9.

Lois de réciprocité.

(Par Mr. *G. Eisenstein* à Berlin.)

Nouvelle démonstration du théorème fondamental sur les résidus quadratiques dans la théorie des nombres complexes. Démonstration du théorème fondamental sur les résidus biquadratiques. Le théorème le plus général sur les caractères biquadratiques, qui comprend, comme cas particulier, le théorème fondamental.

Soit p un nombre premier réel $4n+1$, soient p_1, p_2 les deux nombres premiers *complexes* de la forme $\alpha+\beta i$ qui, ayant p pour norme commune, sont tels que $p_1 \equiv p_2 \equiv 1 \pmod 2$ et $p_1 p_2 = p$. Soit de plus r une racine de l'équation $\frac{x^p-1}{x-1} = 0$, et désignons par le symbole $\left[\frac{k}{p_1}\right]$ la puissance évidemment unique de i qui satisfait la congruence

$$k^{\frac{1}{4}(p-1)} \equiv \left[\frac{k}{p_1}\right] \pmod{p_1}.$$

Cela posé, on a comme l'on sait, et comme nous l'avons déjà prouvé,

$$\left(\sum_{k=1}^{k=p-1}\left[\frac{k}{p_1}\right]r^k\right)^4 = S^4 = p(a+bi)^2; \quad (a+bi)(a-bi) = p,$$

$$\left(\sum_{k=1}^{k=p-1}\left[\frac{k}{p_1}\right]^3 r^k\right)^4 = T^4 = p(a-bi)^2; \quad a+bi \equiv a-bi \equiv 1 \pmod 2.$$

Je dis que l'on peut poser $a+bi = p_1$. Nous avons prouvé dans une autre occasion*) que l'on a

$$a+bi = \sum_{\sigma=1}^{\sigma=p-2}\left[\frac{\sigma}{p_1}\right]\left[\frac{\sigma+1}{p_1}\right]^2, \quad a-bi = \sum_{\sigma=1}^{\sigma=p-2}\left[\frac{\sigma}{p_1}\right]^3\left[\frac{\sigma+1}{p_1}\right]^2,$$

ce qui donne

$$a+bi \equiv \sum_{\sigma=1}^{\sigma=p-2} \sigma^{\frac{1}{4}(p-1)}(\sigma+1)^{\frac{1}{4}(p-1)} \pmod{p_1},$$

$$a-bi \equiv \sum_{\sigma=1}^{\sigma=p-2} \sigma^{\frac{1}{4}(p-1)}(\sigma+1)^{\frac{1}{4}(p-1)} \pmod{p_1};$$

mais il a été aussi démontré que ces deux dernières sommes sont respectivement

$$\equiv 0 \pmod p, \quad \equiv -\frac{(\frac{1}{2}(p-1))!}{(\frac{1}{4}(p-1))!\,(\frac{1}{4}(p-1))!} \pmod p:$$

*) Voir „Beiträge zur Kreistheilung" cahier 3. vol. 27. de ce journal.

en désignant par $m!$ le produit $1.2.3....m$. On a donc

$$a+bi \equiv 0 \pmod{p_1}, \quad a-bi \equiv -\frac{(\frac{1}{2}(p-1))!}{(\frac{1}{4}(p-1))!\,(\frac{1}{4}(p-1))!} \pmod{p_1}.$$

Mais p_2 n'étant pas divisible par p_1, il faut que $a+bi = p_1$. Celà étant, on obtient encore $a-bi = p_2$, parsuite

$$p_2 \equiv -\frac{(\frac{1}{2}(p-1))!}{(\frac{1}{4}(p-1))!\,(\frac{1}{4}(p-1))!} \pmod{p_1},$$

et de même

$$p_1 \equiv -\frac{(\frac{1}{2}(p-1))!}{(\frac{1}{4}(p-1))!\,(\frac{1}{4}(p-1))!} \pmod{p_2},$$

ce que je remarque en passant.

Dans ce qui suit nous ferons surtout usage de ces deux équations:

$$(1.) \quad \Big(\sum_{k=1}^{k=p-1}\Big[\frac{k}{p_1}\Big]r^k\Big)^4 = S^4 = pp_1^2,$$

$$(2.) \quad \Big(\sum_{k=1}^{k=p-1}\Big[\frac{k}{p_1}\Big]^3 r^k\Big)^4 = T^4 = pp_2^2.$$

Soit q un nombre premier *réel* de la forme $4n+3$. En élévant les deux membres de l'équation (1.) à la puissance $\frac{1}{4}(q^2+3)$ il vient

$$(3.) \quad S^{q^2+3} = (pp_1^2)^{\frac{1}{4}(q^2+3)}.$$

D'un autre côté, on a aussi, comme l'on sait,

$$(4.) \quad \sum_{k=1}^{k=p-1}\Big[\frac{k}{p_1}\Big]r^{q^2k} = S_{q^2} = \Big[\frac{q_1}{p_1}\Big].S.$$

En combinant cette équation, après l'avoir multipliée par S^3, avec l'équation (1.) on en tire

$$(5.) \quad S^3 S_{q^2} = \Big[\frac{q^2}{p_1}\Big]pp_1^2.$$

Retranchant l'équation (5.) de celle (3.) il vient

$$(6.) \quad S^3\{S^{q^2} - S_{q^2}\} = pp_1^2\Big\{(pp_1^2)^{\frac{1}{4}(q^2-1)} - \Big[\frac{q^2}{p_1}\Big]\Big\}.$$

