Racines cubiques de nombres entiers et multiplication complexe dans les fonctions elliptiques.

Par

D. MIRIMANOFF à Genève.

Introduction.

Parmi les équations résolubles algébriquement, les plus simples sont les équations abéliennes, à coefficients entiers, dites équations abéliennes absolues. Leurs racines sont des fonctions rationnelles des racines de l'unité. Ce théorème, qui exprime la propriété la plus importante des équations abéliennes absolues, est dû à Kronecker. Il permet de ramener l'étude des équations absolues à celle des équations de la division du cercle.

Bien plus difficile est l'étude des équations abéliennes relatives. Les plus simples parmi ces équations sont celles qui deviennent abéliennes par l'adjonction d'une racine carrée d'un nombre entier négatif. Kronecker a affirmé que les racines de ces équations s'expriment en fonction rationnelle des racines des équations de transformation que nous donne la multiplication complexe dans les fonctions elliptiques*).

D'après M. D. Hilbert, il serait possible de démontrer ce beau théorème de Kronecker, en se basant sur les recherches récentes de M. H. Weber et sur les propriétés très générales des équations abéliennes relatives établies par M. D. Hilbert**).

Les plus simples parmi ces équations abéliennes sont les équations de la forme $x^3 - n = 0$, n étant un entier quelconque. Elles deviennent abéliennes par l'adjonction de $\sqrt{-3}$.

Par conséquent les racines cubiques de nombres entiers s'exprimeraient aussi en fonction rationnelle des racines des équations de transformation.

Il ne serait peut être pas inutile d'indiquer un moyen de former ces expressions.

C'est ce que je me propose de faire dans le présent travail.

*) Sitzungsberichte, 1895, p. 115.

**) D. Hilbert, Jahresbericht der deutschen Mathem.-Vereinigung, 6, p. 94.

§ 1.

Invariants de classe.

Je poserai, avec M. H. Weber

$$j(\omega) = \frac{27 \cdot 64 g_2^3}{g_2^3 - 27 g_3^2} = 27 \cdot 64 J(\omega)$$

ω étant un nombre complexe dans la partie supérieure du plan, g_2 et g_3 les invariants de Weierstrass et $J(\omega)$ l'invariant absolu de M. F. Klein.

$j(\omega)$ appartient au groupe formé par toutes les substitutions linéaires

$$j\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = j(\omega), \quad \alpha\delta - \beta\gamma = 1.$$

Supposons maintenant que ω soit racine d'une équation quadratique

$$(1) \quad A\omega^2 + B\omega + C = 0$$

à discriminant négatif, A, B, C étant trois entiers premiers entre eux.

Les invariants correspondants $j(\omega)$ sont dits invariants singuliers ou invariants de classe*).

A chaque équation (1) correspond une forme quadratique primitive positive. Si B est pair, la forme correspondante $(A, \frac{B}{2}, C)$ est de première espèce (proprement primitive); si B est impair, la forme correspondante $(2A, B, 2C)$ est de 2^{me} espèce (improprement primitive). Soit $-m$ le discriminant de la forme. Dans le premier cas

$$-m = \frac{B^2 - 4AC}{4}$$

dans le second

$$-m = B^2 - 4AC.$$

L'invariant singulier $j(\omega)$ est racine d'une équation irréductible à coefficients entiers, dite équation des classes; son degré est égal au nombre des classes primitives de 1^{re} ou de 2^{me} espèce, suivant la parité de B . Cette équation n'est pas abélienne dans le domaine des nombres entiers; elle devient abélienne par l'adjonction de la racine carrée $\sqrt{-m}$.

Supposons que le nombre entier m soit de la forme $3k^2$. Dans ce cas les équations des classes deviennent abéliennes par l'adjonction de $\sqrt{-3}$. Leurs racines forment une catégorie spéciale d'invariants de classe.

D'autre part les équations de la forme

$$(2) \quad x^3 - n = 0$$

n étant un entier quelconque, deviennent abéliennes par l'adjonction de $\sqrt{-3}$.

* H. Weber, l. c. 87, Encyklopädie, ICh. J. de Séguier, Formes quadratiques et multiplication complexe, Berlin 1894, § 31.

Nous allons essayer d'exprimer les racines de (2) en fonction rationnelle des invariants de discriminant $-3k^2$.

