Journal of the Mathematical Society of Japan Vol. 10, No. 1, January, 1958

Correspondances modulaires et les fonctions ζ de courbes algébriques.

Par Gorô SHIMURA

(Reçu le 5 Nov., 1957)

M. Eichler [3] a découvert qu'il y a une relation étroite entre l'opérateur T_p défini par E. Hecke et les fonctions ζ de certains corps de fonctions modulaires elliptiques qui sont en rapport avec les formes quadratiques. Dans ce travail nous allons généraliser cette relation.

Soient N un entier positif et $\mathfrak{M}_N$ le corps complet des fonctions modulaires elliptiques d'espèce («Stufe») N; $\mathfrak{M}_N$ est un corps de fonctions algébriques d'une variable sur le corps des nombres complexes $\boldsymbol{C}$. Nous pouvons montrer qu'il y a un sous-corps $\mathfrak{K}$ ayant le corps des nombres rationnels $\boldsymbol{Q}$ comme corps de constantes, qui engendre $\mathfrak{M}_N$ sur $\boldsymbol{C}$. Nous allons démontrer que les fonctions ζ d'un tel corps $\mathfrak{K}$, choisi convenablement, et de certains sous-corps de $\mathfrak{K}$ sont représentées explicitement par la fonction ζ de Riemann et les produits d'Euler introduits par E. Hecke et que les valeurs absolues des racines caractéristiques de l'opérateur T_p de Hecke pour les formes paraboliques («Spitzenformen») de degré 2 ne dépassent pas $2\sqrt{p}$ pour presque tous les nombres premiers p.

Nous démontrerons ces résultats en établissant deux formules de congruence ((I) et (II) dans § 3) pour les correspondances modulaires. Nous représentons d'abord le corps $\mathfrak{M}_N$ par les coordonnées des points t tels que $Nt=0$ sur une courbe elliptique E dont l'invariant est transcendant sur $\boldsymbol{Q}$. L'opérateur T_p de Hecke peut être regardé comme la différentielle d'une correspondance algébrique que nous pouvons définir d'une manière algébro-géométrique par un homomorphisme λ de E tel que $\nu(\lambda)=p$ et que nous appelons la correspondance modulaire de degré p. Dans la théorie de la multiplication complexe ([6], [7]), la relation de congruence ou la décomposition de l'homomorphisme π a été obtenue par la réduction d'homomorphismes d'une variété abélienne modulo un diviseur premier du corps de base. Une méthode analogue est employée ici pour démontrer la formule (I); nous considèrerons la réduction de l'homomorphisme λ modulo un diviseur premier. Seulement nous nous occupons au cas présent d'une courbe elliptique sans multiplication complexe, mais on pourrait considérer λ comme une «multiplication générique» de la courbe elliptique. La formule com-

plémentaire (II) est démontrée au moyen du fait qui s'exprime dans la prop. 7 (§ 2). Le résultat pour les racines caractéristiques de l'opérateur T_p est une conséquence de la formule (I).

§ 1. Courbes elliptiques.

1. Nous désignerons par $\boldsymbol{Z}$, $\boldsymbol{Q}$ et $\boldsymbol{C}$ respectivement l'anneau des entiers rationnels, le corps des nombres rationnels et le corps des nombres complexes.

Soit A une variété abélienne[1]. Nous désignerons par $\mathfrak{A}(A)$ l'anneau des endomorphismes de A, par $\mathfrak{A}_0(A)$ le produit tensoriel $\mathfrak{A}(A)\times\boldsymbol{Q}$ et par δ_A l'élément unité de $\mathfrak{A}(A)$. Soient B une autre variété abélienne de même dimension que A et λ un homomorphisme de A sur B. Soient k un corps de définition pour A, B et λ; x un point générique de A par rapport à k. Nous poserons

$$\nu(\lambda)=[k(x):\ k(\lambda(x)]\,,\qquad \nu_s(\lambda)=[k(x):k(\lambda x)]_s\,,$$
$$\nu_i(\lambda)=[k(x):k(\lambda x)]_i\,.$$

Ces entiers ne dépendent que de A, B et λ et non du choix de k et de x. Nous désignerons par $\mathfrak{g}(\lambda)$ le noyau de λ et par $\mathfrak{g}(n, A)$ le noyau de $n\delta_A$ pour chaque entier n. Le groupe $\mathfrak{g}(\lambda)$ est d'ordre $\nu_s(\lambda)$. Si A est de dimension d, on a $\nu(n\delta_A)=n^{2d}$; par suite $\mathfrak{g}(n, A)$ est d'ordre n^{2d} si n n'est pas multiple de la caractéristique de k ([11]). Pour le cas où n est la caractéristique de k, on a le lemme suivant dont la démonstration est donnée dans [8].

LEMME 1. *Soient k un corps de caractéristique $p\neq 0$ et A une variété abélienne de dimension d définie par rapport à k. On a alors*

$$\nu_i(p\delta_A)\geqq p^d\,,\quad \nu_s(p\delta_A)\leqq p^d\,.$$

Soient k un corps de caractéristique $p\neq 0$, $q=p^f$ une puissance de p, où f est un entier positif ou négatif. Nous désignerons par k^q le corps des q-ièmes puissances des éléments de k. En faisant correspondre $z\in k$ à $z^q\in k^q$ on obtient un isomorphisme σ de k sur k^q. Soient V une variété définie par rapport à k et x un point de V. Nous désignerons par V^q et par x^q la variété V^σ transformée par σ et le point de V^q dont les coordonnées sont les q-ièmes puissances de celles de x. Soient h une application rationnelle de V dans une variété W, définie par rapport à k, et H le graphe de h. Nous désignerons par h^q l'application de V^q dans W^q dont le graphe est

---

1) Il sera constamment fait usage des définitions et des résultats de [9], [10], [11].

H^q. Soient A une variété abélienne définie par rapport à k et O l'élément neutre de A. Nous entendrons par la notation A^q toujours la variété abélienne dont l'élément neutre est O^q. Si λ est un homomorphisme de A dans une variété abélienne, défini par rapport à k, λ^q est un homomorphisme de A^q. Soit x un point générique de A par rapport à k; x^q est alors un point générique de A^q par rapport à k. Comme on a $k(x)\supset k(x^q)$ on obtient une application rationnelle π de A sur A^q telle que $\pi x=x^q$; π est un homomorphisme de A sur A^q; on a $\pi t=t^q$ pour tout point t de A. Nous appellerons π *l'homomorphisme de q-ième puissance de* A. Si A est de dimension d, on a $\nu(\pi)=\nu_i(\pi)=q^d$.

Lemme 2. *Soient A, B, C trois variétés abéliennes de même dimension, λ un homomorphisme de A sur B et μ un homomorphisme de A sur C. Supposons que $\mathcal{A}(A)$ soit isomorphe à $\boldsymbol{Z}$ et que l'on ait $\nu(\lambda)=\nu(\mu)$, $\nu_i(\lambda)=\nu_i(\mu)=1$. Alors, pour que B soit isomorphe à C, il faut et il suffit qu'on ait $\mathfrak{g}(\lambda)=\mathfrak{g}(\mu)$.*

D'après le th. 17 de [11] n°34, si l'on a $\mathfrak{g}(\lambda)=\mathfrak{g}(\mu)$, B est isomorphe à C. Réciproquement supposons qu'il existe un isomorphisme η de B sur C. D'après le th. 27 de [11] n°52, il y a un homomorphisme α de C sur A. $\alpha\eta\lambda$ et $\alpha\mu$ sont contenus dans $\mathcal{A}(A)$. Comme $\mathcal{A}(A)$ est isomorphe à $\boldsymbol{Z}$, il y a deux entiers n, n' autres que 0 tels que $n\alpha\eta\lambda=n'\alpha\mu$. On a alors $\nu(n\delta_A)\nu(\alpha)\nu(\eta)\nu(\lambda)=\nu(n'\delta_A)\nu(\alpha)\nu(\mu)$. Si l'on désigne par d la dimension de A, on a $\nu(n\delta_A)=n^{2d}$, $\nu(n'\delta_A)=n'^{2d}$. Comme $\nu(\eta)=1$ et $\nu(\lambda)=\nu(\mu)$, on a $n=\pm n'$ et par conséquent $\eta\lambda=\pm\mu$; d'où résulte $\mathfrak{g}(\lambda)=\mathfrak{g}(\eta\lambda)=\mathfrak{g}(\mu)$.

Lemme 3. *Les notations A, B, C, λ, μ et les hypothèses étant celles du lemme 2, soient k un corps de définition pour A, B, C, λ, μ et σ un isomorphisme de k tel que $A^\sigma=A$, $B^\sigma=C$. On a alors $\lambda^\sigma=\pm\mu$.*

D'après le lemme 2, on a $\mathfrak{g}(\lambda^\sigma)=\mathfrak{g}(\mu)$. Il y a donc un automorphisme ε de C tel que $\lambda^\sigma=\varepsilon\mu$ en vertu du th. 17 de [11] n°34. Comme C est isogène à A, $\mathcal{A}(C)$ est isomorphe à $\boldsymbol{Z}$; on en déduit que $\varepsilon=\pm1$; ce qui prouve notre lemme.

2. Une variété abélienne de dimension 1 est une courbe algébrique de genre 1. Réciproquement, une courbe algébrique de genre 1, définie par rapport à un corps k, ayant un point rationnel par rapport à k a une structure de variété abélienne définie par rapport à k. Ci-après, par une *courbe elliptique définie par rapport à* k, nous entendrons une variété abélienne de dimension 1 définie par rapport à k.

Soit k un corps dont la caractéristique n'est ni 2 ni 3. Soient γ_2, γ_3, deux éléments de k tels que $\gamma_2^3-27\gamma_3^2\neq0$ et E_1 la courbe définie par l'équation

$$X_0X_2^2=4X_1^3-\gamma_2X_0^2X_1-\gamma_3X_0^3 \tag{1}$$

dans le plan projectif. En prenant le point $(X_0, X_1, X_2)=(0, 0, 1)$ pour l'élément neutre de variété de groupe, nous pouvons considérer E_1 comme une variété abélienne définie par rapport à k. En posant $X=X_1/X_0$ et $Y=X_2/X_0$ dans l'équation (1), on a l'équation affine

$$Y^2=4X^3-\gamma_2 X-\gamma_3 . \tag{2}$$

Nous conviendrons d'entendre par la courbe elliptique définie par l'équation (2) la courbe elliptique projective définie par l'équation (1), ayant le point $(0, 0, 1)$ comme l'élément neutre 0. La correspondance $(X, Y)\to(X, -Y)$ donne l'endomorphisme -1 de la courbe elliptique.

Soit E une courbe elliptique définie par rapport à k. Il est bien connu que E est isomorphe à une courbe elliptique définie par une équation $Y^2=4X^3-\gamma_2 X-\gamma_3$ où γ_2, γ_3 sont deux éléments de k. Nous appellerons $\gamma_2^3/(\gamma_2^3-27\gamma_3^2)$ l'invariant de E et le désignerons par j_E ou $j(E)$; $j(E)$ est contenu dans tout corps de définition pour E. Pour que deux courbes elliptiques soient isomorphes, il faut et il suffit qu'elles aient le même invariant. Si σ est un isomorphisme d'un corps de définition pour une courbe elliptique E, on a $j(E^\sigma)=j(E)^\sigma$.

Soient E la courbe elliptique définie par l'équation (2) et h la fonction sur E qui prend les coordonnées aux points de E (autrement dit, la fonction X_1/X_0 sur la courbe (1)). Nous appellerons *h la fonction canonique sur E.* On voit que

$$h(u)=h(v) \Longleftrightarrow u=\pm v . \tag{3}$$

3. Soient E une courbe elliptique et $\mathfrak{g}$ un sous-groupe fini de E. D'après le th. 17 de [11] n°34, il y a une courbe elliptique E' et un homomorphisme λ de E sur E' tel qu'on ait $\mathfrak{g}=\mathfrak{g}(\lambda)$, $\nu_i(\lambda)=1$. D'après le même théorème, l'invariant $j(E')$ de E' ne dépend que de $E, \mathfrak{g}$ et non du choix de E' et de λ. Nous désignerons $j(E')$ par $j(E/\mathfrak{g})$.

PROPOSITION 1. *Soient E, E' deux courbes elliptiques isogènes et k_0 le corps premier contenu dans un corps de définition pour E, E'. Alors $j(E')$ est algébrique sur $k_0(j_E)$.*

D'après la définition d'isogénéité, il existe un homomorphisme λ de E sur E'. Soient k un corps de définition pour E, E', λ et x un point générique de E par rapport à k; posons $q=\nu_i(\lambda)$. Alors il y a un sous-corps K de $k(x)$ tel que $k(x)$ soit une extension purement inséparable de K de degré q et K soit séparable sur $k(\lambda x)$. Comme $k(x)$ est de dimension 1 sur k, on a $K=k(x^q)$; par suite, en posant $\mu x^q=\lambda x$, on obtient un homomorphisme μ de E^q sur E' défini par rapport à k, pour lequel on a $\nu_i(\mu)=1$. Soit σ un isomorphisme du corps $k(j_E, j_{E'})$ fixant tous les éléments de $k_0(j_E)$; μ^σ est

alors un homomorphisme de $(E^q)^\sigma$ sur E'^σ. On a $j(E'^\sigma)=j(E')^\sigma$ et $j(E^{q\sigma})=(j(E)^q)^\sigma=j(E)^q$. Comme $E^{q\sigma}$ a l'invariant $j(E)^q=j(E^q)$, il y a un isomorphisme η de E^q sur $E^{q\sigma}$. $\mu^\sigma\eta$ est un homomorphisme de E^q sur E'^σ dont le noyau $\mathfrak{g}(\mu^\sigma\eta)$ est d'ordre $\nu(\mu)$. Comme on a $\nu_i(\mu^\sigma\eta)=1$, on a $j(E'^\sigma)=j(E^q/\mathfrak{g}(\mu^\sigma\eta))$. Il n'y a qu'un nombre fini de sous-groupes de E^q ayant l'ordre $\nu(\mu)$; par suite il n'y a qu' un nombre fini de $j(E')^\sigma$; ce qui montre que $j(E')$ est algébrique sur $k_0(j_E)$.

Proposition 2. *Soient E, E' deux courbes elliptiques définies par rapport à un corps de caractéristique $p\neq 0$ et λ un homomorphisme de E sur E' tel qu'on ait $\nu_s(\lambda)=1$. Alors $\nu(\lambda)$ est une puissance q de p; il existe un isomorphisme ε de E^q sur E' tel qu'on ait $\lambda t=\varepsilon t^q$ pour tout $t\in E$.*

Soient k un corps de définition pour E, E', λ et x un point générique de E par rapport à k. Comme $\nu_s(\lambda)=1$, $k(x)$ est purement inséparable sur $k(\lambda x)$; par suite $\nu(\lambda)=[k(x):k(\lambda x)]$ est une puissance q de p. Comme $k(x)$ est de dimension 1 sur k, on a $k(\lambda x)=k(x^q)$. On obtient donc un isomorphisme ε de E^q sur E', défini par rapport à k, tel que $\varepsilon x^q=\lambda x$. On vérifie aisément $\varepsilon t^q=\lambda t$ pour tout $t\in E$.

