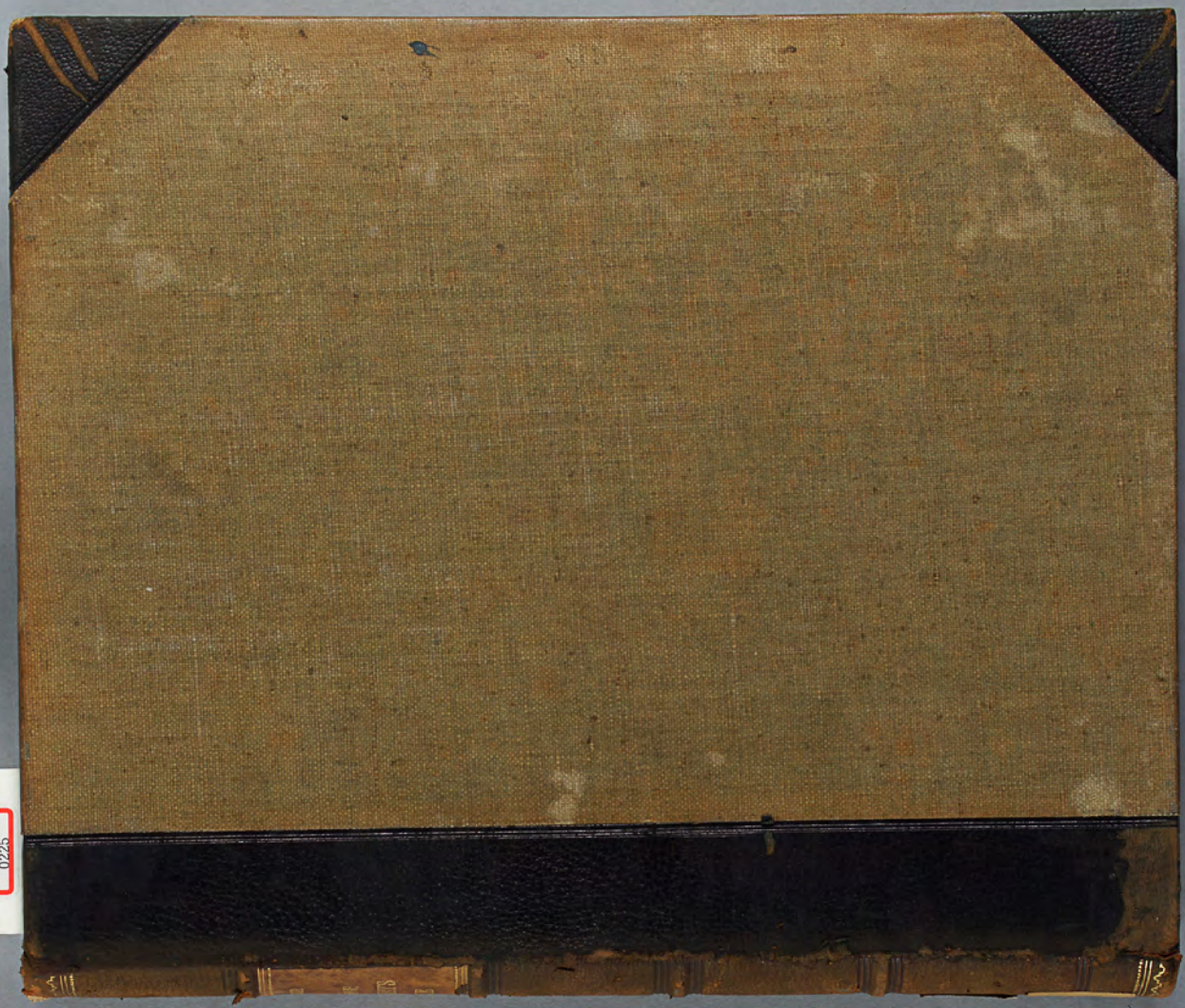

G. Lejeune Dirichlet

Photogravure u. Druck v. H. Hoffarth, Berlin.

