ARKIV FÖR MATEMATIK Band 5 nr 10

Communiqué le 11 septembre 1963

Contributions à la théorie des corps et des polynomes cyclotomiques

Par TRYGVE NAGELL

§ 1. Les polynomes cyclotomiques

1. Propriétés fondamentales. Nous désignons par $F_n(x)$ le polynome cyclotomique d'index n, c'est-à-dire

$$F_n(x) = \prod_{\xi}(x - \xi), \tag{1}$$

le produit étant étendu à toutes les racines n-ièmes primitives de l'unite ξ. Les zéros de ce polynome sont les $\varphi(n)$ nombres

$$\xi = e^{\frac{1}{n}2\pi i a},$$

où a parcourt un système réduit de résidus modulo n; ainsi $(a, n) = 1$.

Rappelons les résultats suivants relatifs aux polynomes cyclotomiques : Les coefficients de $F_n(x)$ sont des nombres entiers rationnels. Le premier coefficient ainsi que le dernier sont égaux à 1 pourvu que $n > 1$. Le polynome est irréductible dans $\mathbf{K}(1)$. Pour $n > 1$ on a

$$x^{\varphi(n)} F_n(x^{-1}) = F_n(x). \tag{2}$$

On a de plus la formule

$$F_n(x) = \frac{\prod_0 \prod_2 \prod_4 \cdots}{\prod_1 \prod_3 \prod_5 \cdots}; \tag{3}$$

ici $\prod_0$ représente le polynome $x^n - 1$; $\prod_1$ représente le produit des polynomes $x^{\frac{n}{p}} - 1$, où p parcourt tous les diviseurs premiers de n; $\prod_2$ représente le produit des polynomes $x^{\frac{n}{pq}} - 1$, où p et q parcourent tous les diviseurs premiers choisis différents l'un de l'autre de toutes les manières possibles; de la même manière $\prod_3$ représente le produit des polynomes $x^{\frac{n}{pqr}} - 1$, où p, q et r sont des diviseurs premiers de n différents entre eux, et ainsi de suite.

On a encore les identités

$$F_{np}(x) = \frac{F_n(x^p)}{F_n(x)}, \tag{4}$$

pourvu que p soit un nombre premier qui ne divise pas n, et

$$F_{np}(x) = F_n(x^p), \tag{5}$$

si le nombre premier p divise n.

Pour la démonstration de ces résultats voir p. ex. Nagell [1], p. 158–164[1].

De la formule (3) on obtient pour $n > 1$:

$$F_n(1) = \begin{cases} p \text{ si } n = p^\alpha, \ p \text{ nombre premier,} \\ 1 \text{ dans les autres cas,} \end{cases} \tag{6}$$

et pour $n > 2$:

$$F_n(-1) = \begin{cases} p \text{ si } n = 2p^\alpha, \ p \text{ nombre premier,} \\ 1 \text{ dans les autres cas.} \end{cases} \tag{7}$$

A l'aide de la formule (3) on montre aisément que la somme des zéros de $F_n(n)$ est égale à $\mu(n)$, fonction de Möbius.

Nous désignerons par $F_n(x, y)$ le polynome

$$y^{\varphi(n)} F_n\left(\frac{x}{y}\right) = \prod_{\xi} (x - y\xi),$$

où ξ a la même signification que dans (1), Ce polynome est une forme homogène dans x et y. Pour $n > 1$ on a

$$F_n(x, y) = F_n(y, x).$$

De plus on a les identités analogues aux identités (4) et (5) :

$$F_{np}(x, y) = \frac{F_n(x^p, y^p)}{F_n(x, y)}, \tag{4'}$$

quand le nombre premier p ne divise pas n, et

$$F_{np}(x, y) = F_n(x^p, y^p) \tag{5'}$$

quand p divise n.

2. Les diviseurs premiers de $F_n(x)$. Il est bien connu que les diviseurs premiers du polynome cyclotomique sont caractérisés par les propositions suivantes :

I. Si q est un nombre premier qui ne divise pas n, la condition nécessaire et suffisante pour que la congruence

$$F_n(x) \equiv 0 \pmod{q} \tag{8}$$

soit résoluble est que $q \equiv 1 \pmod{n}$.

Si $q \equiv 1 \pmod{n}$ les solutions de la congruence (8) sont les nombres qui appartiennent à l'exposant n modulo q. Ainsi le nombre de solutions incongrues modulo q est égal à $\varphi(n)$.

[1] Les numéros figurant entre crochets renvoient à la bibliographie placée à la fin de ce mémoire.

Si x est une solution de la congruence (8) le nombre $F_n(x)$ est divisible par la même puissance de q qui divise x^n-1.

II. Soit q un diviseur premier de n et posons $n=q^\alpha n_1$ où n_1 n'est pas divisible par q. Alors la condition nécessaire et suffisante pour que la congruence

$$F_n(x)\equiv 0 \pmod{q} \tag{8'}$$

soit résoluble est que $q\equiv 1 \pmod{n_1}$.

Si $q\equiv 1 \pmod{n_1}$ les solutions de la congruence (8') sont les nombres qui appartiennent à l'exposant n_1 modulo q. Ainsi le nombre de solutions incongrues modulo q est égal à $\varphi(n_1)$. Dans ce cas q est nécessairement le plus grand nombre premier qui divise n.

Si x est une solution de la congruence (8') le nombre $F_n(x)$ est divisible par q et non par q^2 pourvu que $n>2$.

Pour la démonstration de ces propositions voir Nagell [1], p. 164–167. Dans la démonstration de la première proposition il faut observer une faute d'impression dans la 5^e ligne de la page 165 : Entre les mots *thus* et *a* il faut ajouter *n/μ is.*

On voit aisément comment les propositions I et II s'adaptent au polynome $F_n(x,y)$, quand x et y sont des nombres entiers premiers entre eux.

Nous allons établir le résultat suivant :

Lemme 1. *Soient x et y des nombres entiers premiers entre eux tels que $x>|y|\geqslant 1$. Alors on a, pour $n>2$,*

$$F_n(x,y)>2^{\frac{1}{2}\varphi(n)}. \tag{9}$$

Démonstration. D'après la définition de $F_n(x,y)$ on a, si $n\geqslant 3$,

$$(x-|y|)^{\varphi(n)}\leqslant F_n(x,y)\leqslant (x+|y|)^{\varphi(n)}.$$

Si $x-|y|\geqslant 2$ il en résulte

$$F_n(x,y)>2^{\varphi(n)}.$$

Ici, le signe d'égalité est exclu, $F_n(x,y)$ n'étant jamais divisible par 4.

Supposons ensuite que $x=|y|+1$ et que $n=mp^\alpha$, où m n'est pas divisible par le nombre premier p. Si $m=1$ et $p=2$ on a

$$F_n(x,y)=x^{\frac{1}{2}n}+y^{\frac{1}{2}n}\geqslant 2^{\frac{1}{2}n}+1>2^{\varphi(n)}.$$

Posons $s=p^{\alpha-1}$ et considérons le cas de $\alpha\geqslant 2$. Alors on a $s\geqslant p\geqslant 2$ et

$$F_n(x,y)=F_{mp}(x^s,y^s)\geqslant [x^s-(x-1)^s]^{\varphi(mp)}.$$

Ici on a évidemment, pour tous les $x\geqslant 2$,

$$x^s-(x-1)^s>2^{\frac{1}{2}s}.$$

En effet, on voit aisément que la fonction

$$\psi(x)=x^s-(x-1)^s-2^{\frac{1}{2}s},$$

où $s\geqslant 2$, est positive pour tous les $x\geqslant 2$. Donc

$$F_n(x, y) > 2^{\frac{1}{2}\varphi(n)}.$$

Considérons ensuite le cas de $\alpha = 1$. On peut évidemment supposer que n n'est divisible par aucun carré > 1. Alors on a

$$F_n(x, y) = \frac{F_m(x^p, y^p)}{F_m(x, y)} \geqslant \left[\frac{x^p - |y|^p}{x + |y|}\right]^{\varphi(m)} = \left[\frac{x^p - (x-1)^p}{2x-1}\right]^{\varphi(m)}.$$

Or, on vérifie sans difficulté que la fonction

$$\psi(x) = x^p - (x-1)^p - (2x-1)\,2^{\frac{1}{2}(p-1)}$$

est toujours positive pour $x \geqslant 2$ et $p \geqslant 5$. On en conclut

$$F_n(x, y) > 2^{\frac{1}{2}\varphi(n)}.$$

Il est évident qu'on peut supposer que p est le plus grand facteur premier de n. Ainsi il reste seulement les cas de $n = 3$ et $n = 6$. Vu que $F_3(x, y)$ et $F_6(x, y)$, pour $x \geqslant 2$, sont toujours $\geqslant 3$, le lemme se trouve démontré.

Si p désigne le plus grand facteur premier de n on aura comme corrollaire :

Les entiers x, y et n satisfaisant aux mêmes conditions que plus haut on a

$$F_n(x, y) > p,$$

exception faite des cas suivants

$$F_3(2, -1) = 3, \quad F_6(2, 1) = 3. \tag{10}$$

A propos du lemme 1 voir Nagell [2], p. 95 et Kanold [3], p. 284–287. Il résulte de ce lemme que toutes les solutions des équations $F_n(x, y) = 1$ et $= p$, $xy \neq 0$, p facteur premier de $n (> 2)$, sont données par les relations (6), (7) et (10).

En combinant le lemme 1 avec les propositions I et II nous concluons : *Si $|x| \geqslant 2$ et $n \geqslant 3$, $F_n(x)$ est divisible par, au moins, un nombre premier $\equiv 1$ (modulo n), exception faite des cas $F_3(-2) = 3$ et $F_6(2) = 3$.* Il en résulte :

Si n est un entier $\geqslant 3$, le plus petit nombre premier $\equiv 1$ (mod n) est $< 3^{\varphi(n)}$.

Un résultat plus précis a été obtenu par Kanold [3], p. 284–287; comparez aussi Schinzel [4], p. 555–562.

3. Lemme sur les nombres qui sont premiers à un nombre naturel donné. Nous avons besoin du résultat suivant :

Lemme 2. *Soient $a_1, a_2, \ldots, a_{\varphi(n)}$ un système réduit de résidus modulo n, et soient $b_1, b_2, \ldots, b_{\varphi(d)}$ un système réduit de résidus modulo d, où d est un diviseur quelconque de n. Alors il y a exactement $\varphi(n)/\varphi(d)$ nombres a qui sont congrus au même nombre b modulo d.*

Démonstration. Si b est donné il existe toujours un nombre a qui est congru à b modulo d. Cela est évident quand $(b, n) = 1$. Supposons maintenant que $(b, n) = (b, n/d) > 1$. Désignons par $p_1, p_2, \ldots, p_r$ les nombres premiers qui divisent chacun des deux nombres b et $n/d = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$. Cela étant, le nombre

$$c = b + \frac{n}{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}}$$

est premier à n. En effet c est premier et à n/d et à d.

Supposons maintenant que la congruence $x \equiv b \pmod{d}$ est satisfaite par les nombres $a_1, a_2, \dots, a_\nu$ et qu'elle n'est satisfaite par aucun autre des nombres a_i. Puis désignons par b_* un autre des nombres b_i. D'après ce que nous venons de montrer il existe (au moins) un nombre a tel que

$$a \equiv b^{\varphi(d)-1} b_* \pmod{d},$$

c'est-à-dire

$$ab \equiv b_* \pmod{d}.$$

On en conclut que tous les nombres (classes de résidus modulo n)

$$aa_1, aa_2, \dots, aa_\nu, \tag{11}$$

incongrus entre eux modulo n, satisfont à la congruence $x \equiv b_* \pmod{d}$. On montre aisément que les classes de résidus modulo n représentées par (11) sont les seules qui satisfont à cette congruence. En effet, soit a_k un nombre parmi les $a_i (1 \leqq i \leqq \varphi(n))$ tel que

$$a_k \equiv b_* \pmod{d}.$$

Alors il existe un nombre a_m tel que

$$aa_m \equiv a_k \pmod{n}.$$

On aura donc

$$aa_m \equiv b_* \equiv ab \pmod{d},$$

et par suite

$$a_m \equiv b \pmod{d}.$$

Cela entraîne que l'index m a une des valeurs $1, 2, \dots, \nu$. Il en résulte que le nombre des classes de résidus modulo n qui satisfont à la congruence $x \equiv b_i \pmod{d}$, pour une valeur fixe de b_i, est indépendant de i, c'est-à-dire : ce nombre a la valeur $\varphi(n)/\varphi(d)$, ce qu'il fallait démontrer.

Nous savons que la somme des zéros de $F_n(x)$ est égale à $\mu(n)$. On voit sans peine que ce résultat, à l'aide du lemme 2, peut être généralisé comme il suit :

$$\sum_a e^{\frac{2\pi i a m}{n}} = \frac{\varphi(n)}{\varphi\left(\frac{n}{f}\right)} \cdot \mu\left(\frac{n}{f}\right), \tag{12}$$

où la somme est étendue à tous les nombres naturels a, premiers à n et $< n$, et où m est un nombre entier, tel que $(m, n) = f$.

§ 2. Discriminant et base d'un corps cyclotomique

4. Le discriminant du polynome $F_n(x)$. Si $D_m (m > 2)$ désigne le discriminant de $F_m(x)$ nous avons

$$D_m = (-1)^h \cdot \prod_{\varepsilon} F'_m(\varepsilon), \tag{13}$$

où ε parcourt toutes les racines primitives m-ièmes de l'unité et où $h = \frac{1}{2}\varphi(m)\,[\varphi(m) - 1]$. Conformément à (13) nous écrivons $D_1 = 1$ et $D_2 = 1$.

Il résulte de (4) qu'on a, pour $\alpha \geqslant 1$,

$$F_{np^\alpha}(x) = \frac{F_n(x^{p^\alpha})}{F_n(x^{p^{\alpha-1}})}, \tag{14}$$

lorsque n n'est pas divisible par le nombre premier p. En différentiant cette équation par rapport à x nous aurons

$$F'_{npg}(x) = \frac{pgx^{pg-1} \cdot F'_n(x^{pg}) \cdot F_n(x^g) - gx^{g-1} \cdot F'_n(x^g) \cdot F_n(x^{pg})}{[F_n(x^g)]^2}$$

où nous avons posé, pour simplifier, $g = p^{\alpha-1}$. Donc, pour $m = np^\alpha = npg$, l'équation (13) devient

$$D_{npg} = (-1)^h \prod_{\varepsilon} \left[pg\varepsilon^{pg-1} \cdot \frac{F'_n(\varepsilon^{pg})}{F_n(\varepsilon^g)} \right] = (-1)^h (pg)^{\varphi(m)} \prod_{\varepsilon} \left[\frac{F'_n(\varepsilon^{pg})}{F_n(\varepsilon^g)} \right]$$

En employant le lemme 2 du numéro précédent nous aurons la formule

$$D_{npg} = (-1)^h (pg)^{\varphi(m)} \cdot \frac{[\prod_{\varrho} F'_n(\varrho)]^{\varphi(pg)}}{[\prod_{\omega} F_n(\omega)]^g}, \tag{15}$$

où ϱ parcourt les racines primitives n-ièmes de l'unité, tandis que ω parcourt les racines primitives (np)-ièmes de l'unité. En vertu de la formule (3) de $F_n(x)$ nous aurons, si $np > 2$,

$$\prod_{\omega} F_n(\omega) = \prod_{\omega} \left[\frac{(1-\omega^n)\prod(1-\omega^{\frac{n}{qr}})\ldots}{\prod(1-\omega^{\frac{n}{q}})\prod(1-\omega^{\frac{n}{qrs}})\ldots} \right]. \tag{16}$$

Profitant encore une fois du lemme 2 nous obtenons

$$\prod_{\omega} \left(1 - \omega^{\frac{n}{d}}\right) = [F_{dp}(1)]^{\frac{\varphi(n)}{\varphi(d)}},$$

d étant un diviseur quelconque positif de n.

D'après la formule (6) le nombre $F_n(1)$ est égal à p si n est une puissance du nombre premier p et égal à 1 dans le cas contraire. En vertu de ce fait l'équation (16) deviendra (pour $np > 2$)

$$\prod_{\omega} F_n(\omega) = p^{\varphi(n)}.$$

En introduisant ce résultat dans (15) nous aurons la formule

$$D_{np^\alpha} = (-1)^h \cdot p^{\varphi(np^\alpha)\left[\alpha - \frac{1}{p-1}\right]} \cdot [\prod_{\varrho} F'_n(\varrho)]^{\varphi(p^\alpha)}, \tag{17}$$

formule qui est encore valable pour $n=1$, $p=2$ si $np^\alpha>2$, c'est-à-dire si $\alpha\geqslant 2$; car dans ce cas nous aurons

$$\prod_\omega F_n(\omega)=-2 \quad \text{et} \quad [\prod_\omega F_n(\omega)]^{p^{\alpha-1}}=(-2)^{2^{\alpha-1}}=2^{2^{\alpha-1}}.$$

Il résulte de l'équation (17) que le signe de D_{np^α} est égal à $(-1)^h$ si $np^\alpha>2$. Alors celle-ci peut s'écrire

$$|D_{np^\alpha}|=p^{\varphi(np^\alpha)\cdot\left[\alpha-\frac{1}{p-1}\right]}\cdot|D_n|^{\varphi(p^\alpha)},$$

valable pour $n\geqslant 1$. Au moyen de cette formule on trouvera facilement par induction l'expression connue ($n>2$):

$$D_n=(-1)^{\frac{1}{2}\varphi(n)}\prod_p p^{p^{\varphi(n)\left[\alpha-\frac{1}{p-1}\right]}}, \tag{18}$$

où le produit est étendu à tous les facteurs premiers différents p de n, et où α désigne l'exposant de la puissance la plus haute de p qui divise n.