Il est aisé de voir que le premier membre de cette dernière équation peut prendre la forme

$$q(A+Br+Cr^2+....)$$

où $A, B, C, ...$ sont des *entiers* complexes. On a donc

$$(7.) \quad pp_1^2.\Big\{(pp_2^1)^{\frac{1}{4}(q^2-1)} - \Big[\frac{q^2}{p_1}\Big]\Big\} = q(A+Br+Cr^2+....).$$

Comme cette équation subsiste quel que soit la valeur de la racine r, elle prouve que l'entier complexe qui compose le premier membre est divisible par q. Si l'on remarque encore que pp_1^2 n'est pas divisible par le nombre premier q, on a la congruence

$$(8.) \quad (pp_1^2)^{\frac{1}{4}(q^2-1)} \equiv \left[\frac{q^2}{p_1}\right] \pmod{q},$$

et cela donne, q^2 étant la norme de q,

$$\left[\frac{pp_1^2}{q}\right] = \left[\frac{q^2}{p_1}\right].$$

Puisque évidemment $\left[\frac{p}{q}\right] = 1$, il vient

$$(9.) \quad \left[\frac{p_1}{q}\right]^2 = \left[\frac{q}{p_1}\right]^2.$$

Mais $\left[\frac{p_1}{q}\right]^2 = 1$, ou $= -1$, selon que p_1 est résidu ou non-résidu quadratique de q (dans la théorie de nombres complexes), et $\left[\frac{q}{p_1}\right]^2 = +1$, ou $= -1$, selon que q est résidu ou non-residu quadratique de p_1; et comme l'expression $\left[\frac{p_1}{q}\right]^2$ ne change pas de valeur en remplaçant p_1 par $-p_1$, l'équation que nous venons de trouver donne le théorème suivant:

Théorème I. *„Etant donnés deux nombres premiers complexes qui sont respectivement de première et de seconde espèce, et dont les parties réelles sont impaires, le premier est ou n'est pas résidu quadratique du second, selon que le second est ou n'est pas résidu quadratique du premier.*

Soit maintenant h un autre nombre premier réel de la forme $4n+1$, différent de p, et soient h_1, h_2 (que l'on suppose $\equiv 1 \pmod{2}$) les deux nombres premiers complexes conjugués qui ont h pour norme commune. En élévant les deux membres de l'équation (1.) à la puissance $\frac{1}{4}(h+3)$, on aura

$$(10.) \quad S^{h+3} = (pp_1^2)^{\frac{1}{4}(h+3)}.$$

D'un autre côté on a

$$(11.) \quad \sum_{k=1}^{k=p-1} \left[\frac{k}{p_1}\right] r^{hk} = S_h = \left[\frac{h}{p_1}\right]^3 S.$$

Multipliant par S^3 et substituant la valeur de S^4 donnée par (1.), il viendra

$$(12.) \quad S^3 S_h = \left[\frac{h}{p_1}\right]^3 pp_1^2.$$

Enfin les deux équations (10.) et (12.) donnent, en les retranchant l'une de l'autre:

$$(13.) \quad S^3\{S^h - S_h\} = pp_1^2\left\{(pp_1^2)^{\frac{1}{4}(h-1)} - \left[\frac{h}{p_1}\right]^3\right\}.$$

Le premier membre de cette équation étant développé, peut prendre la forme

$$h(A + Br + Cr^2 + \ldots),$$

où A, B, C, ... sont des *entiers* complexes; de sorte que l'on a

$$(14.)\quad pp_1^2\left\{(pp_1^2)^{\frac{1}{4}(h-1)}-\left[\frac{h}{p_1}\right]^3\right\}=h(A+Br+Cr^2+\ldots).$$

Comme cette équation subsiste quel que soit la racine r, on en peut conclure que le premier membre est divisible par h, et cela, pp_1^2 n'ayant pas de facteur commun avec h, donne:

$$(15.)\quad (pp_1^2)^{\frac{1}{4}(h-1)}\equiv\left[\frac{h}{p_1}\right]^3\ (\text{mod. } h).$$

On a donc à plus forte raison

$$(16.)\quad (pp_1^2)^{\frac{1}{4}(h-1)}\equiv\left[\frac{h}{p_1}\right]^3\ (\text{mod. } h_1),$$

d'où l'on tire, h étant la norme de h_1,

$$(17.)\quad \left[\frac{pp_1^2}{h_1}\right]=\left[\frac{h^3}{p_1}\right].$$

De même, en échangeant entre eux les nombres premiers réels p et h de la forme $4n+1$, on a

$$(18.)\quad \left[\frac{hh_1^2}{p_1}\right]=\left[\frac{p^3}{h_1}\right].$$

Donc

$$\left[\frac{pp_1^2}{h_1}\right]=\left[\frac{h^3}{p_1}\right]\quad\text{et}\quad\left[\frac{p^3}{h_1}\right]=\left[\frac{hh_1^2}{p_1}\right],$$

ce qui donne, en multipliant,

$$\left[\frac{p^4p_1^2}{h_1}\right]=\left[\frac{h^4h_1^2}{p_1}\right].$$

$$\text{Or}\quad\left[\frac{p^4}{h_1}\right]=\left[\frac{h^4}{p_1}\right]=1,\quad\text{donc}$$

$$(19.)\quad\left[\frac{p_1}{h_1}\right]^2=\left[\frac{h_1}{p_1}\right]^2.$$

Cette équation fournit le théorème suivant:

Théorème II. *„Des deux nombres premiers complexes de seconde espèce, dont les parties réelles sont impaires, le premier est ou n'est pas résidu quadratique du second, selon que le second est ou n'est pas résidu quadratique du premier.“*

Si les nombres premiers q et q' sont tous deux de première espèce, c'est à dire $\equiv 3$ (mod. 4), on a suivant le théorème de *Fermat* $q'^{\frac{1}{2}(q^2-1)}=(q'^{\frac{1}{4}(q+1)})^{q-1}\equiv 1$ (mod. q), donc on a nécessairement $\left[\frac{q'}{q}\right]=1$, et de même $\left[\frac{q}{q'}\right]=1$, et aussi dans ce cas $\left[\frac{q'}{q}\right]=\left[\frac{q}{q'}\right]$, et $\left[\frac{q'}{q}\right]^2=\left[\frac{q}{q'}\right]^2$. A l'aide de cette re-

marque nous pouvons réunir dans l'énoncé suivant les deux théorèmes que nous venons de trouver.