On peut remplacer $j(\omega)$ par d'autres fonctions modulaires, pourvu que ces fonctions appartiennent au corps $K(j(\omega), \sqrt{-m})$. Tout nombre algébrique primitif du corps K sera dit invariant de classe.

Je montrerai d'abord que les racines cubiques $\sqrt[3]{2}$ et $\sqrt[3]{3}$ sont fonctions rationnelles (dans le domaine $(\sqrt{-3})$) des invariants de classe. Je passerai ensuite au cas général.

§ 2.

Racines cubiques $\sqrt[3]{2}$, $\sqrt[3]{3}$.

Posons

$$q = e^{\pi i \omega}.$$

Considérons la fonction modulaire

$$f(\omega) = q^{-\frac{1}{24}} \prod_{n=1}^{\infty} (1 + q^{2n-1})$$

$f(\omega)$ est liée à $j(\omega)$ par la relation

$$j(\omega) = \frac{(f(\omega)^{24} - 16)^3}{f(\omega)^{24}}$$

$j(\omega)$ est une fonction rationnelle de $f(\omega)^*$.

Faisons $\omega = \sqrt{-3}$. On sait que $f(\sqrt{-3}) = \sqrt[3]{2}$, par suite $j(\sqrt{-3})$ est un nombre entier et $f(\sqrt{-3})^3$ est une fonction rationnelle de $j(\sqrt{-3})$; $f(\sqrt{-3})^3$ est un invariant de classe.

De même $f(3\sqrt{-3})^3$ est un invariant de classe. En effet, $f(3\omega)^3$ est liée à $f(\omega)^3$ par une équation du 4^e degré donnée par Schläefli**).

Cette équation est

$$(3) \quad \left(\frac{u}{v}\right)^6 + \left(\frac{v}{u}\right)^6 - (uv)^3 + \frac{8}{(uv)^3} = 0$$

en posant $u = f(\omega)$, $v = f(3\omega)$.

Faisons $\omega = \sqrt{-3}$, $v^3 = 2x$; x est racine de

$$(3') \quad x^3 - 3x^2 - 3x - 1 = 0$$

x est un invariant de classe, puisque l'invariant $j(3\sqrt{-3})$ est racine d'une équation irréductible du 3^e degré, à coefficients entiers.

Or

$$\frac{1}{x} = \sqrt[3]{2} - 1.$$

*) H. Weber, l. c. § 21.

**) H. Weber, l. c. § 76 et § 97.

Par conséquent

$$(4) \quad \sqrt[3]{2} = 1 + \frac{2}{f(\sqrt{-27})^3}$$

$\sqrt[3]{2}$ est une fonction rationnelle des invariants de classe. Posons maintenant, dans (3), $u^3 = f(\sqrt{-27})^3 = 2x$, $v^3 = 2y$

$$y_1 = \frac{f(3\sqrt{-27})^3}{2}$$

est racine de l'équation

$$(5) \quad y^3 + (1-4x^3)y^2 + (1-4x^3)y + (1+2x-4x^3) = 0$$

y_1 est une fonction rationnelle de $j(3\sqrt{-27})$; c'est un invariant de classe, de même que les deux autres racines de (5).

Posons $2x + 1 = t$ il vient, eu égard à (3'),

$$1 - 4x^3 = -3t^2; \quad 1 + 2x - 4x^3 = -x^4 = -\frac{t^3}{3}.$$

Le discriminant D de l'équation (5) est égal à $-3 \cdot 4t^6(9x+4)^2$.

Soit y_2 cette des racines imaginaires de (5) qui est située dans la partie supérieure du plan, y_3 sa conjuguée. Considérons les fonctions cycliques

$$\psi_1^3 = (y_1 + ry_2 + r^2y_3)^3,$$

$$\psi_2^3 = (y_1 + r^2y_2 + ry_3)^3,$$

en posant

$$r = e^{\frac{2\pi i}{3}}.$$

Or u_1, u_2, u_3 étant 3 indéterminées, on a

$$(u_1 + ru_2 + r^2u_3)^3 = f_1^3 - \frac{9}{2}f_1f_2 + \frac{27}{2}f_3 + \frac{3}{2}\sqrt{-3}\sqrt{D}$$

f_1, f_2, f_3 étant les trois fonctions symétriques élémentaires des u_i et D le discriminant.