Proposition 3. *Soit E une courbe elliptique définie par rapport à un corps de caractéristique $p\neq 0$ telle qu'on ait $j(E)^{p^2}\neq j(E)$. On a alors $\nu_i(p\delta_E)=\nu_s(p\delta_E)=p$; $\mathfrak{g}(p, E)$ est d'ordre p.*

D'après le lemme 1, on a $\nu_i(p\delta_E)\geqq p$; $\nu_i(p\delta_E)$ est donc égal à p ou p^2. Supposons qu'on ait $\nu_i(p\delta_E)=p^2$. Alors on a $\nu_s(p\delta_E)=1$. D'après la prop. 2, E est isomorphe à E^{p^2}; par suite on a $j(E)=j(E^{p^2})=j(E)^{p^2}$; ce qui est en contradiction avec l'hypothèse de la proposition. On a donc $\nu_i(p\delta_E)=p$ et par suite $\nu_s(p\delta_E)=p$, de sorte que $\mathfrak{g}(p, E)$ est d'ordre p.

Proposition 4. *Soit E une courbe elliptique telle que $j(E)$ soit transcendant sur le corps premier. $\mathcal{A}(E)$ est alors isomorphe à $\boldsymbol{Z}$.*

Cette proposition est bien connue au cas où la caractéristique du corps de base est 0. Supposons donc que la caractéristique soit autre que 0. $\mathcal{A}_0(E)$ est un corps (commutatif ou non-commutatif). D'après la prop. 3 et d'après le th. 14 de [11] n°31, il existe un homomorphisme φ de $\mathcal{A}_0(E)$ dans le corps des nombres p-adiques; φ est un isomorphisme puisque $\mathcal{A}_0(E)$ est un corps. $\mathcal{A}_0(E)$ est donc un corps commutatif. On a $[\mathcal{A}_0(E):\boldsymbol{Q}]\leqq 2$ puisque, d'après le cor. 2 du th. 36 de [11] n°69, tout élément de $\mathcal{A}_0(E)$ satisfait à une équation à coefficients rationnels de degré 2. Supposons que l'on ait $[\mathcal{A}_0(E):\boldsymbol{Q}]=2$. Soit l un nombre premier qui reste premier dans $\mathcal{A}_0(E)$. Soit $\mathfrak{g}$ un sous-groupe de E d'ordre l; Il y a une courbe elliptique E' et un homomorphisme λ de E sur E' tels que $\mathfrak{g}(\lambda)=\mathfrak{g}$. Pour un l approprié, on peut facilement voir que $\mathcal{A}(E')$ n'est pas isomorphe à $\mathcal{A}(E)$[2]. D'autre

2) C'est une conséquence des résultats dans [8].

part, d'après la prop. 1, si l'on désigne par k_0 le corps premier, $j(E)$ est algébrique sur $k_0(j(E'))$, de sorte que $j(E')$ est transcendant sur k_0; on peut en déduire que $\mathcal{A}(E')$ est isomorphe à $\mathcal{A}(E)$; ce qui est absurde. On a donc $[\mathcal{A}_0(E); \boldsymbol{Q}]=1$; par suite $\mathcal{A}(E)$ est isomorphe à $\boldsymbol{Z}$.

§ 2. Correspondances modulaires.

4. Soient γ une variable sur $\boldsymbol{Q}$ et E la courbe elliptique définie par l'équation

$$Y^2=4X^3-\gamma X-\gamma . \tag{4}$$

Posons $j=j(E)$. On a alors $j=\gamma/(\gamma-27)$, $\gamma=27j/(j-1)$ et $\boldsymbol{Q}(\gamma)=\boldsymbol{Q}(j)$; j est donc une variable sur $\boldsymbol{Q}$. Nous désignons par $\boldsymbol{F}$ la clôture algébrique du corps $\boldsymbol{Q}(j)$. Soit h la fonction canonique sur E. Dans cette section nous employons ces notations $E, \gamma, j, h, \boldsymbol{F}$ toujours en ce sens.

Nous désignerons par $K_N^*(E)$ et par $K_N(E)$, ou simplement par K_N^* et par K_N, respectivement les corps

$$\boldsymbol{Q}(j, t \mid t\in\mathfrak{g}(N, E))$$

$$\text{et } \boldsymbol{Q}(j, h(t) \mid t\in\mathfrak{g}(N, E))$$

pour chaque entier $N>0$. Ces corps sont galoisiens sur $\boldsymbol{Q}(j)$. Nous désignerons par $G_N(E)$ le groupe de Galois de $K_N(E)$ sur $\boldsymbol{Q}(j)$. Soit $\{t_1, t_2\}$ un système de générateurs de $\mathfrak{g}(N, E)$; on a alors

$$\mathfrak{g}(N, E)=\{\alpha t_1+\beta t_2 \mid \ 0\leqq\alpha<N, 0\leqq\beta<N\} .$$

Soit σ un élément de $G_N(E)$; σ est prolongé à un automorphisme de K_N^* que nous désignons aussi par σ. $\{t_1^\sigma, t_2^\sigma\}$ est un système de générateurs de $\mathfrak{g}(N, E)$; il y a donc une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients entiers telle qu'on ait

$$\begin{pmatrix} t_1^\sigma \\ t_2^\sigma \end{pmatrix}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} t_1 \\ t_2 \end{pmatrix},$$

et par suite

$$h(\alpha t_1+\beta t_2)^\sigma=h(\alpha' t_1+\beta' t_2), \qquad (\alpha' \ \beta')=(\alpha \ \beta)\begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{5}$$

L'automorphisme σ est determiné par la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et s'appellera *l'automorphisme de* $K_N(E)$ *correspondant à* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *par rapport à* $\{t_1, t_2\}$. Nous désignerons par G_N^* le groupe des matrices de degré 2 à coefficients dans l'anneau $\boldsymbol{Z}/N\boldsymbol{Z}$ dont les déterminants sont inversibles et par S_N^* le sous-groupe de G_N^* consistant en les éléments unimodulaires (*c.-à-d.* de déterminant

$=1$). Nous désignerons respectivement par G_N et S_N les groupes $G_N^*/\{\pm I\}$ et $S_N^*/\{\pm I\}$. Comme ci-dessus nous pouvons faire correspondre à chaque $\sigma \in G_N(E)$, une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_N^*$. Tenant compte de (3), on vérifie facilement que l'application $\sigma \to \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ donne un isomorphisme de $G_N(E)$ dans $G_N = G_N^*/\{\pm I\}$. Cet isomorphisme est surjectif :

Proposition 5. *En faisant correspondre une matrice* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *à* $\sigma \in G_N(E)$ *par la relation* (5), *on obtient un isomorphisme de* $G_N(E)$ *sur* G_N.

Soit $S_N(E)$ le sous-groupe de $G_N(E)$ correspondant au sous-groupe S_N de G_N par cet isomorphisme. $S_N(E)$ ne dépend pas du choix de $\{t_1, t_2\}$.

Proposition 6. *Le sous-corps de* K_N *correspondant au sous-groupe* $S_N(E)$ *de* $G_N(E)$ *est le corps* $\boldsymbol{Q}(j, \zeta_N)$ *où* ζ_N *désigne une racine primitive N-ième d'unité.* $\boldsymbol{Q}(\zeta_N)$ *est algébriquement fermé dans* K_N.

Dans §§ 2, 3, nous désignerons par ζ_N une racine primitive N-ième d'unité.

Proposition 7. *Soit* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *un élément de* G_N^* *et* σ *l'automorphisme de* K_N *correspondant à* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. *On a alors* $\zeta_N{}^{\sigma} = \zeta_N^{ad-bc}$. *En d'autres termes, si* $ad-bc$ *est congru à un nombre premier p modulo N,* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *donne la substitution de Frobenius* $\left(\frac{\boldsymbol{Q}(\zeta_N)/\boldsymbol{Q}}{p}\right)$ *dans* $\boldsymbol{Q}(\zeta_N)$.

Nous démontrerons les prop. 5–7 dans le § 4.

5. Maintenant nous allons déterminer les sous-groupes de $G_N(E)$ correspondant à certains sous-corps de $K_N(E)$. Dans ce but nous fixons un système de générateurs $\{t_1, t_2\}$ de $\mathfrak{g}(N, E)$ et identifions $G_N(E)$ avec G_N par l'isomorphisme donné ci-dessus.

Proposition 8. *Soient* $\mathfrak{g}, \mathfrak{g}'$ *deux sous-groupes d'ordre N de E et* σ *un automorphisme de* $\boldsymbol{F}$ *sur* $\boldsymbol{Q}(j)$. *Alors pour qu'on ait* $j(E/\mathfrak{g})^{\sigma} = j(E/\mathfrak{g}')$, *il faut et il suffit que* $\mathfrak{g}^{\sigma} = \mathfrak{g}'$; $j(E/\mathfrak{g})$ *est contenu dans* $K_N(E)$.

La première assertion est une conséquence immédiate de la prop. 4 et du lemme 2. Si σ est l'identité dans $K_N(E)$, on a $h(t^{\sigma}) = h(t)$ pour $t \in \mathfrak{g}(N, E)$; par suite on a $t^{\sigma} = \pm t$ pour $t \in \mathfrak{g}$, de sorte qu'on a $\mathfrak{g}^{\sigma} = \mathfrak{g}$ et $j(E/\mathfrak{g})^{\sigma} = j(E/\mathfrak{g})$. Il s'ensuit de là que $j(E/\mathfrak{g})$ est contenu dans $K_N(E)$.

Soient $\mathfrak{g}_{(1)}$, $\mathfrak{g}_{(2)}$ respectivement les sous-groupes de E engendrés par t_1 et par t_2 ; posons $j_{(1)} = j(E/\mathfrak{g}_{(1)})$, $j_{(2)} = j(E/\mathfrak{g}_{(2)})$. Nous avons le tableau suivant :

Sous-corps de $K_N(E)$	Sous-groupe de $G_N(E)$
$\boldsymbol{Q}(j, j_{(1)})$	$\left\{\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}\right\}/\{\pm I\}$
$\boldsymbol{Q}(j, j_{(2)})$	$\left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right\}/\{\pm I\}$
$\boldsymbol{Q}(j, h(t_1))$	$\left\{\begin{pmatrix} \pm 1 & 0 \\ c & d \end{pmatrix}\right\}/\{\pm I\}$
$\boldsymbol{Q}(j, h(t_2))$	$\left\{\begin{pmatrix} a & b \\ 0 & \pm 1 \end{pmatrix}\right\}/\{\pm I\}$
$\boldsymbol{Q}(j, j_{(2)}, h(t_1))$	$\left\{\begin{pmatrix} \pm 1 & 0 \\ 0 & d \end{pmatrix}\right\}/\{\pm I\}$
$\boldsymbol{Q}(j, j_{(1)}, h(t_2))$	$\left\{\begin{pmatrix} a & 0 \\ 0 & \pm 1 \end{pmatrix}\right\}/\{\pm I\}$

où les groupes au côté droit désignent les sous-groupes de $G_N(E)$ correspondant aux sous-corps de $K_N(E)$ au côté gauche; les lettres a, d désignent les éléments inversibles de $\boldsymbol{Z}/N\boldsymbol{Z}$ et b, c désignent les éléments quelconques de $\boldsymbol{Z}/N\boldsymbol{Z}$. Soit en effet σ un élément de $G_N(E)$ donné par une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$; on a alors $h(t_1^{\sigma})=h(at_1+bt_2)$; d'où résulte $\pm t_1^{\sigma}=at_1+bt_2$. D'après la prop. 8, pour qu'on ait $j_{(1)}^{\sigma}=j_{(1)}$, il faut et il suffit qu'on ait $\mathfrak{g}_1^{\sigma}=\mathfrak{g}_1$, ou qu'on ait $b=0$. De plus, pour qu'on ait $h(t_1)^{\sigma}=h(t_1)$, il faut et il suffit qu'on ait $a=\pm 1$, $b=0$. Nous obtenons le tableau par ces relations.

6. Soient maintenant n un entier positif tel que $(n, N)=1$ et $\mathfrak{g}_{\alpha}$ $(1\leqq\alpha\leqq s)$ les sous-groupes cycliques de E d'ordre n; posons $j_{\alpha}=j(E/\mathfrak{g}_{\alpha})$. D'après la prop. 1, j est algébrique sur $\boldsymbol{Q}(j_{\alpha})$, de sorte que j_{α} est transcendant sur $\boldsymbol{Q}$ pour chaque α. Il existe donc un isomorphisme τ_{α} de $\boldsymbol{Q}(j)$ sur $\boldsymbol{Q}(j_{\alpha})$ tel que $j^{\tau_{\alpha}}=j_{\alpha}$ pour chaque α. Posons $\gamma_{\alpha}=\gamma^{\tau_{\alpha}}$, $E_{\alpha}=E^{\tau_{\alpha}}$, $h_{\alpha}=h^{\tau_{\alpha}}(1\leqq\alpha\leqq s)$; E_{α} est alors défini par l'équation

$$Y^2=4X^3-\gamma_{\alpha}X-\gamma_{\alpha}; \tag{6}$$

h_{α} est la fonction canonique sur E_{α}. Comme on a $j(E_{\alpha})=j_{\alpha}=j(E/\mathfrak{g}_{\alpha})$, il existe un homomorphisme λ_{α} de E sur E_{α} tel que $\mathfrak{g}_{\alpha}=\mathfrak{g}(\lambda_{\alpha})$ pour chaque α.

PROPOSITION 9. *Il existe un isomorphisme σ_{α} de $K_N(E)$ sur $K_N(E_{\alpha})$ tel que*

$$j^{\sigma_{\alpha}}=j_{\alpha},\ h(t)^{\sigma_{\alpha}}=h_{\alpha}(\lambda_{\alpha}t)\ \textit{pour}\ t\in\mathfrak{g}(N, E)$$

pour chaque α; σ_{α} est déterminé par ces relations.