Théorème III. *„Désignant par $\alpha+\beta i$, $\gamma+\delta i$ (β et δ étant pairs et réduisible à zéro) deux nombres premiers complexes quelconques, le premier est ou n'est pas résidu quadratique du second selon que le second est ou n'est pas résidu quadratique du premier.*"

Ce théorème remarquable qui embrasse presque tout ce qu'il y a à dire sur la théorie des résidus quadratiques est redevable à Mr. ***Gauss.*** Il a été démontré pour la première fois par Mr. ***Dirichlet*** dans le 9ième vol. de ce journal. La démonstration que donne ce grand géomètre est fondé sur le théorème analogue dans la théorie réelle, généralement connu sous le nom „Loi de réciprocité de ***Legendre,***" tandis que la nôtre est entièrement indépendante de cet autre théorème.

Passons aux résidus ***biquadratiques.*** Toutes les lettres ayant la même signification comme dans ce qui précède, si l'on élève l'équation (1.) à la puissance $\frac{1}{8}(q^2-1)$, on obtient

$$(20.) \qquad S^{\frac{1}{8}(p^2-1)} = p^{\frac{1}{8}(q^2-1)} p_1^{\frac{1}{4}(q^2-1)}.$$

La puissance $S^{\frac{1}{8}(q^2-1)}$ peut s'écrire $(S^{q+1})^{\frac{1}{8}(q-1)}$. L'expression S^q étant développée suivant le théorème polynomial, peut prendre la forme

$$q(A+Br+Cr^2+\ldots.)+\sum_{k=1}^{k=p-1}\left[\frac{k}{p_1}\right]^q r^{qk},$$

où A, B, C, ... sont des entiers complexes. Or $q\equiv 3 \pmod 4$, donc

$$\left[\frac{k}{p_1}\right]^q = \left[\frac{k}{p_1}\right]^3, \quad \text{et partant} \quad \Sigma\left[\frac{k}{p_1}\right]^q r^{qk} = \Sigma\left[\frac{k}{p_1}\right]^3 r^{qk} = \left[\frac{q}{p_1}\right] T.$$

Substituant, il vient

$$S^q = q(A+Br+Cr^2+\ldots.)+\left[\frac{q}{p_1}\right] T.$$

Multipliant par S et élévant à la puissance $\frac{1}{2}(q-1)$, on a

$$\begin{aligned} S^{\frac{1}{8}(q^2-1)} &= S^{\frac{1}{2}(q-1)}\left\{q(A'+B'r+C'r^2+\ldots.)+\left[\frac{q}{p_1}\right]^{\frac{1}{2}(q-1)} T^{\frac{1}{2}(q-1)}\right\} \\ &= q(A''+B''r+C''r^2+\ldots.)+\left[\frac{q}{p_1}\right]^{\frac{1}{2}(q-1)} (ST)^{\frac{1}{2}(q-1)} \\ &= q(A''+B''r+C''r^2+\ldots.)+\left[\frac{q}{p_1}\right]^{\frac{1}{2}(q-1)} p^{\frac{1}{2}(q-1)} (-1)^{\frac{1}{4}(p-1)\frac{1}{4}(q-1)}, \end{aligned}$$

où A' etc. A'' etc. sont également des entiers complexes. Il suit de là et

de l'équation (20.), que la différence

$$p^{\frac{1}{8}(q^2-1)}p_1^{\frac{1}{4}(q^2-1)} - \left[\frac{q}{p_1}\right]^{\frac{1}{2}(q-1)} p^{\frac{1}{2}(q-1)}(-1)^{\frac{1}{4}(p-1)\frac{1}{2}(q-1)}$$

est *divisible par q*. D'un autre côté, en se servant de la notation de *Legendre*, on a

$$p^{\frac{1}{2}(q-1)} \equiv \left(\frac{p}{q}\right) \pmod{q},$$

$$p^{\frac{1}{8}(q^2-1)} = (p^{\frac{1}{2}(q-1)})^{\frac{1}{4}(q+1)} \equiv \left(\frac{p}{q}\right)^{\frac{1}{4}(q+1)} \pmod{q},$$

donc, en remarquant que $\frac{1}{2}(q-1)$ est impair, on a

$$(21.) \quad p_1^{\frac{1}{4}(q^2-1)} \equiv \left[\frac{q}{p_1}\right]^{\frac{1}{2}(q-1)}\left(\frac{p}{q}\right)^{\frac{1}{4}(q-3)}(-1)^{\frac{1}{4}(p-1)} \pmod{q}.$$

Cette congruence donne l'équation

$$(22.) \quad \left[\frac{p_1}{q}\right] = \left[\frac{q}{p_1}\right]^{\frac{1}{2}(q-1)}\left(\frac{p}{q}\right)^{\frac{1}{4}(q-3)}(-1)^{\frac{1}{4}(p-1)}.$$

Soit en premier lieu q de la forme $8n+3$, on a $\frac{1}{2}(q-1) \equiv 1 \pmod 4$ $\frac{1}{4}(q-3) \equiv 0 \pmod 2$, donc

$\left[\frac{p_1}{q}\right] = \left[\frac{q}{p_1}\right](-1)^{\frac{1}{4}(p-1)}$, or $(-1)^{\frac{1}{4}(p-1)} = \left[\frac{-1}{p_1}\right]$, donc $\left[\frac{p_1}{p}\right] = \left[\frac{-q}{p_1}\right]$.