On tire de là

$$\psi_1^3 = 2 \cdot 9t^3(x^2 - x - 1)^3,$$

$$\psi_2^3 = 4 \cdot 3 \cdot 27(xt)^3$$

et enfin

$$(6) \quad \sqrt[3]{2} \cdot \sqrt[3]{3} = \frac{y_1 + r^2y_2 + ry_3}{3x(2x+1)}.$$

Comme $\sqrt[3]{2}$ est une fonction rationnelle de x , la racine cubique $\sqrt[3]{3}$ est une fonction rationnelle de x et des y , dans le domaine $K(\sqrt{-3})$.

$\sqrt[3]{3}$ est une fonction rationnelle des invariants de Classe.

§ 3.

Cas général.

Il suffit de montrer que les racines cubiques de nombres premiers p supérieurs à 3 s'expriment en fonction rationnelle des invariants de classe.

Considérons les formes quadratiques proprement primitives de discriminant $-3p^2$. Soit (A, B, C) l'une de ces formes, ω celle des racines de

$$A\omega^2 + 2B\omega + C = 0$$

qui est située dans la partie supérieure du plan.

L'invariant singulier $j(\omega)$ est racine d'une équation irréductible à coefficients entiers, de degré h , h étant le nombre des classes proprement primitives de discriminant $-3p^2$.

Le nombre h est égal à $p + 1$, si $\left(\frac{-3}{p}\right) = -1$ et à $p - 1$, si $\left(\frac{-3}{p}\right) = +1$.

Dans le premier cas p est de la forme $6k - 1$, dans le second de la forme $6k + 1$.

L'équation des classes $H_m(u) = 0$ peut être formée directement de la manière suivante.

On sait que les fonctions modulaires $u = j(\omega)$ et $v = j(p\omega)$ sont liées, quelque soit ω , par une équation de transformation

$$(7) \quad F_p(u, v) = 0.$$

Son degré est égal à $p + 1$, ses racines v sont les invariants $j(p\omega)$ et $j\left(\frac{c + \omega}{p}\right)$ ($c = 0, 1, \dots, p - 1$). Faisons maintenant $\omega = \sqrt{-3}$; $j(\sqrt{-3})$ est un nombre entier, $j(p\sqrt{-3})$ est un invariant proprement primitif de discriminant $-3p^2$.

Si donc p est de la forme $6k - 1$, $F_p(u, v) = 0$ est l'équation des classes qu'il s'agissait de trouver. Si p est de la forme $6k + 1$, l'équation (7) admet un facteur du second degré à coefficients entiers; on la divisera par ce facteur.

Mais les équations (7) ne sont pas faciles à former. Leurs coefficients sont très grands et croissent rapidement avec p .

Considérons la fonction modulaire $f(\omega)$.

Les fonctions $u = f(\omega)$ et $v = f(p\omega)$ sont liées par une équation de degré $p + 1$ donnée par Schlaefli. Les autres racines v de cette équation sont $f\left(\frac{48c + \omega}{p}\right)$ ($c = 0, 1, \dots, p - 1$). Soit $\omega = \sqrt{-3}$, $u = f(\sqrt{-3}) = \sqrt[3]{2}$, les coefficients de l'équation en v sont des fonctions rationnelles de $\sqrt[3]{2}$.

Mais posons $x = v\sqrt[3]{2}$, si p est de la forme $6k - 1$, et $x = \frac{v}{\sqrt[3]{2}}$, si p est de la forme $6k + 1$.

En vertu de la forme particulière des équations de Schlaefli, les coefficients de l'équation en x sont des nombres entiers.

Si p est de la forme $6k - 1$, le degré de l'équation en x est égal à h ; si p est de la forme $6k + 1$, ce degré est égal à $h + 2$, mais l'équation en x admet un facteur du second degré à coefficients entiers, on la divisera par ce facteur.

D'autre part $j\left(\frac{48c + \omega}{p}\right)$ est une fonction rationnelle de la racine correspondante x . Il en résulte que les racines de l'équation en x s'expriment en fonction rationnelle des racines correspondantes de l'équation des classes. Les racines x sont des invariants de classe. A chaque racine de l'équation $H_m(u) = 0$ correspond une racine déterminée de l'équation en x .