G. LEJEUNE DIRICHLET'S WERKE.

HERAUSGEGEBEN AUF VERANLASSUNG
DER
KÖNIGLICH PREUSSISCHEN AKADEMIE DER WISSENSCHAFTEN.

IN ZWEI BÄNDEN.

BERLIN.
DRUCK UND VERLAG VON GEORG REIMER.
1889.

G. LEJEUNE DIRICHLET'S WERKE.

HERAUSGEGEBEN AUF VERANLASSUNG
DER
KÖNIGLICH PREUSSISCHEN AKADEMIE DER WISSENSCHAFTEN
VON
L. KRONECKER.

ERSTER BAND.

MIT G. LEJEUNE DIRICHLET'S BILDNISS.

BERLIN.
DRUCK UND VERLAG VON GEORG REIMER.
1889.

VORWORT.

Es war anfangs meine Absicht, die sämmtlichen von DIRICHLET selbst veröffentlichten Arbeiten, welche in dieser Ausgabe seiner Werke die erste Abtheilung bilden sollen, in einem Bande zu vereinigen. Aber ein solcher wäre, wie sich erst beim weiteren Fortschreiten des nicht raumsparenden Druckes zeigte, für den Handgebrauch zu umfangreich geworden. Der Band musste deshalb schon vor Beendigung der ersten Abtheilung an einer geeigneten Stelle förmlich abgeschlossen werden; er enthält nunmehr, grossen Theils in chronologischer Folge, alle Arbeiten, welche DIRICHLET vor 1843, also vor seiner italienischen Reise, veröffentlicht hat, sowie den im Monatsbericht der hiesigen Akademie vom März 1846 erschienenen Aufsatz „*Zur Theorie der complexen Einheiten*“, welcher sich gedanklich unmittelbar an die drei vorhergehenden Arbeiten anreiht. Diesen Aufsatz hat DIRICHLET zwar erst ein Jahr nach seiner Rückkehr aus Italien in der Akademie gelesen, aber die ebenso grundlegenden als weittragenden Untersuchungen, über welche er darin „einige Mittheilungen machte“, hatte er — wie ich aus seinem eigenen Munde weiss — bereits während seines Aufenthaltes in Italien vollständig zu Ende geführt.

Die Abhandlung „*Mémoire sur l'impossibilité de quelques Équations indéterminées du cinquième degré*“, mit welcher der Band beginnt, ist typographisch getreu nach einem Exemplar abgedruckt, welches sich in DIRICHLET's Nachlass vorgefunden hat. Dieses zeigt vielfach redactionelle Abweichungen von der unter demselben Titel im CRELLEschen Journal veröffentlichten, im vorliegenden Bande an zweiter Stelle abgedruckten Abhandlung, enthält den Text

aber wahrscheinlich genau so, wie er im Jahre 1825 der Pariser Akademie vorgelegen hat. Gewisses lässt sich freilich nicht darüber feststellen, da die Aufnahme der Abhandlung in die Sammlung der *Mémoires des Savans étrangers* nur beschlossen worden aber niemals erfolgt ist. Exemplare derselben Art, wie das erwähnte in DIRICHLET's Nachlass, finden sich meines Wissens noch in Göttingen im Nachlass von GAUSS, hier in Berlin in der königlichen Bibliothek, in Paris in der Bibliothek des Instituts und zwar im *Fonds Huzard*. Sie tragen auf der letzten (zwanzigsten) Seite den Vermerk: *„Imprimerie de Huzard-Courcier, Rue du Jardinet n° 12"*. Ueber ihre Entstehungsweise habe ich aber noch nicht vollständige Aufklärung erlangen können. Was ich darüber in Erfahrung gebracht habe, werde ich in den Anmerkungen im zweiten Bande mittheilen, namentlich alle Ergebnisse der Akten der Pariser *Académie des Sciences*, welche deren beständiger Secretar, Herr BERTRAND, mit gewohnter Sorgfalt ermittelt und mit freundlichster Bereitwilligkeit zu meiner Verfügung gestellt hat, sowie ferner einige werthvolle Notizen, welche ich den Herren ERNST SCHERING in Göttingen und JULES TANNERY in Paris verdanke.