J'ai publié cette démonstration de la formule (18) dans une note antérieure; voir Nagell [6], p. 5–7. Dans le numéro suivant ce résultat nous servira à déterminer une base des entiers d'un corps cyclotomique.

5. Base des entiers d'un corps cyclotomique. Le corps algébrique de degré $\varphi(n)$ engendré par l'équation $F_n(x)=0$ sera appelé *corps cyclotomique d'index n*. Il y a plusieurs méthodes pour déterminer une base des entiers de ce corps. La méthode de Hasse exposée dans son livre [7] est basée sur une théorie générale et très embrassante des corps algébriques. Dans son cours d'algèbre [8] Fricke se sert d'un théorème sur la relation entre le discriminant d'un corps algébrique $\boldsymbol{K}$ et le discriminant d'un sous-corps de $\boldsymbol{K}$. Nous allons montrer comment on peut déterminer une base par une méthode plus simple que les méthodes mentionnées.

Nous commençons par le

Lemme 3. *Soit p un nombre premier et posons $s=p^\nu$, $\alpha\geqslant 1$, et $m=\varphi(s)$. Si $\varepsilon=e^{\frac{2\pi i}{s}}$ les nombres $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{m-1}$ constituent une base du corps $\boldsymbol{K}(\varepsilon)$.*

Démonstration. D'après la formule (18) du numéro précédent le discriminant $D(\varepsilon)$ de ε n'est divisible par aucun autre nombre premier que p. Par conséquent il suffit de montrer que le nombre

$$\xi=\frac{1}{p}(a_0+a_1\varepsilon+a_2\varepsilon^2+\ldots+a_{m-1}\varepsilon^{m-1}),$$

où les coefficients $a_0, a_1, \ldots, a_{m-1}$ sont des entiers rationnels, est un nombre entier dans $\boldsymbol{K}(\varepsilon)$ seulement si tous les nombres a_i ($i=0, 1, \ldots, m-1$) sont divisibles par p.

Si nous posons $1-\varepsilon=\theta$, l'idéal (θ) est un idéal premier dans $\boldsymbol{K}(\varepsilon)$; et nous avons évidemment la relation $(p)=(\theta)^m$. Vu que $D(\theta)=D(\varepsilon)$ il suffit de montrer que le nombre

$$\xi=\frac{1}{p}(b_0+b_1\theta+b_2\theta^2+\ldots+b_{m-1}\theta^{m-1}), \tag{19}$$

où les coefficients $b_0, b_1, \ldots, b_{m-1}$ sont des entiers rationnels, est un entier dans $\boldsymbol{K}(\varepsilon)$

seulement si tous les nombres $b_i (i = 0, 1, \ldots, m-1)$ sont divisibles par p. Si ξ est un nombre entier on obtient, en multipliant (19) par θ^m, la congruence

$$0 \equiv \xi\theta^m \equiv b_0\eta \pmod{\theta}.$$

où η est une unité dans $\mathbf{K}(\varepsilon)$. Ainsi b_0 est divisible par θ et par conséquent divisible par p. Multiplions ensuite (19) par θ^{m-1}. Il en résulte la congruence

$$0 \equiv (\xi - \frac{1}{p} b_0)\theta^{m-1} \equiv b_1\eta_1 \pmod{\theta},$$

où η_1 est une unité dans $\mathbf{K}(\varepsilon)$. D'une façon analogue on en conclut que b_1 est divisible par p. Il est évident que, en continuant de cette manière, on montrera successivement que tous les nombres b_i sont divisibles par p. Le lemme 3 se trouve ainsi démontré. Notre méthode ne se distingue pas beaucoup de celle utilisée par Fricke, voir [8], p. 190–195. Passons à la démonstration du théorème analogue sur la base dans le cas général.

Théorème. *Soit ζ une racine primitive N-ième de l'unité. Alors les nombres* $1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(N)-1}$ *constituent une base du corps* $\mathbf{K}(\zeta)$.

Démonstration. Le théorème est vrai quand l'index N est la puissance d'un nombre premier. Supposons maintenant qu'il est vrai pour l'index $n (> 1)$. Alors il suffit de montrer que le théorème est vrai pour l'index $N = np^r$, où p est un nombre premier quelconque qui ne divise pas n. Posons pour abrégér

$$s = p^r,\ m = \varphi(s),\ \mathbf{K}(\zeta) = \mathbf{K}_N \quad \text{et} \quad \mathbf{K}(e^{\frac{2\pi i}{n}}) = \mathbf{K}_n.$$

Les nombres ε et θ ont la même signification que plus haut.

Il est évident que tout nombre entier ξ dans $\mathbf{K}_N$ peut s'écrire

$$\xi = \gamma_0 + \gamma_1\theta + \gamma_2\theta^2 + \ldots + \gamma_{m-1}\theta^{m-1}, \tag{20}$$

où $\gamma_0, \gamma_1, \ldots, \gamma_{m-1}$ sont des nombres appartenant à $\mathbf{K}_n$. En effet, le degré de $\mathbf{K}_N$ relativement à $\mathbf{K}_n$ est égal à $\frac{\varphi(N)}{\varphi(n)} = \varphi(s) = m$. De la manière usuelle on déduit de (20) que le nombre $D(\theta)\gamma_k$, pour $k = 0, 1, \ldots, m-1$, est un nombre algébrique *entier*. En vertu du lemme 3 le discriminant $D(\theta)$ est une puissance de p. Ainsi ξ sera de la forme

$$\xi = \frac{1}{p^b}(\alpha_0 + \alpha_1\theta + \alpha_2\theta^2 + \ldots + \alpha_{m-1}\theta^{m-1}), \tag{21}$$

où b est un nombre naturel, et où les coefficients $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$ sont des nombres *entiers* $\mathbf{K}_n$. Nous allons montrer que tous les nombres $\alpha_i (i = 0, 1, \ldots, m-1)$ sont divisibles par p^b. En multipliant (21) par p^b nous aurons la congruence

$$0 \equiv \xi p^b \equiv \alpha_0 \pmod{\theta}.$$

Ainsi α_0 est divisible par θ. Comme α_0^m est divisible par θ^m nous aurons

$$\alpha_0^m \equiv 0 \pmod{p}.$$

Il en résulte que α_0 est divisible par chacun des idéaux premiers qui divisent (p) dans $\mathbf{K}_n$. Vu que le discriminant de $\mathbf{K}_n$ n'est pas divisible par p, il n'y a aucun idéal premier dans $\mathbf{K}_n$ dont le carré divise p. Par conséquent, α_0 est divisible par p.

Supposons maintenant que les nombres $\alpha_0, \alpha_1, \ldots, \alpha_{k-1}$ sont $\equiv 0 \pmod{p}$, tandis que $\alpha_k \not\equiv 0 \pmod{p}$, $0 < k \leqslant m-1$. Alors on obtient de (21)

$$0 \equiv \theta^{m-k}\left[\xi p^{b-1} - \frac{1}{p}(\alpha_0 + \alpha_1\theta + \alpha_2\theta^2 + \ldots + \alpha_{k-1}\theta^{k-1})\right] \equiv \alpha_k \pmod{\theta}.$$

Comme tout à l'heure pour α_0 on en conclut que α_k est nécessairement divisible par p, contrairement à l'hypothèse. Par conséquent, tous les nombres $\alpha_i (0 \leqslant i \leqslant m-1)$ sont divisibles par p. Pour $\alpha_i = p\alpha_i'$ l'équation (21) peut s'écrire

$$\xi = \frac{1}{p^{b-1}}(\alpha_0' + \alpha_1'\theta + \ldots + \alpha_{m-1}'\theta^{m-1}). \tag{21'}$$

Si $b > 1$ on peut continuer de la même manière que ci-dessus et montrer que tous les nombres α_i' sont divisibles par p. On arrivera finalement à la conclusion: Tous les entiers dans $\mathbf{K}_N$ sont de la forme

$$\alpha_0 + \alpha_1\theta + \ldots + \alpha_{m-1}\theta^{m-1},$$

où $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$ sont des entiers dans $\mathbf{K}_n$. Ici on peut remplacer θ par $\varepsilon = 1 - \theta$. Nous avons supposé que le théorème est vrai pour $\mathbf{K}_n$. Ainsi, dans ce corps une base est constitutée par les nombres $1, \eta, \eta^2, \ldots, \eta^{\varphi(n)-1}$, où η est une racine primitive n-ième de l'unité. Il en résulte qu'une base de $\mathbf{K}_N$ est donnée par les nombres

$$\eta^h\varepsilon^k (h = 0, 1, \ldots, \varphi(n)-1; \quad k = 0, 1, \ldots, \varphi(s)-1).$$

On voit aisément que ces nombres coincident avec les nombres $1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(N)-1}$. Le théorème se trouve ainsi démontré.

§ 3. Sous-corps quadratiques d'un corps cyclotomique

6. Sommes de Gauss. Nous avons besoin des résultats suivants dus à Gauss.

Lemme 4. *Soit P un nombre naturel impair > 1 qui n'est divisible par aucun carré > 1. Si $\varepsilon = e^{\frac{2\pi i}{P}}$ on a les deux formules*

$$\sum_a \varepsilon^{am} = \frac{1}{2}\left[\mu(P) + \left(\frac{m}{P}\right) i^{\frac{1}{2}(P-1)^2}\sqrt{P}\right],$$

$$\sum_b \varepsilon^{bm} = \frac{1}{2}\left[\mu(P) - \left(\frac{m}{P}\right) i^{\frac{1}{2}(P-1)^2}\sqrt{P}\right],$$

où la première somme est étendue à tous les nombres naturels $a < P$ pour lesquels le symbole de Jacobi $\left(\frac{a}{P}\right)$ a la valeur $+1$, tandis que la seconde somme est étendue à tous

les nombres naturels $b < P$ pour lesquels le symbole $\left(\frac{b}{P}\right)$ a la valeur -1. m est un nombre entier, premier à P. $\sqrt{P}$ signifie la valeur positive.

Si $(m, P) = f > 1$ on a

$$\sum_a \varepsilon^{am} = \sum_b \varepsilon^{bm} = \tfrac{1}{2} \cdot \frac{\varphi(P)}{\varphi\left(\frac{P}{f}\right)} \cdot \mu\left(\frac{P}{f}\right),$$

où la sommation est la même que ci-dessus.

Voir *p.* ex. Gauss [9], p. 443, ou Dirichlet [10], p. 365. Comparez aussi la formule (12) dans le numéro 4.

Lemme 5. *Soit n un nombre naturel et posons $\varepsilon = e^{\frac{2\pi i}{n}}$. Alors on a*

$$\sum_{s=0}^{n-1} \varepsilon^{s^2} = \begin{cases} (1+i)\sqrt{n} & \text{si} \quad n \equiv 0 \pmod 4, \\ \sqrt{n} & \text{si} \quad n \equiv 1 \pmod 4, \\ 0 & \text{si} \quad n \equiv 2 \pmod 4, \\ i\sqrt{n} & \text{si} \quad n \equiv 3 \pmod 4. \end{cases}$$

Ici $\sqrt{n}$ signifie la valeur positive.

Pour la démonstration voir Gauss [9], p. 430, ou Dirichlet [10], p. 293–296.

7. Sur la réductibilité d'un polynome dans un corps quadratique. Soit donné le polynome

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n \tag{22}$$

à coefficients $a_1, a_2, \ldots, a_n$ entiers rationnels. Supposons que $f(x)$ est irréductible dans $\mathbf{K}(1)$. Soit Δ un nombre entier rationnel $\neq 1$ qui n'est divisible par aucun carré > 1. Nous supposons que $f(x)$ est réductible dans $\mathbf{K}(\sqrt{\Delta})$, ainsi

$$f(x) = A(x)\, B(x), \tag{23}$$

où l'on a $$A(x) = G(x) + \sqrt{\Delta} H(x), \; B(x) = G_1(x) + \sqrt{\Delta} H_1(x),$$

$G(x), G_1(x), H(x)$ et $H_1(x)$ étant des polynomes dans $\mathbf{K}(1)$. Il est évident qu'on peut supposer que le coefficient de la plus haute puissance de x dans $A(x)$ est égal à 1 ; même chose pour $B(x)$. Le degré de $H(x)$ est évidemment inférieur au degré de $G(x)$; même chose pour $H_1(x)$ et $G_1(x)$. Si $\Delta \equiv 2$ ou $\equiv 3 \pmod 4$ chacun des polynomes $G(x), H(x), G_1(x), H_1(x)$ a des coefficients entiers. Si $\Delta \equiv 1 \pmod 4$ chacun des polynomes $2G(x), 2H(x), 2G_1(x), 2H_1(x)$ a des coefficients entiers.

Soit ξ une racine de $f(x) = 0$ et de $A(x) = 0$. Alors on aura

$$\sqrt{\Delta} = -\frac{G(\xi)}{H(\xi)}.$$

Donc $\sqrt{\Delta}$ appartient à $\mathbf{K}(\xi)$, et le degré n est pair. $\mathbf{K}(\sqrt{\Delta})$ est un sous-corps de tous les corps conjugués de $\mathbf{K}(\xi)$.

En effectuant, dans (23), la multiplication de $A(x)$ et $B(x)$ on obtient

$$G(x)\,H_1(x)\,G_1(x)\,H(x)=0. \tag{24}$$

$G(x)$ et $H(x)$ ne peuvent avoir aucun diviseur commun parce que $f(x)$ est irréductible; même chose pour $G_1(x)$ et $H_1(x)$. Alors il résulte de (24) que $G(x)$ divise $G_1(x)$ et inversement. Il faut donc que $G_1(x)=kG(x)$ et $H_1(x)=-kH(x)$, où k est une constante. Comme le coefficient de la plus haute puissance de x dans $G(x)$, ainsi que dans $G_1(x)$, est égal à 1, on a évidemment $k=1$.

Par conséquent, l'équation (23) doit avoir la forme

$$f(x)=[G(x)]^2-\Delta[H(x)]^2, \tag{25}$$

où le degré de $G(x)$ est égal à $\frac{1}{2}n$, et où celui de $H(x)$ est $\leqslant \frac{1}{2}n-1$.

On peut montrer que le polynome $A(x)=G(x)+\sqrt{\Delta}H(x)$ est irréductible dans $\mathbf{K}(\sqrt{\Delta})$. En effet, supposons qu'on ait

$$A(x)=A_1(x)\,A_2(x), \tag{26}$$

où $A_1(x)$ et $A_2(x)$ sont des polynomes, non constants, dans $\mathbf{K}(\sqrt{\Delta})$. Si $F(x)$ est un polynome dans $\mathbf{K}(\sqrt{\Delta})$ nous désignons par $\bar{F}(x)$ le polynome conjugué dans ce corps. La relation (26) entraîne la relation conjuguée

$$\bar{A}(x)=\bar{A}_1(x)\,\bar{A}_2(x).$$

On aura donc

$$f(x)=A(x)\,\bar{A}(x)=A_1(x)\,\bar{A}_1(x)\cdot A_2(x)\,\bar{A}_2(x).$$

Ici $A_1(x)\,\bar{A}_1(x)$ et $A_2(x)\,\bar{A}_2(x)$ sont des polynomes dans $\boldsymbol{K}(1)$. Or cela est impossible vu que $f(x)$ est irréductible dans $\boldsymbol{K}(1)$. Par conséquent, les polynomes $A(x)$ et $B(x)$ sont irréductibles dans $\mathbf{K}(\sqrt{\Delta})$. Il en résulte de plus que la décomposition de $f(x)$ en deux facteurs $A(x)$ et $B(x)$ satisfaisant aux conditions fixées ci-dessus est unique.

En généralisant le raisonnement on aura évidemment le résultat :

Soit donné le polynom (22) à coefficients appartenant au corps algébrique Ω. Supposons que $f(x)$ est irréductible dans Ω. Soit Δ un nombre dans Ω, tel que $\sqrt{\Delta}$ n'appartienne pas à Ω. Alors, si $f(x)$ est réductible dans $\Omega(\sqrt{\Delta})$ de façon que

$$f(x)=A(x)\,B(x),$$

où $A(x)$ et $B(x)$ sont des polynomes (non constants) dans $\Omega(\sqrt{\Delta})$, jouissant de la propriété que le coefficient de la plus haute puissance de x est égal à 1, on a

$$A(x)=G(x)+\sqrt{\Delta}H(x),\quad B(x)=G(x)-\sqrt{\Delta}H(x),$$

$G(x)$ et $H(x)$ étant des polynomes dans Ω déterminés d'une manière unique. Le degré n de $f(x)$ est un nombre pair $=2m$. Le degré de $G(x)$ est $=m$, et celui de $H(x)$ est $\leqslant m-1$. $A(x)$ et $B(x)$ sont irréductibles dans $\Omega(\sqrt{\Delta})$.