Soit en second lieu q de la forme $8n+7$, on a $\frac{1}{2}(q-1) \equiv 3 \pmod 4$, $\frac{1}{4}(q-3) \equiv 1 \pmod 2$, donc

$$\left[\frac{p_1}{q}\right] = \left[\frac{q}{p_1}\right]^3\left(\frac{p}{q}\right)\left[\frac{-1}{p_1}\right].$$

Or p étant de la forme $4n+1$, on peut remplacer $\left(\frac{p}{q}\right)$ par $\left(\frac{q}{p}\right)$. Je dis maintenant que l'on a $\left(\frac{q}{p}\right) = \left[\frac{q}{p_1}\right]^2$. En effet, $\left(\frac{q}{p}\right) \equiv (q^2)^{\frac{1}{4}(p-1)} \pmod{p_1}$, donc à plus forte raison $\left(\frac{q}{p}\right) \equiv (q^2)^{\frac{1}{4}(p-1)} \pmod{p_1}$, ce qui donne $\left(\frac{q}{p}\right) = \left[\frac{q^2}{p_1}\right] = \left[\frac{q}{p_1}\right]^2$. Substituant cette valeur, il vient

$$\left[\frac{p_1}{q}\right] = \left[\frac{q}{p_1}\right]^5\left[\frac{-1}{p_1}\right] = \left[\frac{-q}{p_1}\right].$$

Les deux cas que nous venons de distinguer conduisant au même résultat, nous pouvons énoncer le théorème suivant:

Théorème IV. „*Désignant par q un nombre premier réel et positiv* $4n+3$, *et par* p_1 *un nombre premier complexe de seconde espèce, dont la partie réelle est impaire, le caractère biquadratique de* $-q$ *par rapport à* p_1 *est toujours le même que le caractère biquadratique de* p_1 *par rapport à q.*"

Voilà la première partie du théorème fondamental sur les résidus biquadratiques.

Pour les recherches que nous aurons à exposer encore, il sera convenable de généraliser la signification du symbole $\left[\frac{M}{l}\right]$. Ce symbole, tel que nous l'avons employé jusqu'ici, suppose que l soit un nombre premier complexe impair, M étant un entier complexe quelconque non-divisible par l, et nous avons désigné par là la puissance évidemment unique de i qui satisfait à la congruence

$$M^{\frac{1}{4}(N(l)-1)} \equiv \left[\frac{M}{l}\right] \pmod{l},$$

$N(l)$ étant la norme de l.

Soient $l, l', l'', \ldots$ des nombres premiers complexes impairs non-diviseurs de M, mais d'ailleurs égaux ou inégaux, et soit $ll'l''\ldots = L$, nous désignerons désormais par

$$\left[\frac{M}{L}\right]$$

le produit

$$(23.) \quad \left[\frac{M}{L}\right] = \left[\frac{M}{l}\right]\left[\frac{M}{l'}\right]\left[\frac{M}{l''}\right]\ldots.$$

L'exposant de la puissance de i qui équivaut à $\left[\frac{M}{L}\right]$ sera nommé le *caractère biquadratique* de M par rapport à L.

Par rapport à notre symbole ainsi généralisé, on aura les formules suivantes dont la démonstration se présente d'elle même et dont l'usage est très fréquent:

$$(24.) \quad \left[\frac{M}{L}\right] = \left[\frac{P}{L}\right], \quad \left[\frac{MM'}{L}\right] = \left[\frac{M}{L}\right]\left[\frac{M'}{L}\right], \quad \left[\frac{M}{LL'}\right] = \left[\frac{M}{L}\right]\left[\frac{M}{L'}\right],$$
$$\left[\frac{M}{L}\right]^2 = \pm 1, \quad \left[\frac{M}{L}\right]^4 = 1:$$

équations qui supposent, la première, que M, toujours sans diviseurs commun avec l'entier complexe impair L, est $\equiv P \pmod{L}$; la seconde que M et M' sont premiers à M, et la troisième que M est premier aux entiers impairs L et L'.

Lemme I. „$\alpha+\beta i$ et $\gamma+\delta i$ étant deux entiers complexes quelconques sans diviseur commun, on a toujours

$$\left[\frac{\alpha+\beta i}{\gamma+\delta i}\right] = \left[\frac{\alpha-\beta i}{\gamma-\delta i}\right]^3."$$ *)

*) Ici et dans tout ce qui va suivre on suppose tacitement que les dénominateurs des

La vérité du lemme sera évidente, si nous pouvons le vérifier dans les cas particulier où $\gamma+\delta i$ se réduit à un nombre premier. Avec cette restriction on aura

$$\left[\frac{\alpha-\beta i}{\gamma-\delta i}\right] \equiv (\alpha-\beta i)^{\frac{1}{4}(\gamma^2+\delta^2-1)} \pmod{(\gamma-\delta i)},$$

c'est à dire

$$\left[\frac{\alpha-\beta i}{\gamma-\delta i}\right] = (m+ni)(\gamma-\delta i)+(\alpha-\beta i)^{\frac{1}{4}(\gamma^2+\delta^2-1)} = i^k$$

où m et n sont deux entiers réels. De là, en remplaçant partout i par $-i$, il suit

$$(-i)^k = \left[\frac{\alpha-\beta i}{\gamma-\delta i}\right]^3 \equiv (\alpha+\beta i)^{\frac{1}{4}(\gamma^2+\delta^2-1)} \pmod{\gamma+\delta i},$$

ce qu'il s'agissait de prouver.