Prenons maintenant une forme quadratique $(2A, B, 2C)$ de 2^{me} espèce (improprement primitive) de discriminant $-3p^2$; B est impair,

$$B^2 - 4AC = -m = -3p^2.$$

L'argument correspondant ω' est racine de l'équation

$$A\omega'^2 + B\omega' + C = 0.$$

Si l'on pose, dans l'équation de transformation $F_2(u, v) = 0$, $u = j(\omega')$, les trois racines v sont représentées par $v = j(2\omega')$, $j\left(\frac{\omega'}{2}\right)$, $j\left(\frac{\omega' + 1}{2}\right)$. Or AC étant impair, les trois formes correspondantes sont des formes proprement primitives de discriminant $-m$. On voit que les racines j de l'équation des classes et par conséquent les x peuvent être groupées trois à trois; j'appellerai racines conjuguées les trois racines d'un même groupe.

Considérons en particulier la forme $(2, p, 2p^2)$; l'argument ω' est égal à pr , en posant $r = e^{\frac{2\pi i}{3}}$. Les trois arguments conjugués sont

$$\omega_1 = 2pr; \quad \omega_2 = \frac{pr}{2}; \quad \omega_3 = \frac{1 + pr}{2}.$$

Quelles sont les racines correspondantes v de l'équation de Schlaefli?

L'argument d'une racine v est l'un des nombres

$$p\sqrt{-3}, \quad \frac{48c + \sqrt{-3}}{p}.$$

Or ω_1 est équivalent à $p\sqrt{-3}$.

La substitution linéaire $\begin{vmatrix} 0 & 1 \\ -1 & \delta_2 \end{vmatrix}$, δ_2 étant un entier, transforme ω_2 en $\frac{\delta_2 p + 1 + \sqrt{-3}}{p}$.

La substitution $\begin{vmatrix} 0 & 1 \\ -1 & \delta_3 \end{vmatrix}$ transforme $\frac{p(r+1)}{2}$, qui est équivalent à ω_3 , en $\frac{\delta_3 p - 1 + \sqrt{-3}}{p}$.

Les racines v correspondant à $\omega_1, \omega_2, \omega_3$ sont donc $f(\Omega_1), f(\Omega_2), f(\Omega_3)$, en posant

$$\Omega_1 = p \sqrt{-3}; \quad \Omega_2 = \frac{\delta_2 p + 1 + \sqrt{-3}}{p}; \quad \Omega_3 = \frac{\delta_3 p - 1 + \sqrt{-3}}{p}$$

δ_2 et δ_3 étant deux nombres tels que $\delta_2 p + 1 \equiv \delta_3 p - 1 \equiv 0 \pmod{48}$.

§ 4.

Propriétés des racines conjuguées $f(\Omega_1), f(\Omega_2), f(\Omega_3)$.

En même temps que la fonction $f(\omega)$, M. H. Weber a introduit les fonctions

$$f_1(\omega) = q^{-\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^{2n-1}) \quad \text{et} \quad f_2(\omega) = \sqrt{2} q^{\frac{1}{12}} \prod_{n=1}^{\infty} (1 + q^{2n}).$$

La considération de ces fonctions*) va nous permettre de donner aux racines $f(\Omega_i)$ une forme particulièrement simple. Les trois fonctions de M. Weber sont liées par les relations

$$\begin{aligned} f(\omega + 1) &= e^{-\frac{\pi i}{24}} f_1(\omega), & f_1(\omega) &= f_2\left(-\frac{1}{\omega}\right), \\ f_1(\omega + 1) &= e^{-\frac{\pi i}{24}} f(\omega), & f_1(\omega) f_2\left(\frac{\omega}{2}\right) &= \sqrt{2}. \\ f_2(\omega + 1) &= e^{+\frac{\pi i}{12}} f_2(\omega), \end{aligned}$$

On en tire immédiatement

$$f(\Omega_1) = \sqrt{2} \frac{e^{-\frac{p\pi i}{24}}}{f_2(pr)}; \quad f(\Omega_2) = \sqrt{2} \frac{e^{-\frac{\delta_2 \pi i}{24}}}{f_1(pr)}; \quad f(\Omega_3) = \sqrt{2} \frac{e^{\frac{(p-\delta_3)\pi i}{24}}}{f(pr)}.$$

Posons

$$f(\Omega_1) = v_1; \quad f(\Omega_2) = v_2; \quad f(\Omega_3) = v_3.$$

Il vient

$$v_1^8 = 16 \frac{e^{-\frac{p\pi i}{8}}}{f_2^8(pr)}; \quad v_2^8 = 16 \frac{e^{\frac{p\pi i}{8}}}{f_1^8(pr)}; \quad v_3^8 = 16 \frac{1}{f^8(pr)}$$

puisque

$$\delta_2 \equiv -p \pmod{6} \quad \text{et} \quad \delta_3 \equiv p \pmod{6}.$$

*) Les fonctions $f_1(\omega)$, $f_2(\omega)$ et $f_3(\omega)$ s'expriment très-simplement au moyen des fonctions $\varphi(\omega)$, $\psi(\omega)$ et $\chi(\omega)$ introduites par Hermite.