Supposons spécialement que Δ et les coefficients de $f(x)$ sont des nombres entieres dans Ω. Alors les coefficients de $A(x)$ et $B(x)$ sont des entiers dans $\Omega(\sqrt{\Delta})$, et les coefficients de $2G(x)$ sont des entiers dans Ω.

8. Les sous-corps quadratiques du corps cyclotomique. Nous désignons par $\mathbf{K}_N$ le corps cyclotomique engendré par une racine primitive N-ième de l'unité, et par Δ un nombre entier (rationnel) $\neq 1$ qui n'est divisible par aucun carré > 1. Nous avons besoin des lemmes suivants :

Lemme 6. *Si $\mathbf{K}_N$ contient le nombre $\sqrt{\Delta}$, l'index N est divisible par Δ our par 2Δ selon que Δ est impair ou pair.*

Lemme 7. *Si $\sqrt{\Delta}$ est contenu dans $\mathbf{K}_N$, le corps $\mathbf{K}_{MN}$ contient aussi $\sqrt{\Delta}$.*

Lemme 8. *Si N est divisible par le nombre premier $p \geqslant 3$, le corps $\mathbf{K}_N$ contient le nombre $\sqrt{(-1)^{\frac{1}{2}(p-1)}p}$.*

Lemme 9. *La condition nécessaire et suffisante pour que le nombre $i = \sqrt{-1}$ appartienne à $\mathbf{K}_N$, est que N soit divisible par 4.*

Lemme 10. *La condition nécessaire et suffisante pour que le nombre $\sqrt{2}$ appartienne à $\mathbf{K}_N$, est que N soit divisible par 8. $\mathbf{K}_N$ contient $\sqrt{-2}$ s'il contient $\sqrt{2}$ et inversement.*

Pour démontrer le lemme 6 supposons que

$$\pm\Delta = p_1 p_2 \cdots p_r,$$

où les p_i sont des nombres premiers différents. Soit, pour $i = 1, 2, \ldots, r$,

$$(p_i) = \mathfrak{p}_{i1}\mathfrak{p}_{i2}\cdots,$$

où les $\mathfrak{p}_{ij}$ sont des idéaux premiers dans $\mathbf{K}_N$. Donc

$$(\sqrt{\Delta})^2 = \prod_{i,j} \mathfrak{p}_{ij}.$$

Vu que $\mathfrak{p}_{ij} \neq \mathfrak{p}_{hk}$ quand $i \neq h$, on en conclut : si p_i est divisible par l'idéal premier $\mathfrak{p}$ il est aussi divisible par $\mathfrak{p}^2$. Il en résulte, d'après un résultat bien connu, que p_i divise le discriminant de $\mathbf{K}_N$. En appliquant la formule (18), établie dans le numéro 4, on en conclut que N est divisible par p_i et si $p_i = 2$ par 4. Donc N est divisible par Δ et par 2Δ si Δ est pair.

Le lemme 7 est évident. La vérité du lemme 8 se reconnaît par le lemme 5. Pour que $\mathbf{K}_N$ contienne le nombre $i = \sqrt{-1}$ il faut et il suffit qu'on ait, pour un nombre entier h, $\frac{2\pi i}{N} h = \frac{2\pi i}{4}$, c'est-à-dire $N \equiv 0 \pmod 4$. Cela démontre le lemme 9.

Si $\mathbf{K}_N$ contient le nombre $\sqrt{2}$ l'index N est divisible par 4 d'après le lemme 6. Alors $\mathbf{K}_N$ contient le nombre $i = \sqrt{-1}$ et donc aussi le nombre $\frac{1}{2}(\sqrt{2} + \sqrt{-2}) = e^{\frac{1}{4}\pi i}$. Il en résulte que N est divisible par 8. Cette condition est évidemment suffisante. Si $\mathbf{K}_N$ contient le nombre $\sqrt{-2}$ la démonstration est analogue. Ainsi le lemme 10 est démontré.

A l'aide de ces lemmes nous pouvons maintenant établir le résultat suivant :

Théorème 1. *Soit $\mathbf{K}_N$ le corps cyclotomique engendré par une racine primitive n-ième de l'unité. Soit Δ un nombre entier (rationnel) $\neq 1$ qui n'est divisible par aucun carré*

>1. *La condition nécessaire et suffisante pour que le corps quadratique* $\mathbf{K}(\sqrt{\Delta})$ *soit un sous-corps de* $\mathbf{K}_n$, *est qu'on ait l'un ou l'autre des deux cas suivants :*

1°) $\Delta \equiv 1 \pmod 4$ *et* $n \equiv 0 \pmod \Delta$;

2°) $\Delta \equiv 2$ *ou* $\equiv 3 \pmod 4$ *et* $n \equiv 0 \pmod{4\Delta}$.

Démonstration. Considérons d'abord le cas où $\Delta \equiv 1 \pmod 4$. Si $\mathbf{K}_n$ contient le nombre $\sqrt{\Delta}$ il suit du lemme 6 que $n \equiv 0 \pmod \Delta$. Inversement, si $n \equiv 0 \pmod \Delta$ il résulte du lemme 8 que $\mathbf{K}_n$ contient le nombre

$$\sqrt{(-1)^{\frac{1}{2}(d-1)}d},$$

où $d = |\Delta|$. On voit sans peine que ce nombre est égal à $\sqrt{\Delta}$.

Considérons ensuite le cas où $\Delta \equiv 3 \pmod 4$. Si $\mathbf{K}_n$ contient $\sqrt{\Delta}$ il suit du lemme 6 que $n \equiv 0 \pmod \Delta$. Du lemme 8 il résulte que $\mathbf{K}_n$ contient le nombre $\sqrt{-\Delta}$. Donc $\mathbf{K}_n$ contient le nombre $i = \sqrt{-1}$. Ainsi n est divisible par 4 (lemme 9) et par conséquent par 4Δ. Inversement, si $n \equiv 0 \pmod{4\Delta}$ il résulte des lemmes 8 et 9 que $\mathbf{K}_n$ contient les deux nombres $\sqrt{-\Delta}$ et $\sqrt{-1}$. Donc $\sqrt{\Delta}$ appartient à $\mathbf{K}_n$.

Considérons enfin le cas où $\Delta \equiv 2 \pmod 4$. Si $\mathbf{K}_n$ contient $\sqrt{\Delta}$ il suit du lemme 6 que $n \equiv 0 \pmod{2\Delta}$. Alors en vertu du lemme 9 $\mathbf{K}_n$ contient le nombre $\sqrt{-1}$. En appliquant le lemme 8 on voit donc que $\mathbf{K}_n$ contient les nombres $\sqrt{\pm\frac{1}{2}\Delta}$. Par conséquent, $\mathbf{K}_n$ contient les nombres $\sqrt{\pm 2}$ et ainsi n est divisible par 4Δ (lemme 10).

Inversement, si $n \equiv 0 \pmod{4\Delta}$ il résulte du lemme 10 que les nombres $\sqrt{-1}$, $\sqrt{2}$ et $\sqrt{-2}$ appartiennent à $\mathbf{K}_n$. En vertu du lemme 8 les nombres $\sqrt{\pm\frac{1}{2}\Delta}$ sont contenus dans $\mathbf{K}_n$. Par conséquent, $\sqrt{\Delta}$ appartient à $\mathbf{K}_n$.

La démonstration du théorème 1 se trouve ainsi achevée. Comparez Hasse [7], p. 393–399.

9. Autres propriétés du corps cyclotomique. Soit ε une racine primitive n-ième de l'unité ($n>2$). Il est bien connu que le corps réel $\mathbf{K}(\varepsilon+\varepsilon^{-1})$ est du degré $\nu = \frac{1}{2}\varphi(n)$. Si nous posons $\xi = \varepsilon + \varepsilon^{-1}$, les nombres $1, \xi, \xi^2, \ldots, \xi^{\nu-1}$ constituent une base des entiers de $\mathbf{K}(\xi)$. Voir p. ex. Fricke [8], p. 200–202.

On montre aisément que $\mathbf{K}(\xi)$ est le seul sous-corps *réel* de $\mathbf{K}(\varepsilon)$ de degré ν. En effet, soit $\mathbf{K}(\eta)$ un autre sous-corps *réel* de ce degré. Alors le corps composé $\mathbf{K}(\xi,\eta)$ est d'un degré $\geqslant 2\nu = \varphi(n)$, c'est-à-dire ce corps est nécessairement identique à $\mathbf{K}(\varepsilon)$. Or cela est impossible vu que $\mathbf{K}(\xi,\eta)$ est réel. *Ainsi tous les nombres réels de* $\mathbf{K}(\varepsilon)$ *sont contenus dans* $\mathbf{K}(\xi)$.

Il faut observer que, ordinairement, il existe des sous-corps *non-réels* de $\mathbf{K}(\varepsilon)$ de degré ν. On le voit de l'exemple suivant : Soit $n = 11 \cdot 13$ avec $\nu = \frac{1}{2}\varphi(n) = 60$. Alors le corps engendré par les deux nombres

$$e^{\frac{2\pi i}{11}} \quad \text{et} \quad e^{\frac{2\pi i}{13}} \quad \text{et} \quad e^{-\frac{2\pi i}{13}}$$

est du degré 60. Le corps engendré par les deux nombres

$$e^{\frac{2\pi i}{11}} + e^{-\frac{2\pi i}{11}} \quad \text{et} \quad e^{\frac{2\pi i}{13}}$$

est du degré 60. Ces deux corps sont non-réels et différents entre eux.

Il est évident qu'il existe toujours des sous-corps de cette espèce quand n a (au moins) deux facteurs premiers impairs et distincts.

La proposition suivante est un supplément au théorème 1.

Théorème 2. *Soient m un nombre naturel $\geqslant 3$ et a un nombre rationnel tel que le nombre $\alpha = \sqrt[m]{a}$ soit du degré m. Alors α n'est jamais contenu dans un corps cyclotomique, sauf dans le cas suivant :*

$$m = 2^{\mu},\ -a = c^{\frac{1}{2}m},\ \mu \geqslant 2,$$

où c est un nombre rationnel $\neq 0$.

Démonstration. Considérons d'abord le cas de a positif. Supposons que α est réel et que α appartient au corps cyclotomique engendré par la racine de l'unité ε. Alors le nombre α appartient au corps réel $\mathbf{K}$ engendré par le nombre $\varepsilon + \varepsilon^{-1}$. Donc tous les nombres conjugués de α appartiennent à $\mathbf{K}$. Or cela est impossible vu qu'il y a au moins un nombre conjugué qui est imaginaire.

Considerons ensuite le cas que a est négatif. Les nombres conjugués de α sont $(1 \leqslant s \leqslant m)$

$$\alpha^{(s)} = e^{\frac{\pi i}{m}(2k+1)} \sqrt[m]{-a},\ (k = 0, 1, 2, \ldots, m-1)$$

où $\sqrt[m]{-a}$ signifie la valeur positive. Si α appartient à un corps cyclotomique tous les conjugués $\alpha^{(s)}$ doivent appartenir à ce corps. Donc le nombre $\sqrt[m]{-a}$ appartient aussi à un certain corps cyclotomique. D'après ce que nous venons de montrer cela est possible seulement si

$$\sqrt[m]{-a} = \sqrt{b},$$

où b est un nombre positif rationnel, d'où

$$a^2 = b^m.$$

Premier cas. Le nombre b est le carré d'un nombre rationnel, c'est-à-dire : $b = c^2$, $c > 0$, $-a = c^m$ et

$$\alpha^{(s)} = e^{\frac{\pi i}{m}(2k+1)} c.$$

Ici $\alpha^{(s)}$ est du m-ième degré, tandis que le nombre à droite est du degré $\varphi(2m)$. Ainsi on aura $m = \varphi(2m)$ et par conséquent $m = 2^{\mu}$, $-a = c^m$ avec $\mu \geqslant 2$.

Second cas. Le nombre b n'est pas le carré d'un nombre rationnel. Alors m est pair et on obtient $-a = b^{\frac{1}{2}m}$. Dans l'équation

$$[\alpha^{(s)}]^2 = e^{\frac{2\pi i}{m}(2k+1)} b$$

le nombre à gauche est du degré $\frac{1}{2}m$, tandis que le degré du nombre à droite est égal à $\varphi(m)$. Ainsi on aura $m = 2\varphi(m)$, ce qui entraîne $m = 2^{\mu}$, avec $\mu \geqslant 2$. Si $\mu = 2$ il

faut exclure la possibilité $b=2c^2$, c rationnel. En effet, dans ce cas le polynome z^4+4c^4 est réductible.

Le théorème 2 se trouve ainsi démontré.

Remarque. Soient m un nombre naturel $\geqslant 2$ et a un nombre rationnel entier ($\neq 1$) qui n'est divisible par aucun carré >1. Soit **K** un corps algébrique quelconque, et désignons par D le discriminant de **K**. Cela étant on montre aisément : Si **K** contient le nombre $\xi=\sqrt[m]{a}$, le discriminant D est divisible par a. En effet, supposons que

$$a=\pm p_1 p_2 p_3 \cdots p_r,$$

où les p_i sont des nombres premiers différents. Soit, pour $i=1, 2, \ldots, r$,

$$(p_i)=\mathfrak{p}_{i1}\mathfrak{p}_{i2}\ldots,$$

où les $\mathfrak{p}_{ij}$ sont des idéaux premiers dans **K**. Donc

$$(\xi)^m=\prod_{i,j}\mathfrak{p}_{ij}.$$

Vu que $\mathfrak{p}_{ij}\neq\mathfrak{p}_{hk}$ quand $i\neq h$, on en conclut, pour $i=1, 2, \ldots, r$,

$$(p_i)=\mathfrak{a}^m,$$

où $\mathfrak{a}$ est un idéal dans **K**. Il en résulte que D est divisible par chacun des nombres premiers p_i et, par conséquent, par a.

§ 4. Sur les décompositions du polynome cyclotomique

10. L'identité de Gauss–Dedekind. Soit n un nombre impair >1 qui n'est divisible par aucun carré >1. Considérons les polynomes

$$\left.\begin{aligned} A(x)&=\prod_a (x-e^{\frac{2\pi i}{n}a}),\\ B(x)&=\prod_b (x-e^{\frac{2\pi i}{n}b}),\end{aligned}\right\} \tag{27}$$

où le premier produit est étendu aux $\nu=\frac{1}{2}\varphi(n)$ nombres a $(0<a<n)$ pour lesquels le symbole de Jacobi $\left(\frac{a}{n}\right)$ a la valeur $+1$, tandis que le second produit est étendu aux ν nombres b $(0<b<n)$ pour lesquels on a $\left(\frac{b}{n}\right)=-1$. Posons, pour raccourcir, $(-1)^{\frac{1}{2}(n-1)}n=n^*$. Alors il est bien connu qu'on a les relations

$$\left.\begin{aligned} 2A(x)&=X(x)-\sqrt{n^*}\,Y(x),\\ 2B(x)&=X(x)+\sqrt{n^*}\,Y(x),\end{aligned}\right\} \tag{28}$$

où $X(x)$ et $Y(x)$ sont des polynomes en x à coefficients entiers rationnels. $\sqrt{n^*}$ signifie la valeur positive quand n^* est positif et le nombre $i\sqrt{-n^*}$ quand n^* est négatif. Le degré du polynome $X(x)$ est égal à ν, et le coefficient de x^ν est égal à 2. Le degré du polynome $Y(x)$ est égal à $\nu-1$ et le coefficient de $x^{\nu-1}$ est égal à 1. De (28) il résulte

$$4F_n(x) = [X(x)]^2 - n^*[Y(x)]^2 \tag{29}$$

Tous ces résultats sont dus à Dedekind; pour la démonstration voir Dirichlet [10], supplemént VII, p. 360–370; pour n premier les résultats se trouvent déjà chez Gauss, voir [9], p. 443.

Pour les polynomes $A(x)$, $B(x)$, $X(x)$ et $Y(x)$ on a encore les relations suivantes : Si $n \equiv 1 \pmod 4$,

$$\left.\begin{aligned} A(x) &= x^\nu A(x^{-1}), \\ B(x) &= x^\nu B(x^{-1}), \end{aligned}\right\} \tag{30}$$

et si $n \equiv 3 \pmod 4$ et $n \geqslant 7$,

$$\left.\begin{aligned} A(x) &= (-x)^\nu B(x^{-1}), \\ B(x) &= (-x)^\nu A(x^{-1}). \end{aligned}\right\} \tag{30'}$$

Pour $n \equiv 1 \pmod 4$ on a

$$\left.\begin{aligned} X(x) &= x^\nu X(x^{-1}), \\ Y(x) &= x^\nu Y(x^{-1}), \end{aligned}\right\} \tag{31}$$

et pour $n \equiv 3 \pmod 4$, si $n \geqslant 7$,

$$\left.\begin{aligned} X(x) &= (-x)^\nu X(x^{-1}). \\ -Y(x) &= (-x)^\nu Y(x^{-1}). \end{aligned}\right\} \tag{31'}$$

Les coefficients des polynomes $A(x)$ et $B(x)$ sont des nombres entiers dans le corps quadratique $\mathbf{K}$ engendré par le nombre $\sqrt{n^*}$. La formule (29) est évidemment une conséquence immédiate du fait que le corps $\mathbf{K}$ est un sous-corps du corps $\mathbf{K}_n$ engendré par une racine n-ième primitive de l'unité; comparez le théorème 1 et le numéro 7. Il est évident que, à tout sous-corps quadratique de $\mathbf{K}_n$ correspond une identité analogue á (29). Nous allons étudier les identités en question pour toutes les valeurs de n.