Bei der Herausgabe dieses Bandes hat mich Herr LAMPE auf's Wirksamste unterstützt, ferner bei der Textrevision der sämmtlichen (mehr als funfzig Bogen füllenden) französischen Arbeiten auch Herr MOLK, und mein verehrter Freund, Herr HERMITE, hat die grosse Güte gehabt, mit seinem Kennerblick jeden einzelnen der französischen Correcturbogen durchzusehen. Ausserdem habe ich mich bei der Revision von Originaltexten und Correcturbogen noch der gefälligen Mithülfe der Herren HENSEL, HETTNER und SCHWERING erfreut, und auch die Herren GUTZMER, RICHARD MÜLLER und SCHRENTZEL haben mir in den Angelegenheiten der Herausgabe bereitwilligst Beistand geleistet.

Es ist mir eine angenehme Pflicht den genannten Herren an dieser Stelle meinen wärmsten Dank auszusprechen.

Berlin, den 14. October 1889.

L. KRONECKER.

INHALTS-VERZEICHNISS.

I. ABTHEILUNG,

ENTHALTEND

DIE VON G. LEJEUNE DIRICHLET SELBST VERÖFFENTLICHTEN ARBEITEN.

MÉMOIRE

Sur l'impossibilité de quelques Équations indéterminées du cinquième degré,

LU A L'ACADÉMIE ROYALE DES SCIENCES (INSTITUT DE FRANCE), LE 11 JUILLET 1825,
PAR G. LEJEUNE DIRICHLET.

(D'après le Rapport de MM. Lacroix et Legendre, ce Mémoire a été approuvé, et doit être imprimé dans le Recueil des Mémoires des Savans étrangers.)

(Abgedruckt nach einem Exemplare, welches sich in Lejeune Dirichlet's Nachlass vorgefunden hat.)

MÉMOIRE

Sur l'impossibilité de quelques Équations indéterminées du cinquième degré,

LU A L'ACADÉMIE ROYALE DES SCIENCES (INSTITUT DE FRANCE), LE 11 JUILLET 1825,
PAR G. LEJEUNE DIRICHLET.

(D'après le Rapport de MM. Lacroix et Legendre, ce Mémoire a été approuvé, et doit être imprimé dans le Recueil des Mémoires des Savans étrangers.)

On sait que la théorie des équations indéterminées des degrés supérieurs au second, est encore très peu avancée; il est vrai qu'il y a une infinité d'équations de tous les degrés dont on peut démontrer l'impossibilité en faisant voir que quelles que soient les valeurs que l'on attribue aux indéterminées, les deux membres de l'équation proposée ne peuvent jamais donner le même reste lorsqu'on les divise par un certain nombre ou module; mais lorsqu'une équation ne peut pas être traitée par ce moyen, il devient difficile de prouver qu'elle est impossible, et on n'y est parvenu, jusqu'à présent, que pour un très petit nombre d'équations. Toutes ces équations sont très particulières, et d'une forme telle, que lorsqu'on cherche à les résoudre, on est naturellement conduit à une ou plusieurs formules quadratiques qu'il s'agit d'égaler à des puissances parfaites. On satisfait ensuite de la manière la plus générale à cette condition, en exprimant les indéterminées par d'autres indéterminées, dont les premières deviennent des fonctions entières, et il se trouve, du moins dans tous les cas où la méthode dont il est question réussit, que les nouvelles indéterminées ou d'autres quantités qui en dépendent d'une manière très simple, satisfont également à une équation semblable à l'équation proposée. Comme les nouvelles indéterminées sont en même temps plus petites que les indéterminées primitives, l'impossibilité de l'équation proposée se trouve établie; car il est évident que si elle était possible, on aurait le moyen d'obtenir une suite décroissante et indéfinie de nombres entiers, ce qui implique contradiction. C'est de cette

manière que Fermat et Euler ont prouvé l'impossibilité de plusieurs équations du troisième et du quatrième degré.