Lemme II. „A et B étant deux entiers ***réels*** et sans diviseur commun, on a toujours $\left[\frac{A}{B}\right] = 1$."

Soit d'abord q un nombre premier réel de la forme $4n+3$ (abstraction faite du signe), on aura évidemment $\left[\frac{A}{q}\right]=1$, puisque $\left[\frac{A}{q}\right]\equiv(A^{\frac{1}{2}(q+1)})^{q-1}$ $\equiv 1 \pmod{q}$, en vertu du théorème de ***Fermat.*** Soient en second lieu p_1 et p_2 deux nombres premiers conjugués de seconde espèce qui ont p pour norme commune, on a (Lemme I.), A étant réel,

$$\left[\frac{A}{p_1}\right] = \left[\frac{A}{p_2}\right]^3, \quad \text{donc} \quad \left[\frac{A}{p_1}\right]\left[\frac{A}{p_2}\right] = \left[\frac{A}{p}\right] = \left[\frac{A}{p_2}\right]^4 = 1.$$

Si donc on suppose $B = qq'q''\ldots pp'p''\ldots$, $q, q', q'', \ldots$ étant des nombres premiers ***réels*** $4n+3$, $p, p', p'', \ldots$ des nombres premiers ***réels*** $4n+1$, on a

$$\left[\frac{A}{B}\right] = \left[\frac{A}{q}\right]\left[\frac{A}{q'}\right]\left[\frac{A}{q''}\right]\ldots\left[\frac{A}{p}\right]\left[\frac{A}{p'}\right]\left[\frac{A}{p''}\right]\ldots = 1.$$

Lemme III. „Désignant par A un entier ***réel*** qui avec son signe est $\equiv 1 \pmod{4}$, et par L un entier complexe quelconque, je dis qu'on a l'équation $\left[\frac{L}{A}\right] = \left[\frac{A}{L}\right]$."

L'entier réel A étant $\equiv 1 \pmod{4.}$, il peut être décomposé dans un nombre de facteurs premiers réels q de la forme $4n+3$ pris chacun avec

---

symboles [=] sont impairs et qu'ils n'ont pas de diviseur commun avec les numérateurs. On suppose aussi que tous les entiers complexes impairs sont pris tels, que leur parties réelles soint impaires.

le signe *moins,* et dans un nombre de facteurs premiers réels p de la forme $4n+1$ pris chacun avec le signe *plus.* A l'aide de la seconde et de la troisième des équations (24.) tout se réduit donc à prouver que

$$\left[\frac{L}{-q}\right] = \left[\frac{-q}{L}\right] \quad \text{et} \quad \left[\frac{L}{p}\right] = \left[\frac{p}{L}\right].$$

En se servant toujours de la seconde et de la troisième formule de décomposition (24.), la première proposition résulte immédiatement du Théorème IV. et du Lemme II. Quant à la seconde, elle se déduit de l'équation (18.), c'est a dire de l'équation $\left[\frac{h_1^3 h_2}{p_1}\right] = \left[\frac{p^3}{h_1}\right]$, où p, h sont des nombres prémiers réels $4n+1$, et où $p = p_1 p_2$, $h = h_1 h_2$; p_1, p_2, h_1, h_2 étant des nombres premiers complexes de seconde espèce ayant resp. p, h pour normes communes. En effet h_1, h_2 étant conjugués et p étant réel, le Lemme I. donne

$$\left[\frac{h_1^3}{p_1}\right] = \left[\frac{h_2}{p_2}\right], \quad \left[\frac{p^3}{h_1}\right] = \left[\frac{p}{h_2}\right];$$

donc il vient

$$\left[\frac{h_2}{p_2}\right]\left[\frac{h_2}{p_1}\right] = \left[\frac{h_2}{p}\right] = \left[\frac{p}{h_2}\right].$$

Or désignant par B le plus grand entier réel qui divise L, et par h_2, h_2', h_2'' etc. les autres facteurs simples de seconde espèce de L, on aura

$$L = B h_2 h_2' h_2'' \ldots,$$

$$\left[\frac{L}{p}\right] = \left[\frac{B}{p}\right]\left[\frac{h_2}{p}\right]\left[\frac{h_2'}{p}\right]\left[\frac{h_2''}{p}\right] \ldots$$

$$\left[\frac{p}{L}\right] = \left[\frac{p}{B}\right]\left[\frac{p}{h_2}\right]\left[\frac{p}{h_2'}\right]\left[\frac{p}{h_2''}\right] \ldots;$$

mais $\left[\frac{B}{p}\right] = \left[\frac{p}{B}\right] = 1$ (Lem. II.), et de plus $\left[\frac{h_2}{p}\right] = \left[\frac{p}{h_2}\right]$, $\left[\frac{h_2'}{p}\right] = \left[\frac{p}{h_2'}\right]$, $\left[\frac{h_2''}{p}\right] = \left[\frac{p}{h_2''}\right]$ etc. en vertu de ce que nous venons de trouver: donc aussi

$$\left[\frac{L}{p}\right] = \left[\frac{p}{L}\right].$$

Lemme IV. „Désignant par m un entier réel impair positif ou négatif, on a $\left[\frac{i}{m}\right] = 1$ pour $m \equiv 1, 7 \pmod 8$ et $\left[\frac{i}{m}\right] = -1$ pour $m \equiv 3, 5 \pmod 8$, ou, ce qui revient au même, on a toujours $\left[\frac{i}{m}\right] = \left(\frac{2}{m}\right)$. De là comme corollaire il suit que

$\left[\frac{i}{m}\right]\left[\frac{i}{m'}\right] = 1$, lorsque $m \equiv m'$ (mod. 8), et

$\left[\frac{i}{m}\right]\left[\frac{i'}{m'}\right] = -1$, lorsque $m \equiv m'+4$ (mod. 8)."