11. Les polynomes $A(x)$ et $B(x)$ dans le cas général. Dans ce qui suivra $\mathbf{K}_n$ signifie le corps cyclotomique d'index $n(>2)$. Posons comme ci-dessus $\nu = \frac{1}{2}\varphi(n)$. Soit $\Delta(\neq 1)$ un nombre entier rationnel qui n'est divisible par aucun carré >1. Supposons que $\sqrt{\Delta}$ appartient à $\mathbf{K}_n$. Alors on a la decomposition

$$F_n(x) = A(x)\,B(x), \tag{32}$$

où $A(x)$ et $B(x)$ sont des polynomes en x du degré ν, à coefficients entiers dans $\mathbf{K}(\sqrt{\Delta})$, et conjugués dans ce corps, c'est-à-dire

$$\left.\begin{aligned} A(x) &= X(x) - \sqrt{\Delta}\,Y(x), \\ B(x) &= X(x) + \sqrt{\Delta}\,Y(x), \end{aligned}\right\} \tag{32'}$$

où $X(x)$ et $Y(x)$ sont des polynomes en x à coefficients rationnels. Dans les cas où $\Delta \equiv 2$ ou $\equiv 3 \pmod 4$ les coefficients sont entiers, tandis que dans le cas ou $\Delta \equiv 1 \pmod 4$ ceux-ci seront entiers après la multiplication par 2. En effectuant la multiplication dans (32) on aura

$$F_n(x) = [X(x)]^2 - \Delta[Y(x)]^2. \tag{32''}$$

Il faut observer que, dans (32'), le signe de $\sqrt{\Delta}$ n'est pas encore fixé; on observe encore que les polynomes $X(x)$ et $Y(x)$ se distinguent des polynomes correspondants dans (28) par le facteur 2. Ici nous ne pouvons pas distinguer entre les polynomes $A(x)$ et $B(x)$ ainsi que est le cas dans (28).

Il est évident qu'on peut supposer que $X(x)$ est du degré ν, et que le coefficient de x^ν est égal à 1. Alors $Y(x)$ est au plus du degré $\nu-1$; comparez le numéro 7.

Remarque. S'il n'y a aucune unité irrationnelle dans le corps $\mathbf{K}(\sqrt{\Delta})$, il n'existe pas d'autres possibilités pour les polynomes $X(x)$ et $Y(x)$, abstraction faite d'un changement de signe. Supposons maintenant que $u+v\sqrt{\Delta}$, u et v rationnels, $v\neq 0$, est une unité dans $\mathbf{K}(\sqrt{\Delta})$ à norme positive. Alors on a

$$[X(x)+\sqrt{\Delta}\,Y(x)]\cdot[u+v\sqrt{\Delta}]=X_1(x)+\sqrt{\Delta}\,Y_1(x),$$

où

$$X_1(x)=uX(x)+v\Delta Y(x),$$
$$Y_1(x)=vX(x)+uY(x).$$

Il est évident que les polynomes $X_1(x)$ et $Y_1(x)$ satisfont à (32''). Cela arrive pour $\Delta=-1$, pour $\Delta=-3$ et pour toutes les valeurs positives de Δ; dans le dernier de ces cas il y a ainsi une infinité de solutions de (32'').

Nous désignons par $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_\nu$ les zéros de $A(x)$. Les autres racines primitives n-ièmes de l'unité sont les zéros de $B(x)$.

Soit ε un zéro de $A(x)$ et supposons que ε^{-1} est aussi un zéro de $A(x)$. Alors on aura

$$X(\varepsilon)-\sqrt{\Delta}\,Y(\varepsilon)=0,$$
$$X(\varepsilon^{-1})-\sqrt{\Delta}\,Y(\varepsilon^{-1})=0,$$

donc

$$\sqrt{\Delta}=\frac{X(\varepsilon)+X(\varepsilon^{-1})}{Y(\varepsilon)+Y(\varepsilon^{-1})}.$$

Ici le numérateur aussi bien que le dénominateur sont réels vu que $\varepsilon^m+\varepsilon^{-m}$ est réel quand m est un nombre naturel. Donc Δ est positif. Inversement, si Δ est positif le polynome $A(x)$ est réel. Par conséquent, si ε est un zéro de $A(x)$ le nombre conjugué (au sens propre) ε^{-1} l'est aussi. Cela est aussi vrai pour $B(x)$.

Du raisonnement précédent nous pouvons aussi faire la conclusion suivante : Si Δ est négatif et si l'équation $A(x)=0$ a les racines $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_\nu$, l'équation $B(x)=0$ a les racines $\varepsilon_1^{-1}, \varepsilon_2^{-1}, \ldots, \varepsilon_\nu^{-1}$.

Premier cas : Δ est positif.

Dans ce cas le nombre $\nu=\frac{1}{2}\varphi(n)$ est évidemment pair. Nous allons montrer que les formules (30) et (31) sont toujours valables. En effet, si $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_\nu$ sont les racines de $A(x)=0$, le produit $\varepsilon_1\varepsilon_2\ldots\varepsilon_\nu$ est, d'après ce que nous venons de montrer, égal à 1. Donc nous avons

$$x^\nu A(x^{-1})=x^\nu\prod_k(x^{-1}-\varepsilon_k)=\prod_k\varepsilon_k(x-\varepsilon_k^{-1})=A(x).$$

D'une manière analogue on aura

$$x^{\nu}B(x^{-1}) = B(x).$$

En vertu de (32′) on obtient

$$2X(x) = A(x) + B(x),$$

$$2\sqrt{\Delta}\,Y(x) = -A(x) + B(x).$$

On en conclut que

$$x^{\nu}X(x^{-1}) = X(x),$$

$$x^{\nu}Y(x^{-1}) = Y(x).$$

Second cas : Δ est négatif.

Ici le nombre $\nu = \frac{1}{2}\varphi(n)$ est pair, sauf dans les trois cas suivants : $n = 4$, $n = p^{\alpha}$ et $n = 2p^{\alpha}$, où p est un nombre premier $\equiv 3 \pmod 4$.

Nous allons déterminer les relations auxquelles satisfont les polynomes $A(x)$, $B(x)$, $X(x)$ et $Y(x)$, relations analogues aux formules (30′) et (31′).

Si $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\nu}$ sont les racines de $A(x) = 0$, les racines de $B(x) = 0$ sont $\varepsilon_1^{-1}, \varepsilon_2^{-1}, \ldots, \varepsilon_{\nu}^{-1}$. Cela étant, on obtient

$$(-x)^{\nu}B(x^{-1}) = (-x)^{\nu}\prod_k (x^{-1} - \varepsilon_k^{-1}) = \varepsilon_1(\varepsilon_2 \ldots \varepsilon_{\nu})^{-1}A(x). \tag{33}$$

Le produit $\varepsilon_1\varepsilon_2\ldots\varepsilon_{\nu}$ est une unité dans $\mathbf{K}(\sqrt{\Delta})$. Dans la suite nous excluons les cas $\Delta = -1$ et $\Delta = -3$. Alors ce produit a l'une des valeurs $+1$ ou -1. Supposons d'abord que n n'est pas la puissance d'un nombre premier. Alors on a

$$F_n(1) = 1 = A(1)\,B(1),$$

d'où $A(1) = B(1) = \pm 1$. En posant dans la formule (33) $x = 1$ on aura

$$\varepsilon_1\varepsilon_2\ldots\varepsilon_{\nu} = (-1)^{\nu}.$$

De la même formule il résulte donc, pour tous les $n \neq p^{\nu}$,

$$\left.\begin{aligned} x^{\nu}B(x^{-1}) &= A(x), \\ x^{\nu}A(x^{-1}) &= B(x). \end{aligned}\right\} \tag{34}$$

Vu que

$$\left.\begin{aligned} 2X(x) &= A(x) + B(x), \\ 2\sqrt{\Delta}\,Y(x) &= -A(x) + B(x), \end{aligned}\right\} \tag{35}$$

on aura donc

$$\left.\begin{aligned} x^{\nu}X(x^{-1}) &= X(x), \\ x^{\nu}Y(x^{-1}) &= -Y(x). \end{aligned}\right\} \tag{36}$$

Considérons maintenant le cas où $n = p^{\alpha}$. Alors on a nécessairement (voir le théorème 1) $\Delta = -p$ où $p \equiv 3 \pmod 4$ et $p \neq 3$. En posant dans (33) $x = 1$ on aura

$$p = A(1)\,B(1),$$

où $A(1)$ et $B(1)$ sont des nombres conjugués dans $\mathbf{K}(\sqrt{-p})$. Donc

$$A(1) = \tfrac{1}{2}(u \pm v\sqrt{-p}),\ B(1) = \tfrac{1}{2}(u \mp v\sqrt{-p}),$$

où u et v sont des nombres entiers rationnels. Or, l'équation $u^2+pv^2=4p$ entraîne $u=0$, $v=\pm 1$, Donc

$$A(1)=-B(1)=\pm\sqrt{-p}.$$

Le nombre ν étant dans ce cas-ci impair, on aura

$$\varepsilon_1\varepsilon_2\ldots\varepsilon_\nu=1.$$

Par conséquent

$$\left.\begin{aligned} x^\nu B(x^{-1}) &= -A(x),\\ x^\nu A(x^{-1}) &= -B(x).\end{aligned}\right\} \tag{37}$$

A l'aide des formules (35) on aura encore

$$\left.\begin{aligned} x^\nu X(x^{-1}) &= -X(x),\\ x^\nu Y(x^{-1}) &= Y(x).\end{aligned}\right\} \tag{38}$$

Ainsi, les relations (37) et (38) sont valables pour tous les $n=p^\alpha$, $p(\neq 3)$ nombre premier $\equiv 3 \pmod 4$. Les relations (34) et (36) sont valables pour toutes les autres valeurs de n.

Les cas où $\Delta=-1$ et $\Delta=-3$ seront traités dans un supplément.

12. Exemples numériques.

Exemple 1. Soit $n=24$. Les valeurs possibles de Δ sont $-1, 2, -2, 3, -3, 6$ et -6. Le polynome

$$F_{24}(x)=x^8-x^4+1$$

peut s'écrire de sept manières sous la forme (32'') :

$$\begin{aligned}
&(x^4-1)^2+(x^2)^2,\\
&(x^4+x^2+1)^2-2(x^3+x)^2,\\
&(x^4-x^2+1)^2+2(x^3-x)^2,\\
&(x^4+1)^2-3(x^2)^2,\\
&(x^4-\tfrac{1}{2})^2+3(\tfrac{1}{2})^2,\\
&(x^4+3x^2+1)^2-6(x^3+x)^2,\\
&(x^4-3x^2+1)^2+6(x^3-x)^2.
\end{aligned}$$

Exemple 2. Prenons $n=20$. Les valeurs possibles de Δ sont -1, 5 et -5. Le polynome

$$F_{20}(x)=x^8-x^6+x^4-x^2+1$$

peut s'écrire de trois manières sous la forme (32'') :

$$\begin{aligned}
&(x^4-x^2+1)^2+(x^3-x)^2\\
&(x^4-\tfrac{1}{2}x^2+1)^2-5(\tfrac{1}{2}x^2)^2,\\
&(x^4-3x^2+1)^2+5(x^3-x)^2.
\end{aligned}$$

Exemple 3. Quand $n = 15$, les valeurs possibles de Δ sont -3, 5 et -15. Le polynome

$$F_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

peut s'écrire de trois manières sous la forme (32'') :

$$(x^4 - \tfrac{1}{2}x^3 - \tfrac{1}{2}x^2 + x - \tfrac{1}{2})^2 + 3(\tfrac{1}{2}x^3 - \tfrac{1}{2}x^2 + \tfrac{1}{2})^2,$$
$$(x^4 - \tfrac{1}{2}x^3 + \tfrac{1}{2}x^2 - \tfrac{1}{2}x + 1)^2 - 5(\tfrac{1}{2}x^3 - \tfrac{1}{2}x^2 + \tfrac{1}{2}x)^2,$$
$$(x^4 - \tfrac{1}{2}x^3 + 2x^2 - \tfrac{1}{2}x + 1)^2 + 15(\tfrac{1}{2}x^3 - \tfrac{1}{2}x)^2.$$

Exemple 4. Quand $n = 21$, les valeurs possibles de Δ sont -3, -7 et 21. Le polynome

$$F_{21}(x) = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1$$

peut s'écrire de trois manières sous la forme (32'') :

$$(x^6 - \tfrac{1}{2}x^5 - \tfrac{1}{2}x^4 + x^3 - \tfrac{1}{2}x^2 - \tfrac{1}{2}x + 1)^2 + 3(\tfrac{1}{2}x^5 - \tfrac{1}{2}x^4 + \tfrac{1}{2}x^2 - \tfrac{1}{2}x)^2,$$
$$(x^6 - \tfrac{1}{2}x^5 - x^4 - x^2 - \tfrac{1}{2}x + 1)^2 + 7(\tfrac{1}{2}x^5 - \tfrac{1}{2}x)^2,$$
$$(x^6 - \tfrac{1}{2}x^5 + \tfrac{5}{2}x^4 - \tfrac{7}{2}x^3 + \tfrac{5}{2}x^2 - \tfrac{1}{2}x + 1)^2 - 21(\tfrac{1}{2}x^5 - \tfrac{1}{2}x^4 + \tfrac{1}{2}x^3 - \tfrac{1}{2}x^2 + \tfrac{1}{2}x)^2.$$

§ 5. Les zéros des polynomes $A(x)$ et $B(x)$

13. Lemmes ultérieurs. Supposons que $F_n(x)$ est réductible dans le corps quadratique engendré par $\sqrt{\Delta}$, où Δ est un nombre entier rationnel $\neq 1$ qui n'est divisible par aucun carré > 1. Les polynomes $A(x)$ et $B(x)$, définis par les équations (32) et (32') dans le numéro 11, dépendent de n et de Δ. Dans la suite nous avons besoin de signaler ce fait en employant les notations plus precises

$$A_n(x; \Delta) \quad \text{et} \quad B_n(x; \Delta).$$

Nous prescrivons que le nombre $e^{\frac{2\pi i}{n}}$ soit un zéro du premier de ces polynomes pour toutes les valeurs de n et Δ. Cela est parfaitement d'accord avec la formule (27). Ainsi les deux polynomes sont caractérisés de façon qu'on puisse les distinguer l'un de l'autre.

Si p est un nombre premier qui divise n, nous avons, d'aprés la formule (5) du numéro 1,

$$F_{np}(x) = F_n(x^p).$$

Alors nous avons

$$A_{np}(x; \Delta)\, B_{np}(x; \Delta) = A_n(x^p; \Delta)\, B_n(x^p; \Delta).$$

D'après le résultat du numéro 7 les deux polynomes à gauche sont irréductibles dans $\mathbf{K}(\sqrt{\Delta})$. Il en resulte que les deux polynomes à droite le sont aussi. Par définition le nombre $e^{\frac{2\pi i}{np}}$ est un zéro de $A_{np}(x; \Delta)$. Or, il est évident que ce nombre est aussi un zéro de $A_n(x^p; \Delta)$. Donc on aura, si le nombre premier p divise n, les lemmes

$$\left.\begin{aligned} A_{np}(x; \Delta) &= A_n(x^p; \Delta), \\ B_{np}(x; \Delta) &= B_n(x^p; \Delta). \end{aligned}\right\} \tag{39}$$

Considérons maintenant le cas où le nombre premier p ne divise pas n, et dans lequel on a

$$F_{np}(x) = \frac{F_n(x^p)}{F_n(x)}.$$

Il en résulte

$$A_{np}(x;\Delta)\,B_{np}(x;\Delta) = \frac{A_n(x^p;\Delta)\,B_n(x^p;\Delta)}{A_n(x;\Delta)\,B_n(x;\Delta)}. \tag{40}$$

Ici les deux polynomes à gauche et les deux polynomes dans le dénominateur à droite sont irréductibles dans le corps $\mathbf{K}(\sqrt{\Delta})$ (voir le numéro 7). Il est évident que le nombre $e^{\frac{2\pi i}{np}}$ est un zéro de chacun des deux polynomes $A_{np}(x;\Delta)$ et $A_n(x^p;\Delta)$. Ainsi le dernier de ces polynomes est divisible par le premier. On en conclut que le polynome $B_n(x^p;\Delta)$ est divisible par le polynome $B_{np}(x;\Delta)$. Les zéros de $A_n(x^p;\Delta)$ sont évidemment les nombres

$$e^{\frac{2\pi i}{np}\cdot a + \frac{2\pi i}{p}\cdot h}, \tag{41}$$

où a parcourt un certain système de $\frac{1}{2}\varphi(n)$ nombres premiers à n, incongrus modulo n, et où h parcourt un système complet de résidus modulo p. Le nombre $\xi = e^{\frac{2\pi i}{n}}$ est un zéro de $A_n(x;\Delta)$. Si ξ se trouve parmi les nombres (41), il est évident que $A_n(x^p;\Delta)$ est divisible par $A_n(x;\Delta)$, vu que ce dernier polynome est irréductible dans $\mathbf{K}(\sqrt{\Delta})$. Autrement $A_n(x;\Delta)$ divise $B_n(x^p;\Delta)$. Pour que ξ se trouve parmi les nombres (41) il faut et il suffit qu'il y ait une valeur de a telle que la congruence

$$a + nh \equiv p \pmod{np} \tag{42}$$

soit satisfaite par une valeur de h. Si cette congruence est satisfaite on aura donc

$$\left.\begin{aligned} A_{np}(x;\Delta) &= \frac{A_n(x^p;\Delta)}{A_n(x;\Delta)}, \\ B_{np}(x;\Delta) &= \frac{B_n(x^p;\Delta)}{B_n(x;\Delta)}. \end{aligned}\right\} \tag{43}$$

Autrement on aura

$$\left.\begin{aligned} A_{np}(x;\Delta) &= \frac{A_n(x^p;\Delta)}{B_n(x;\Delta)}, \\ B_{np}(x;\Delta) &= \frac{B_n(x^p;\Delta)}{A_n(x;\Delta)}. \end{aligned}\right\} \tag{44}$$

Dans les lemmes (43) et (44) n n'est pas divisible par p.