En essayant d'appliquer des considérations semblables à quelques équations du cinquième degré et d'une forme analogue à celles des équations traitées par Fermat et Euler, on est arrêté tout aussitôt. La formule quadratique à laquelle on arrive, et qu'il faut égaler à une cinquième puissance, admet plusieurs solutions différentes, et parmi ces solutions, il n'y en a qu'une seule qui conduise à une équation semblable à l'équation proposée. En réfléchissant à cette difficulté, j'ai reconnu qu'elle pouvait être levée très simplement en assujettissant à quelques conditions le nombre déterminé qui entre dans l'équation. Il résulte d'un théorème exposé dans les préliminaires, que lorsque ces conditions se trouvent remplies, les différentes solutions dont la formule quadratique est susceptible, en général, doivent être rejetées, à l'exception d'une seule, qui est précisément celle de laquelle on déduit des nombres qui satisfont à une équation semblable à l'équation proposée. On parvient ainsi à établir l'impossibilité d'une classe assez étendue d'équations indéterminées du cinquième degré. Le premier membre de ces équations est la somme ou la différence de deux cinquièmes puissances, et le second membre est le produit d'une cinquième puissance et d'un nombre déterminé assujetti à différentes conditions. En attribuant à ce nombre des valeurs particulières compatibles avec ces conditions, on peut obtenir autant de théorèmes particuliers que l'on veut. Cette généralité de nos théorèmes est d'autant plus singulière, que les équations analogues du troisième et du quatrième degré, dont l'impossibilité a été démontrée jusqu'à présent, ne sont qu'en nombre fini et même très petit.

Les nombres P et Q devant être premiers entre eux, l'un pair, l'autre impair, et le premier de plus non-divisible par 5, on peut démontrer que, pour égaler le binome P^2-5Q^2 à une cinquième puissance avec toute la généralité convenable, on n'a qu'à poser

$$P+Q\sqrt{5} = (M\pm N\sqrt{5})^5(t\pm u\sqrt{5}),$$

les parties rationnelles et les coefficiens de $\sqrt{5}$ étant égalés séparément, t et u satisfaisant généralement à l'équation $t^2-5u^2 = 1$, et les nombres M et N étant premiers entre eux, l'un pair, l'autre impair, et le premier non-divisible

par 5 (*). Cela supposé, il n'est pas difficile d'établir le théorème que nous allons énoncer.

Théorème I.

„Les nombres P et Q devant être premiers entre eux, l'un pair, l'autre „impair, et le dernier devant être de plus divisible par 5, je dis que pour „égaler le binome P^2-5Q^2 de la manière la plus générale à une cinquième „puissance, il suffira de poser

$$P+Q\sqrt{5} = (\varphi+\psi\sqrt{5})^5.$$

„Les indéterminées φ et ψ étant premières entre elles, l'une paire, l'autre „impaire, et la première de plus non-divisible par 5 (**).“