Soit $p = p_1 p_2$ un nombre premier positif $4n+1$, on aura (Lemme I.) $\left[\frac{i}{p_2}\right] = \left[\frac{-i}{p_1}\right]^3$; multipliant par $\left[\frac{i}{p_1}\right]$ il vient

$$\left[\frac{i}{p}\right] = \left[\frac{-i}{p_1}\right]^3\left[\frac{i}{p_1}\right] = \left[\frac{-1}{p_1}\right] = (-1)^{\frac{1}{4}(p-1)};$$

donc $\left[\frac{i}{p}\right] = +1$ ou $= -1$, selon que $p \equiv 1$ ou $\equiv 5$ (mod. 8), et par conséquent $\left[\frac{i}{\pm p}\right] = +1$ ou $= -1$, selon que $p \equiv \pm 1$ ou $p \equiv \pm 5$ (mod. 8), c'est à dire selon que $\pm p \equiv 1, 7$ ou $\pm p \equiv 3, 5$ (mod. 8). Soit en second lieu q un nombre premier positif $4n+3$, on aura

$$\left[\frac{i}{\pm q}\right] = i^{\frac{1}{4}(q^2-1)} = (-1)^{\frac{1}{8}(q^2-1)}, \text{ donc } \left[\frac{i}{\pm q}\right] = \left(\frac{2}{\pm q}\right).$$

Quel que soit donc le nombre premier réel (a) on aura toujours $\left[\frac{i}{\pm a}\right] = \left(\frac{2}{\pm a}\right)$. Celà étant, on peut toujours supposer

$$m = \pm a\, a'\, a'' \ldots .$$

où a, a', a'', ... sont les facteurs simples réels de m; il suit donc que

$$\left[\frac{i}{m}\right] = \left[\frac{i}{a}\right]\left[\frac{i}{a'}\right]\left[\frac{i}{a''}\right] \ldots . = \left(\frac{2}{a}\right)\left(\frac{2}{a'}\right)\left(\frac{2}{a''}\right) \ldots . = \left(\frac{2}{m}\right),$$

ce qu'il s'agissoit de prouver.

Nous considérerons dorénavant avec Mr. *Gauss* comme nombre *primaire* parmi quatre entiers complexes impairs *associés* qui forment un même groupe, celui $a+bi$, évidemment unique, pour lequel on a

ou $a \equiv 1$ (mod. 4), et en même temps $b \equiv 0$ (mod. 4),
ou $a \equiv 3$ (mod. 4), et en même temps $b \equiv 2$ (mod. 4).

Mais cette expression ne doit pas être confondue avec ce que Mr. *Dirichlet* appelle nombre primaire. On conclura aisément de la convention que nous venons de poser, que le produit de deux, et par conséquent d'un nombre quelconque d'entiers primaires est lui même un entier primaire. Tous les entiers primaires peuvent être distribués en deux classes distinctes, en comprenant dans la *première classe* tous ceux qui sont $\equiv 1$ (mod. 4) et dans la

seconde tous ceux qui sont $\equiv 3+2i \pmod 4$. Cette distinction est d'une grande utilité dans la théorie des résidus biquadratiques, et il sera bon de l'appliquer à des exemples.

Les entiers *réels* impairs, pour être *primaires,* doivent être pris avec le signe *plus,* ou avec le signe *moins,* selon qu'ils sont, abstraction faite du signe, $\equiv 1 \pmod 4$ ou $\equiv 3 \pmod 4$. Les entiers réels et primaires appartiennent donc toujours à la première classe, puisque leur partie imaginaire est zéro, et partant $\equiv 0 \pmod 4$.

Ces préliminaires posés, soient $a+bi$ et $c+di$ deux entiers complexes primaires premiers entre eux dont les éléments a et b, c et d *n'ont pas de diviseur commun.* Cela étant, on aura évidemment la congruence

$$(A.) \qquad c^4(a+bi) \equiv c^3(ac+bd) \pmod{c+di}.$$

En effet, la différence des deux membres est $= ac^4+bc^4i-ac^4-bc^3d = bc^4i-bc^3d = bc^3i(c+di)$ et parsuite divisible par le module $c+di$. Suivant l'hypothèse admise sur les entiers c et d, c n'aura pas de diviseur commun avec le module; mais $a+bi$ étant également premier à $c+di$, le premier membre de la congruence (*A.*), et par suite aussi le second, n'auront pas de diviseur commun avec le module. On tirera donc de là l'équation

$$(B.) \qquad \left[\frac{a+bi}{c+di}\right] = \left[\frac{c}{c+di}\right]^3 \left[\frac{ac+bd}{c+di}\right].$$

Les entiers a et b n'ayant pas également de diviseur commun, on aura de même

$$(C.) \qquad \left[\frac{c+di}{a+bi}\right] = \left[\frac{a}{a+bi}\right]^3 \left[\frac{ac+bd}{a+bi}\right]$$

et partant (Lemme I.)

$$(D.) \qquad \left[\frac{c+di}{a+bi}\right]^3 = \left[\frac{a}{a+bi}\right]\left[\frac{ac+bd}{a-bi}\right].$$

Multipliant entre elles les équations (*B.*) et (*D.*), il vient

$$(E.) \qquad \left[\frac{a+bi}{c+di}\right]\left[\frac{c+di}{a+bi}\right]^3 = \left[\frac{c}{c+di}\right]^3 \left[\frac{a}{a+bi}\right]\left[\frac{ac+bd}{(c+di)(a-bi)}\right].$$