Considérons le trinôme

$$\psi(\alpha) = \frac{1}{v_1^3} + \alpha \frac{1}{v_2^3} + \alpha^2 \frac{1}{v_3^3}$$

α étant une racine cubique imaginaire de l'unité.

En vertu de la relation $f^3 = f_1^3 + f_2^3$, ce trinôme s'annule pour
 $\alpha = e^{\frac{2p\pi i}{3}}$

Posons

$$\psi\left(e^{\frac{2p\pi i}{3}}\right) = \psi_1; \quad \psi\left(e^{-\frac{2p\pi i}{3}}\right) = \psi_2,$$

$\psi_1 = 0$, ψ_2 n'est pas nul.

D'autre part on a

$$\psi_1^3 = A - \frac{3}{2} \sqrt{-3D},$$

$$\psi_2^3 = A + \frac{3}{2} \sqrt{-3D}.$$

A étant une fonction symétrique entière des trois racines $\frac{1}{v_i^3}$, D leur discriminant.

Il en résulte que ψ_2^3 est une fonction symétrique des trois racines conjuguées, — c'est une fonction rationnelle de l'invariant correspondant $j(\omega') = j(pr)$ de 2^{me} espèce.

$$\psi_2^3 = R(j(\omega')) = 2A = 3\sqrt{-3D}$$

— $3D$ est le carré d'une fonction symétrique.

Posons

$$f^3(\omega') = \xi; \quad -f_1^3(\omega') = \eta; \quad -f_2^3(\omega') = \xi.$$

Soient

D_1 le discriminant de ξ, η, ξ ,

D_2 celui de $\xi, e^{\frac{2p\pi i}{3}}\eta, e^{-\frac{2p\pi i}{3}}\xi$,

D_3 celui de $\xi, e^{-\frac{2p\pi i}{3}}\eta, e^{\frac{2p\pi i}{3}}\xi$.

On a

$$D = \frac{1}{16^3} D_2,$$

$$D_1 = 4(j(\omega') - 3^3 \cdot 4^3),$$

puisque ξ, η, ξ sont racines de

$$u^3 - \gamma_2(\omega')u - 16 = 0,$$

la fonction modulaire $\gamma_2(\omega)$ étant définie par la relation

$$\gamma_2(\omega) = \frac{f(\omega)^{24} - 16}{f(\omega)^8} = \sqrt[3]{j(\omega)}.$$

Le discriminant des cubes ξ^3, η^3, ζ^3 est égal à $4j(\omega')^2(j(\omega') - 3^3 \cdot 4^3)$. Il en résulte que

$$D_2 \cdot D_3 = j^2(\omega').$$

Or D_2 appartient au corps $K(j(\omega'))$, par conséquent D_3 appartient au même corps.

D_2 et D_3 sont des nombres algébriques entiers appartenant au corps $K(j(\omega'))$. Par conséquent $(16\psi_2)^3$ est un nombre algébrique entier faisant partie du même corps $K(j(\omega'))$.

La norme de $(16\psi_2)^3$ étendue aux différentes racines $j(\omega')$ de 2^e espèce est un diviseur de celle de $j(\omega')$, si l'on fait abstraction du facteur 3.

§ 5.

Racines de l'équation en x .

Soient x_1, x_2, x_3 les racines de l'équation en x qui correspondent aux racines v_1, v_2, v_3 . Posons $e^{-\frac{2p\pi i}{3}} = \alpha$.

Le trinôme

$$\frac{1}{x_1^3} + \alpha \frac{1}{x_2^3} + \alpha^2 \frac{1}{x_3^3}$$

appartient au corps $K(j(\omega), \sqrt{-3})$. A chaque racine de 2^e espèce correspond un trinôme analogue.

Soit Π le produit de tous ces trinômes.

Π est un nombre algébrique entier divisé par une puissance entière de 2.

Π^3 est un nombre entier ordinaire divisé par une puissance de 2. C'est un diviseur de la norme de $j(\omega')$, si l'on fait abstraction des facteurs 2 et 3.

Soit maintenant π un diviseur premier de Π^3 , supérieur à 3.