Pour déterminer les racines des équations $A_n(x;\Delta) = 0$ et $B_n(x;\Delta) = 0$ il faut distinguer plusieurs cas.

14. Théorèmes principaux sur les zéros du polynome $A_n(x;\Delta)$. Le but du présent chapitre est d'établir les théorèmes suivants:

Théorème 3. *Lorsque* $\Delta \equiv 1 \pmod 4$ *les zéros du polynome* $A_n(x;\Delta)$ *sont les nombres* ε^a, *où* a *parcourt tous les nombres naturels satisfaisant aux conditions suivantes :*

$$a<n,\ (a,n)=1,\ \left(\frac{a}{|\Delta|}\right)=+1.$$

Théorème 4. *Les zéros du polynome* $A_n(x;-1)$ *sont les nombres* ε^a, *où* a *parcourt tous les nombres naturels satisfaisant aux conditions suivantes :*

$$a<n,\ (a,n)=1,\ a\equiv 1 \pmod 4.$$

Théorème 5. *Lorsque* $\Delta\equiv 3 \pmod 4$ *les zéros du polynome* $A_n(x;\Delta)$ *sont les nombres* ε^a, *où* a *parcourt tous les nombres naturels satisfaisant ou au premier ou au second des deux systèmes de conditions :*

$$1^\circ)\ a<n,\ (a,n)=1,\ a\equiv 1 \pmod 4,\quad \left(\frac{a}{|\Delta|}\right)=+1;$$

$$2^\circ)\ a<n,\ (a,n)=1,\ a\equiv 3 \pmod 4,\quad \left(\frac{a}{|\Delta|}\right)=-1.$$

Théorème 6. *Les zéros du polynome* $A_n(x;2)$ *sont les nombres* ε^a, *où* a *parcourt tous les nombres naturels satisfaisant aux conditions suivantes :*

$$a<n,\ (a,n)=1,\ a\equiv \pm 1 \pmod 8.$$

Théorème 7. *Les zéros du polynome* $A_n(x;-2)$ *sont les nombres* ε^a, *où* a *parcourt tous les nombres naturels satisfaisant aux conditions suivantes :*

$$a<n,\ (a,n)=1,\ a\equiv 1 \text{ ou } \equiv 3 \pmod 8.$$

Théorème 8. *Lorsque* $\Delta=2 \pmod 8$, *les zéros du polynome* $A_n(x;\Delta)$ *sont les nombres* ε^a, *où* a *parcourt tous les nombres naturels satisfaisant ou au premier ou au second des deux systèmes de conditions :*

$$1^\circ)\ a<n,\ (a,n)=1,\ a\equiv \pm 1 \pmod 8,\quad \left(\frac{a}{\frac{1}{2}|\Delta|}\right)=+1;$$

$$2^\circ)\ a<n,\ (a,n)=1,\ a\equiv \pm 3 \pmod 8,\quad \left(\frac{a}{\frac{1}{2}|\Delta|}\right)=-1.$$

Théorème 9. *Lorsque* $\Delta\equiv -2 \pmod 8$, *les zéros du polynome* $A_n(x;\Delta)$ *sont les nombres* ε^a, *où* a *parcourt tous les nombres naturels satisfaisant ou au premier ou au second des deux systèmes de conditions :*

$$1^\circ)\ a<n,\ (a,n)=1,\ a\equiv 1 \text{ ou } \equiv 3 \pmod 8,\quad \left(\frac{a}{\frac{1}{2}|\Delta|}\right)=+1;$$

$$2^\circ)\ a<n,\ (a,n)=1,\ a\equiv 5 \text{ ou } \equiv 7 \pmod 8,\quad \left(\frac{a}{\frac{1}{2}|\Delta|}\right)=-1.$$

Ici, ε signifie le nombre $e^{\frac{2\pi i}{n}}$. La démonstration de ces théorèmes sera réalisée dans les numéros suivants. Pour cela il nous faut encore un lemme.

Lemme 11. *Il suffit d'établir les théorèmes 3–9 pour le polynome* $A_d(x;\Delta)$, *où* $d=|\Delta|$ *dans le théorème 3 et où* $d=4|\Delta|$ *dans les autres théorèmes.*

Demonstration. A chaque valeur de Δ correspond un certain théorème parmi les théorèmes 3–9. Supposons que ce théorème soit vrai pour $A_d(x;\Delta)$. Cela posé nous

allons montrer que le théorème est vrai pour tous les polynomes $A_N(x;\Delta)$ où N est un multiple de d. Nous le ferons par induction de la manière suivante. En supposant que le théorème soit vrai pour $A_n(x;\Delta)$ nous montrerons qu'il est aussi vrai pour $A_{np}(x;\Delta)$ où p est un nombre premier quelconque.

Le théorème étant supposé vrai pour $A_n(x;\Delta)$ les zéros ε^a de ce polynome sont caractérisés par des conditions du type suivant :

$$0<a<n,\ (a,n)=1,\ a\equiv r \pmod{\frac{d}{\delta}},\ \left(\frac{a}{\delta}\right)=e,$$

où $\delta=|\Delta|$ ou $=\frac{1}{2}|\Delta|$ selon que Δ est impair ou pair, où $r=1$ pour $d/\delta=1$, $r=\pm 1$ pour $d/\delta=4$, $r=\pm 1,\ \pm 3$ pour $d/\delta=8$, et où $e=\pm 1$.

D'après les lemmes du numéro 13 nous avons

$$A_{np}(x;\Delta)=\frac{A_n(x^p;\Delta)}{C(x)}.$$

Ici $C(x)=1$, quand le nombre premier p divise n. Si n n'est pas divisible par p on a ou $C(x)=A_n(x;\Delta)$ ou $C(x)=B_n(x;\Delta)$. Les zéros de $A_n(x^p;\Delta)$ sont, en vertu de notre supposition, les nombres

$$e^{\frac{2\pi i a}{np}+\frac{2\pi i h}{p}}=e^{\frac{2\pi i(a+hn)}{np}}, \tag{45}$$

où la signification de a est la même que plus haut, tandis que h parcourt les valeurs $0,1,2,\ldots,p-1$. En posant $c=a+hn$ on aura : $0<c<np$ et $\left(\frac{c}{\delta}\right)=\left(\frac{a}{\delta}\right)=e$ et $c\equiv a\equiv r \pmod{d/\delta}$, vu que n est divisible par chacun des deux nombres δ et d/δ. Si p divise n, on a de plus $(c,np)=1$; et dans ce cas les nombres (45) constituent tous les zéros de $A_{np}(x;\Delta)$. Si p ne divise pas n, il y a, parmi les nombres (45), exactement $\frac{1}{2}\varphi(n)$ nombres pour lesquels $c=a+hn$ est divisible par p; ces nombres sont du degré $\frac{1}{2}\varphi(n)$; les autres $\frac{1}{2}\varphi(n)p-\frac{1}{2}\varphi(n)=\frac{1}{2}\varphi(np)$ nombres, qui sont du degré $\frac{1}{2}\varphi(np)$, représentent les zéros de $A_{np}(x;\Delta)$. Ainsi le lemme 11 est démontré.

Dans la suite nous écrirons $E(z)$ pour la fonction $e^{2\pi i z}$. Comme plus haut, $\sqrt{c}$ signifiera la valeur positive quand c est positif, et le nombre $i\sqrt{-c}$ quand c est négatif.

15. Démonstration des théorèmes 3, 4, 5, 6 et 7. Considérons d'abord le cas où $\Delta\equiv 1 \pmod 4$ et le théorème 3. D'apres le résultat de Dedekind (voir le numéro 10) le théorème est vrai pour le polynome $A_{|\Delta|}(x;\Delta)$. Par conséquent, en vertu du lemme 11 le théorème 3 est vrai pour chaque valeur de l'index n.

Considérons ensuite le cas où $\Delta=-1$. Nous avons $A_4(x;-1)=x-i$, et ainsi le théorème 4 est vrai pour ce polynome. Donc, en vertu du lemme 11, le théorème 4 se trouve démontrè pour toute valeur de n.

Pour démontrer le théorème 5 il suffit de l'établir pour le polynome $A_{4|\Delta|}(x;\Delta)$, où $\Delta\equiv -1 \pmod 4$. Considérons maintenant le nombre

$$\xi_m=\sum_c E\left(\frac{cm}{4|\Delta|}\right), \tag{46}$$

où la somme est étendue à tous les nombres naturels c satisfaisant aux conditions que voici : $c<4|\Delta|$, $(c,4|\Delta|)=1$, $c\equiv +1 \pmod 4$ lorsque $\left(\frac{c}{|\Delta|}\right)=+1$ et $c\equiv -1$

(mod 4) lorsque $\left(\frac{c}{|\Delta|}\right) = -1$. m est un nombre naturel quelconque. Le nombre des termes dans (46) est égal à $\frac{1}{2}\varphi(4|\Delta|) = \varphi(2|\Delta|)$.

Nous allons établir le résultat suivant :

Lemme 12. 1°) *Lorsque m est impair et $(m, |\Delta|) = 1$ on a*

$$\xi_m = \left(\frac{-1}{m}\right)\left(\frac{m}{|\Delta|}\right)\sqrt{\Delta}.$$

2°) *Lorsque m est impair et $(m, |\Delta|) = d > 1$ on a*

$$\xi_m = 0.$$

3°) *Lorsque m est pair et $(m, |\Delta|) = d \geqslant 1$ on a*

$$\xi_m = (-1)^{\frac{1}{2}m} \cdot \mu\left(\frac{|\Delta|}{d}\right) \frac{\varphi(|\Delta|)}{\varphi\left(\frac{|\Delta|}{d}\right)}.$$

Démonstration. Considérons d'abord le cas où $m \equiv 2 \pmod 4$ et posons $m = 2s$, où s est impair. Alors

$$\xi_m = \sum_c E\left(\frac{cs}{2|\Delta|}\right), \tag{47}$$

où la sommation est comme dans (46). En multipliant par $-1 = e^{\pi i s}$ on aura

$$-\xi_m = \sum_c E\left(\frac{c + |\Delta|}{2|\Delta|} s\right).$$

Une congruence de la forme

$$\tfrac{1}{2}(c + |\Delta|) \equiv \tfrac{1}{2}(c^* + |\Delta|) \pmod{|\Delta|}$$

ne peut pas avoir lieu. En effet, celle-ci entraînerait $c \equiv c^* \pmod{2|\Delta|}$, donc $c^* \equiv c + 2|\Delta| \pmod{4|\Delta|}$. Il en résulte que

$$\left(\frac{c}{|\Delta|}\right) = \left(\frac{c^*}{|\Delta|}\right),$$

tandis que $c^* \equiv c + 2 \equiv -c \pmod 4$. Cela montre que les nombres c et c^* ne peuvent pas paraître tous les deux dans la somme (47). Il en résulte que les nombres $\frac{1}{2}(c + |\Delta|)$ sont incongrus modulo $|\Delta|$. Leur nombre total est $= \varphi(2|\Delta|) = \varphi(|\Delta|)$ et $(\frac{1}{2}(c + |\Delta|), |\Delta|) = 1$. Donc

$$-\xi_m = \sum_f E\left(\frac{fs}{|\Delta|}\right),$$

où f parcourt un système réduit de résidus modulo $|\Delta|$. Supposons que $(m, |\Delta|) = d$. En vertu de la formule (12) dans le numéro 3 on obtient alors

$$\xi_m = -\mu\left(\frac{|\Delta|}{d}\right) \frac{\varphi(|\Delta|)}{\varphi\left(\frac{|\Delta|}{d}\right)}.$$

Traitons ensuite le cas où $m \equiv 0 \pmod 4$ et posons $m = 4s$. On a

$$\xi_m = \sum_c E\left(\frac{cs}{|\Delta|}\right).$$

Ici les nombres c sont incongrus modulo $|\Delta|$. En effet $c \equiv c^* \pmod{|\Delta|}$ entraînerait $\left(\frac{c}{|\Delta|}\right) = \left(\frac{c^*}{|\Delta|}\right)$ et donc $c \equiv c^* \pmod 4$, et $c \equiv c^* \pmod{4|\Delta|}$ ce qui est exclu. Ainsi les nombres c constituent un système réduit de résidus modulo $|\Delta|$. Supposons que $(m, |\Delta|) = d$. En vertu de la formule (12) dans le numéro 3 on obtient alors

$$\xi_m = \mu\left(\frac{|\Delta|}{d}\right) \frac{\varphi(|\Delta|)}{\varphi\left(\frac{|\Delta|}{d}\right)}.$$

Soit maintenant m impair. En multipliant (46) par $i^m = e^{\frac{1}{2}\pi i m}$ on aura

$$\xi_m i^m = \sum_a E\left(\frac{a+|\Delta|}{4|\Delta|} m\right) + \sum_{a^*} E\left(\frac{a^*+|\Delta|}{4|\Delta|} m\right), \tag{48}$$

où la première somme est étendue à tous les nombres naturels a qui satisfont aux conditions suivantes : $a < 4|\Delta|$, $(a, 4|\Delta|) = 1$, $\left(\frac{a}{|\Delta|}\right) = +1$, $a \equiv 1 \pmod 4$, tandis que la seconde somme est étendue à tous les nombres naturels a^* qui satisfont aux conditions suivantes : $a^* < 4|\Delta|$, $(a^*, 4|\Delta|) = 1$, $\left(\frac{a^*}{|\Delta|}\right) = -1$, $a^* \equiv -1 \pmod 4$. Nous désignons la première somme par α_m et la seconde somme par β_m.

Premier cas. Soit Δ négatif, donc $|\Delta| \equiv 1 \pmod 4$. Il est évident que

$$-\alpha_m = \sum_f E\left(\frac{fm}{|\Delta|}\right),$$

où la somme est étendue à tous les $\frac{1}{2}\varphi(|\Delta|)$ nombres $f = \frac{1}{4}(a + 3|\Delta|)$; on voit que ces nombres sont incongrus modulo $|\Delta|$; on a encore $(f, |\Delta|) = 1$ et $\left(\frac{f}{|\Delta|}\right) = \left(\frac{a}{|\Delta|}\right) = +1$. En appliquant le lemme 4 on aura donc, si $(m, |\Delta|) = 1$,

$$-\alpha_m = \tfrac{1}{2}\left[\mu(|\Delta|) + \left(\frac{m}{|\Delta|}\right)\sqrt{|\Delta|}\right],$$

et si $(m, |\Delta|) = d > 1$,

$$-\alpha_m = \tfrac{1}{2}\mu\left(\frac{|\Delta|}{d}\right) \frac{\varphi(|\Delta|)}{\varphi\left(\frac{|\Delta|}{d}\right)}.$$

Pour la deuxième somme on aura d'une façon analogue

$$\beta_m = \sum_g E\left(\frac{gm}{|\Delta|}\right),$$

où la sommation est étendue à tous les $\frac{1}{2}\varphi(|\Delta|)$ nombres $g = \frac{1}{4}(a^* + |\Delta|)$; on voit que ces nombres sont incongrus modulo $|\Delta|$; on a encore $(g, |\Delta|) = 1$ et $\left(\frac{g}{|\Delta|}\right) = -1$.