Prolongeons l'isomorphisme τ_{α} à un automorphisme de $\boldsymbol{F}$ que nous désignons aussi par τ_{α}. L'application $t\to t^{\tau_{\alpha}^{-1}}$ donne un isomorphisme de $\mathfrak{g}(N, E_{\alpha})$ sur $\mathfrak{g}(N, E)$. D'autre part, comme $(n, N)=1$, l'application $t\to\lambda_{\alpha}t$

donne un isomorphisme de $\mathfrak{g}(N, E)$ sur $\mathfrak{g}(N, E_\alpha)$; par suite $t \to (\lambda_\alpha t)^{\tau_\alpha^{-1}}$ donne un automorphisme de $\mathfrak{g}(N, E)$; il existe donc une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients entiers telle que

$$\begin{pmatrix} \lambda_\alpha t_1 \\ \lambda_\alpha t_2 \end{pmatrix}^{\tau_\alpha^{-1}} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \end{pmatrix}.$$

D'après la prop. 5, il existe un automorphisme ρ_α de $K_N(E)$ donné par $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$; on a alors $j^{\rho_\alpha} = j$, $h(t)^{\rho_\alpha} = h((\lambda_\alpha t)^{\tau_\alpha^{-1}})$. Posons $\sigma_\alpha = \rho_\alpha \tau_\alpha$; on a alors $j^{\sigma_\alpha} = j_\alpha$, $h(t)^{\sigma_\alpha} = h_\alpha(\lambda_\alpha t)$. Comme j, $h(t)$ engendrent $K_N(E)$ sur $\boldsymbol{Q}$, σ_α est déterminé par ces relations.

Proposition 10. *Soit $u = (u_1, \cdots, u_m)$ un ensemble fini d'éléments de $K_N(E)$ tel que j soit contenu dans $\boldsymbol{Q}(u)$. Soient $\sigma_1, \cdots, \sigma_s$ les isomorphismes de K_N déterminés dans la prop. 9. Alors $\boldsymbol{Q}(u, j^{\sigma_\alpha})$ contient $\boldsymbol{Q}(u^{\sigma_\alpha})$; $(u^{\sigma_1}, \cdots, u^{\sigma_s})$ est l'ensemble complet des conjugués de u^{σ_1} sur $\boldsymbol{Q}(u)$.*

Soit τ un automorphisme de la clôture algébrique $\boldsymbol{F}$ de $\boldsymbol{Q}(j)$ qui fixe u, j_α. Comme j est contenu dans $\boldsymbol{Q}(u)$, τ laisse fixe j; on a donc $E^\tau = E$, $E_\alpha{}^\tau = E_\alpha$. D'après le lemme 3, on a $\lambda_\alpha{}^\tau = \pm\lambda_\alpha$. Il en résulte que

$$h(t)^{\sigma_\alpha \tau} = h_\alpha(\lambda_\alpha t)^\tau = h_\alpha(\pm\lambda_\alpha t^\tau) = h_\alpha(\lambda_\alpha t^\tau) = h(t^\tau)^{\sigma_\alpha} = h(t)^{\tau\sigma_\alpha}$$

pour chaque $t \in \mathfrak{g}(N, E)$. On vérifie aisément $j^{\sigma_\alpha \tau} = j_\alpha = j^{\tau\sigma_\alpha}$. Comme j et $h(t)$ engendrent $K_N(E)$, on a $\sigma_\alpha \tau = \tau\sigma_\alpha$; par suite on a $(u^{\sigma_\alpha})^\tau = (u^\tau)^{\sigma_\alpha} = u^{\sigma_\alpha}$; ce qui montre que $\boldsymbol{Q}(u^{\sigma_\alpha})$ est contenu dans $\boldsymbol{Q}(u, j_\alpha)$. On déduit de là

$$[\boldsymbol{Q}(u, u^{\sigma_\alpha}) : \boldsymbol{Q}(u)] = [\boldsymbol{Q}(u, j_\alpha) : \boldsymbol{Q}(u)] \leqq [\boldsymbol{Q}(j, j_\alpha) : \boldsymbol{Q}(j)].$$

Soit σ un automorphisme de $\boldsymbol{F}$ sur $\boldsymbol{Q}(j)$; $\mathfrak{g}_1{}^\sigma$ est alors un des $\mathfrak{g}_\alpha$; par suite, d'après la prop. 8, les conjugués de j_1 sur $\boldsymbol{Q}(j)$ sont contenus dans $\{j_1, \cdots, j_s\}$; ce qui montre $[\boldsymbol{Q}(j, j_\alpha) : \boldsymbol{Q}(j)] \leqq s$. Comme on a $\boldsymbol{Q}(u^{\sigma_\alpha}) \supset \boldsymbol{Q}(j^{\sigma_\alpha})$ et $j^{\sigma_\alpha} \neq j^{\sigma_\beta}$ pour $\alpha \neq \beta$, $u^{\sigma_1}, \cdots, u^{\sigma_s}$ sont différents l'un de l'autre. Notre proposition sera donc démontrée si nous faisons voir que u^{σ_α} est un conjugué de u^{σ_1} sur $\boldsymbol{Q}(u)$ pour chaque α. Soit $\{t_1', t_2'\}$ un système de générateurs de $\mathfrak{g}(nN, E)$; $\{Nt_1'\ Nt_2'\}$ est alors un système de générateurs de $\mathfrak{g}(n, E)$. D'après la prop. 5, il existe un automorphisme ρ de $K_n{}^*(E)$ sur $\boldsymbol{Q}(j)$ tel que $\mathfrak{g}_1{}^\rho = \mathfrak{g}_\alpha$. Soit $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ une matrice de $G_n{}^*$ à laquelle ρ correspond par rapport à $\{Nt_1', Nt_2'\}$. Comme on a $(n, N) = 1$, il existe une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de G_{nN}^* telle que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mod n,$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N.$$

Désignons par σ l'automorphisme de $K_{nN}(E)$ correspondant à $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ par rapport à $\{t_1', t_2'\}$. On a alors $z^\sigma=z$ pour $z\in K_N(E)$ et $w^\sigma=w^\rho$ pour $w\in K_n(E)$; on a donc $E^\sigma=E$, $\mathfrak{g}_1{}^\sigma=\mathfrak{g}_\alpha$, $E_1{}^\sigma=E_\alpha$, $j_1{}^\sigma=j_\alpha$, $h_1{}^\sigma=h_\alpha$, $\lambda_1{}^\sigma=\pm\lambda_\alpha$ en vertu du lemme 3 et $t^\sigma=\pm t$ pour $t\in\mathfrak{g}(N, E)$; il s'ensuit de là que, pour $t\in\mathfrak{g}(N, E)$, on a

$$h(t)^{\sigma_1\sigma}=h_1(\lambda_1 t)^\sigma=h_\alpha(\pm\lambda_\alpha(\pm t))=h_\alpha(\lambda_\alpha t)=h(t)^{\sigma_\alpha}$$

et $j^{\sigma_1\sigma}=j^{\sigma_\alpha}$. Comme j et $h(t)$ pour $t\in\mathfrak{g}(N, E)$ engendrent $K_N(E)$, on obtient $\sigma_1\sigma=\sigma_\alpha$ sur $K_N(E)$; on a donc $(u^{\sigma_1})^\sigma=u^{\sigma_\alpha}$. Comme σ est l'identité sur $K_N(E)$, u^{σ_α} est un conjugué de u^{σ_1} sur $K_N(E)$; ceci achève la démonstration.

PROPOSITION 11. *Les notations étant celles de la prop.* 10, *on a*

$$[\boldsymbol{Q}(u, u^{\sigma_1}): \boldsymbol{Q}(u)]=[\boldsymbol{Q}(u, u^{\sigma_1}): \boldsymbol{Q}(u^{\sigma_1})].$$

D'après le th. 27 de [11] n°52, il existe un homomorphisme μ de E_1 sur E tel que $\mu\lambda_1=n\delta_E$. En appliquant la prop. 9 à E_1, μ, E, on peut montrer qu'il y a un isomorphisme τ de $K_N(E_1)$ sur $K_N(E)$ tel que

$$j_1{}^\tau=j,\ h_1(t_1)^\tau=h(\mu t_1) \text{ pour } t_1\in\mathfrak{g}(N, E_1).$$

On a alors $j^{\sigma_1\tau}=j$, $h(t)^{\sigma_1\tau}=h(nt)$ pour $t\in\mathfrak{g}(N, E)$; autrement dit, $\sigma_1\tau$ est l'élément de $G_N(E)$ correspondant à $\begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}$. $\sigma_1\tau$ est donc contenu dans le centre du groupe $G_N(E)$; il en résulte qu'on a $\boldsymbol{Q}(u^{\sigma_1\tau})=\boldsymbol{Q}(u)$. D'après la prop. 10, on a $[\boldsymbol{Q}(u, u^{\sigma_1}): \boldsymbol{Q}(u)]=s=$ le nombre des sous-groupes cycliques de E d'ordre n. En appliquant ce résultat à u^{σ_1}, τ, on obtient $[\boldsymbol{Q}(u^{\sigma_1}, u^{\sigma_1\tau}): \boldsymbol{Q}(u^{\sigma_1})]=s$; ce qui prouve la proposition.

7. Soit L un sous-corps de $K_N(E)$ tel que $L\supset\boldsymbol{Q}(j)$, $L\cap\boldsymbol{Q}(\zeta_N)=\boldsymbol{Q}$. Comme $\boldsymbol{Q}(\zeta_N)$ est algébriquement fermé dans K_N, $\boldsymbol{Q}$ est algébriquement fermé dans L. Il y a donc une courbe complète Γ définie par rapport à $\boldsymbol{Q}$, sans point multiple, telle qu'on ait $L=\boldsymbol{Q}(u)$ pour un point générique u de Γ par rapport à $\boldsymbol{Q}$. Le système $\{\Gamma, u\}$ s'appellera un *modèle de* L. Nous fixons pour le moment L et $\{\Gamma, u\}$. Nous allons définir maintenant certaines correspondances algébriques sur la courbe Γ.

Soient σ_1 l'isomorphisme de K_N déterminé à la prop. 9 et X_n le diviseur premier rationnel par rapport à $\boldsymbol{Q}$ sur $\Gamma\times\Gamma$ ayant $u\times u^{\sigma_1}$ comme point générique sur $\boldsymbol{Q}$. D'après la prop. 10 et d'après le th. 12 de [9] chap. VIII, on a

$$X_n\cdot(u\times\Gamma)=u\times\sum_{\alpha=1}^{s}u^{\sigma_\alpha}. \tag{7}$$

X_n s'appellera *la correspondance modulaire de degré n sur* Γ. D'après la prop. 11, on a

(8) $$d(X_n)=d'(X_n)=s\ ^{3)}.$$

Soit ρ_n l'élément de $G_N(E)$ correspondant à la matrice $\begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}$. Il est clair que cet automorphisme de K_N ne dépend pas du choix d'un système de générateurs pour $\mathfrak{g}(N, E)$. Soit Y_n le lieu de $u\times u^{\rho n}$ sur $\Gamma\times\Gamma$ par rapport à $\boldsymbol{Q}$. Comme $\begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}$ est contenu dans le centre du groupe $G_N{}^*$, ρ_n donne un automorphisme de L; il en résulte que l'on a $\boldsymbol{Q}(u)=\boldsymbol{Q}(u^{\rho n})$, de sorte que Y_n donne une correspondance birationnelle de Γ. On a donc

(9) $$Y_n(u)=u^{\rho n}.$$

Si $n\equiv n'$ mod. N, on a $Y_n=Y_{n'}$.

8. En outre de X_n, Y_n nous avons besoin d'une autre correspondance pour exprimer la formule de congruence (II); pour la définir nous nous bornons à considérer le cas particulier où le corps L est explicitement donné ainsi qu'il suit.

Fixons un système de générateurs $\{t_1, t_2\}$ de $\mathfrak{g}(N, E)$ et identifions $G_N(E)$ avec G_N au moyen de l'isomorphisme défini par $\{t_1, t_2\}$. Nous désignerons par H_N le sous-groupe $\left\{\begin{pmatrix} a & 0 \\ 0 & \pm 1 \end{pmatrix} \middle| (a, N)=1\right\}\Big/\{\pm I\}$ de G et par L_N le sous-corps de K_N correspondant à H_N. On voit que

$$H_N S_N=G_N, \qquad H_N\cap S_N=\{e\};$$

on a donc

$$L_N\cap\boldsymbol{Q}(\zeta_N)=\boldsymbol{Q}, \qquad L_N(\zeta_N)=K_N.$$

D'après le tableau dans **5,** on a

$$L_N=\boldsymbol{Q}(j, j_{(1)}, h(t_2)).$$

Nous fixons un modèle de L_N et le désignons par $\{\Gamma_N, u\}$. Soit ψ l'automorphisme de K_N correspondant à $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ par rapport à $\{t_1, t_2\}$. Il est clair que $\boldsymbol{Q}(\zeta_N, u)=\boldsymbol{Q}(\zeta_N, u^{\psi})=K_N$. Soit A le lieu de $u\times u^{\psi}$ sur $\Gamma_N\times\Gamma_N$ par rapport à $\boldsymbol{Q}(\zeta_N)$; A donne une correspondance birationnelle de Γ_N; on a donc

(10) $$A(u)=u^{\psi}.$$

Proposition 12. *Soit φ_n l'automorphisme de $\boldsymbol{Q}(\zeta_N)$ tel que $\zeta_N{}^{\varphi_n}=\zeta_N{}^n$. On a alors*

$$A^{\varphi_n}\circ Y_n=A.$$

Soient τ_n et $\tau_{n'}$ les automorphismes de K_N qui correspondent respective-

3) Pour les définitions des notations $d(X)$, $d'(X)$, voir [10] p. 31.

ment à $\begin{pmatrix}1 & 0\\ 0 & n\end{pmatrix}$ et $\begin{pmatrix}n & 0\\ 0 & 1\end{pmatrix}$; d'après la prop. 7, on a $\tau_n=\tau_n'=\varphi_n$ sur $\boldsymbol{Q}(\zeta_N)$. On vérifie aisément $\psi\tau_n=\tau_n'\psi$ et $\tau_n'\tau_n=\rho_n$. Comme τ_n' est contenu dans H_N, on a

$$(u\times u^{\psi})^{\tau_n}=u^{\tau_n}\times u^{\psi\tau_n}=u^{\tau_n'\tau_n}\times u^{\tau_n'\psi}=u^{\rho_n}\times u^{\psi};$$

$u^{\rho_n}\times u^{\psi}$ est donc un point générique de A^{φ_n} sur $\boldsymbol{Q}(\zeta_N)$; d'où résultent les relations

$$A^{\varphi_n}(u^{\rho_n})=u^{\psi},\quad (A^{\varphi_n})'(u^{\psi})=u^{\rho_n}.$$

Par suite on a

$$A^{\varphi_n}[Y_n(u)]=u^{\psi}=A(u),\quad Y_n'[(A^{\varphi_n})'(u^{\psi})]=u=A'(u^{\psi}).$$

A et Y_n sont rationnels par rapport à $\boldsymbol{Q}(\zeta_N)$ et u, u^{ψ} sont génériques sur Γ par rapport à $\boldsymbol{Q}(\zeta_N)$. Il s'ensuit donc de la définition de $A^{\varphi_n}\circ Y_n$ ([10] II, § 1, n°5) que $A^{\varphi_n}\circ Y_n=A$.