Pour pouvoir appliquer *le troisième Lemme* au second membre de cette équation, il faut que les numérateurs des symboles qui y entrent soient $\equiv 1 \pmod 4$. Soit donc pour abréger $\delta = \pm 1$, $\varepsilon = \pm 1$, où les signes sont pris tels, qu'on ait

$$a \equiv \delta \pmod 4, \qquad c \equiv \varepsilon \pmod 4.$$

Cela posé, on aura $\varepsilon c \equiv 1 \pmod 4$, $\delta a \equiv 1 \pmod 4$, $\delta\varepsilon(ac+bd) \equiv \delta\varepsilon ac \equiv 1 \pmod 4$. Donnons donc au second membre de l'équation (*E.*) la forme

$$(F.)\quad \left[\frac{\varepsilon c}{c+di}\right]^3\left[\frac{\delta a}{a+bi}\right]\left[\frac{\delta\varepsilon(ac+bd)}{ac+bd+i(ad-bc)}\right]\left[\frac{\varepsilon}{a+bi}\right]\left[\frac{\delta}{c+di}\right]:$$

forme dont la legitimité résulte de ce que $\delta^2 = \varepsilon^2 = 1$. Comme les numérateurs des trois premiers symboles sont ici des entiers réels et $\equiv 1 \pmod 4$, on pourra (Lemme III.) remplacer ces trois symboles respectivement par les symboles inverses

$$(G.)\quad \left[\frac{c+di}{c}\right]^3,\quad \left[\frac{a+bi}{a}\right],\quad \left[\frac{ac+bd+i(ad-bc)}{ac+bd}\right],$$

respectivement équivalents aux suivants:

$$\left[\frac{di}{c}\right]^3 = \left[\frac{i}{c}\right]^3 = \left[\frac{i}{c}\right],\quad \left[\frac{bi}{a}\right] = \left[\frac{i}{a}\right],\quad \left[\frac{i(ad-bc)}{ac+bd}\right] = \left[\frac{i}{ac+bd}\right],$$

de sorte que la valeur du produit des trois premiers termes qui entrent dans l'expression (*F.*) se réduit à

$$(H.)\quad \left[\frac{i}{ac}\right]\left[\frac{i}{ac+bd}\right].$$

Il reste encore les deux derniers facteurs du produit (*F.*). Je dis que le produit de ces deux facteurs se réduit toujours à l'unité prise positivement. En effet, comme l'on a $\varepsilon = (-1)^{\frac{1}{2}(c-1)}$, $\delta = (-1)^{\frac{1}{2}(a-1)}$, le produit dont il s'âgit peut s'écrire ainsi:

$$\left[\frac{-1}{a+bi}\right]^{\frac{1}{2}(c-1)}\left[\frac{-1}{c+di}\right]^{\frac{1}{2}(a-1)}.$$

Or

$$\left[\frac{-1}{a+bi}\right] = (-1)^{\frac{1}{2}(a-1)},\quad \left[\frac{-1}{c+di}\right] = (-1)^{\frac{1}{2}(c-1)},$$

donc

$$(-1)^{\frac{1}{2}(a-1)\frac{1}{2}(c-1)}.(-1)^{\frac{1}{2}(c-1)\frac{1}{2}(a-1)} = +1.$$

Toute la valeur du second membre de l'équation (*E.*) se réduit donc à l'expression (*H.*). Cherchons la valeur de cette expression. Lorsque les entiers complexes primaires $a+bi$ et $c+di$ n'appartiennent pas tous deux à la seconde classe, le produit bd sera nécessairement divisible par 8, d'où l'on tire $ac \equiv ac+bd \pmod 8$, et l'expression (*H.*) aura la valeur $+1$. Mais si les nombres $a+bi$ et $c+di$ appartiennent tous les deux à la seconde classe, b et d seront de la forme $4n+2$ et par conséquent bd sera de la forme $8n+4$, et parsuite $ac \equiv ac+bd+4 \pmod 8$, et l'expression (*H.*) se réduira à -1 (Lemme IV.).

Or multipliant l'équation (*E.*) de part et d'autre par $\left[\frac{c+di}{c+di}\right]$ et ob-

servant que $\left[\frac{c+di}{a+bi}\right]^4 = 1$, on voit que les deux expressions

$$(I.) \quad \left[\frac{a+bi}{c+di}\right] \text{ et } \left[\frac{c+di}{a+bi}\right]$$

sont ou égales ou opposées, selon que les deux entiers primaires qui y entrent n'appartiennent pas ou appartiennent tous les deux à la seconde classe.

Pour généraliser encore le résultat que nous venons de trouver, soient

$$A+Bi=\mu(a+bi), \quad C+Di=\nu(c+di)$$

deux entiers complexes quelconques primaires premiers entre eux, μ et ν étant deux entiers réels que nous supposons tous les deux $\equiv 1 \pmod 4$, et $a+bi$, $c+di$ ayant la même signification que dans ce qui précède; il n'existe pas de nombre primaire, qui ne soit pas représenté sous cette forme. Cela posé, les équations (24.) donnent

$$\left[\frac{A+Bi}{C+Di}\right] = \left[\frac{\mu}{\nu}\right]\left[\frac{\mu}{c+di}\right]\left[\frac{a+bi}{\nu}\right]\left[\frac{a+bi}{c+di}\right],$$

$$\left[\frac{C+Di}{A+Bi}\right] = \left[\frac{\nu}{\mu}\right]\left[\frac{c+di}{\mu}\right]\left[\frac{\nu}{a+bi}\right]\left[\frac{c+di}{a+bi}\right].$$