En appliquant le lemme 4 on trouve

$$\beta_m = \tfrac{1}{2}\left[\mu(|\Delta|) - \left(\frac{m}{|\Delta|}\right)\sqrt{|\Delta|}\right],$$

lorsque $(m, |\Delta|) = 1$. Si $(m, |\Delta|) = d > 1$ on aura

$$\beta_m = \tfrac{1}{2}\mu\left(\frac{|\Delta|}{d}\right)\frac{\varphi(|\Delta|)}{\varphi\left(\frac{|\Delta|}{d}\right)}.$$

Par conséquent, lorsque $(m, |\Delta|) = 1$,

$$\xi_m = i^{-m}(\alpha_m + \beta_m) = (-1)^{\frac{1}{2}(m-1)}\left(\frac{m}{|\Delta|}\right)\sqrt{\Delta},$$

et, lorsque $(m, |\Delta|) > 1$,

$$\xi_m = i^{-m}(\alpha_m + \beta_m) = 0.$$

Deuxième cas. Soit Δ positif, donc $|\Delta| \equiv 3 \pmod 4$. Par un raisonnement analogue à celui qui précède on aura évidemment

$$\alpha_m = \sum_f E\left(\frac{fm}{\Delta}\right),$$

où la sommation est étendue à tous les $\frac{1}{2}\varphi(\Delta)$ nombres $f = \frac{1}{4}(a + \Delta)$; on voit que ces nombres sont incongrus modulo Δ; on a encore $(f, \Delta) = 1$ et $\left(\frac{f}{\Delta}\right) + = 1$. Donc, lorsque $(m, \Delta) = 1$,

$$\alpha_m = \tfrac{1}{2}\left[\mu(\Delta) + i\left(\frac{m}{\Delta}\right)\sqrt{\Delta}\right],$$

et, lorsque $(m, \Delta) = d > 1$,

$$\alpha_m = \tfrac{1}{2}\mu\left(\frac{\Delta}{d}\right)\frac{\varphi(\Delta)}{\varphi\left(\frac{\Delta}{d}\right)}.$$

Pour la deuxième somme on aura

$$-\beta_m = \sum_g E\left(\frac{gm}{\Delta}\right),$$

où la sommation est étendu à tous les $\frac{1}{2}\varphi(\Delta)$ nombres $g = \frac{1}{4}(a^* + 3\Delta)$; on voit que ces nombres sont incongrus modulo Δ; on a encore $(g, \Delta) = 1$ et $\left(\frac{g}{\Delta}\right) = -1$. Donc, lorsque $(m, \Delta) = 1$,

$$-\beta_m = \tfrac{1}{2}\left[\mu(\Delta) - i\left(\frac{m}{\Delta}\right)\sqrt{\Delta}\right],$$

et, lorsque $(m, \Delta) = d > 1$,

$$-\beta_m = \tfrac{1}{2}\mu\left(\frac{\Delta}{d}\right)\frac{\varphi(\Delta)}{\varphi\left(\frac{\Delta}{d}\right)}.$$

Par conséquent, on obtiendra, comme dans le premier cas,

$$\xi_m = (-1)^{\frac{1}{4}(m-1)} \left(\frac{m}{\Delta}\right) \sqrt{\Delta} \quad \text{ou} \quad \xi_m = 0,$$

selon que (m, Δ) est égal à 1 ou >1. Cela démontre le lemme 12.

Il résulte de ce lemme que tous les nombres ξ_m appartiennent au corps $\mathbf{K}(\sqrt{\Delta})$. On en conclut que toute fonction rationnelle symétrique, à coefficients rationnels des nombres $E\left(\frac{c}{4|\Delta|}\right)$, où c varie comme dans (46), appartient à $\mathbf{K}(\sqrt{\Delta})$. Le polynome $A_{4|\Delta|}(x; \Delta)$ étant irréductible dans $\mathbf{K}(\sqrt{\Delta})$, il est donc évident que les nombres $E\left(\frac{c}{4|\Delta|}\right)$ sont les zéros de ce polynome. Le théorème 5 se trouve ainsi démontré.

Considérons finalement les deux cas où $\Delta = +2$ et $\Delta = -2$. Vu qu'on ait

$$A_8(x; 2) = x^2 - \sqrt{2}x + 1 = (x - e^{\frac{1}{4}\pi i})(x - e^{-\frac{1}{4}\pi i})$$

et

$$A_8(x; -2) = x^2 - \sqrt{-2}x + 1 = (x - e^{\frac{1}{4}\pi i})(x - e^{\frac{3}{4}\pi i}),$$

les théorèmes 6 et 7 sont vrais pour l'index $n = 8$. Alors, en vertu du lemme 11, ils sont vrais pour toutes les valeurs de l'index n.

16. Préliminaires sur le théorème 8. Pour démontrer le théorème 8 il suffit de l'établir pour le polynome $A_{4|\Delta|}(x; \Delta)$ où $\Delta \equiv 2 \pmod 8$. Considérons le nombre

$$\xi_m = \sum_c E\left(\frac{cm}{4|\Delta|}\right), \tag{49}$$

où la sommation est étendue à tous les nombres naturels c premiers $4|\Delta|$ et $<4|\Delta|$, tels qu'on ait $c \equiv \pm 1 \pmod 8$ lorsque $\left(\frac{c}{\frac{1}{2}|\Delta|}\right) = +1$, et $c \equiv \pm 3 \pmod 8$ lorsque $\left(\frac{c}{\frac{1}{2}|\Delta|}\right) = -1$. m signifie un nombre naturel quelconque. Le nombre total des nombres c est évidemment $= \frac{1}{2}\varphi(4|\Delta|)$.

Notre but dans ce numéro et les deux numéros suivants est d'établir le lemme suivant :

Lemme 13. 1°) *Lorsque m est impair et $(m, \frac{1}{2}|\Delta|) = 1$, on a*

$$\xi_m = \left(\frac{2}{m}\right)\left(\frac{m}{\frac{1}{2}|\Delta|}\right)\sqrt{\Delta}.$$

2°) *Lorsque m est impair et $(m, \frac{1}{2}|\Delta|) = d > 1$, on a*

$$\xi_m = 0.$$

3°) *Lorsque $m \equiv 2 \pmod 4$, on a*

$$\xi_m = 0.$$

4°) *Lorsque $m \equiv 0 \pmod 4$ et $(m, \frac{1}{2}|\Delta|) = d \geqslant 1$, on a*

$$\xi_m = 2(-1)^{\frac{1}{4}m} \cdot \mu\left(\frac{\frac{1}{2}|\Delta|}{d}\right) \frac{\varphi(\frac{1}{2}|\Delta|)}{\varphi\left(\frac{\frac{1}{2}|\Delta|}{d}\right)}.$$

Le théorème 8 est une conséquence immédiate de ce lemme. En effet, il en résulte que tous les nombres ξ_m appartiennent au corps $\mathbf{K}(\sqrt{\Delta})$. On en conclut que toute fonction rationnelle symétrique, à coefficients rationnels des nombres $E\left(\frac{c}{4|\Delta|}\right)$, où c varie comme dans (49), appartient à $\mathbf{K}(\sqrt{\Delta})$. Par consequent, le polynome $A_{4|\Delta|}(x;\Delta)$ étant irréductible dans $\mathbf{K}(\sqrt{\Delta})$, il est évident que les nombres $E\left(\frac{c}{4|\Delta|}\right)$ sont les zéros de ce polynome.

Dans la démonstration du lemme 13 il faut distinguer les quatre cas suivants : 1°) $\Delta\equiv 10 \pmod{16}$ et $\Delta>0$; 2°) $\Delta\equiv 10 \pmod{16}$ et $\Delta<0$; 3°) $\Delta\equiv 2 \pmod{16}$ et $\Delta>2$; 4°) $\Delta\equiv 2 \pmod{16}$ et $\Delta<0$.

Supposons que m est impair. En multipliant ξ_m par $e^{\frac{1}{4}\pi i m}+e^{-\frac{1}{4}\pi i m}$ nous obtenons

$$2\cos\tfrac{1}{4}\pi m\cdot\xi_m=\sum_{k=1}^{8}\sum_k^{(m)}, \tag{50}$$

où $\sum_k^{(m)}$ signifie

$$\sum_c E\left(\frac{c+\frac{1}{2}|\Delta|}{4|\Delta|}m\right) \quad \text{ou} \quad \sum_c E\left(\frac{c-\frac{1}{2}|\Delta|}{4|\Delta|}m\right)$$

selon que $k=1,2,3,4$ ou $k=5,6,7,8$, et où les sommes sont étendues aux valeurs de $c\equiv 1 \pmod 8$ pour $k=1$ et 5, aux valeurs de $c\equiv -1 \pmod 8$ pour $k=2$ et 6, aux valeurs de $c\equiv 3 \pmod 8$ pour $k=3$ et 7, aux valeurs de $c\equiv -3 \pmod 8$ pour $k=4$ et 8. Le nombre des termes dans $\sum_k^{(m)}$ est $=\frac{1}{8}\varphi(4|\Delta|)=\frac{1}{2}\varphi(|\Delta|)=\frac{1}{2}\varphi(\frac{1}{2}|\Delta|)$.

Nous avons besoin du lemme suivant :

Lemme 14. 1°) *Lorsque* $\Delta\equiv 10 \pmod{16}$ *et* $\Delta>0$, *on a*

$$\sum_3^{(m)}=\sum_8^{(m)}=\sum_f E\left(\frac{fm}{\frac{1}{2}|\Delta|}\right), \tag{51}$$

$$\sum_2^{(m)}=\sum_5^{(m)}=\sum_f E\left(\frac{fm}{|\Delta|}\right). \tag{52}$$

2°) *Lorsque* $\Delta\equiv 10 \pmod{16}$ *et* $\Delta<0$, *on a*

$$\sum_4^{(m)}=\sum_7^{(m)}=\sum_f E\left(\frac{fm}{\frac{1}{2}|\Delta|}\right), \tag{53}$$

$$\sum_1^{(m)}=\sum_6^{(m)}=\sum_f E\left(\frac{fm}{|\Delta|}\right). \tag{54}$$

3°) *Lorsque* $\Delta\equiv 2 \pmod{16}$ *et* $\Delta>0$, *on a*

$$\sum_2^{(m)}=\sum_5^{(m)}=\sum_f E\left(\frac{fm}{\frac{1}{2}|\Delta|}\right), \tag{55}$$

$$\sum_3^{(m)}=\sum_8^{(m)}=\sum_g E\left(\frac{gm}{|\Delta|}\right). \tag{56}$$

4°) *Lorsque* $\Delta\equiv 2 \pmod{16}$ *et* $\Delta<0$, *on a*

$$\sum_1^{(m)}=\sum_6^{(m)}=\sum_f E\left(\frac{fm}{\frac{1}{2}|\Delta|}\right), \tag{57}$$

$$\sum_4^{(m)} = \sum_7^{(m)} = \sum_g E\left(\frac{gm}{|\Delta|}\right). \tag{58}$$

Ici les sommes dans (51), (53), (55) *et* (57) *sont étendues à tous les nombres naturels* $f < \frac{1}{2}|\Delta|$ *pour lesquels* $\left(\frac{f}{\frac{1}{2}|\Delta|}\right) = +1$. *Les sommes dans* (52) *et* (54) *sont étendues à tous les nombres naturels* f *premiers à* $|\Delta|$ *et* $< |\Delta|$ *pour lesquels* $\left(\frac{f}{\frac{1}{2}|\Delta|}\right) = +1$. *Les sommes dans* (56) *et* (58) *sont étendues à tous les nombres naturels* g *premiers à* $|\Delta|$ *et* $< |\Delta|$ *pour lesquels* $\left(\frac{g}{\frac{1}{2}|\Delta|}\right) = -1$.

Démonstration. Considérons d'abord le cas où $\Delta \equiv 10 \pmod{16}$ et $\Delta > 0$. Dans la somme

$$\sum_3^{(m)} = \sum_{c \equiv 3(8)} E\left(\frac{c + \frac{1}{2}|\Delta|}{4|\Delta|} m\right) = \sum_f E\left(\frac{fm}{\frac{1}{2}|\Delta|}\right)$$

les nombres $f = \frac{1}{8}(c + \frac{1}{2}|\Delta|)$ sont des entiers premiers à $\frac{1}{2}|\Delta|$ et incongrus modulo $\frac{1}{2}|\Delta|$, et leur nombre total est $= \frac{1}{2}\varphi(\frac{1}{2}|\Delta|)$. On a encore

$$\left(\frac{f}{\frac{1}{2}|\Delta|}\right) = \left(\frac{2c}{\frac{1}{2}|\Delta|}\right) = -\left(\frac{2}{\frac{1}{2}|\Delta|}\right) = +1.$$

Par un raisonnement analogue on trouve que la somme

$$\sum_8^{(m)} = \sum_{c \equiv -3(8)} E\left(\frac{c - \frac{1}{2}|\Delta|}{4|\Delta|} m\right)$$

a la même valeur que $\sum_3^m$.

Dans la somme

$$\sum_2^{(m)} = \sum_{c \equiv -1(8)} E\left(\frac{c + \frac{1}{2}|\Delta|}{4|\Delta|} m\right) = \sum_f E\left(\frac{fm}{|\Delta|}\right)$$

les nombres $f = \frac{1}{4}(c + \frac{1}{2}|\Delta|)$ sont des entiers premiers à $|\Delta|$ et incongrus modulo $|\Delta|$, et leur nombre total est $= \frac{1}{2}\varphi(\frac{1}{2}|\Delta|)$. On a encore

$$\left(\frac{f}{\frac{1}{2}|\Delta|}\right) = \left(\frac{c}{\frac{1}{2}|\Delta|}\right) = +1.$$

Par un raisonnement analogue on trouve que la somme

$$\sum_5^{(m)} = \sum_{c \equiv 1(8)} E\left(\frac{c - \frac{1}{2}|\Delta|}{4|\Delta|} m\right)$$

a la même valeur que $\sum_2^{(m)}$.

Considérons ensuite le cas où $\Delta \equiv 10 \pmod{16}$ et $\Delta < 0$. Dans la somme

$$\sum_4^{(m)} = \sum_{c \equiv -3(8)} E\left(\frac{c + \frac{1}{2}|\Delta|}{4|\Delta|} m\right) = \sum_f E\left(\frac{fm}{\frac{1}{2}|\Delta|}\right)$$

les nombres $f = \frac{1}{8}(c + \frac{1}{2}|\Delta|)$ sont des entiers premiers à $\frac{1}{2}|\Delta|$ et incongrus modulo $\frac{1}{2}|\Delta|$; leur nombre total est $= \frac{1}{2}\varphi(\frac{1}{2}|\Delta|)$. On a encore

$$\left(\frac{f}{\frac{1}{2}|\Delta|}\right)=\left(\frac{2c}{\frac{1}{2}|\Delta|}\right)=-\left(\frac{2}{\frac{1}{2}|\Delta|}\right)=+1.$$

Par un raisonnement analogue on trouve que la somme

$$\sum_7^{(m)}=\sum_{c\equiv 3(8)} E\left(\frac{c-\frac{1}{2}|\Delta|}{4|\Delta|}m\right)$$

a la même valeur que $\sum_4^{(m)}$.

Dans la somme

$$\sum_1^{(m)}=\sum_{c\equiv 1(8)} E\left(\frac{c+\frac{1}{2}|\Delta|}{4|\Delta|}m\right)=\sum_f E\left(\frac{fm}{|\Delta|}\right)$$

les nombres $f=\frac{1}{4}(c+\frac{1}{2}|\Delta|)$ sont des entiers premiers à $|\Delta|$ et incongrus modulo $\Delta|$; et leur nombre total est $=\frac{1}{2}\varphi(4|\Delta|)$. On a encore

$$\left(\frac{f}{\frac{1}{2}|\Delta|}\right)=\left(\frac{c}{\frac{1}{2}|\Delta|}\right)=+1.$$

Par un raisonnement analogue on trouve que la somme

$$\sum_6^{(m)}=\sum_{c\equiv -1(8)} E\left(\frac{c-\frac{1}{2}|\Delta|}{4|\Delta|}m\right)$$

a la même valeur que $\sum_1^{(m)}$.

Considérons le cas où $\Delta\equiv 2 \pmod{16}$ et $\Delta>0$. Dans la somme

$$\sum_2^{(m)}=\sum_{c\equiv -1(8)} E\left(\frac{c+\frac{1}{2}|\Delta|}{4|\Delta|}m\right)=\sum_f E\left(\frac{fm}{\frac{1}{2}|\Delta|}\right)$$

les nombres $f=\frac{1}{8}(c+\frac{1}{2}|\Delta|)$ sont des entiers premiers à $\frac{1}{2}|\Delta|$ et incongrus modulo $\frac{1}{2}|\Delta|$; leur nombre total est $=\frac{1}{2}\varphi(\frac{1}{2}|\Delta|)$. On a encore

$$\left(\frac{f}{\frac{1}{2}|\Delta|}\right)=\left(\frac{2c}{\frac{1}{2}|\Delta|}\right)=\left(\frac{2}{\frac{1}{2}|\Delta|}\right)=+1.$$

Par un raisonnement analogue on trouve que la somme

$$\sum_5^{(m)}=\sum_{c\equiv 1(8)} E\left(\frac{c-\frac{1}{2}|\Delta|}{4|\Delta|}m\right)$$

a la même valeur que $\sum_2^{(m)}$.

Dans la somme

$$\sum_3^{(m)}=\sum_{c\equiv 3(8)} E\left(\frac{c+\frac{1}{2}|\Delta|}{4|\Delta|}m\right)=\sum_g E\left(\frac{gm}{|\Delta|}\right)$$

les nombres $g=\frac{1}{4}(c+\frac{1}{2}|\Delta|)$ sont des entiers premiers à $|\Delta|$ et incongrus modulo $|\Delta|$; et leur nombre total est $=\frac{1}{2}\varphi(4|\Delta|)$. On a encore

$$\left(\frac{g}{\frac{1}{2}|\Delta|}\right)=\left(\frac{c}{\frac{1}{2}|\Delta|}\right)=-1.$$

Par un raisonnement analogue on trouve que la somme

$$\sum_8^{(m)} = \sum_{c \equiv -3 (8)} E\left(\frac{c - \frac{1}{2}|\Delta|}{4|\Delta|} m\right)$$

a la même valeur que $\sum_3^{(m)}$.