Soit $\mathfrak{h}$ un sous-groupe du groupe d'éléments inversibles de $\boldsymbol{Z}/N\boldsymbol{Z}$; nous supposons que $\mathfrak{h}$ contienne -1. Nous désignerons par $H_{N,\mathfrak{h}}$ le sous-groupe $\left\{\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}\middle|\,(a,N)=1,\ d\in\mathfrak{h}\right\}\Big/\{\pm I\}$ de G_N et par $M_{N,\mathfrak{h}}$ le sous-corps de K_N correspondant à $H_{N,\mathfrak{h}}$. Nous désignerons aussi par $H_{N,\mathfrak{h}}'$ le sous-groupe $\left\{\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}\middle|\,(d,N)=1,\ a\in\mathfrak{h}\right\}\Big/\{\pm I\}$ de G_N et par $M_{N,\mathfrak{h}}'$ le sous-corps de K_N correspondant à $H_{N,\mathfrak{h}}'$. On voit que

$$H_{N,\mathfrak{h}}S_N=H_{N,\mathfrak{h}}'S_N=G_N,\quad H_{N,\mathfrak{h}}\cap S_N=H_{N,\mathfrak{h}}'\cap S_N;$$

on a donc

$$M_{N,\mathfrak{h}}\cap\boldsymbol{Q}(\zeta_N)=M_{N,\mathfrak{h}}'\cap\boldsymbol{Q}(\zeta_N)=\boldsymbol{Q},\quad M_{N,\mathfrak{h}}(\zeta_N)=M_{N,\mathfrak{h}}'(\zeta_N). \tag{11}$$

Selon que $\mathfrak{h}$ ne contient que ±1 ou que $\mathfrak{h}$ contient tous les éléments inversibles de $\boldsymbol{Z}/N\boldsymbol{Z}$ nous désignerons $H_{N,\mathfrak{h}}$, $H_{N,\mathfrak{h}}'$, $M_{N,\mathfrak{h}}$, $M_{N,\mathfrak{h}}'$ respectivement par $H_{N,1}$, $H_{N,1}'$, $M_{N,1}$, $M_{N,1}'$ ou par $H_{N,0}$, $H_{N,0}'$, $M_{N,0}$, $M_{N,0}'$. On a alors

$$H_{N,0}\supset H_{N,\mathfrak{h}}\supset H_{N,1},\qquad H_{N,0}'\supset H_{N,\mathfrak{h}}'\supset H_{N,1}',$$

$$M_{N,0}\subset M_{N,\mathfrak{h}}\subset M_{N,1},\qquad M_{N,0}'\subset M_{N,\mathfrak{h}}'\subset M_{N,1}'$$

pour chaque $\mathfrak{h}$; on voit aussi que $H_{N,0}=H_{N,0}'$ et $M_{N,0}=M_{N,0}'$.

Nous allons démontrer qu'il existe un isomorphisme de $M_{N,\mathfrak{h}}$ sur $M_{N,\mathfrak{h}}'$. $\{t_1, t_2\}$ étant le système de générateurs pour $\mathfrak{g}(N, E)$ que nous avons fixé, nous désignons par $\mathfrak{g}$ le groupe engendré par t_2. Posons $j'=j(E/\mathfrak{g})$. D'après la prop. 1, j' est transcendant sur $\boldsymbol{Q}$ et $\boldsymbol{F}$ est la clôture algébrique de $\boldsymbol{Q}(j')$. Soit σ un automorphisme de $\boldsymbol{F}$ tel que $j^{\sigma}=j'$; posons $E'=E^{\sigma}$. Il existe alors un homomorphisme λ de E sur E' tel que $\mathfrak{g}=\mathfrak{g}(\lambda)$. D'après le th. 27 de [11] n°52, il existe un homomorphisme μ de E' sur E tel que $\mu\lambda=N\delta_E$, $\lambda\mu=N\delta_{E'}$.

Posons $t_1'=\lambda t_1$. On voit que $\mu t_1'=0$ et que t_1' est d'ordre N. Comme on a $\nu(\mu)=N$, t_1' engendre $\mathfrak{g}(\mu)$. t_2^{σ} est un point de E' d'ordre N; par suite, d'après la prop. 5, il existe un automorphisme τ de $\boldsymbol{F}$ sur $\boldsymbol{Q}(j')$ tel que $(t_2^{\sigma})^{\tau}=\pm t_1'$; posons $\rho=\sigma\tau$; alors ρ est un automorphisme de $\boldsymbol{F}$. On a $j^{\rho}=j'$, $E^{\rho}=E'$, $t_2^{\rho}=\pm t_1'$, de sorte qu'on a $\mathfrak{g}(\lambda^{\rho})=\mathfrak{g}(\lambda)^{\rho}=\mathfrak{g}(\mu)$; on en conclut que E'^{ρ} est isomorphe à E; on a donc $j'^{\rho}=j$. En rappelant que E est la courbe définie par l'équation (4), on voit que $E'^{\rho}=E^{\sigma\rho}$ est définie par l'équation

$$Y^2=4X^3-\gamma^{\sigma\rho}X-\gamma^{\sigma\rho}.$$

On a $\gamma^{\sigma\rho}=27j^{\sigma\rho}/(j^{\sigma\rho}-1)=27j/(j-1)=\gamma$; ce qui montre que $E'^{\rho}=E$. Soient α et α' les automorphismes de $\boldsymbol{F}$ qui correspondent respectivement à $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ et $\begin{pmatrix} d & b \\ 0 & a \end{pmatrix}$ par rapport à $\{t_1, t_2\}$; on a alors $t_1^{\alpha}=\pm(at_1+bt_2)$ et $t_2^{\alpha'}=\pm at_2$. Nous allons maintenant montrer que $\rho\alpha=\alpha'\rho$ sur $M_{N,1}$. D'après le tableau dans **5**, on a $M_{N,1}=\boldsymbol{Q}(j, h(t_2))$, $M_{N,0}=M_{N,0}'=\boldsymbol{Q}(j, j')$. Comme α et α' fixent les éléments de $M_{N,0}$, on a $E^{\alpha}=E^{\alpha'}=E$, $E'^{\alpha}=E'^{\alpha'}=E'$. D'après le lemme 3, on a $\lambda^{\alpha}=\pm\lambda$, $\lambda^{\alpha'}=\pm\lambda$. On voit que $j^{\rho\alpha}=j'=j^{\alpha'\rho}$, $h^{\rho\alpha}=h^{\rho}=h^{\alpha'\rho}$ et

$$h(t_2)^{\rho\alpha}=[h^{\rho}(\pm t_1')]^{\alpha}=[h^{\rho}(\lambda t_1)]^{\alpha}=h^{\rho}(\lambda(at_1+bt_2))$$
$$=h^{\rho}(a\lambda t_1)=h^{\rho}(\pm at_1')=h(at_2)^{\rho}=h(t_2)^{\alpha'\rho}.$$

On obtient ainsi $j^{\rho\alpha}=j^{\alpha'\rho}$ et $h(t_2)^{\rho\alpha}=h(t_2)^{\alpha'\rho}$; il s'ensuit de là qu'on a $\rho\alpha=\alpha'\rho$ sur $M_{N,1}$. Si $a\in\mathfrak{h}$, α' fixe les éléments de $M_{N,\mathfrak{h}}$; on a alors $\rho\alpha=\rho$ sur $M_{N,\mathfrak{h}}$; autrement dit, si $a\in\mathfrak{h}$, α fixe les éléments de $M_{N,\mathfrak{h}}{}^{\rho}$; d'où résulte $M_{N,\mathfrak{h}}{}^{\rho}\subset M_{N,\mathfrak{h}}'$. D'autre part, comme on a bien $M_{N,0}{}^{\rho}=M_{N,0}=M_{N,0}'$ et comme $[M_{N,\mathfrak{h}}: M_{N,0}]$, $[M_{N,\mathfrak{h}}': M_{N,0}']$ sont égaux à l'indice du groupe $\mathfrak{h}$, on a

$$[M_{N,\mathfrak{h}}{}^{\rho}: M_{N,0}]=[M_{N,\mathfrak{h}}: M_{N,0}]=[M_{N,\mathfrak{h}}': M_{N,0}];$$

ce qui montre $M_{N,\mathfrak{h}}{}^{\rho}=M_{N,\mathfrak{h}}'$.

Soient maintenant $\{\Gamma_{N,\mathfrak{h}}, u\}$ un modèle du corps $M_{N,\mathfrak{h}}$ et B le lieu de $u\times u^{\rho}$ sur $\Gamma_{N,\mathfrak{h}}\times\Gamma_{N,\mathfrak{h}}$ par rapport à $\boldsymbol{Q}(\zeta_N)$, D'après la relation (11) et $M_{N,\mathfrak{h}}{}^{\rho}=M_{N,\mathfrak{h}}'$, B donne une correspondance birationnelle de $\Gamma_{N,\mathfrak{h}}$. En vertu de la relation $\rho\alpha=\alpha'\rho$ que l'on a vue ci-dessus, on peut démontrer la proposition suivante de la même manière que la prop. 12.

Proposition 13. *Soit φ_n l'automorphisme de $\boldsymbol{Q}(\zeta_N)$ tel que $\zeta_N{}^{\varphi_n}=\zeta_N{}^n$. On a alors*

$$B^{\varphi_n}\circ Y_n=B.$$

§ 3. Formules de congruence.

9. Dans cette section nous démontrerons quelques relations de congruence pour les correspondances définies dans § 2. Pour cela, nous profiterons

de la notion de réduction des variétés algébriques modulo p, et nous servirons des termes et des résultats dans [5-8].

Soient k un corps, $\mathfrak{p}$ un diviseur premier de k et $\tilde{k}$ le corps des restes modulo $\mathfrak{p}$. Si $\mathfrak{X}$ représente un objet algébro-géométrique défini par rapport à k, nous indiquerons par $\mathfrak{X}(\mathfrak{p})$ ou $\tilde{\mathfrak{X}}$ la réduction de $\mathfrak{X}$ modulo $\mathfrak{p}$.

Soit Γ une courbe complète sans point multiple, définie par rapport à k. Nous dirons que Γ *n'a pas de défaut pour* $\mathfrak{p}$, si Γ est $\mathfrak{p}$-simple et $\mathfrak{p}$-complet et la réduction $\tilde{\Gamma}$ n'a pas de point multiple; s'il en est ainsi, Γ et $\tilde{\Gamma}$ ont le même genre et Γ n'a pas de défaut comme variété abélienne lorsque Γ est une courbe elliptique.

Maitenant supposons que $\mathfrak{p}$ ne divise ni 2, ni 3. Soit j un élément de k. Pour qu'il existe une courbe elliptique E', définie par rapport à une extension k' de k, sans défaut pour chaque prolongement de $\mathfrak{p}$ dans k', telle que $j(E')=j$, il faut et il suffit que j soit $\mathfrak{p}$-entier; s'il en est ainsi, on a $j(E'(\mathfrak{p}))=j(E')(\mathfrak{p}')$ où $\mathfrak{p}'$ désigne un prolongement de $\mathfrak{p}$ dans k' (cf. [2] § 4).

Soient Γ, Γ' deux courbes complètes sans point multiple définies par rapport à k et X une correspondance entre Γ et Γ' rationnelle par rapport à k. Supposons que Γ, Γ' n'aient pas de défaut pour $\mathfrak{p}$. On obtient alors une correspondance $\tilde{X}=X(\mathfrak{p})$ entre $\tilde{\Gamma}$ et $\tilde{\Gamma}'$; on vérifie aisément $X'(\mathfrak{p})=X(\mathfrak{p})'$. Soient w et $\tilde{w}$ respectivement un point générique de Γ par rapport à k et un point générique de $\tilde{\Gamma}$ par rapport à $\tilde{k}$. Les produits $X\cdot(w\times\Gamma')$ et $\tilde{X}\cdot(\tilde{w}\times\tilde{\Gamma}')$ sont alors définis. La spécialisation $w\to\tilde{w}[\mathfrak{p}]$ définit un prolongement $\mathfrak{p}_1$ dans $k(w)$; d'après le th. 17 de [5], $\tilde{X}\cdot(\tilde{w}\times\tilde{\Gamma}')$ est la réduction de $X\cdot(w\times\Gamma')$ modulo $\mathfrak{p}_1$. Par suite on a $d(X)=d(\tilde{X})$ et semblablement $d'(X)=d'(\tilde{X})$. Soient J, J' respectivement une jacobienne de Γ et une jacobienne de Γ'; soient φ une application canonique de Γ dans J et φ' une application canonique de Γ' dans J'. Nous supposons que J, J', φ, φ' soient définis par rapport à k et que J, J' n'aient pas de défaut pour $\mathfrak{p}$. Alors, on peut démontrer que J est une jacobienne de $\tilde{\Gamma}$, que $\tilde{\varphi}$ est une application canonique de $\tilde{\Gamma}$ dans J et de même pour $\tilde{\Gamma}', \tilde{J}', \tilde{\varphi}'$. Soit ξ l'homomorphisme de J dans J' correspondant à X. Alors on vérifie aisément que $\tilde{\xi}$ est l'homomorphisme de J dans J' correspondant à $\tilde{X}$.