Pour égaler P^2-5Q^2 à une cinquième puissance, nous poserons, d'après ce qui vient d'être dit,

$$P+Q\sqrt{5} = (M\pm N\sqrt{5})^5(t\pm u\sqrt{5}).$$

N n'étant pas divisible par 5, si nous faisons pour un instant

$$(M+N\sqrt{5})^5 = M'+N'\sqrt{5},$$

il sera facile de voir que N′ est divisible par 5, et que M′ ne l'est pas. En substituant l'expression précédente dans la valeur de $P+Q\sqrt{5}$, on aura

$$P+Q\sqrt{5} = (M'\pm N'\sqrt{5})(t\pm u\sqrt{5}),$$

d'où l'on tire

$$Q = \pm M'u\pm N't.$$

N′ étant divisible par 5, et M′ ne l'étant pas, il est évident que Q ne pourra être divisible par 5, qu'autant que u le sera. Les valeurs les plus petites qui satisfassent à l'équation

$$t^2-5u^2 = 1,$$

sont celles-ci,

$$t = 9, \quad u = 4.$$

(*) Pour ne pas donner trop d'étendue à ce Mémoire, je supprime ici une première partie du mémoire manuscrit contenant quelques théorèmes sur les nombres en tant qu'ils sont de la forme t^2-au^2, et la démonstration de la proposition dont il s'agit, fondée sur ces théorèmes.

(**) Il n'est peut-être pas inutile de faire remarquer qu'il y a des théorèmes analogues pour beaucoup d'autres nombres premiers, et que pour les établir, on peut faire usage des mêmes considérations dont nous nous servons ici.

Les valeurs générales seront par conséquent données par cette formule,

$$t+u\sqrt{5} = (9+4\sqrt{5})^p,$$

dans laquelle p est un nombre entier, positif quelconque (*); on tire de là

$$u = \frac{p}{1}9^{p-1}.4 + \frac{p(p-1)(p-2)}{1.2.3}9^{p-3}.4^3.5 + \text{etc.}$$

Tous les termes de cette valeur, à partir du second, étant divisibles par 5, quel que soit p, on voit que pour que u puisse être divisible par 5, il faut que le premier terme, et par conséquent aussi p, soit divisible par 5. Si nous faisons donc $p = 5p'$, p' étant un entier, et que nous substituions la valeur de $t+u\sqrt{5}$ dans celle de $P+Q\sqrt{5}$, nous aurons

$$P+Q\sqrt{5} = (M\pm N\sqrt{5})^5(9\pm 4\sqrt{5})^{5\psi},$$

résultat qui, par l'introduction des nouvelles indéterminées, φ et ψ qui sont telles que

$$(M\pm N\sqrt{5})(9\pm 4\sqrt{5})^{\psi} = \varphi+\psi\sqrt{5},$$

se change en celui-ci,

$$P+Q\sqrt{5} = (\varphi+\psi\sqrt{5})^5.$$

La forme de la solution donnée par l'énoncé du théorème se trouvant ainsi justifiée, il ne reste plus qu'à déterminer la nature des indéterminées.

Comme on a

$$P^2-5Q^2 = (\varphi^2-5\psi^2)^5,$$

et que les nombres P et Q sont respectivement divisibles par φ et ψ, on voit facilement que les indéterminées φ et ψ doivent être supposées premières entre elles, l'une paire, l'autre impaire, et la première de plus non-divisible par 5. On peut même ajouter que φ ou ψ sera impaire selon que P et Q l'est. Réciproquement, si les indéterminées φ et ψ satisfont aux conditions précédentes, les nombres P et Q déterminés par la formule

$$P+Q\sqrt{5} = (\varphi+\psi\sqrt{5})^5,$$

seront premiers entre eux, comme il est facile de s'en assurer. Ces préliminaires établis, nous pourrons nous occuper des théorèmes qui font l'objet principal de ce Mémoire. Le premier de ces théorèmes peut s'énoncer de la manière suivante.

(*) Voyez les Additions à l'Algèbre d'Euler (art. 75), ou les *Disquisitiones arithmeticae* (art. 200).

Théorème II.