Considérons finalement le cas où $\Delta \equiv 2 \pmod{16}$ et $\Delta < 0$. Dans la somme

$$\sum_1^{(m)} = \sum_{c \equiv 1 (8)} E\left(\frac{c + \frac{1}{2}|\Delta|}{4|\Delta|} m\right) = \sum_f E\left(\frac{fm}{\frac{1}{2}|\Delta|}\right)$$

les nombres $f = \frac{1}{8}(c + \frac{1}{2}|\Delta|)$ sont des entiers premiers à $\frac{1}{2}|\Delta|$ et incongrus modulo $\frac{1}{2}|\Delta|$; leur nombre total est $= \frac{1}{2}\varphi(\frac{1}{2}|\Delta|)$. On a encore

$$\left(\frac{f}{\frac{1}{2}|\Delta|}\right) = \left(\frac{2c}{\frac{1}{2}|\Delta|}\right) = \left(\frac{2}{\frac{1}{2}|\Delta|}\right) = +1.$$

Par un raisonnement analogue on trouve que la somme

$$\sum_6^{(m)} = \sum_{c \equiv -1 (8)} E\left(\frac{c - \frac{1}{2}|\Delta|}{4|\Delta|} m\right)$$

a la même valeur que $\sum_1^{(m)}$.

Dans la somme

$$\sum_4^{(m)} = \sum_{c \equiv -3 (8)} E\left(\frac{c + \frac{1}{2}|\Delta|}{4|\Delta|} m\right) = \sum_g E\left(\frac{gm}{|\Delta|}\right)$$

les nombres $g = \frac{1}{4}(c + \frac{1}{2}|\Delta|)$ sont des entiers premiers à $|\Delta|$ et incongrus modulo $|\Delta|$; et leur nombre total est $= \frac{1}{2}\varphi(4|\Delta|)$. On a encore

$$\left(\frac{g}{\frac{1}{2}|\Delta|}\right) = \left(\frac{c}{\frac{1}{2}|\Delta|}\right) = -1.$$

Par un raisonnement analogue on trouve que la somme

$$\sum_7^{(m)} = \sum_{c \equiv 3 (8)} E\left(\frac{c - \frac{1}{2}|\Delta|}{4|\Delta|} m\right)$$

a la même valeur que $\sum_4^{(m)}$.

Lemme 15. *Désignons par S la somme*

$$\sum_b E\left(\frac{bm}{2|\Delta|}\right),$$

où b parcourt un système réduit de résidus modulo $2|\Delta|$. *Alors, pour* Δ *positif, la somme*

$$\sum_1^{(m)} + \sum_4^{(m)} + \sum_6^{(m)} + \sum_7^{(m)} \tag{59}$$

est égale à S. Encore, pour Δ *négatif, la somme*

$$\sum_2^{(m)} + \sum_3^{(m)} + \sum_5^{(m)} + \sum_8^{(m)} \tag{60}$$

est égale à S. Quand m est impair on a $S = 0$.

Démonstration. On vérifie aisément que, pour toutes les valeurs de c qui entrent dans la somme (59), pour $\Delta > 0$, ou dans la somme (60), pour $\Delta < 0$, tous les nombres $b = \frac{1}{2}(c + \frac{1}{2}|\Delta|)$ et $b^* = \frac{1}{2}(c^* - \frac{1}{2}|\Delta|)$ sont premiers à $2|\Delta|$. De plus, ils sont incongrus modulo $2|\Delta|$. En effet, c et c^* étant supposés incongrus modulo $4|\Delta|$, les nombres $\frac{1}{2}(c + \frac{1}{2}|\Delta|)$ et $\frac{1}{2}(c^* + \frac{1}{2}|\Delta|)$ ne peuvent pas être congrus modulo $2|\Delta|$. Supposons qu'on ait

$$\tfrac{1}{2}(c + \tfrac{1}{2}|\Delta|) \equiv \tfrac{1}{2}(c^* - \tfrac{1}{2}|\Delta|) \pmod{2|\Delta|}.$$

Cette congruence entraine $c \equiv c^* \pmod{\frac{1}{2}|\Delta|}$. et par suite $\left(\frac{c}{\frac{1}{2}|\Delta|}\right) = \left(\frac{c^*}{\frac{1}{2}|\Delta|}\right)$, donc $c \equiv \pm c^* \pmod 8$. Le signe supérieur étant impossible il faut que $c \equiv -c^* \pmod 8$. Lorsque $\Delta > 0$ on aurait les possibilités suivantes: $c \equiv 1 \pmod 8$ correspondant à $c^* \equiv -1 \pmod 8$; $c \equiv -3 \pmod 8$ correspondant à $c^* \equiv 3 \pmod 8$. Cela entraînerait ou $1 + \frac{1}{2}|\Delta| \equiv 0 \pmod 4$ ou $-3 + \frac{1}{2}|\Delta| \equiv 0 \pmod 4$, ce qui est impossible. Lorsque $\Delta < 0$ on aurait les possibilités : $c \equiv -1 \pmod 8$ correspondant à $c^* \equiv 1 \pmod 8$; $c \equiv 3 \pmod 8$ correspondant à $c^* \equiv -3 \pmod 8$. Cela entraînerait ou $-1 + \frac{1}{2}|\Delta| \equiv 0 \pmod 4$ ou $3 + \frac{1}{2}|\Delta| \equiv 0 \pmod 4$, ce qui est impossible. Enfin, le nombre total des nombres b est $= \varphi(2|\Delta|)$. Cela démontre la première partie du lemme 15. Soit $(m, 2|\Delta|) = d$. D'après la formule (12) du numéro 4 on a évidemment

$$S = \mu\left(\frac{2|\Delta|}{d}\right) \frac{\varphi(2|\Delta|)}{\varphi\left(\frac{2|\Delta|}{d}\right)}.$$

Si m est impair, d est aussi impair, et par conséquent $S = 0$.

17. Démonstration du lemme 13 dans le cas où *m* est pair. Si $m = 4s$ on a

$$\xi_m = \sum_c E\left(\frac{cm}{4|\Delta|}\right) = \sum_c E\left(\frac{cs}{|\Delta|}\right), \tag{61}$$

où la somme est étendue comme dans la formule (49). Supposons d'abord que s est impair et multiplions par $-1 = e^{\pi i s}$; nous aurons

$$-\xi_m = \sum_c E\left(\frac{c + \frac{1}{2}|\Delta|}{|\Delta|} s\right),$$

où tous les nombres $c + \frac{1}{2}|\Delta|$ sont pairs. Considérons la congruence

$$\tfrac{1}{2}(c + \tfrac{1}{2}|\Delta|) \equiv \tfrac{1}{2}(c^* + \tfrac{1}{2}|\Delta|) \pmod{\tfrac{1}{2}|\Delta|}. \tag{62}$$

Celle-ci entraîne $c \equiv c^* \pmod{\frac{1}{2}|\Delta|}$. En vertu des propriétés des nombres c il en résulte que $c \equiv \pm c^* \pmod 8$. Vu que c et c^* sont incongrus modulo $4|\Delta|$, il faut prendre le signe inférieur, donc $c \equiv -c^* \pmod 8$. En posant dans (62) $c = 8t + r$ et $c^* = 8t^* - r$ on obtient la congruence

$$4(t-t^*)+r\equiv 0 \pmod{\tfrac{1}{2}|\Delta|},$$

où $r=\pm 1$ ou $=\pm 3$. On en conclut que à chaque valeur de c correspond exactement une valeur de c^* telle que la congruence (62) soit satisfaite et telle que c^* ne soit pas congru à c modulo $4|\Delta|$. Ainsi le nombre des nombres $g=\frac{1}{2}(c+\frac{1}{2}|\Delta|)$ qui sont incongrus modulo $\frac{1}{2}|\Delta|$, est $=\frac{1}{2}\varphi(2|\Delta|)=\varphi(\frac{1}{2}|\Delta|)$. Par conséquent, nous aurons

$$-\xi_m=2\sum_g E\left(\frac{gs}{\frac{1}{2}|\Delta|}\right), \tag{63}$$

où g parcourt un système réduit de résidus modulo $\frac{1}{2}|\Delta|$. En appliquant la formule (12) on obtient donc

$$\xi_m=-2\mu\left(\tfrac{1}{2}\frac{|\Delta|}{d}\right)\frac{\varphi(\frac{1}{2}|\Delta|)}{\varphi\left(\frac{1}{2}\frac{|\Delta|}{d}\right)},$$

où $d=(m,\frac{1}{2}|\Delta|)$.

Considérons ensuite le cas où s est pair dans (61). Nous allons montrer qu'on a

$$\xi_m=2\sum_b E\left(\frac{b}{\frac{1}{2}|\Delta|}\cdot\tfrac{1}{2}s\right), \tag{64}$$

où b parcourt un système réduit de résidus modulo $\frac{1}{2}|\Delta|$.

Nous pouvons supposer que tous les nombres b sont impairs. Dans un système réduit de résidus modulo $4|\Delta|$ il y a exactement quatre nombres qui sont congrus à un nombre fixe b modulo $\frac{1}{2}|\Delta|$. On peut supposer que ces nombres (classes de résidus modulo $4|\Delta|$) sont représentés par les nombres

$$x,\ x-|\Delta|,\ x+|\Delta|,\ x+2|\Delta|, \tag{65}$$

x parcourant un système réduit de résidus modulo $\frac{1}{2}|\Delta|$. Ceux-ci sont tous impairs et incongrus modulo 8. Exactement deux de ces nombres appartiennent au système des nombres c satisfaisant aux conditions de la somme (61). En effet, si $\left(\frac{b}{\frac{1}{2}|\Delta|}\right)=+1$ il y a parmi les nombres (65) un seul qui est $\equiv +1 \pmod 8$ et un seul qui est $\equiv -1 \pmod 8$; les deux autres sont congrus à $+3$ ou à $-3 \pmod 8$. On peut faire le même raisonnement quand $\left(\frac{b}{\frac{1}{2}|\Delta|}\right)=-1$. Ainsi la congruence $b\equiv c \pmod{\frac{1}{2}|\Delta|}$ est satisfaite par deux nombres c lorsque b est fixe. Cela démontre la formule (64).

En appliquant la formule (12) à l'expression de ξ_m donnée par (64) on aura

$$\xi_m=2\mu\left(\tfrac{1}{2}\frac{|\Delta|}{d}\right)\frac{\varphi(\frac{1}{2}|\Delta|)}{\varphi\left(\frac{1}{2}\frac{|\Delta|}{d}\right)},$$

où $d=(m,\frac{1}{2}|\Delta|)$.

Considérons enfin le cas où $m\equiv 2 \pmod 4$. En posant $m=2s$ on a

$$\xi_m=\sum_c E\left(\frac{cs}{2|\Delta|}\right), \tag{65}$$

où s est impair, et où la sommation est comme dans la formule (61). En multipliant par $i^s=e^{\frac{1}{2}\pi i s}$ on aura

$$i^s\xi_m = \sum_c E\left(\frac{c+\frac{1}{2}|\Delta|}{2|\Delta|}s\right) + \sum_{c^*} E\left(\frac{c^*+\frac{1}{2}|\Delta|}{2|\Delta|}s\right),$$

où la première somme est étendue à tous les nombres c tels que $c+\frac{1}{2}|\Delta| \equiv 0 \pmod 4$, tandis que la deuxième somme est étendue à tous les nombres c^* tels que $c^*+\frac{1}{2}|\Delta| \equiv 2 \pmod 4$. Désignons la première somme par α et la seconde somme par β. Considérons les termes dans la somme α. On peut montrer que la relation

$$\tfrac{1}{4}(c+\tfrac{1}{2}|\Delta|) \equiv \tfrac{1}{4}(c_1+\tfrac{1}{2}|\Delta|) \pmod{\tfrac{1}{2}|\Delta|}$$

n'a jamais lieu. En effet, celle-ci entraînerait $c \equiv c_1 \pmod{2|\Delta|}$, donc $c_1 \equiv c+2|\Delta| \pmod{4|\Delta|}$. Or, il en résulterait que $c_1 \equiv c+4 \pmod 8$, ce qui est impossible, vu que $c_1 \equiv \pm c \pmod 8$ lorsque $\left(\frac{c}{\frac{1}{2}|\Delta|}\right) = \left(\frac{c_1}{\frac{1}{2}|\Delta|}\right)$.

Donc, les nombres $f = \frac{1}{4}(c+\frac{1}{2}|\Delta|)$ sont incongrus modulo $\frac{1}{2}|\Delta|$, et le nombre total de ces nombres est $= \frac{1}{4}\varphi(4|\Delta|) = \varphi(\frac{1}{2}|\Delta|)$. Ainsi on aura

$$\alpha = \sum_f E\left(\frac{fs}{\frac{1}{2}|\Delta|}\right), \tag{66}$$

où f parcourt un système réduit de résidus modulo $\frac{1}{2}|\Delta|$.

Considérons ensuite la somme β. En multipliant par $-1 = e^{\pi i s}$ nous aurons

$$-\beta = \sum_{c^*} E\left(\frac{c^*+\frac{3}{2}|\Delta|}{2|\Delta|}s\right).$$

Ici les nombres $f^* = \frac{1}{4}(c^*+\frac{3}{2}|\Delta|)$ sont entiers et incongrus modulo $\frac{1}{2}|\Delta|$, ce qui peut être vérifié de la même manière que tout à l'heure. Il en résulte $\beta = -\alpha$. Par conséquent, pour $m \equiv 2 \pmod 4$, on a $\xi_m = 0$.

En résumant, nous avons démontré le lemme 13 pour toutes les valeurs de m.

18. Démonstration du lemme 13 dans le cas où m est impair. Dans les formules (51), (53), (55) et (57) du lemme 14 figure la somme

$$\sum_f E\left(\frac{fm}{\frac{1}{2}|\Delta|}\right)$$

étendue à tous les nombres f d'un système réduit de résidus modulo $\frac{1}{2}|\Delta|$ pour lesquels $\left(\frac{f}{\frac{1}{2}|\Delta|}\right) = +1$. D'après le lemme 4 cette somme est égale à

$$\tfrac{1}{2}\left[\mu(\tfrac{1}{2}|\Delta|) + \left(\frac{m}{\frac{1}{2}|\Delta|}\right)\varrho\sqrt{\tfrac{1}{2}|\Delta|}\right],$$

lorsque $(m, \frac{1}{2}|\Delta|) = 1$, ϱ signifiant 1 ou i selon que $\frac{1}{2}|\Delta|$ est $\equiv +1$ ou $\equiv -1 \pmod 4$. Lorsque $(m, \frac{1}{2}|\Delta|) = d > 1$ la somme a la valeur

$$\tfrac{1}{2}\mu\left(\tfrac{1}{2}\frac{|\Delta|}{d}\right) \cdot \frac{\varphi(\frac{1}{2}|\Delta|)}{\varphi\left(\frac{1}{2}\frac{|\Delta|}{d}\right)}.$$

Dans les formules (52) et (54) du lemme 14 figure la somme

$$\sum_f E\left(\frac{fm}{|\Delta|}\right) \tag{67}$$

étendue à tous les nombres $f=\frac{1}{4}(c+\frac{1}{2}|\Delta|)$ d'un système réduit de résidus modulo $|\Delta|$ pour lesquels $\left(\frac{f}{\frac{1}{2}|\Delta|}\right)=+1$. On doit observer qu'on a $c\equiv -1 \pmod 8$ quand $\frac{1}{2}|\Delta|\equiv -3 \pmod 8$, et $c\equiv +1 \pmod 8$ quand $\frac{1}{2}|\Delta|\equiv +3 \pmod 8$. Pour calculer la somme (67) nous multiplions par $-1=e^{\pi i m}$. Alors la somme prendra la forme

$$\sum_c E\left(\frac{c+\frac{5}{2}|\Delta|}{4|\Delta|}m\right).$$

Ici les nombres $g=\frac{1}{8}(c+\frac{5}{2}|\Delta|)$ sont évidemment entiers et premiers à $\frac{1}{2}|\Delta|$. De plus, ces nombres sont incongrus modulo $\frac{1}{2}|\Delta|$. En effet, la congruence

$$\tfrac{1}{8}(c+\tfrac{5}{2}|\Delta|)\equiv\tfrac{1}{8}(c^*+\tfrac{5}{2}|\Delta|) \pmod{\tfrac{1}{2}|\Delta|}$$

entraînerait $c\equiv c^* \pmod{4|\Delta|}$. On a en outre

$$\left(\frac{g}{\frac{1}{2}|\Delta|}\right)=\left(\frac{2f}{\frac{1}{2}|\Delta|}\right)=\left(\frac{2c}{\frac{1}{2}|\Delta|}\right)=\left(\frac{2}{\frac{1}{2}|\Delta|}\right)=-1,$$

puisque $\frac{1}{2}|\Delta|\equiv \pm 3 \pmod 8$. Il en résulte que la somme (67) est égale à

$$-\sum_g E\left(\frac{gm}{\frac{1}{2}|\Delta|}\right),$$

où la somme est étendue à tous les nombres g d'un système réduit de résidus modulo $\frac{1}{2}|\Delta|$ pour lesquels $\left(\frac{g}{\frac{1}{2}|\Delta|}\right)=-1$. En appliquant le lemme 4 on aura donc les valeurs suivantes pour la somme (67) :

Lorsque $(m, \frac{1}{2}|\Delta|)=1$,

$$\tfrac{1}{2}\left[-\mu(\tfrac{1}{2}|\Delta|)+\left(\frac{m}{\frac{1}{2}|\Delta|}\right)\varrho\sqrt{\tfrac{1}{2}|\Delta|}\right],$$

où ϱ signifie 1 ou i selon que $\frac{1}{2}|\Delta|\equiv +1$ ou $\equiv -1 \pmod 4$.