10. Soit maintenant E la courbe elliptique avec l'invariant transcendant j sur $\boldsymbol{Q}$, que nous avons considérée dans § 2. Soient N un entier positif et p un nombre premier qui ne divise pas $6N$. En regardant ce nombre premier p comme le nombre n dans **6**, nous obtenons les sous-groupes $\mathfrak{g}_\alpha$ de E d'ordre p, les courbes elliptiques E_α et les homomorphismes λ_α. Le nombre s des $\mathfrak{g}_\alpha$ est ici égal à $p+1$. Pour chaque α, soit μ_α un homomorphisme de E_α sur E tel que $\mu_\alpha\lambda_\alpha=p\delta_E$ et $\lambda_\alpha\mu_\alpha=p\delta_{E_\alpha}$. Nous nous servirons des mêmes notations que dans **6-8.**

Soit k_1 une extension de degré fini de $K_{pN}^*(E)$ telle que tous les λ_ν, μ_ν soient définis par rapport à k_1. Soit $\mathfrak{p}_1$ un diviseur premier de k_1 prolongeant le diviseur premier p de $\boldsymbol{Q}$ tel que $j(\mathfrak{p}_1)$ soit transcendant sur le corps premier. D'après un résultat classique[4], tous les j_α sont $\mathfrak{p}_1$-entiers. Il existe donc pour chaque α une courbe elliptique E_α' isomorphe à E_α qui n'a pas de défaut pour tout prolongement de $\mathfrak{p}_1$. Soient λ_α' un homomorphisme de E sur E_α' tel que $\mathfrak{g}(\lambda_\alpha')=\mathfrak{g}_\alpha$ et μ_α' un homomorphisme de E_α' sur E tel que $\mu_\alpha'\lambda_\alpha'=p\delta_E$, $\lambda_\alpha'\mu_\alpha'=p\delta_{E_\alpha'}$. Soient k une extension finie de k_1 par rapport à laquelle tous les E_α' et tous les λ_α', μ_α' sont définis et $\mathfrak{p}$ un prolongement de $\mathfrak{p}_1$ dans k. En réduisant modulo $\mathfrak{p}$, on a $\tilde{\mu}_\alpha'\tilde{\lambda}_\alpha'=p\delta_{\tilde{E}}$. D'après la prop. 3, on a $\nu_s(\tilde{\mu}_\alpha')\nu_s(\tilde{\lambda}_\alpha')=p$; il en résulte que l'on a $\nu_s(\tilde{\mu}_\alpha')=1$ ou $\nu_s(\tilde{\lambda}_\alpha')=1$. D'après la prop. 2, on a $\tilde{j}_\alpha=\tilde{j}^p$ ou $\tilde{j}_\alpha^p=\tilde{j}$; par suite tous les $\tilde{j}_\alpha$ sont transcendants sur le corps premier. Comme E_α est défini par l'équation (6) et $\gamma_\alpha=27j_\alpha/(j_\alpha-1)$, E_α n'a pas de défaut pour $\mathfrak{p}$; $\tilde{E}_\alpha$ est alors défini par l'équation

$$Y^2=4X^3-\tilde{\gamma}_\alpha X-\tilde{\gamma}_\alpha. \tag{12}$$

La réduction modulo $\mathfrak{p}$ donne un homomorphisme de $\mathfrak{g}(p, E)$ *sur* $\mathfrak{g}(p, \tilde{E})$. Comme le groupe $\mathfrak{g}(p, E)$ est d'ordre p^2 et comme, d'après la prop. 3, le groupe $\mathfrak{g}(p, \tilde{E})$ est d'ordre p, le noyau de cet homomorphisme est d'ordre p; donc il coïncide avec un des $\mathfrak{g}_\alpha$, mettons $\mathfrak{g}_1$. On a alors $\mathfrak{g}(\tilde{\lambda}_1)=\tilde{\mathfrak{g}}_1=\{0\}$. Si $\alpha>1$, on a $\mathfrak{g}(p, E)=\mathfrak{g}_1+\mathfrak{g}_\alpha$, de sorte qu'on a $\mathfrak{g}(\tilde{\lambda}_\alpha)=\tilde{\mathfrak{g}}_\alpha=\mathfrak{g}(p, \tilde{E})$. On a donc $\nu_s(\tilde{\lambda}_1)=1$ et $\nu_s(\tilde{\lambda}_\alpha)=p$ pour $\alpha>1$. Comme on a $\tilde{\mu}_\alpha\tilde{\lambda}_\alpha=p\delta_{\tilde{E}}$, d'après la prop. 3 on a $\nu_s(\tilde{\mu}_1)=p$ et $\nu_s(\tilde{\mu}_\alpha)=1$ pour $\alpha>1$. Il en résulte d'après la prop. 2, qu'il y a un isomorphisme ε de $\tilde{E}^p$ sur $\tilde{E}_1$ et un isomorphisme ε_α de $\tilde{E}_\alpha{}^p$ sur $\tilde{E}$ pour chaque $\alpha>1$ tels que

$$\begin{aligned} &\tilde{\lambda}_1\tilde{x}=\varepsilon\tilde{x}^p \quad \text{pour} \quad \tilde{x}\in\tilde{E}, \\ &\tilde{\mu}_\alpha\tilde{x}_\alpha=\varepsilon_\alpha\tilde{x}_\alpha{}^p \quad \text{pour} \quad \tilde{x}_\alpha\in\tilde{E}_\alpha \qquad (\alpha>1). \end{aligned} \tag{13}$$

On a donc

$$\begin{aligned} &\tilde{j}_1=\tilde{j}^p, \quad \tilde{\gamma}_1=\tilde{\gamma}^p, \\ &\tilde{j}=\tilde{j}_\alpha{}^p, \quad \tilde{\gamma}=\tilde{\gamma}_\alpha{}^p \qquad (\alpha>1). \end{aligned} \tag{14}$$

On en déduit que $\tilde{E}_1=\tilde{E}^p$, $\tilde{E}=\tilde{E}_\alpha{}^p$ $(\alpha>1)$ comme les équations de E et de E_α ont les formes (4) et (6); les isomorphismes ε, ε_α sont donc éguax à ±1. Soient h et h_α respectivement les fonctions canoniques sur E et sur E_α comme dans **6~8**; on a alors $\tilde{h}_1=\tilde{h}^p$ et $\tilde{h}=\tilde{h}_\alpha{}^p$ pour $\alpha>1$. Il s'ensuit donc de la relation (13) que

$$\begin{aligned} &\tilde{h}_1(\tilde{\lambda}_1\tilde{t})=\tilde{h}^p(\pm\tilde{t}^p)=\tilde{h}(\tilde{t})^p \quad \text{pour} \quad \tilde{t}\in\mathfrak{g}(N, \tilde{E}), \\ &\tilde{h}(\tilde{\mu}_\alpha\tilde{t}_\alpha)=\tilde{h}_\alpha{}^p(\pm\tilde{t}_\alpha{}^p)=\tilde{h}_\alpha(\tilde{t}_\alpha)^p \quad \text{pour} \quad \tilde{t}_\alpha\in\mathfrak{g}(N, \tilde{E}_\alpha), \qquad (\alpha>1). \end{aligned} \tag{15}$$

4) Une démonstration moderne de ce résultat est donnée dans [2] § 6.

En substituant $\tilde{\lambda}_\alpha \tilde{t}$ à $\tilde{t}_\alpha$ on obtient

$$\tilde{h}_\alpha(\tilde{\lambda}_\alpha \tilde{t})^p = \tilde{h}(p\tilde{t}) \qquad \text{pour} \quad \tilde{t} \in \mathfrak{g}(N, \tilde{E}). \tag{15'}$$

Soient σ_α pour $1 \leqq \alpha \leqq p+1$ et ρ_n les isomorphismes du corps $K_N(E)$ définis dans **6.** Les relations (14), (15), (15') montrent que K_N a un système de générateurs $(x)=(x_1, \cdots, x_c)$ sur $\boldsymbol{Q}$ tel que tous les $x_i, x_i^{\sigma_\alpha}, x_i^{\rho_p}$ soient $\mathfrak{p}$-entiers et que l'on ait

$$\begin{aligned} & x_i^{\sigma_1} \equiv x_i^p \qquad \text{mod. } \mathfrak{p}, \\ & (x_i^{\sigma_\alpha})^p \equiv x_i^{\rho_p} \ (1 < \alpha \leqq p+1) \qquad \text{mod. } \mathfrak{p}. \end{aligned} \tag{16}$$

11. Nous allons maintenant nous occuper des correspondances définies dans **7.** Soient L un sous-corps de K_N tel que $L \supset \boldsymbol{Q}(j)$, $L \cap \boldsymbol{Q}(\zeta_N) = \boldsymbol{Q}$ et $\{\Gamma, u\}$ un modèle de L. Soient X_p, Y_p les correspondances sur Γ définies dans **7.** Γ n'a pas de défaut pour presque tous les diviseurs premiers de $\boldsymbol{Q}$. Pour chacun de ces diviseurs premiers de $\boldsymbol{Q}$, nous prenons un de ses prolongements dans $\boldsymbol{F}$ et le fixons; nous désignons le diviseur premier de $\boldsymbol{F}$ prolongeant (p) aussi par p. On vérifie facilement que le point u reste générique par rapport au corps premier modulo presque tous les p.

Soient $u_1, \cdots, u_z$ les coordonnées du point u; chaque u_i s'exprime sous la forme $u_i = f_i(x)/g_i(x)$ où f_i, g_i sont deux polynomes à coefficients entiers. Tous les $g_i(x)$, $g_i(x)^{\rho_n}$ $(1 \leqq i \leqq z,\ 1 \leqq n \leqq N,\ (n, N)=1)$ sont des p-unités pour presque tous les diviseurs premiers p. La formule (16) montre que les $g_i(x)^{\sigma_\alpha}$ sont des p-unités pour ces p. Il s'ensuit donc de (16) que l'on a pour presque tous les p,

$$\tilde{u}^{\sigma_1} = \tilde{u}^p, \quad (\tilde{u}^{\sigma_\alpha})^p = \tilde{u}^{\rho_p} \qquad (\alpha > 1). \tag{17}$$

Si $\tilde{u}$ est générique sur $\tilde{\Gamma}$ par rapport au corps premier, les produits d'intersection $\tilde{X}_p \cdot (\tilde{u} \times \tilde{\Gamma})$ et $\tilde{Y}_p \cdot (\tilde{u} \times \tilde{\Gamma})$ sont définis. Il résulte alors de (7), (9), (17) et du th. 17 de [5] que l'on a

$$\tilde{X}_p(\tilde{u}) = \tilde{u}^p + p\tilde{Y}_p(\tilde{u})^{1/p}.$$

$\tilde{Y}_n$ donne, pour chaque n, une correspondance birationnelle de $\tilde{\Gamma}$ pour presque tous les p. Soit Π le lieu de $\tilde{u} \times \tilde{u}^p$ sur $\tilde{\Gamma} \times \tilde{\Gamma}$ par rapport au corps premier. Alors on a

$$\tilde{X}_p(\tilde{u}) = (\Pi + \Pi' \circ \tilde{Y}_p)(\tilde{u});$$

on en déduit que $\tilde{X}_p - (\Pi + \Pi' \circ \tilde{Y}_p)$ est un cycle $\mathfrak{a} \times \tilde{\Gamma}$ où $\mathfrak{a}$ est un diviseur sur $\tilde{\Gamma}$ en vertu du th. 2 de [10]. Comme $\Pi + \Pi' \circ \tilde{Y}_p$ n'a pas de composant de la forme $a \times \tilde{\Gamma}$, on voit que $\mathfrak{a} > 0$. D'autre part on a $d(\tilde{X}_p) = d'(\tilde{X}_p) = p+1$ en vertu de (8) et $d'(\Pi + \Pi' \circ \tilde{Y}_p) = p+1$; d'où résulte $\mathfrak{a} = 0$. Nous obtenons ainsi *la première formule de congruence pour la correspondance modulaire*

(I) $$\tilde{X}_p = \Pi + \Pi' \circ \tilde{Y}_p$$

pour presque tous les nombres premiers p.

12. Nous prenons maintenant pour L le corps L_N ou le corps $M_{N,\mathfrak{h}}$ définis dans **8.** Soient les notations A, B, φ_n comme dans **8.** D'après la prop. 7, φ_p donne un automorphisme de Frobenius $\left(\frac{\boldsymbol{Q}(\zeta_N)/\boldsymbol{Q}}{p}\right)$. Il s'ensuit de là que l'on a $\tilde{A}^{\varphi_p} = \tilde{A}^p$, $\tilde{B}^{\varphi_p} = \tilde{B}^p$. D'après la prop. 12 et la prop. 13, on a

(18) $$\tilde{A}^p \circ \tilde{Y}_p = \tilde{A} \quad \text{sur} \quad \tilde{\Gamma}_N,$$
$$\tilde{B}^p \circ \tilde{Y}_p = \tilde{B} \quad \text{sur} \quad \tilde{\Gamma}_{N,\mathfrak{h}}.$$

Comme A est une correspondance birationnelle, on a $A' \circ A = \Delta$ et par conséquent

(19) $$\tilde{A}' \circ \tilde{A} = \tilde{\Delta}.$$

D'autre part, on vérifie aisément

(20) $$\Pi \circ \mathfrak{X} = \mathfrak{X}^p \circ \Pi \quad \text{et} \quad \mathfrak{X} \circ \Pi' = \Pi' \circ \mathfrak{X}^p$$

pour toute correspondance $\mathfrak{X}$. Il s'ensuit alors des formules (18), (19), (20) que l'on a

$$\tilde{A}' \circ \Pi' \circ \tilde{A} = \tilde{A}' \circ \Pi' \circ \tilde{A}^p \circ \tilde{Y}_p = \tilde{A}' \circ \tilde{A} \circ \Pi' \circ \tilde{Y}_p = \Pi' \circ \tilde{Y}_p$$

sur $\tilde{\Gamma}_N$. Il en est de même pour $\tilde{B}, \tilde{\Gamma}_{N,\mathfrak{h}}$. On obtient ainsi *la deuxième formule de congruence*:

(II) $$\Pi' \circ \tilde{Y}_p = \tilde{A}' \circ \Pi' \circ \tilde{A} \quad \text{sur} \quad \tilde{\Gamma}_N,$$
$$\Pi' \circ \tilde{Y}_p = \tilde{B}' \circ \Pi' \circ \tilde{B} \quad \text{sur} \quad \tilde{\Gamma}_{N,\mathfrak{h}}$$

pour presque tous les nombres premiers p.

13. Nous allons récrire les formules (I), (II) en termes d'endomorphismes de la jacobienne.

Soient L, Γ comme dans **11,** J une jacobienne de Γ et φ une application canonique de Γ dans J. Comme Γ est défini par rapport à $\boldsymbol{Q}$, on peut supposer d'après [1] ou d'après [12] que J soit défini par rapport à $\boldsymbol{Q}$; de plus si Γ a un point rationnel par rapport à $\boldsymbol{Q}$, on peut aussi supposer que φ soit défini par rapport à $\boldsymbol{Q}$. Cela posé, nous désignerons par ξ_n et η_n les endomorphismes de J correspondant à X_n et à Y_n. Nous désignerons la jacobienne J de Γ par J_N ou $J_{N,\mathfrak{h}}$ selon que L est égal à L_N ou à $M_{N,\mathfrak{h}}$; nous désignerons aussi par α et β les endomorphismes de J_N et de $J_{N,\mathfrak{h}}$ correspondant à A et à B, respectivement. Nous démontrerons, dans **17,** que $\Gamma_N, \Gamma_{N,\mathfrak{h}}$ ont des points rationnels par rapport à $\boldsymbol{Q}$.

Pour presque tous les nombres premiers p, J n'a pas de défaut, $\tilde{J}$ est une jacobienne de $\tilde{\Gamma}$ et $\tilde{\varphi}$ est une application canonique dans $\tilde{\Gamma}$. D'après (I), (II), nous obtenons donc les relations suivantes pour presque tous les nombres premiers p:

$$\text{(I}'\text{)} \qquad \tilde{\xi}_p=\pi+\pi'\tilde{\eta}_p \qquad \text{sur } J,$$

$$\text{(II}'\text{)} \qquad \begin{aligned} \pi'\tilde{\eta}_p&=\tilde{\alpha}^{-1}\pi'\tilde{\alpha} && \text{sur } J_N,\\ \pi'\tilde{\eta}_p&=\tilde{\beta}^{-1}\pi'\tilde{\beta} && \text{sur } J_{N,\mathfrak{h}} \end{aligned}$$

où π désigne l'homomorphisme de p-ième puissance de J.