Or $\left[\frac{\mu}{\nu}\right] = \left[\frac{\nu}{\mu}\right]$ (Lemme II.), $\left[\frac{\mu}{c+di}\right] = \left[\frac{c+di}{\mu}\right]$, $\left[\frac{\nu}{a+bi}\right] = \left[\frac{a+bi}{\nu}\right]$ (Lemme III.), et enfin d'après ce que nous venons de trouver,

$$\left[\frac{a+bi}{c+di}\right] = -\left[\frac{c+di}{a+bi}\right] \text{ ou } = +\left[\frac{c+di}{a+bi}\right],$$

selon que $a+bi$ et $c+di$ appartiennent ou n'appartiennent pas tous les deux à la seconde classe, ou ce qui revient au même, μ et ν étant $\equiv 1 \pmod 4$, selon que $A+Bi$ et $C+Di$ appartiennent ou n'appartiennent pas tous les deux à la seconde classe. Il vient donc selon ces deux cas

$$\left[\frac{A+Bi}{C+Di}\right] = \mp\left[\frac{C+Di}{A+Bi}\right],$$

c'est à dire

$$\left[\frac{A+Bi}{C+Di}\right] = (-1)^{\frac{1}{4}(A-1)\frac{1}{4}(C-1)}\cdot\left[\frac{C+Di}{A+Bi}\right].$$

Théorème fondamental. „*Désignant par $A+Bi$ et $C+Di$ deux entiers complexes primaires sans diviseur commun, c'est à dire tels que l'on ait, ou simultanément $A\equiv 1$, $B\equiv 0 \pmod 4$, ou simultanément $A\equiv 3$, $B\equiv 2$ (mod. 4), ou, ce qui revient au même, tels que l'on ait $A+Bi\equiv C+Di\equiv 1$ (mod. $2+2i$), le caractère biquadratique du premier*

„par rapport au second est égal au caractère biquadratique du second „par rapport au premier, lorsque ou l'un et l'autre ou du moins l'un „des deux est $\equiv 1 \pmod 4$; *mais ces caractères biquadratiques diffèrent „de deux unités, lorsque* $A+Bi$ *et* $C+Di$ *sont tous les deux* $\equiv 3+2i$ „(mod. 4)."

On voit que ce théorème comprend comme cas particulier le théorème célèbre de Mr. *Gauss*, que ce profond analyste a énoncé dans le §. 67. de ses recherches sur les résidus biquadratiques. Voici donc la démonstration rigoureuse et générale de ce théorème celèbre, laquelle l'illustre auteur que nous venons de citer juge sujette à de si grandes difficultés, qu'il la renvoie aux plus profonds mystères de l'arithmétique transcendante *). Néanmoins il y a d'autant plus lieu de s'étonner que personne n'a songé d'en exposer une démonstration, puisque toute la théorie des nombres complexes paraît être inventée, pour ainsi dire, en faveur de ce théorème.

La démonstration que nous venons de présenter est très simple, et quoique elle paraît être un peu longue, on remarquera que nous n'avons presque rien supposé connu, excepté quelques formules fort simples que nous avons prouvées dans un autre lieu déjà cité, et dont la démonstration repose sur ce seul principe qu'un système de résidus, multiplié par un entier premier au module, reproduit un système de résidus. Au reste je suis parvenu encore à une autre démonstration de ce théorème excellent, que j'exposerai plus tard.

Parmi les conséquences nombreuses du théorème que nous venons d'énoncer, nous ne citerons qu'une seule qui est surtout remarquable et dont la démonstration se présente facilement.

„Désignant par L un entier complexe impair donné, par x un entier complexe variable: tous les facteurs complexes simples premier à L qui divisent la forme $x^4 - L$ sont contenus dans nn nombre déterminé de formules linéaires telles que $4Ly+b$, où y est un entier complexe variable et b un entier complexe déterminé.

Remarque. Dans les recherches qui précèdent nous avons souvent employé la conclusion suivante:

---

*) Voici ses propres mots: „At non obstante summa hujus theorematis simplicitate, ipsius demonstratio inter mysteria arithmeticae sublimioris maxime recondita referenda est, ita ut, saltem ut nunc res est, subtilissimas tantummodo investigationes enodari possit, quae limites praesentis commentationis longe transgrederentur." La troisième partie de ces recherches, à laquelle l'illustre auteur renvoie sa démonstration, n'a pas encore parue.

„Le produit d'un entier complexe α et d'une fonction entière de r à coëfficients entiers complexes étant égal à un autre entier complexe β, et cette égalité subsistant quelle que soit la racine r de l'équation $\frac{x^p-1}{x-1}=0$, il suit de là que β est nécessairement divisibe par α."

La légitimité de cette conclusion peut être démontrée aisément comme suit. Chaque fonction entière de r, telle que nous venons de définir, peut prendre la forme

$$A+Br+Cr^2+\ldots.+Kr^{p-1},$$

$A, B, C, \ldots. K$ étant des entiers complexes; on a donc suivant l'hypothèse

$$\alpha(A+Br+Cr^2+\ldots.+Kr^{p-1}) = \beta,$$
$$\alpha(A+Br^2+Cr^4+\ldots.+Kr^{2(p-1)}) = \beta,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\alpha(A+Br^{p-1}+Cr^{2(p-1)}+\ldots.+Kr^{(p-1)^2}) = \beta.$$

En multipliant ces équations resp. par $r, r^2, \ldots. r^{p-1}$, et les ajoutant, il vient

$$\alpha(-A-B-C-\ldots.+(p-1)K) = -\beta,$$

donc β est divisible par α, ce qu'il s'agissait de prouver.

Berlin, Juin 1844.