Lorsque $(m, \frac{1}{2}|\Delta|)=d>1$,

$$-\tfrac{1}{2}\mu\left(\tfrac{1}{2}\frac{|\Delta|}{d}\right)\cdot\frac{\varphi(\frac{1}{2}|\Delta|)}{\varphi\left(\frac{1}{2}\frac{|\Delta|}{d}\right)}.$$

Dans les formules (56) et (58) du lemme 14 figure la somme

$$\sum_g E\left(\frac{gm}{|\Delta|}\right) \tag{68}$$

étendue à tous les nombres $g=\frac{1}{4}(c-\frac{1}{2}|\Delta|)$ d'un système réduit de résidus modulo $|\Delta|$ pour lesquels $\left(\frac{g}{\frac{1}{2}|\Delta|}\right)=-1$. On doit observer qu'on a $c\equiv +3 \pmod 8$ quand

$\frac{1}{2}|\Delta| \equiv +1 \pmod 8$ et $c \equiv -3$ quand $\frac{1}{2}|\Delta| \equiv -1 \pmod 8$. Pour calculer la somme (68) nous multiplions par $-1 = e^{\pi i m}$. Alors la somme prendra la forme

$$\sum_c E\left(\frac{c+\frac{3}{2}|\Delta|}{4|\Delta|} m\right).$$

Ici les nombres $h = \frac{1}{8}(c+\frac{3}{2}|\Delta|)$ sont évidemment entiers et premiers à $\frac{1}{2}|\Delta|$. De plus, ces nombres sont incongrus modulo $\frac{1}{2}|\Delta|$. En effet, la congruence

$$\tfrac{1}{8}(c+\tfrac{3}{2}|\Delta| \equiv \tfrac{1}{8}(c^*+\tfrac{3}{2}|\Delta|) \pmod{\tfrac{1}{2}|\Delta|}$$

entrainerait $c \equiv c^* \pmod{4|\Delta|}$. On a encore

$$\left(\frac{h}{\frac{1}{2}|\Delta|}\right) = \left(\frac{2g}{\frac{1}{2}|\Delta|}\right) = \left(\frac{2c}{\frac{1}{2}|\Delta|}\right) = -\left(\frac{2}{\frac{1}{2}|\Delta|}\right) = -1,$$

puisque $\frac{1}{2}|\Delta| \equiv \pm 1 \pmod 8$. Il en résulte que la somme est égale à

$$-\sum_h E\left(\frac{hm}{\frac{1}{2}|\Delta|}\right),$$

où la somme est étendue à tous les nombres h d'un système réduit de résidus modulo $\frac{1}{2}|\Delta|$ pour lesquels $\left(\frac{h}{\frac{1}{2}|\Delta|}\right) = -1$. En appliquant le lemme 4 on aura donc les valeurs suivantes pour la somme (67) :

Lorsque $(m, \frac{1}{2}|\Delta|) = 1$,

$$\tfrac{1}{2}\left[-\mu(\tfrac{1}{2}|\Delta|) + \left(\frac{m}{\frac{1}{2}|\Delta|}\right)\varrho\sqrt{\tfrac{1}{2}|\Delta|}\right],$$

où ϱ signifie 1 ou i selon que $\frac{1}{2}|\Delta| \equiv +1$ ou $\equiv -1 \pmod 4$.

Lorsque $(m, \frac{1}{2}|\Delta|) = d > 1$,

$$-\tfrac{1}{2}\mu\left(\tfrac{1}{2}\frac{|\Delta|}{d}\right) \cdot \frac{\varphi(\frac{1}{2}|\Delta|)}{\varphi\left(\frac{1}{2}\frac{|\Delta|}{d}\right)}.$$

En combinant les résultats de ce numéro avec les résultats du numéro 16, et en se rappelant que $2\cos\frac{1}{4}\pi m = \left(\frac{2}{m}\right)\sqrt{2}$ pour m impair, on obtient de la relation (50) :

$$\sqrt{2}\left(\frac{2}{m}\right)\xi_m = 2\left(\frac{m}{\frac{1}{2}|\Delta|}\right)\varrho\sqrt{\tfrac{1}{2}|\Delta|},$$

quand $(m, \frac{1}{2}|\Delta|) = 1$, et

$$\sqrt{2}\left(\frac{2}{m}\right)\xi_m = 0,$$

quand $(m, \frac{1}{2}|\Delta|) > 1$.

Le lemme 13 se trouve ainsi établi pour toutes les valeurs de m, attendu que le cas où m est pair a déjà été traité complètement dans le numéro 17. Par conséquent, la demonstration du théorème 8 est achevée.

19. Démonstration du théorème 9. Pour démontrer le théorème 9 il suffit de l'établir pour le polynome $A_{4|\Delta|}(x;\Delta)$ où $\Delta \equiv -2 \pmod 8$. Considérons le nombre

$$\eta_m = \sum_a E\left(\frac{am}{4|\Delta|}\right), \tag{69}$$

où la sommation est étendue à tous les nombres naturels a premiers á $4|\Delta|$ et $<4|\Delta|$, tels qu'on ait $a \equiv +1$ ou $\equiv +3 \pmod 8$ lorsque $\left(\frac{a}{\frac{1}{2}|\Delta|}\right) = +1$, et $a \equiv -1$ ou $\equiv -3 \pmod 8$ lorsque $\left(\frac{a}{\frac{1}{2}|\Delta|}\right) = -1$. m signifie un nombre naturel quelconque. Le nombre total des nombres a est évidemment $= \frac{1}{2}\varphi(4|\Delta|)$.

Nous allons d'abord établir le résultat suivant analogue au lemme 13 :

Lemme 16. 1°) *Lorsque m est impair et $(m, \frac{1}{2}|\Delta|) = 1$, on a*

$$\eta_m = \left(\frac{-2}{m}\right)\left(\frac{m}{\frac{1}{2}|\Delta|}\right)\sqrt{\Delta}.$$

2°) *Lorsque m est impair et $(m, \frac{1}{2}|\Delta|) = d > 1$, on a*

$$\eta_m = 0.$$

3°) *Lorsque $m \equiv 2 \pmod 4$, on a*

$$\eta_m = 0.$$

4°) *Lorsque $m \equiv 0 \pmod 4$ et $(m, \frac{1}{2}|\Delta|) = d \geqslant 1$, on a*

$$\eta_m = 2(-1)^{\frac{1}{4}m} \cdot \mu\left(\frac{\frac{1}{2}|\Delta|}{d}\right) \cdot \frac{\varphi(\frac{1}{2}|\Delta|)}{\varphi\left(\frac{\frac{1}{2}|\Delta|}{d}\right)}.$$

Le théorème 9 est une conséquence immédiate de ce lemme. En effet, il en résulte que tous les nombres η_m appartiennent au corps $\mathbf{K}(\sqrt{\Delta})$. On en conclut que toute fonction rationnelle symétrique, à coefficients rationnels des nombres $E(a/4|\Delta|)$, où a varie comme dans (69), appartient à $\mathbf{K}(\sqrt{\Delta})$. Par conséquent, le polynome $A_{4|\Delta|}(x;\Delta)$ étant irréductible dans $\mathbf{K}(\sqrt{\Delta})$, il est évident que les nombres $E(a/4|\Delta|)$ sont les zéros de ce polynome.

Nous allons montrer comment le lemme 16 se déduit d'une manière très simple du lemme 13. Considérons d'abord le cas où Δ est positif. En multipliant dans (69) par i^m nous aurons

$$\eta_m i^m = \sum_c E\left(\frac{cm}{4|\Delta|}\right),$$

où $c = a + |\Delta|$. Lorsque $a \equiv +1 \pmod 8$ on aura $c \equiv 1 - 2 \equiv -1 \pmod 8$ et

$$\left(\frac{c}{\frac{1}{2}|\Delta|}\right) = \left(\frac{a}{\frac{1}{2}|\Delta|}\right) = +1.$$

Lorsque $a \equiv +3 \pmod 8$ on aura $c \equiv 3 - 2 \equiv +1 \pmod 8$ et

$$\left(\frac{c}{\frac{1}{2}|\Delta|}\right) = \left(\frac{a}{\frac{1}{2}|\Delta|}\right) = +1.$$

Lorsque $a \equiv -1 \pmod 8$ on aura $c \equiv -1-2 \equiv -3 \pmod 8$ et

$$\left(\frac{c}{\frac{1}{2}|\Delta|}\right) = \left(\frac{a}{\frac{1}{2}|\Delta|}\right) = -1.$$

Lorsque $a \equiv -3 \pmod 8$ on aura $c \equiv -3-2 \equiv +3 \pmod 8$ et

$$\left(\frac{c}{\frac{1}{2}|\Delta|}\right) = \left(\frac{a}{\frac{1}{2}|\Delta|}\right) = -1.$$

Il en résulte

$$\eta_m = i^{-m}\xi_m(-\Delta), \tag{70}$$

où $\xi_m(-\Delta)$ désigne le nombre défini par l'équation (49), lorsque Δ a été remplacé par $-\Delta$.

Considérons ensuite le cas où Δ est négatif. En multipliant dans (69) par i^{-m} nous aurons

$$\eta_m i^{-m} = \sum_c E\left(\frac{cm}{4|\Delta|}\right),$$

où $c = a - |\Delta|$. Lorsque $a \equiv +1 \pmod 8$ on aura $c \equiv 1-2 \equiv -1 \pmod 8$ et

$$\left(\frac{c}{\frac{1}{2}|\Delta|}\right) = \left(\frac{a}{\frac{1}{2}|\Delta|}\right) = +1.$$

Lorsque $a \equiv +3 \pmod 8$ on aura $c \equiv 3-2 \equiv +1 \pmod 8$ et

$$\left(\frac{c}{\frac{1}{2}|\Delta|}\right) = \left(\frac{a}{\frac{1}{2}|\Delta|}\right) = +1.$$

Lorsque $a \equiv -1 \pmod 8$ on aura $c \equiv -1-2 \equiv -3 \pmod 8$ et

$$\left(\frac{c}{\frac{1}{2}|\Delta|}\right) = \left(\frac{a}{\frac{1}{2}|\Delta|}\right) = -1.$$

Lorsque $a \equiv -3 \pmod 8$ on aura $c \equiv -3-2 \equiv +3 \pmod 8$ et

$$\left(\frac{c}{\frac{1}{2}|\Delta|}\right) = \left(\frac{a}{\frac{1}{2}|\Delta|}\right) = -1.$$

Il en résulte

$$\eta_m = i^{m}\xi_m(-\Delta), \tag{71}$$

où $\xi_m(-\Delta)$ désigne le nombre défini par l'équation (49), lorsque Δ a été remplacé par $-\Delta$.

Soit m impair et $(m, \frac{1}{2}|\Delta|) = 1$. Alors, en appliquant le lemme 13, on obtient de (70), pour $\Delta > 0$,

$$\eta_m = (-1)^{\frac{1}{4}(m-1)} i^{-1} \left(\frac{2}{m}\right)\left(\frac{m}{\frac{1}{2}|\Delta|}\right)\sqrt{-\Delta},$$

et de (71), pour $\Delta < 0$,

$$\eta_m = (-1)^{\frac{1}{2}(m-1)} i \left(\frac{2}{m}\right) \left(\frac{m}{\frac{1}{2}|\Delta|}\right) \sqrt{-\Delta},$$

c'est-à-dire, dans tous les deux cas,

$$\eta_m = \left(\frac{-2}{m}\right) \left(\frac{m}{\frac{1}{2}|\Delta|}\right) \sqrt{\Delta}.$$

Quand $m \equiv 0 \pmod 4$ on obtient $\eta_m = \xi_m(-\Delta) = \xi_m$ et dans tous les autres cas $\eta_m = 0$.

Le lemme 16 se trouve ainsi démontré et, par conséquent, aussi le théorème 9.

Supplément au numéro 11

20. Dans le numéro 11 nous avons exclu les cas où $\Delta = -1$ et $\Delta = -3$, vu que la méthode y adaptée ne suffisait pas pour déterminer le produit $\varepsilon_1 \varepsilon_2 \ldots \varepsilon_\nu$ des racines de $A(x) = 0$. En vertu des résultats des numéros 13 et 14 nous avons maintenant les moyens de déterminer ce produit dans les cas en question.

La formule (33) dans le numéro 11 est toujours valable (pour $\Delta < 0$) et peut s'écrire

$$A_n(x; \Delta) = \lambda_n x^\nu B_n(x^{-1}; \Delta), \tag{72}$$

où λ_n signifie le terme constant du polynome $A_n(x; \Delta)$ du degré $\frac{1}{2}\varphi(n) = \nu$. Il s'agit de déterminer λ_n. En vertu des formules (39) du numéro 13 nous avons évidemment

$$\lambda_{np} = \lambda_n \tag{73}$$

lorsque le nombre premier p divise n. Si p ne divise pas n nous obtenons des formules (43) et (44)

$$\lambda_{np} = \frac{\lambda_n}{\lambda_n} = 1, \tag{74}$$

lorsque la congruence (42) est résoluble, et

$$\lambda_{np} = \frac{\lambda_n}{\lambda_n'} = \lambda_n^2 \tag{75}$$

dans le cas contraire. Ici λ_n' signifie le nombre conjugué de λ_n dans le corps $\mathbf{K}(\sqrt{\Delta})$, donc $\lambda_n \lambda_n' = 1$ vu que $\Delta < 0$.

Lorsque $\Delta = -3$, n est divisible par 3. Lorsque $\Delta = -1$, n est divisible par 4.

Le cas où $\Delta = -1$.

Nous avons $A_4(x; -1) = x - i$, donc $\lambda_4 = -i$. Ainsi, il résulte de (73) que $\lambda_N = -i$ lorsque N est une puissance de 2.

Si dans la congruence (42) $n = 4$, il faut prendre $a = 1$. Donc, pour que cette congruence soit résoluble il faut et il suffit que le nombre premier p soit $\equiv +1 \pmod 4$. En utilisant (74) et (75) on en conclut

$$\lambda_{4p} = (-1)^{\frac{1}{2}(p-1)}.$$

Maintenant on arrivera sans peine, par la méthode d'induction multiplicative, au résultat général : Soit $N(>1)$ un nombre naturel qui n'est pas une puissance de 2, et soit h le nombre des nombres premiers *différents* $\equiv -1 \pmod 4$ qui divisent N. Alors on a

$$\lambda_{4N} = (-1)^h.$$

Il en résulte : Si h est pair, les relations (34) et (36) sont toujours valables pour $n = 4N$ et $\Delta = -1$. Si h est impair, il faut remplacer ces relations par (37) et (38). Quand N est une puissance de 2, il n'existe pas de formules analogues.

Le cas où $\Delta = -3$.

Nous avons $A_3(x; -3) = x - \varrho$, où $\varrho = e^{\frac{2}{3}\pi i}$, donc $\lambda_3 = -\varrho$. Ainsi il résulte de (73) que $\lambda_N = -\varrho$ lorsque N est une puissance de 3.

Si dans la congruence (42) $n = 3$, il faut prendre $a = 1$. Donc, pour que cette congruence soit résoluble il faut et il suffit que le nombre premier p soit $\equiv +1 \pmod 3$. On en conclut, en utilisant (74) et (75),

$$\lambda_{3p} = \varrho^{2(p-1)}.$$

Enfin on arrivera, par la méthode d'induction multiplicative, au résultat général : Soit $N(>1)$ un nombre naturel qui n'est pas une puissance de 3, et soit h le nombre des nombres premiers différents $\equiv -1 \pmod 3$ qui divisent N. Alors on a

$$\lambda_{3N} = \varrho^{2h}.$$

Il en résulte : Si h est divisible par 3, les relations (34) et (36) sont toujours valables pour $n = 3N$ et $\Delta = -3$. Dans le cas contraire il n'y a pas de relations analogues; même chose si N est une puissance de 3.

INDEX BIBLIOGRAPHIQUE

1. NAGELL, T., Introduction to number theory, Stockholm, New York 1951.
2. —— Problem 23, Norsk Matematisk Tidsskrift, Bd. 2, Oslo 1920, p. 95.
3. KANOLD, H. J., Abschätzungen bei Kreisteilungspolynomen und daraus hergeleitete Bedingungen für die kleinsten Primzahlen gewisser arithmetischer Folgen, Mathematische Zeitschrift, Bd. 55, 1952.
4. SCHINZEL, A., On primitive prime factors of $a^n - b^n$, Proceedings of the Cambridge Philosophical Society, Vol. 58, 1962.
5. NAGELL, T., Über einige Sinus- und Cosinus-Produkte, Nyt Tidsskrift f. Matematik, Bd. 28, Köbenhavn 1917.
6. —— Le discriminant de l'équation de la division du cercle, Norsk Matematisk Tidsskrift, Bd. 1, Oslo 1919.
7. HASSE, H., Zahlentheorie, Berlin 1949.
8. FRICKE, R., Lehrbuch der Algebra, Bd. 3, Braunschweig 1928.
9. GAUSS, C. F., Werke, Bd. 1.
10. DIRICHLET, P. G. LEJEUNE, Vorlesungen über Zahlentheorie, herausg. v. R. Dedekind, Braunschweig 1894.

Tryckt den 9 december 1963

Uppsala 1963. Almqvist & Wiksells Boktryckeri AB