Dans le corps $K(j(\omega), \sqrt{-3})$ le nombre entier π se décompose en un produit d'idéaux

$$\pi = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots$$

$\mathfrak{p}_1, \mathfrak{p}_2, \dots$ étant des idéaux premiers et $e_1, e_2, \dots$ des nombres entiers.

Si π^k est la puissance maximum de π divisant Π^3 , on aura

$$ke_i \equiv 0 \pmod{3}$$

quel que soit i .

Si donc les exposants e_i sont égaux à 1, k est divisible par 3; π^k est un cube.

Je partirai du *postulatum* suivant:

Aucun des exposants e_i ne peut être supérieur à 1, si π ne divise pas $2m^*$.

*) Comp. H. Weber, Ellipt. Funct., p. 453. D. Hilbert, Jahresbericht der d. Math. Ver., 6, p. 94. H. Weber, Mathem. Annalen, t. 48, 49, 50.

Dans le cas qui nous occupe $m = 3p^2$.

Par conséquent, seul le nombre p , parmi les nombres premiers supérieurs à 3, pourrait être divisible par le carré d'un idéal $\mathfrak{p}_i$.

Voyons combien la norme de $j(\omega')$ contient de facteurs égaux à p .

§ 6.

Divisibilité de la norme de $j(\omega')$ par p .

La norme de $j(\omega')$ est divisible par p . En effet, $u = j(\omega)$ et $v = j(p\omega)$ sont liés par une équation de la forme

$$(u^p - v)(u - v^p) - pP = 0.$$

P étant un polynome en u, v de degré p , à coefficients entiers*)

La fonction $u = j(\omega)$ s'annule pour $\omega = r$ et si l'on pose $v = p^{\frac{1}{p+1}} t$, t est un nombre algébrique entier. Du reste les racines $\gamma_2(\omega')$ étant aussi divisibles par $p^{\frac{1}{p+1}}$, les $j(\omega')$ sont divisibles par $p^{\frac{3}{p+1}}$. La norme de $j(\omega')$ est divisible par p . Voyons si elle est divisible par p^2 .

Posons

$$\eta(\omega) = q^{\frac{1}{12}} \prod_{n=1}^{\infty} (1 - q^{2n}).$$

M. Kiepert à montré**), que les fonctions modulaires

$$y = p \left(\frac{\eta(p\omega)}{\eta(\omega)} \right)^2; \quad y_h = (-1)^{\frac{p-1}{2}} \left(\frac{\eta\left(\frac{12h+\omega}{p}\right)}{\eta(\omega)} \right)^2 \quad (h=0, 1, \dots, p-1)$$

sont racines d'une équation de la forme

$$(8) \quad y^{p+1} + a_1 y^p + \dots + a_p y + p = 0$$

les coefficients $a_1, a_2, \dots, a_p$ étant des fonctions entières de $\gamma_2(\omega)$ et $\gamma_3(\omega)$, à coefficients entiers***), de la forme

$$P(j) \cdot \gamma_2^k \cdot \gamma_3^l$$

$P(j)$ étant un polynome en $j(\omega)$ à coefficients entiers, k et l deux nombres entiers.

Si $p \equiv -1 \pmod{6}$, le coefficient a_p est de la forme

$$P(j) \cdot \gamma_2 \quad (p \equiv 5 \pmod{12}) \quad \text{ou} \quad P(j) \cdot \gamma_2 \cdot \gamma_3 \quad (p \equiv 11 \pmod{12}).$$

*) H. Weber, Ellipt. Functionen, § 72.

**) Journal für die Mathem. t. 87, 88, 95. Mathem. Annalen, t. 26.

***) $\gamma_3(\omega)$ est la fonction $\frac{(f(\omega)^{24} + 8)(f_2(\omega)^8 - f_2(\omega)^8)}{f(\omega)^8} = \sqrt{j(\omega) - 27 \cdot 64}$.

Si $p \equiv 1 \pmod{6}$, a_p est de la forme

$$P(j) \quad (p \equiv 1 \pmod{12}) \quad \text{ou} \quad P(j) \gamma_3 \quad (p \equiv 7 \pmod{12}).$$

Premier cas; $p \equiv -1 \pmod{6}$.