„Les nombres m et n étant positifs, plus grands que zéro, et le second „de plus différent de 2, et le nombre A n'étant divisible ni par 2 ni par 5, „ni par aucun nombre premier de l'une de ces formes $10k\pm1$ (*), il sera im„possible de trouver deux nombres x et y premiers entre eux, tels que „$x^5\pm y^5 = 2^m5^nAz^5$ (α).“

Supposons, contre l'énoncé du théorème, que l'équation soit possible. Comme le second membre est pair (m ayant été supposé >0), il faut que les nombres x et y, qui sont premiers entre eux, soient impairs l'un et l'autre. Si nous faisons $x\pm y = 2p$, $x\mp y = 2q$, et par suite,

$$x = p+q, \quad \pm y = p-q,$$

les nombres p et q seront entiers, premiers entre eux, et de plus l'un pair, l'autre impair. En substituant les valeurs précédentes de x et $\pm y$ dans l'équation (α), on la changera en celle-ci:

$$2p(p^4+10p^2q^2+5q^4) = 2^m5^nAz^5.$$

Le premier membre ne peut être égal au second membre, qui est divisible par 5, qu'autant qu'on suppose p divisible par 5. Faisant donc $p = 5r$, nous aurons

$$2.5^2r(q^4+2.5^2q^2r^2+5^3r^4) = 2^m5^nAz^5.$$

Le nombre n est par hypothèse égal à l'unité ou plus grand que 2. Si n est égal à l'unité, il faudra, dans l'équation précédente, supposer z divisible par 5. On pourra, dans ce cas, mettre $5z$ à la place de z, ou, ce qui est la même chose, donner à 5 l'exposant 6, d'où l'on voit que l'on peut supposer dans tous les cas, que $n>2$. Si l'on met maintenant l'équation précédente sous cette forme,

$$r(q^4+2.5^2q^2r^2+5^3r^4) = 2^{m-1}5^{n-2}Az^5,$$

(*) Les théorèmes de ce Mémoire, de même que ceux qui sont contenus dans l'addition, sont susceptibles d'une extension que je vais indiquer en deux mots. Ces théorèmes ont encore lieu quand même A aurait des diviseurs premiers de la forme $10k-1$. On verra en effet que notre démonstration suppose uniquement que le nombre A ne puisse avoir aucun diviseur commun avec la formule $t^4+10t^2s^2+5s^4$, t et s étant supposés premiers entre eux. Or, cette formule pouvant se mettre sous la forme $\frac{(t+s)^5+(t-s)^5}{2t}$, et le nombre 5 étant premier, il résulte des théorèmes connus d'Euler sur les formes linéaires des diviseurs premiers de l'expression x^n+y^n, que notre formule n'a que des diviseurs premiers de la forme $10k+1$, et est par conséquent première à A. Voyez la Théorie des nombres ou le Mémoire d'Euler, *circa divisores numerorum*, dans le 1er vol. des *Novi Acad. Comment. Petrop.*

et qu'on se rappelle que les nombres q et $p = 5r$, sont premiers entre eux, et de plus, l'un pair, l'autre impair, il sera facile de voir que le facteur trinome est impair, non-divisible par 5, et premier à r; il faut donc que r soit divisible par 5, n étant >2. Choisissons actuellement deux nombres positifs, μ et ν, tels que (*) $m+\mu-1$, $n+\nu-2$, soient divisibles par 5, et un nombre B qui n'ait d'autres diviseurs premiers que le nombre A, et tel que le produit AB soit une cinquième puissance. Si nous multiplions l'équation précédente par $2^\mu 5^\nu B$, nous aurons celle-ci:

$$2^\mu 5^\nu Br(q^4+2.5^2q^2r^2+5^3r^4) = 2^{m+\mu-1}5^{n+\nu-2}ABz^5.$$

Le second membre de cette équation étant une cinquième puissance, le premier membre en sera pareillement une. Or, je dis que les deux facteurs dans lesquels ce premier membre peut se décomposer, le facteur $2^\mu 5^\nu Br$ et le facteur trinome, sont premiers entre eux. En effet, nous avons déjà vu plus haut que le facteur trinome est premier à $2^\mu 5^\nu r$, et pour s'assurer qu'il est également premier à B, on le mettra sous cette forme,