§ 4. Fonctions modulaires elliptiques.

14. Soient ω_1, ω_2 deux nombres complexes tels que $\Im(\omega_1/\omega_2)>0$ et D le réseau dans le plan complexe $\boldsymbol{C}$ engendré par $\{\omega_1, \omega_2\}$. Posons

$$g_2(D)=g_2(\omega_1, \omega_2)=60\sum{}'\omega^{-4},$$

$$g_3(D)=g_3(\omega_1, \omega_2)=140\sum{}'\omega^{-6},$$

$$\wp(z; D)=\wp(z; \omega_1, \omega_2)=z^{-2}+\sum{}'[(z-\omega)^{-2}-\omega^{-2}]$$

où $\sum'$ désigne la sommation étendue à tous les nombres $\omega\neq 0$ de D. La fonction $\wp$ et sa dérivée $\wp'$ satisfont à l'équation

$$\wp'^2=4\wp^3-g_2\wp-g_3.$$

$g_2(\omega_1, \omega_2)$ et $g_3(\omega_1, \omega_2)$ sont les formes modulaires d'espèce («Stufe») 1 respectivement de degré -4 et -6. Elles ont les expressions

$$\text{(21)} \qquad \begin{aligned} g_2(\omega_1, \omega_2)&=\left(\frac{\pi}{\omega_2}\right)^4\left(\frac{1}{12}+20\sum_{n=1}^{\infty}\frac{n^3q^n}{1-q^n}\right),\\ g_3(\omega_1, \omega_2)&=\left(\frac{\pi}{\omega_2}\right)^6\left(\frac{1}{216}-\frac{7}{3}\sum_{n=1}^{\infty}\frac{n^5q^n}{1-q^n}\right). \end{aligned}$$

où $q=e^{2\pi i\tau}$, $\tau=\omega_1/\omega_2$. Nous nous servirons des notations q, τ toujours en ce sens et posons aussi $q_N=e^{2\pi i\tau/N}$, $\zeta_N=e^{2\pi i/N}$.

La fonction $j(\tau)=g_2^3/(g_2^3-27g_3^2)$ est une fonction modulaire d'espèce 1; elle a l'expression

$$\text{(22)} \qquad j(\tau)=12^3(q^{-1}+744+\cdots)$$

dont les coefficients sont rationnels. Soient N un entier >1 et α, β deux entiers tels que $(\alpha, \beta)\not\equiv(0, 0)$ mod. N. La fonction

$$\wp\left(\frac{\alpha\omega_1+\beta\omega_2}{N}; \omega_1, \omega_2\right)$$

est une forme modulaire d'espèce N et de degré -2; elle a l'expression

$$(23)\qquad \wp\Big(\frac{\alpha\omega_1+\beta\omega_2}{N};\ \omega_1,\ \omega_2\Big)=\Big(\frac{2\pi}{\omega_2}\Big)^2\Big\{-\frac{1}{12}+2\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n}-\frac{\zeta_N{}^{\beta}q_N{}^{\alpha}}{(1-\zeta_N{}^{\beta}q_N{}^{\alpha})^2}$$

$$-\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n}(\zeta_N{}^{n\beta}q_N{}^{n\alpha}+\zeta_N{}^{-n\beta}q_N{}^{-n\alpha})\Big\},$$

$$(0\leqq\alpha<N,\ (\alpha,\beta)\not\equiv(0,0)\ \text{mod. } N).$$

Posons maintenant

$$\boldsymbol{f}_{\alpha\beta}(\tau)=\boldsymbol{f}(\alpha,\beta;\tau)=\frac{g_2(\omega_1,\omega_2)}{g_3(\omega_1,\omega_2)}\wp\Big(\frac{\alpha\omega_1+\beta\omega_2}{N};\ \omega_1,\ \omega_2\Big).$$

Les fonctions $\boldsymbol{f}_{\alpha\beta}(\tau)$ sont des fonctions modulaires d'espèce N. Pour qu'on ait $\boldsymbol{f}_{\alpha\beta}=\boldsymbol{f}_{\alpha'\beta'}$, il faut et il suffit que $(\alpha,\beta)\equiv\pm(\alpha',\beta')$ mod. N. Soient a,b,c,d quatre entiers rationnels tels que $ad-bc=1$; on vérifie alors facilement que

$$(24)\qquad \boldsymbol{f}\Big(\alpha,\beta;\frac{a\tau+b}{c\tau+d}\Big)=\boldsymbol{f}(\alpha',\beta';\tau)\ \text{pour}\ (\alpha'\ \beta')=(\alpha\ \beta)\begin{pmatrix}a & b\\ c & d\end{pmatrix}.$$

D'après (21), (23), on voit que tous les $\boldsymbol{f}_{\alpha\beta}(\tau)$ ont des développements en q_N à coefficients dans $\boldsymbol{Q}(\zeta_N)$ et qu'en particulier, $\boldsymbol{f}_{10}(\tau)$ a un développement en q_N à coefficients rationnels; si $N\geqq3$, $\boldsymbol{f}_{1\beta}(\tau)$ a un développement en q_N

$$(25)\qquad \boldsymbol{f}_{1\beta}(\tau)=r_\beta+s_\beta\zeta_N{}^{\beta}q_N+(\text{termes d'ordres plus hauts})$$

où r_β, s_β sont deux nombres rationnels et $s_\beta\neq0$.

15. Soit maintenant τ_0 un nombre complexe tel que $\boldsymbol{j}(\tau_0)$ soit transcendant sur $\boldsymbol{Q}$. Posons $j_0=\boldsymbol{j}(\tau_0)$ et $\gamma_0=27j_0/(j_0-1)$; soient E la courbe elliptique définie par l'equation $Y^2=4X^3-\gamma_0X-\gamma_0$ et h la fonction canonique sur E. Soient ω_{01}, ω_{02} deux nombres complexes tels que $\omega_{01}/\omega_{02}=\tau_0$ et D le réseau engendré par $\{\omega_{01},\omega_{02}\}$. Il existe alors un isomorphisme analytique $u(z)$ de $\boldsymbol{C}/D$ sur E. Nous allons démontrer que l'on a

$$(26)\qquad h(u(z))=\frac{g_2(\omega_{01},\omega_{02})}{g_3(\omega_{01},\omega_{02})}\wp(z;\omega_{01},\omega_{02})$$

pour tout $z\in\boldsymbol{C}$. Posons $\mu=[g_3(D)/g_2(D)]^{1/2}$; on a alors $g_2(\mu D)=g_3(\mu D)$. Puisqu'on a $j_0=\boldsymbol{j}(\tau_0)=g_2(\mu D)/[g_2(\mu D)-27g_2(\mu D)]$, on voit que $\gamma_0=g_2(\mu D)=g_3(\mu D)$. Par suite, pour tout nombre complexe z, $u'(z)=(\wp(\mu z;\mu D),\wp'(\mu z;\mu D))$ est un point sur E; de plus $z\to u'(z)$ donne un isomorphisme analytique de $\boldsymbol{C}/D$ sur E. On a $h(u'(z))=\wp(\mu z;\mu D)=\mu^{-2}\wp(z;D)=\frac{g_2(D)}{g_3(D)}\wp(z;D)$. Comme $\mathcal{A}(E)$ est isomorphe à $\boldsymbol{Z}$, on a $u(z)=\pm u'(z)$; ce qui montre (26). Posons $t_1=u(\omega_{01}/N)$, $t_2=u(\omega_{02}/N)$; $\{t_1,t_2\}$ est alors un système de générateurs pour $\mathfrak{g}(N,E)$. D'après (26), on vérifie aisément

$$(27)\qquad \begin{aligned} j(E)&=\boldsymbol{j}(\tau_0),\\ h(\alpha t_1+\beta t_2)&=\boldsymbol{f}_{\alpha\beta}(\tau_0);\end{aligned}$$

on a donc

$$K_N(E)=\boldsymbol{Q}(\boldsymbol{j}(\tau_0),\ \boldsymbol{f}_{\alpha\beta}(\tau_0)\,|\,0\leqq\alpha<N,\ 0\leqq\beta<N,\ (\alpha,\beta)\not\equiv(0,0)\ \text{mod. } N).$$

Soit $\mathfrak{g}_{(i)}$ le sous-groupe de E engendré par t_i pour $i=1,2$. Soient $D_{(1)}$, $D_{(2)}$ les réseaux respectivement engendrés par $\{\omega_{01}/N,\ \omega_{02}\}$ et $\{\omega_{01},\ \omega_{02}/N\}$. Alors l'application identique $z\to z$ sur le plan complexe $\boldsymbol{C}$ donne un homomorphisme de $\boldsymbol{C}/D$ sur $\boldsymbol{C}/D_{(i)}$ dont le noyau est $D/D_{(i)}$ pour $i=1,2$. On peut en déduire que

$$j(E/\mathfrak{g}_{(1)})=\boldsymbol{j}(\tau_0/N),\quad j(E/\mathfrak{g}_{(2)})=\boldsymbol{j}(N\tau_0). \tag{28}$$

16. Nous désignerons par $\mathfrak{M}_N$ le corps complet des fonctions modulaires elliptiques d'espèce N. $\mathfrak{M}_N$ est un corps de fonctions algébriques d'une variable sur $\boldsymbol{C}$. $\mathfrak{M}_N$ est galoisien sur $\mathfrak{M}_1=\boldsymbol{C}(\boldsymbol{j}(\tau))$; le groupe de Galois de $\mathfrak{M}_N/\mathfrak{M}_1$ est isomorphe au groupe S_N de telle façon que pour chaque $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in S_N{}^*$, l'application

$$\boldsymbol{f}(\tau)\to\boldsymbol{f}\left(\frac{a\tau+b}{c\tau+d}\right)$$

donne un automorphisme de $\mathfrak{M}_N/\mathfrak{M}_1$.

Nous désignerons par $\mathfrak{K}_N$ le corps $\boldsymbol{Q}(\boldsymbol{j}(\tau),\ \boldsymbol{f}_{\alpha\beta}(\tau))$ engendré sur $\boldsymbol{Q}$ par $\boldsymbol{j}(\tau)$ et tous les $\boldsymbol{f}_{\alpha\beta}(\tau)$ $(0\leqq\alpha\leqq N-1, 0\leqq\beta\leqq N-1,\ (\alpha,\beta)\not\equiv(0,0)\ \text{mod. } N)$. D'après la relation (24), a, b, c, d, ayant les mêmes significations que dans cette relation-là, pour qu'on ait $\boldsymbol{f}\left(\frac{a\tau+b}{c\tau+d}\right)=\boldsymbol{f}(\tau)$ pour tous les $\boldsymbol{f}\in\mathfrak{K}_N$, il faut et il suffit qu'on ait $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\equiv\pm I$ mod. N. Cela démontre que $\mathfrak{K}_N$ engendre $\mathfrak{M}_N$ sur $\boldsymbol{C}$, c'est-à-dire

$$\mathfrak{M}_N=\boldsymbol{C}(\boldsymbol{j}(\tau),\ \boldsymbol{f}_{\alpha\beta}(\tau)).$$

E étant la courbe elliptique avec l'invariant j transcendant sur $\boldsymbol{Q}$, définie dans **4**, nous allons démontrer que $K_N(E)$ est isomorphe au corps $\mathfrak{K}_N$. Soit k le corps de constantes du corps $\mathfrak{K}_N$; $\mathfrak{K}_N$ est alors un corps de fonctions algébrique d'une variable sur k. Comme $\mathfrak{K}_N$ est engendré par l'adjonction à $\boldsymbol{Q}$ de quantités en nombre fini, il en est de même pour k; on peut donc prendre un nombre complexe τ_0 tel que $\boldsymbol{j}(\tau_0)$ soit transcendant sur k. On voit que $(\boldsymbol{j}(\tau_0),\ \boldsymbol{f}_{\alpha\beta}(\tau_0))$ est une spécialisation de $(\boldsymbol{j}(\tau),\ \boldsymbol{f}_{\alpha\beta}(\tau))$ par rapport à $\boldsymbol{C}$, et donc naturellement par rapport à k. D'après la définition de k, $(\boldsymbol{j}(\tau),\boldsymbol{f}_{\alpha\beta}(\tau))$ est de dimension 1 sur k. Comme $\boldsymbol{j}(\tau_0)$ est transcendant sur k, $(\boldsymbol{j}(\tau_0),\boldsymbol{f}_{\alpha\beta}(\tau_0))$ est une spécialisation générique de $(\boldsymbol{j}(\tau),\ \boldsymbol{f}_{\alpha\beta}(\tau))$ par rapport à k et donc par rapport à $\boldsymbol{Q}$, de sorte que $\mathfrak{K}_N=\boldsymbol{Q}(\boldsymbol{j}(\tau),\ \boldsymbol{f}_{\alpha\beta}(\tau))$ est isomorphe à $\boldsymbol{Q}(\boldsymbol{j}(\tau_0),\ \boldsymbol{f}_{\alpha\beta}(\tau_0))$. Nous avons vu dans **15**, que l'on a $\boldsymbol{Q}(\boldsymbol{j}(\tau_0),\ \boldsymbol{f}_{\alpha\beta}(\tau_0))=K_N(E_0)$ pour une courbe elliptique E_0 définie par l'équation

$$Y^2=4X^3-\gamma_0X-\gamma_0$$

où $\gamma_0=27\boldsymbol{j}(\tau_0)/[\boldsymbol{j}(\tau_0)-1]$. $\mathfrak{R}_N$ est donc isomorphe à $K_N(E_0)$; de plus on voit que $(\boldsymbol{j}(\tau), \boldsymbol{f}_{\alpha\beta}(\tau))$ est de dimension 1 sur $\boldsymbol{Q}$. L'argument ci-dessus est valable pour E_0 si seulement $\boldsymbol{j}(\tau_0)$ est transcendant sur $\boldsymbol{Q}$. Par suite on peut exprimer les propositions sur $\mathfrak{R}_N$ en termes de courbe elliptique, au moyen de l'isomorphisme donné ainsi par une spécialisation $\tau\to\tau_0$ où τ_0 est un nombre complexe tel que $\boldsymbol{j}(\tau_0)$ soit transcendant sur $\boldsymbol{Q}$. Nous appellerons cette méthode *le principe de spécialisation.*

17. Nous allons maintenant démontrer les propositions 5—7. Pour cela nous démontrons d'abord le lemme suivant:

LEMME 4. *Soient k_0 un corps, k_1 une extension séparable de k_0, x une variable sur k_1 et M une extension de $k_0(x)$, de degré fini, telle que $M\subset k_1(x)$. Alors il existe une extension k de k_0, de degré fini, telle que $M=k(x)$.*

Soit $\bar{k}_0$ la clôture algébrique de k_0. Comme $[M: k_0(x)]$ est fini, il existe un ensemble fini $(y)=(y_1,\cdots,y_s)$ d'éléments de k_1 tel que $M\subset k_0(x, y)$. Comme x est une variable sur $\bar{k}_0(y)$ et comme $\bar{k}_0(y)$ est une extension régulière de $\bar{k}_0$, $\bar{k}_0(x, y)$ est une extension régulière de $\bar{k}_0(x)$; par suite $\bar{k}_0(x)$ est algébriquement fermé dans $\bar{k}_0(x, y)$; il en résulte que $\bar{k}_0(x)=\bar{k}_0M$; on a donc $M\subset\bar{k}_0(x)$. Il existe donc une extension k' de k_0, de degré fini, telle que $M\subset k'(x)$. Posons $k=M\cap k'$; on a alors $k(x)\subset M$ et $\bar{k}\cap M=\bar{k}\cap k'(x)\cap M=k'\cap M=k$. D'autre part, puisque k_1 est séparable sur k_0, on voit que M est une extension séparable de k; on en conclut que M est une extension régulière de k. On a donc

$$[k'(x): M]=[k'M: M]=[k' : k]=[k'(x): k(x)];$$

ce qui montre $M=k(x)$.