Posons $\omega = pr$. Je dis que toutes les racines de l'équation (8) sont divisibles par $p^{\frac{1}{p(p+1)}}$. Si l'on remplace, en effet, ω par $\frac{12h+\omega}{p}$, y se change en $\frac{(-1)^{\frac{p-1}{2}} p}{y_h}$, et par conséquent y_h est racine d'une équation dont tous les coefficients sont divisibles par p , sauf celui de y_h^{p+1} qui est 1 et celui de y_h^p qui est égal à $(-1)^{\frac{p+1}{2}} \bar{a}_p$, $\bar{a}_p$ étant le transformé de a_p . Or $\bar{a}_p$ contient le facteur $\gamma_2\left(\frac{12h+\omega}{p}\right)$ qui pour $\omega = pr$ est divisible par $p^{\frac{1}{p(p+1)}}$. Si donc on pose $y_h = p^{\frac{1}{p(p+1)}} t$, t est un nombre algébrique entier. En remplaçant ω par $p\omega$, on démontre de même que y est divisible par $p^{\frac{1}{p(p+1)}}$. Il en résulte que pour $\omega = pr$ tous les coefficients a_i de l'équ. (8) sont divisibles par $p^{\frac{1}{p(p+1)}}$, et comme pour $\omega = r$ les fonctions $j(\omega)$ et $\gamma_2(\omega)$ sont nulles, tandis que $\gamma_3(\omega)$ est premier à p , les coefficients a_i sont tous divisibles par p , pour $\omega = r$.

Remplaçons maintenant ω par $\frac{\omega}{p}$, dans (8); la racine y se change en $\frac{(-1)^{\frac{p-1}{2}} p}{y_0}$. Faisons $\omega = pr$. Tous les coefficients $\bar{a}_i$ de l'équation transformée sont divisibles par p et si l'on pose $y_0 = p^{\frac{p}{p+1}} t$, on voit que t est un nombre algébrique entier. Par conséquent la racine y_0 est divisible par $p^{\frac{p}{p+1}}$.

D'autre part, en vertu de l'équ. (8) $a_p y_0 + p$ est divisible par y_0^2 . Par conséquent $a_p y_0$ est divisible par p , mais le quotient $\frac{a_p y_0}{p}$ est premier à p . Il en résulte que $\gamma_2(pr) \cdot p^{-\frac{1}{p+1}}$ et $j(pr) \cdot p^{-\frac{3}{p+1}}$ sont premiers à p .

Par conséquent la norme de $j(\omega')$ étendue aux racines de l'équation des classes de 2^e espèce n'est pas divisible par p^2 .

2^e cas. $p \equiv 1 \pmod{6}$.

Le coefficient a_p de l'équation (8) n'étant pas divisible par $\gamma_2(\omega)$, le procédé dont nous nous sommes servi ne s'applique plus, mais il est probable que le résultat que nous avons établi subsiste.

§ 7.

Racines cubiques de nombres premiers de la forme $6k - 1$.

Il résulte de l'analyse précédente que le produit Π^3 n'est pas divisible par p^2 , mais est-il divisible par p ?

Je vais montrer que v_i et v_j étant 2 racines quelconques de l'équation de Schlaefli, la différence $v_i - v_j$ est divisible par $p^{\frac{1}{p+1}}$. En effet, l'équation de Schlaefli peut être mise sous la forme

$$(u^p - v)(u - v^p) - pP = 0,$$

P étant un polynome en u et v^*)

Dans le cas qui nous occupe $u = \sqrt[p]{2}$.

Si maintenant on pose $v = u^p + p^{\frac{1}{p+1}}t$, il vient

$$p^{\frac{1}{p+1}}t(u^{p^2} - u + p^{\frac{p}{p+1}}t^p) - pP' = 0.$$

P' étant un polynome en t .

Or, si p est de la forme $6k - 1$, $u^{p^2} - u \equiv 0 \pmod{p}$; par conséquent t est un nombre algébrique entier et

$$v_i - v_j \equiv 0 \pmod{p^{\frac{1}{p+1}}}.$$

Le trinome $\frac{1}{x_1^3} + \alpha \frac{1}{x_2^3} + \alpha^2 \frac{1}{x_3^3}$ étant divisible par $p^{\frac{1}{p+1}}$, le produit Π^3 est divisible par p .

Par conséquent

$$\Pi^3 = 2^k 3^l n^3 p,$$

n étant un entier, k et l deux entiers positifs ou négatifs.

En extrayant la racine cubique, on aura $\sqrt[p]{p}$ en fonction rationnelle d'invariants de classe.

§ 8.