$$(q^2+5^2r^2)^2-5(10r^2)^2.$$

Les nombres $q^2+5^2r^2$ et $10r^2$ étant évidemment premiers entre eux, tout nombre premier par lequel le facteur trinome est divisible, sera de l'une de ces deux formes, $10k\pm1$, dont aucune ne convient par hypothèse aux nombres premiers diviseurs de A, et par conséquent aussi de B, B n'ayant pas d'autres diviseurs premiers que A. Il faut donc que le nombre $2^\mu 5^\nu Br$ et le facteur trinome soient des cinquièmes puissances l'un et l'autre.

Le facteur trinome pouvant s'écrire de cette manière,

$$(q^2+5^2r^2)^2-5(10r^2)^2,$$

et les nombres $q^2+5^2r^2$, $10r^2$ étant premiers entre eux, le premier impair et le second pair et divisible par 5, il suffira, en vertu du théorème I, pour égaler le facteur trinome avec toute la généralité convenable à une cinquième puissance, de poser ces deux équations,

$$q^2+5^2r^2 = t(t^4+2.5^2t^2s^2+5^3s^4),$$
$$10r^2 = 5s(t^4+10t^2s^2+5s^4).$$

(*) Si $m-1$ était divisible par 5, on choisirait pour μ une autre valeur que zéro pour éviter les exposans négatifs dans ce qui va suivre.

Les nombres s et t doivent être supposés premiers entre eux, et de plus le premier pair et le second impair et non-divisible par 5. Il suit de là que s doit être divisible par 5; en effet t n'étant pas divisible par 5, le second membre de la seconde équation ne peut être divisible par 5^2 qu'autant que s est divisible par 5; mais le premier membre qui a r^2 pour facteur, est divisible par 5^2; donc s est divisible par 5.

Nous avons vu plus haut que $2^\mu 5^\nu Br$ devait être une cinquième puissance. Le nombre $2^{2\mu}5^{2\nu}B^2r^2$, carré du nombre précédent, devra donc être une puissance du même degré, et même du dixième degré. Or, en multipliant par $2^{2\mu-1}5^{2\nu-1}B^2$ les deux membres de la dernière équation, on aura celle-ci:

$$2^{2\mu}5^{2\nu}B^2r^2 = 2^{2\mu-1}5^{2\nu}B^2s(t^4+10t^2s^2+5s^4).$$

Si donc nous faisons pour abréger: $2\mu-1=g$, $2\nu=h$, $B^2=C$, tout se réduira à faire voir qu'il est impossible de trouver deux nombres s et t premiers entre eux, et dont le premier soit de plus pair et divisible par 5, tels que le produit

$$2^g5^hCs(t^4+10t^2s^2+5s^4) \quad (\beta)$$

soit une cinquième puissance.

En ayant égard à la nature des diviseurs premiers de C, on s'assurera facilement que le facteur 2^g5^hCs et le facteur trinôme sont premiers entre eux. Il faudrait donc, pour que le produit (β) pût être une cinquième puissance, que chacun de ces facteurs en fût pareillement une. Le facteur trinôme peut s'écrire de cette manière:

$$(t^2+5s^2)^2-5(2s^2)^2.$$

Comme les nombres t^2+5s^2, $2s^2$ sont évidemment premiers entre eux, et de plus le premier impair et le second pair et divisible par 5, le théorème I est applicable ici, et l'on pourra poser

$$t^2+5s^2 = t'(t'^4+2.5^2t'^2s'^2+5^3s'^4)$$
$$2s^2 = 5s'(t'^4+10t'^2s'^2+5s'^4).$$

Les nombres s' et t' doivent être supposés premiers entre eux, et de plus le premier pair et le second impair et non-divisible par 5. Comme t' n'est pas divisible par 5, il est évident par la seconde équation, dont le premier membre renferme le facteur s^2, et est par conséquent divisible par 5^2, que s'

doit être divisible par 5. Ainsi les nombres s' et t' sont premiers entre eux, de même que les nombres s et t, et le premier s' est en outre pair et divisible par 5 comme s.