$K_N(E)$ est identifié avec $\mathfrak{R}_N$ par l'isomorphisme donné dans **16**; nous fixerons cette identification. On a alors

$$j_{(1)}=\boldsymbol{j}(\tau/N), \qquad j_{(2)}=\boldsymbol{j}(N\tau),$$
$$h(t_1)=\boldsymbol{f}_{10}(\tau), \qquad h(t_2)=\boldsymbol{f}_{01}(\tau)$$

en vertu de (27), (28). La formule (5) prend maintenant la forme

$$\boldsymbol{f}_{\alpha\beta}{}^{\sigma}=\boldsymbol{f}_{\alpha'\beta'}, \qquad (\alpha'\ \beta')=(\alpha\ \beta)\begin{pmatrix}a & b\\ c & d\end{pmatrix};$$

cette formule signifie que pour chaque automorphisme σ de $\mathfrak{R}_N$ sur $\boldsymbol{Q}(\boldsymbol{j}(\tau))$ il existe une telle matrice $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in G_N{}^*$. L'application $\sigma\to\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ est un isomorphisme dans $G_N=G_N{}^*/\{\pm I\}$. Soit G_N' l'image de cet isomorphisme. Il est bien connu que chaque élément de $S_N{}^*$ est représenté par une matrice $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ à coefficients entiers telle que $ad-bc=1$ (non seulement $ad-bc\equiv 1$

mod. N). L'application $\tau \to \frac{a\tau+b}{c\tau+d}$ donne un automorphisme de $\mathfrak{M}_N$ sur $\boldsymbol{Q}(\boldsymbol{j}(\tau))$; par suite on voit que $G_N' \supset S_N$ en vertu de (24). Puisque le groupe quotient G_N/S_N est isomorphe au groupe $(\boldsymbol{Z}/N\boldsymbol{Z})^\times$ d'éléments inversibles de $\boldsymbol{Z}/N\boldsymbol{Z}$, il existe un sous-groupe $\mathfrak{h}$ de $(\boldsymbol{Z}/N\boldsymbol{Z})^\times$ tel qu'on ait

$$G_N' = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, ad-bc \in \mathfrak{h} \right\} \Big/ \{\pm I\}.$$

Soit H' le sous-groupe

$$\left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & a \end{pmatrix} \middle| \, (a, N)=1 \right\} \Big/ \{\pm I\}$$

de G_N. On a alors

$$G_N' \cap H' = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & a \end{pmatrix} \middle| \, \pm a \in \mathfrak{h} \right\}, \tag{29}$$

$$(G_N' \cap H')S_N = G_N', \quad (G_N' \cap H') \cap S_N = \{e\}. \tag{30}$$

Soit $\mathfrak{L}$ le sous-corps de $\mathfrak{K}_N$ correspondant à S_N; alors on a $\boldsymbol{Q}(\boldsymbol{j}) \subset \mathfrak{L} \subset \boldsymbol{C}(\boldsymbol{j})$. Comme $\mathfrak{L}$ est une extension de $\boldsymbol{Q}(\boldsymbol{j})$ de degré fini, il existe, d'après le lemme 4, une extension k de $\boldsymbol{Q}$ de degré fini telle que $\mathfrak{L}=k(\boldsymbol{j})$. Tous les éléments de $\mathfrak{K}_N \cap \boldsymbol{C}$ sont fixés par S_N; on a donc $\mathfrak{K}_N \cap \boldsymbol{C} \subset k(\boldsymbol{j})$; d'où résulte $\mathfrak{K}_N \cap \boldsymbol{C} = k$. Dans **5,** nous avons montré, en supposant que $G_N = G_N'$, que $\boldsymbol{Q}(j, j_{(2)}, h(t_1))$ correspond à H'. Quand on ne suppose pas $G_N = G_N'$, on voit que $\boldsymbol{Q}(j, j_{(2)}, h(t_1))$ correspond à $H' \cap G_N'$. On a $\boldsymbol{Q}(j, j_2, h(t_1)) = \boldsymbol{Q}(\boldsymbol{j}(\tau), \boldsymbol{j}(N\tau), \boldsymbol{f}_{10}(\tau))$ en vertu de notre identification. D'après (30), on a

$$\boldsymbol{Q}(\boldsymbol{j}(\tau), \boldsymbol{j}(N\tau), \boldsymbol{f}_{10}(\tau)) \cap k(\boldsymbol{j}(\tau)) = \boldsymbol{Q}(\boldsymbol{j}),$$

$$\mathfrak{K}_N = k(\boldsymbol{j}(\tau), \boldsymbol{j}(N\tau), \boldsymbol{f}_{10}(\tau)).$$

On peut regarder $\mathfrak{K}_N$ comme un sous-corps du corps $\boldsymbol{Q}(\zeta_N)((q_N))$ des séries formelles en q_N à coefficients dans $\boldsymbol{Q}(\zeta_N)$. L'application $q_N \to 0$ donne un diviseur premier $\mathfrak{P}$ du corps $\mathfrak{K}_N$. D'après la formule (25), on a

$$\frac{f_{1\beta} - r_\beta}{f_{1\beta'} - r_{\beta'}} (\mathfrak{P}) = \frac{s_\beta}{s_{\beta'}} \zeta_N^{\beta-\beta'};$$

ce qui montre que le corps des restes modulo $\mathfrak{P}$ est $\boldsymbol{Q}(\zeta_N)$. $\mathfrak{P}$ induit un diviseur premier $\mathfrak{p}$ dans $\boldsymbol{Q}(\boldsymbol{j}(\tau), \boldsymbol{j}(N\tau), \boldsymbol{f}_{10}(\tau))$. Comme $\boldsymbol{j}(\tau)$, $\boldsymbol{j}(N\tau)$, $\boldsymbol{f}_{10}(\tau)$ ont des développements en q_N à coefficients rationnels, le corps des restes modulo $\mathfrak{p}$ est $\boldsymbol{Q}$. On a donc

$$[H' \cap G_N' : \{e\}] = [\mathfrak{K}_N : \boldsymbol{Q}(\boldsymbol{j}(\tau), \boldsymbol{j}(N\tau), \boldsymbol{f}_{10}(\tau))] \geqq [\boldsymbol{Q}(\zeta_N) : \boldsymbol{Q}] = [H' : \{e\}];$$

d'où résulte $H' \cap G_N' = H'$; par suite on a $G_N = H'S_N = G_N'$; ce qui démontre la prop. 5.

Puisqu'on a $\mathfrak{K}_N \cap \boldsymbol{C} = k$, on a $k \subset \boldsymbol{Q}(\zeta_N)$. D'autre part, on a

$$[k:\boldsymbol{Q}]\geqq[k(j, j_{(2)}, h(t_1)):\boldsymbol{Q}(j, j_{(2)}, h(t_1))]$$
$$=[\mathfrak{R}_N:\boldsymbol{Q}(\boldsymbol{j}(\tau), \boldsymbol{j}(N\tau), \boldsymbol{f}_{10}(\tau))]=[\boldsymbol{Q}(\zeta_N):\boldsymbol{Q}];$$

il s'ensuit de là que $k=\mathrm{Q}(\zeta_N)$; ce qui prouve la prop. 6. Dans le corps $\boldsymbol{Q}(\zeta_N)((q_N))$, l'application $\zeta_N\to\zeta_N^{\alpha}$, $q_N\to q_N$ donne un automorphisme de $\mathfrak{R}_N$ sur $\boldsymbol{Q}(\boldsymbol{j})$ pour chaque α premier avec N. D'après la formule (23), cet automorphisme coïncide avec l'automorphisme correspondant à $\begin{pmatrix}1 & 0\\ 0 & \alpha\end{pmatrix}$. Soit $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ un élément de $G_N{}^*$ tel que $ad-bc=\alpha$; alors, puisque chaque élément de S_N fixe tous les éléments de $\boldsymbol{Q}(\zeta_N)$, $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$, $\begin{pmatrix}1 & 0\\ 0 & \alpha\end{pmatrix}$ donnent le même automorphisme de $\boldsymbol{Q}(\zeta_N)$; ce qui démontre la prop. 7.

Nous avons vu que $\boldsymbol{Q}(j, j_{(2)}, h(t_1))$ a un diviseur premier $\mathfrak{p}$ tel que le corps des restes modulo $\mathfrak{p}$ est $\boldsymbol{Q}$. Cela démontre que Γ_N *a un point rationnel par rapport à* $\boldsymbol{Q}$ comme $L_N=\boldsymbol{Q}(j, j_{(1)}, h(t_2))$ est isomorphe à $\boldsymbol{Q}(j, j_{(2)}, h(t_1))$. Puisque $M_{N,\mathfrak{h}}$ est un sous-corps de L_N, on voit de même que $\Gamma_{N,\mathfrak{h}}$ a un point rationnel par rapport à $\boldsymbol{Q}$.

18. Nous disons que deux matrices $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$, $\begin{pmatrix}a' & b'\\ c' & d'\end{pmatrix}$ à coefficients entiers sont équivalentes s'il existe une matrice $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ à coefficients entiers telle que $\alpha\delta-\beta\gamma=1$ et $\begin{pmatrix}a' & b'\\ c' & d'\end{pmatrix}=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}$. Si p est un nombre premier, il y a $p+1$ classes d'équivalence des matrices $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ telles que $ad-bc=p$. Soient $\begin{pmatrix}a_\nu & b_\nu\\ c_\nu & d_\nu\end{pmatrix}$ $(1\leqq\nu\leqq p+1)$ les représentants de ces classes; de plus, en supposant que p ne divise pas N, on peut les choisir de telle façon que

$$\begin{pmatrix}a_\nu & b_\nu\\ c_\nu & d_\nu\end{pmatrix}\equiv\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\quad\text{mod. } N\qquad(1\leqq\nu\leqq p+1).$$

Cela posé, soient $\begin{pmatrix}a_\nu' & b_\nu'\\ c_\nu' & d_\nu'\end{pmatrix}$ pour $1\leqq\nu\leqq p+1$ les matrices telles que

$$\begin{pmatrix}a_\nu' & b_\nu'\\ c_\nu' & d_\nu'\end{pmatrix}\begin{pmatrix}a_\nu & b_\nu\\ c_\nu & d_\nu\end{pmatrix}=\begin{pmatrix}p & 0\\ 0 & p\end{pmatrix};$$

on a alors

$$\begin{pmatrix}a_\nu' & b_\nu'\\ c_\nu' & d_\nu'\end{pmatrix}\equiv\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}\quad\text{mod. } N. \tag{31}$$

Soient τ_0, E, D, $\{\omega_{01}, \omega_{02}\}$ et $u(z)$ comme dans **15**; posons

$$\begin{pmatrix}\omega_{\nu 1}\\ \omega_{\nu 2}\end{pmatrix}=p^{-1}\begin{pmatrix}a_\nu & b_\nu\\ c_\nu & d_\nu\end{pmatrix}\begin{pmatrix}\omega_{01}\\ \omega_{02}\end{pmatrix}\qquad(1\leqq\nu\leqq p+1); \tag{32}$$

on a alors

$$\begin{pmatrix}\omega_{01}\\ \omega_{02}\end{pmatrix}=\begin{pmatrix}a_\nu' & b_\nu'\\ c_\nu' & d_\nu'\end{pmatrix}\begin{pmatrix}\omega_{\nu 1}\\ \omega_{\nu 2}\end{pmatrix} \qquad (1\leqq\nu\leqq p+1). \tag{33}$$

Soit D_ν le réseau engendré par $\{\omega_{\nu 1}, \omega_{\nu 2}\}$ pour chaque ν; posons $\mathfrak{g}_\nu=u(D_\nu/D)$. $\mathfrak{g}_\nu$ est un sous-groupe de E d'ordre p; on a $\mathfrak{g}_\nu\neq\mathfrak{g}_\mu$ pour $\nu\neq\mu$. Définissons E_ν, λ_ν comme dans **6** pour ces E, $\mathfrak{g}_\nu$; et posons $u_\nu(z)=\lambda_\nu(u(z))$; alors $u_\nu(z)$ donne un isomorphisme analytique de $\boldsymbol{C}/D_\nu$ sur E_ν. Soit h_ν la fonction canonique sur E_ν. En appliquant la formule (26) à E_ν, on a

$$h_\nu(u_\nu(z))=\frac{g_2(\omega_{\nu 1}, \omega_{\nu 2})}{g_3(\omega_{\nu 1}, \omega_{\nu 2})}\wp(z; \omega_{\nu 1}, \omega_{\nu 2}).$$

Posons $t_1=u(\omega_{01}/N)$, $t_2=u(\omega_{02}/N)$; on a alors $\alpha t_1+\beta t_2=u\left(\frac{\alpha\omega_{01}+\beta\omega_{02}}{N}\right)$ et par suite

$$h_\nu(\lambda_\nu(\alpha t_1+\beta t_2))=\frac{g_2(\omega_{\nu 1}, \omega_{\nu 2})}{g_3(\omega_{\nu 1}, \omega_{\nu 2})}\wp\left(\frac{\alpha\omega_{01}+\beta\omega_{02}}{N}; \omega_{\nu 1}, \omega_{\nu 2}\right).$$

D'après les formules (31), (33), on a

$$\frac{\alpha\omega_{01}+\beta\omega_{02}}{N}\equiv\frac{p\alpha\omega_{\nu 1}+\beta\omega_{\nu 2}}{N} \qquad \text{mod. } D_\nu.$$

D'après (32) on a $\omega_{\nu 1}/\omega_{\nu 2}=\frac{a_\nu\tau_0+b_\nu}{c_\nu\tau_0+d_\nu}$. Nous obtenons donc

$$j(E_\nu)=\boldsymbol{j}\left(\frac{a_\nu\tau_0+b_\nu}{c_\nu\tau_0+d_\nu}\right),$$

$$h_\nu(\lambda_\nu(\alpha t_1+\beta t_2))=\boldsymbol{f}\left(p\alpha, \beta; \frac{a_\nu\tau_0+b_\nu}{c_\nu\tau_0+d_\nu}\right). \tag{34}$$

Soient τ_p' l'automorphisme de $\mathfrak{K}_N$ correspondant à $\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}$ et $\bar{\sigma}_\nu$ l'isomorphisme de $\mathfrak{K}_N$ défini par la relation

$$\boldsymbol{g}^{\bar{\sigma}_\nu}(\tau)=\boldsymbol{g}^{\tau_p'}\left(\frac{a_\nu\tau+b_\nu}{c_\nu\tau+d_\nu}\right)$$

pour $\boldsymbol{g}\in\mathfrak{K}_N$. On a alors

$$\boldsymbol{j}^{\bar{\sigma}_\nu}(\tau_0)=j(E_\nu), \quad \boldsymbol{f}_{\alpha\beta}^{\bar{\sigma}_\nu}(\tau_0)=h_\nu(\lambda_\nu(\alpha t_1+\beta t_2)).$$

Par le principe de spécialisation, on peut donc identifier $(K_N, \sigma_\nu, K_N^{\bar{\sigma}_\nu})$ défini dans **6** avec $(\mathfrak{K}_N, \bar{\sigma}_\nu, \mathfrak{K}_N^{\bar{\sigma}_\nu})$.