Exemples. Racines cubiques $\sqrt[3]{5}$ et $\sqrt[3]{7}$.

L'équation de Schlaefli, pour $p = 5$, est

$$v^6 - u^5 v^5 + 4uv + u^6 = 0.$$

Faisons $x = \sqrt[3]{2}v$, l'équation deviendra

$$x^6 - 4x^5 + 16x + 16 = 0.$$

*) H. Weber, Ellipt. Funct., § 77.

Elle se décompose, par l'adjonction de $\sqrt[3]{5}$, en 2 équations du 3-degré; il vient

$$x^3 - 2x^2 - 2x(1 \pm \sqrt[3]{5}) - 4 = 0.$$

A l'invariant de 2^e espèce $j(5r)$ correspondent les racines de l'équation*)

$$(9) \quad x^3 - 2x^2 - 2x(1 + \sqrt[3]{5}) - 4 = 0.$$

Or $j(5r)$ peut être calculé très simplement à l'aide d'un procédé qui a été indiqué par M. Weber**). On a

$$j(5r) = -2^{15} 3^3 \sqrt[3]{5} (2 + \sqrt[3]{5})^5 (4 + \sqrt[3]{5})^3.$$

La norme de $j(5r)$ est

$$-2^{30} \cdot 3^6 \cdot 5 \cdot 11^3.$$

D'autre part le discriminant D_2 est égal à

$$2^8 \cdot 3^3 \cdot 5 (2 + \sqrt[3]{5})^4 (4 + \sqrt[3]{5})^6.$$

C'est un diviseur de $j(5r)^2$; la racine carrée de D_2 est un nombre du domaine $K(5r)$.

Il est aisé d'en déduire la valeur du produit Π^3 et par conséquent $\sqrt[3]{5}$ en fonction des invariants de classe.

Mais on obtient une expression beaucoup plus simple en partant des fonctions cycliques

$$\psi^3 = (x_1 + \alpha x_2 + \alpha^2 x_3)^3$$

x_1, x_2, x_3 étant les racines de l'équation (9) et α une racine cubique imaginaire de l'unité.

Si x_1 est la racine réelle, x_2 la racine imaginaire située dans la partie supérieure du plan et x_3 sa conjuguée, on a

$$(x_1 + r x_2 + r^2 x_3)^3 = 16 \cdot 5,$$

$$(x_1 + r^2 x_2 + r x_3)^3 = 4(20 + 9\sqrt[3]{5}).$$

On en tire

$$2\sqrt[3]{2} \cdot \sqrt[3]{5} = x_1 + r x_2 + r^2 x_3,$$

en posant $r = e^{\frac{2\pi i}{3}}$.

$\sqrt[3]{7}$. Le même procédé donne $\sqrt[3]{7}$ en fonction des invariants de classe. Les fonctions modulaires $u = f(\omega)$ et $v = f(7\omega)$ sont liées par l'équation de Schlaefli

$$v^8 - u^7 v^7 + 7u^4 v^4 - 8uv + u^8 = 0.$$

Posons

$$u = \sqrt[3]{2}, \quad v = x\sqrt[3]{2}.$$

*) Comp. H. Weber, l. c. p. 502. Dans l'équation donnée par M. Weber, le second membre doit être remplacé par $2\sqrt[3]{5}x$.

**) l. c. § 107.

Le premier membre de l'équation en x est divisible par $x^2 + x + 1$; en divisant par ce facteur on a une équation du 6^e degré dont les racines sont les invariants de 1^e espèce et qui se décompose, par l'adjonction de $\sqrt{21}$, en deux équations du 3^e degré.

L'invariant

$$x_1 = \frac{f(7\sqrt{-3})}{\sqrt[3]{2}}$$

est racine de

$$x^3 - \frac{1}{2}(5 + \sqrt{21})x^2 + \frac{1}{2}(3 + \sqrt{21})x - 1 = 0.$$

Soit x_2 celle des racines imaginaires qui est situéé dans la partie supérieure du plan, x_3 sa conjuguée.

Il vient

$$(x_1 + rx_2 + r^2x_3)^3 = 28,$$

$$(x_1 + r^2x_2 + rx_3)^3 = 28 + 6\sqrt{21}.$$

On en tire

$$\sqrt[3]{4}\sqrt[3]{7} = x_1 + rx_2 + r^2x_3$$

x_1, x_2, x_3 sont les invariants du genre principal.

Genève, 1901.