pour que l'on ait $\eta^p \equiv \eta \pmod{\mathfrak{P}'}$ pour tout $\eta \in E_p(L)$ (i.e. pour que $\mathfrak{P}$ soit du premier degré), il faut et suffit que cette condition soit satisfaite pour les nombres $\eta = \xi_i$ $(1 \leq i \leq m)$. Le produit des normes absolues des nombres $\xi_i - \xi_j$ $(i \neq j)$ est un nombre rationnel, dont nous désignerons le numérateur par a' ; si un nombre premier p ne divise pas aa' , aucun des éléments $\xi_i - \xi_j$ $(i \neq j)$ n'est contenu dans $\mathfrak{P}'$. Soit P un ensemble fini de nombres premiers qui contient tous les diviseurs premiers de $aa'f$, tous les nombres premiers exceptionnels (cf. n° 1) et qui est tel que, si $\mathfrak{p}_0$ est un idéal premier de o_0 qui est ramifié soit dans Z soit dans L , le nombre premier contenu dans $\mathfrak{p}_0$ soit dans P . Soit $\mathfrak{p}_0$ un idéal premier du premier degré de o_0

tel que le nombre premier p appartenant à $\mathfrak{p}_0$ ne soit pas dans P ; nous allons montrer qu'une condition nécessaire et suffisante pour que $\mathfrak{p}_0$ soit complètement décomposé dans L est que $\mathfrak{p}_0$ appartienne à H, i.e. soit complètement décomposé dans Z. Il en résultera d'abord, en vertu de ce qui précède que $L \subset Z$, donc que L/K, est une extension galoisienne, et par suite que $Z \subset L$; l'égalité $L = Z$ sera ainsi établie. Nous poserons $\mathfrak{p} = \mathfrak{p}_0 \cap o$; on a donc $N(\mathfrak{p}) = p$, et, pour que $\mathfrak{p}_0 \in H$, il faut et suffit que $\mathfrak{p}$ soit un idéal principal de o. Nous désignerons par $\mathfrak{P}$ l'un quelconque des idéaux premiers de L au-dessus de $\mathfrak{p}_0$: on a $Z_{mp}[\xi_1, \cdots, \xi_m] = E_p(L)$; nous désignerons par $\mathfrak{P}$ l'idéal premier engendré par $\mathfrak{P}$ dans $E_p[L]$. Nous avons à montrer qu'une condition nécessaire et suffisante pour que l'on ait $\xi_i^p \equiv \xi_i \pmod{\mathfrak{P}}$ est que $\mathfrak{p}$ soit un idéal principal de o.

Soit Φ un élément de $\mathfrak{K}$; nous poserons $\xi = j(\Phi)$, $\xi' = j(\theta(\mathfrak{p}).\Phi)$. On a donc $F_p(\xi', \xi) = 0$ (théorème 5). Par ailleurs, les coefficients de F_p sont dans Z_{mp} (théorème 1) et il résulte du théorème 2 que l'on a

$$(\xi'^p - \xi)(\xi' - \xi^p) \equiv 0 \pmod{\mathfrak{P}'} . \tag{4}$$

Supposons d'abord que $\mathfrak{p}$ soit un idéal principal de o. Il résulte alors du théorème 4 que $\xi' = \xi$; on a donc $\xi^p \equiv \xi \pmod{\mathfrak{P}'}$. Ceci étant vrai pour tout $\Phi \in \mathfrak{K}$, $\mathfrak{P}$ est un idéal du premier degré ; $\mathfrak{p}_0$ est donc dans ce cas complètement décomposé dans L.

Supposons maintenant que $\mathfrak{p}$ ne soit pas un idéal principal de o. Observons alors qu'il existe au moins un isomorphisme φ de K sur un sous-corps de $\mathfrak{M}$ tel que $\varphi(o) = \varphi(K) \cap \mathfrak{M}$. Soit en effet $(1, y)$ une base de o ; si $x \in K$, posons $x = a + by$, $xy = c + dy$; l'application qui fait correspondre à x la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est un isomorphisme φ de K sur un sous-corps de $\mathfrak{M}$. Comme $y^2 \in o$, on a $\varphi(o) \subset \mathfrak{O}$; réciproquement, si $m(x) \in \mathfrak{O}$, a et b sont entiers d'où $x \in o$. Soit Φ la classe de l'isomorphisme φ ; elle appartient à $\mathfrak{K}$; et on a $\theta(\mathfrak{p}).\Phi \neq \Phi$ en vertu du théorème 4 ; nous prendrons pour ξ l'invariant de la classe Φ que l'on vient de construire. On a $\theta(f).\Phi \neq \Phi$ (lemme 2) ; il en résulte que $\xi' = j(\theta(\mathfrak{p}).\Phi) \neq \xi$ en vertu du lemme 1. Il résulte alors de la formule (4) qu'il est impossible que l'on ait à la fois $\xi^p \equiv \xi \pmod{\mathfrak{P}'}$ et $\xi'^p \equiv \xi' \pmod{\mathfrak{P}'}$: cela entraînerait en effet

$$\xi - \xi' \equiv 0 \pmod{\mathfrak{P}'} ,$$

ce qui n'est pas puisque $\xi' \neq \xi$ et puisque p ne divise pas a' . On en conclut que $\mathfrak{P}$ n'est pas du premier degré, ce qui achève la démonstration du théorème 6.

BIBLIOGRAPHIE

[1] EICHLER (Martin). - Der hilbertsche Klassenkörper eines imaginärquadratischen Zahlkörpers, Math. Z., t. 64, 1956, p. 229-242.