Soient $\mathfrak{L}$ un sous-corps de $\mathfrak{K}_N$ tel que $\mathfrak{L}\cap\boldsymbol{Q}(\zeta_N)=\boldsymbol{Q}$, $\mathfrak{L}\supset\boldsymbol{Q}(\boldsymbol{j}(\tau))$ et $\{\Gamma, u\}$ un modèle du sous-corps L de K_N correspondant à $\mathfrak{L}$. Si l'on prend $\boldsymbol{C}$ comme le domaine universel, on peut regarder $\boldsymbol{C}\cdot\mathfrak{L}$ comme le corps des fonctions sur Γ, en définissant $\boldsymbol{f}(u)=\boldsymbol{f}(\tau_0)$ pour $\boldsymbol{f}\in\mathfrak{L}$.

Soit $\mathfrak{L}_N$ le sous-corps de $\mathfrak{K}_N$ correspondant au sous-groupe H_N de G_N; on a alors

$$\mathfrak{L}_N=\boldsymbol{Q}(\boldsymbol{j}(\tau),\ \boldsymbol{j}(\tau/N),\ \boldsymbol{f}_{01}(\tau)),\qquad \mathfrak{M}_N=\boldsymbol{C}\mathfrak{L}_N;$$

$\mathfrak{L}_N$ peut être regardé comme le corps des fonctions sur Γ_N définies par rapport à $\boldsymbol{Q}$. Puisque τ_p' est contenu dans H_N, on a

$$\boldsymbol{g}^{\bar{\sigma}_\nu}(\tau)=\boldsymbol{g}\left(\frac{a_\nu\tau+b_\nu}{c_\nu\tau+d_\nu}\right)\qquad (1\leqq\nu\leqq p+1) \tag{35}$$

pour $\boldsymbol{g}\in\mathfrak{L}_N$; on a donc

$$\boldsymbol{g}^{\bar{\sigma}_{\nu'}}(\tau)=\boldsymbol{g}'\left(\frac{a_\nu\tau+b_\nu}{c_\nu\tau+d_\nu}\right)\frac{p}{(c_\nu\tau+d_\nu)^2}\qquad (1\leqq\nu\leqq p+1) \tag{36}$$

pour $\boldsymbol{g}\in\mathfrak{L}_N$, où $\boldsymbol{f}'(\tau)$ désigne la dérivée de $\boldsymbol{f}(\tau)$.

Soit maintenant $\boldsymbol{f}d\boldsymbol{g}$ une forme différentielle sur Γ_N, de première espèce, où $\boldsymbol{f}, \boldsymbol{g}$ sont deux éléments de $\mathfrak{M}_N$; $\boldsymbol{f}(\tau)\boldsymbol{g}'(\tau)$ est alors une forme parabolique de degré 2, d'espèce N. Et réciproquement, chacune de telles formes est obtenue de cette manière. Soit T_p l'opérateur de Hecke ([4]); on a alors

$$(\boldsymbol{f}\boldsymbol{g}'\,|\,T_p)(\tau)=\sum_{\nu=1}^{p+1}\boldsymbol{f}\left(\frac{a_\nu\tau+b_\nu}{c_\nu\tau+d_\nu}\right)\boldsymbol{g}'\left(\frac{a_\nu\tau+b_\nu}{c_\nu\tau+d_\nu}\right)\frac{p}{(c_\nu\tau+d_\nu)^2}. \tag{37}$$

Il s'ensuit des formules (35), (36), en vertu d'une proposition de [8], que $\boldsymbol{f}\boldsymbol{g}'\,|\,T_p$ correspond à la forme différentielle $\delta X_p(\boldsymbol{f}d\boldsymbol{g})$, si $\boldsymbol{f}, \boldsymbol{g}$ sont dans $\mathfrak{L}_N$, où δX_p désigne la différentielle de la correspondance X_p. En d'autres termes, si l'on désigne par M^d une représentation de $\mathcal{A}(J_N)$ par les formes différentielles de première espèce, $M^d(\xi_p)$ peut être regardé comme une représentation de T_p pour les formes paraboliques de degré 2, d'espèce N.

Soient $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ une matrice à coefficients entiers telle que

$$\alpha\delta-\beta\gamma=1,\ \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\equiv\begin{pmatrix}p^{-1} & 0\\ 0 & p\end{pmatrix}\quad \bmod N.$$

et ρ_p l'automorphisme de $\mathfrak{K}_N$ correspondant à $\begin{pmatrix}p & 0\\ 0 & p\end{pmatrix}$. Alors, comme on a

$$\begin{pmatrix}p & 0\\ 0 & p\end{pmatrix}\equiv\begin{pmatrix}p^2 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\quad \text{mod. } N,$$

on voit que

$$\boldsymbol{g}^{\rho_p}(\tau)=\boldsymbol{g}\left(\frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right)\ \text{ pour } \boldsymbol{g}\in\mathfrak{L}_N.$$

D'après la définition de Y_p, on peut donc regarder $M^d(\eta_p)$ comme une représentation de l'opérateur R_p dans [4].

§ 5. Résultats principaux.

19. Les notations étant celles de **13,** soient g le genre de Γ et M_l une représentation l-adique de $\mathcal{A}(J)$. Si $l \neq p$, on peut choisir une représentation l-adique $M_{l,p}$ de $\mathcal{A}(J(p))$ de telle façon que, pour chaque $\mu \in \mathcal{A}(J)$, on ait $M_l(\mu)=M_{l,p}(\mu(p))$. Nous désignerons $M_{l,p}$ aussi par M_l. On a alors d'après (I′)

$$M_l(\xi_p)=M_l(\pi)+M_l(\pi'\eta_p)\,.$$

Comme on a $\pi\pi'=p\delta_J$, U étant une indéterminée, on a

$$I_{2g}-M_l(\xi_p)U+M_l(\eta_p)pU^2=[I_{2g}-M_l(\pi)U][I_{2g}-M_l(\pi'\eta_p)U]$$

où I_m désigne la matrice unité de m lignes. Selon que J est égal à J_N ou à $J_{N,\mathfrak{h}}$, on a en vertu de (II′)

$$I_{2g}-M_l(\pi'\eta_p)U=M_l(\alpha)^{-1}[I_{2g}-M_l(\pi')U]M_l(\alpha)$$

ou

$$I_{2g}-M_l(\pi'\eta_p)U=M_l(\beta)^{-1}[I_{2g}-M_l(\pi')U]M_l(\beta)\,.$$

D'après la formule $M_l(\pi')=E_l(\Theta)^{-1}\,{}^tM_l(\pi)E_l(\Theta)$ dans [11] n°76, on a

$$\det[I_{2g}-M_l(\xi_p)U+M_l(\eta_p)pU^2]=\det[I_{2g}-M_l(\pi)U]^2$$

pour Γ_N ou $\Gamma_{N,\mathfrak{h}}$. Soit M^d une représentation de $\mathcal{A}(J)$ par les formes différentielles de première espèce; alors M_l est équivalent à $M^d \oplus \overline{M}^d$ où $\overline{M}^d$ désigne la représentation imaginaire conjuguée de M^d. Comme $J_N, J_{N,\mathfrak{h}}, \xi_p, \eta_p$ sont définis par rapport à $\boldsymbol{Q}$, on peut choisir la représentation M^d de telle façon que $M^d(\xi_p)=\overline{M}^d(\xi_p)$ et $M^d(\eta_p)=\overline{M}^d(\eta_p)$; on a donc

$$\det[I_{2g}-M_l(\xi_p)U+M_l(\eta_p)pU^2]=\det[I_g-M^d(\xi_p)U+M^d(\eta_p)pU^2]^2$$

et par suite

$$\det[I_{2g}-M_l(\pi)U]=\det[I_g-M^d(\xi_p)U+M^d(\eta_p)pU^2]\,.$$

Désignons par $\zeta(s, \Gamma, p)$ la fonction ζ de $\Gamma(p)$; alors on a

$$\zeta(s, \Gamma, p)=(1-p^{-s})^{-1}(1-p^{1-s})^{-1}\det[I_g-M^d(\xi_p)p^{-s}+M^d(\eta_p)p^{1-2s}]\,.$$

La fonction ζ de la courbe Γ est définie par

$$\zeta(s, \Gamma)=\prod_p \zeta(s, \Gamma, p)\,,$$

où le produit est étendu à tous les nombres premiers pour lesquels Γ n'a pas de défaut. Dans **18,** on a vu que $M^d(\xi_p)$, $M^d(\eta_p)$ ne sont autres que les représentations des opérateurs T_p, R_p pour les formes paraboliques de degré 2 (et d'espèce N).

Nous sommes ainsi parvenus à notre résultat principal:

La fonction ζ de la courbe Γ_N s'exprime sous la forme

$$\zeta(s, \Gamma_N)=f(s)\zeta(s)\zeta(s-1)\Phi(s)^{-1},$$
$$\Phi(s)=\prod_{t,\varepsilon} \det \Phi_{t,\varepsilon}(s)$$

où $\zeta(s)$ *est la fonction* ζ *de Riemann,* $f(s)$ *est une fonction rationnelle de* p^{-s} *et* $\Phi_{t,\varepsilon}(s)$ *désigne le produit d'Euler introduit par E. Hecke* [4], *attaché aux formes paraboliques de degré* 2, *de diviseur* t *et de caractère* $\varepsilon(n)$.

On obtient un résultat analogue aussi pour la fonction ζ de $\Gamma_{N,\mathfrak{h}}$; dans ce cas, il faut seulement limiter (t, ε) à certaines valeurs selon $\mathfrak{h}$ dans le produit pour $\Phi(s)$. Le cas où $\mathfrak{h}$ a l'index 1 ou 2 a été traité par M. Eichler [3].

20. Nous allons maintenant étudier les racines caractéristiques de T_p. Elles sont les racines de l'équation caractéristique de $M_l(\xi_p)=M_l(\tilde{\xi}_p)$ et par suite les racines caractéristiques d'une représentation régulière de $\tilde{\xi}_p$ dans l'algèbre $\mathcal{A}_0(\tilde{J}_N)$. Soit $\mathcal{B}$ l'algèbre sur $\boldsymbol{C}$ déduite de $\mathcal{A}_0(\tilde{J}_N)$ par extension à $\boldsymbol{C}$ du corps de base. Soit σ le prolongement dans $\mathcal{B}$ de la trace de $\mathcal{A}_0(\tilde{J}_N)$ (cf. [10] p. 58); $\sigma(\mu'\mu)$ est une forme d'Hermite positive non-dégénérée dans $\mathcal{B}$; posons $||\mu||=\sigma(\mu'\mu)^{1/2}$ pour $\mu\in\mathcal{B}$. D'après les relations $\pi\pi'=\pi'\pi=p\delta$ et $\tilde{\alpha}'=\tilde{\alpha}^{-1}$, on a

$$||\pi\mu||=\sqrt{p}\,||\mu||, \quad ||(\tilde{\alpha}^{-1}\pi'\tilde{\alpha})\mu||=\sqrt{p}\,||\mu||;$$

par suite, d'après (I'), (II') on a

$$||\tilde{\xi}_p\mu||\leqq||\pi\mu||+||(\tilde{\alpha}^{-1}\pi'\tilde{\alpha})\mu||=2\sqrt{p}\,||\mu||.$$

Il en résulte que les valeurs absolues des racines d'une représentation régulière de $\tilde{\xi}_p$ dans $\mathcal{A}_0(\tilde{J}_N)$ ne dépassent pas $2\sqrt{p}$. Nous obtenons ainsi le résultat suivant:

Les valeurs absolues des racines caractéristiques de l'opérateur T_p *de Hecke pour les formes paraboliques de degré* 2 *ne dépassent pas* $2\sqrt{p}$ *pour presque tous les nombres premiers* p.

Université de Tokyo.

Bibliographie

[1] W. L. Chow, The jacobian variety of an algebraic curve, Amer. J. Math., 76 (1954), pp. 453-476.

[2] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg, 14 (1941), pp. 197-272.

[3] M. Eichler, Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion, Arch. Math., 5 (1954), pp. 355-366.

[4] E. Hecke, Über die Modulfunktionen und die Dirichletschen Reihen mit Eulerschen Produktentwicklung I, II, Math. Ann., 114 (1937), pp. 1-28, 316-351.

[5] G. Shimura, Reduction of algebraic varieties with respect to a discrete valuation of the basic field, Amer. J. Math., 77 (1955), pp. 134-176.
[6] G. Shimura, On complex multiplications, Proc. International Symposium on algebraic number theory, Tokyo-Nikko, (1955), pp. 23-30.
[7] Taniyama, Jacobian varieties and number fields, ibid. pp. 31-45.
[8] G. Shimura et Y. Taniyama, Complex multiplication of abelian varieties and its applications to number theory, à paraître dans J. Math. Soc. Japan.
[9] A. Weil, Foundations of algebraic geometry, New York, (1946).
[10] A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, Paris, (1948).
[11] A. Weil, Variétés abéliennes et courbes algébriques, Paris, (1948).
[12] A. Weil, On algebraic groups and homogeneous spaces, Amer. J. Math., 77 (1955), pp. 493-512.