Il est facile encore de voir que s' est plus petit que s; car on conclut immédiatement de la dernière équation $5^2 s'^5 < 2s^2$ et par suite $s' < \sqrt[5]{\frac{2s^2}{25}}$.

On a vu plus haut que $2^g 5^h C s$ devait être une cinquième puissance. Le nombre $2^{2g} 5^{2h} C^2 s^2$, carré du précédent, devra donc être une puissance du même degré. Or, en multipliant les deux membres de la dernière équation par $2^{2g-1} 5^{2h} C^2$, on aura

$$2^{2g} 5^{2h} C^2 s^2 = 2^{2g-1} 5^{2h+1} C^2 s' (t'^4 + 10 t'^2 s'^2 + 5 s'^4),$$

ou ce qui est la même chose en faisant $2g-1 = g'$, $2h+1 = h'$, $C^2 = C'$, dans le second membre,

$$2^{2g} 5^{2h} C^2 s^2 = 2^{g'} 5^{h'} C' s' (t'^4 + 10 t'^2 s'^2 + 5 s'^4), \quad (\beta')$$

équation dont les deux membres doivent être des puissances du cinquième degré.

Nous voilà donc arrivés à un produit (β') semblable au produit (β), mais dans lequel le nombre s' est plus petit que le nombre s du produit (β), et ce produit (β') serait une cinquième puissance, si le produit (β) en était une. En traitant le produit (β') comme nous avons traité le produit (β), on arriverait à un troisième produit (β''), dans lequel le nombre s'' serait plus petit que s', et l'on pourrait continuer ce procédé aussi loin que l'on voudrait. Il est facile de voir en outre que quelque loin que l'on prolonge les séries $s, s', s'', \ldots$; $t, t', t'', \ldots$, on ne pourra jamais rencontrer un terme égal à zéro; car il est évident que si l'on supposait nul un de ces termes, on conclurait en remontant que $s = 0$, cas évident, et qui d'ailleurs est exclu, puisque les nombres s et t ont été supposés premiers entre eux.

Si donc le produit (β) pouvait être une cinquième puissance, on pourrait obtenir, par l'analyse précédente, une suite indéfinie de nombres entiers positifs, dans laquelle chaque terme serait plus petit que le terme précédent, sans qu'aucun des termes ne fût nul; ce qui implique contradiction. On doit conclure de là que le produit (β) ne saurait être une puissance du cinquième degré.

Le théorème II se trouvant ainsi établi, nous allons donner le moyen d'en déduire un autre théorème plus général. Considérons l'équation

$$x^5 \pm y^5 = 2^m A z^5,$$

dans laquelle nous supposons x et y premiers entre eux, $m > 0$, et A soumis aux mêmes restrictions que dans l'énoncé du théorème II. Soient α, β, γ des nombres positifs moindres que 5, et tels que $x \equiv \alpha$, $\pm y \equiv \beta$, $z \equiv \gamma \pmod 5$ et soit encore H un nombre positif < 25 et tel que $2^m A \equiv H \pmod{25}$. Comme 5 est un nombre premier, on aura

$$x^5 \equiv x, \quad y^5 \equiv y, \quad z^5 \equiv z, \quad \pmod 5.$$

On conclut de là, en ayant égard à l'équation posée plus haut,

$$x \pm y \equiv 2^m A z \pmod 5,$$

et partant

$$\alpha + \beta \equiv H\gamma \pmod 5.$$

Comme α est le reste de x, on pourra poser $x = \alpha + 5k$, k étant un entier; on tire de là, en élevant les deux membres à la cinquième puissance,

$$x^5 = \alpha^5 + 5.\alpha^4 (5k) + \frac{5.4}{1.2} \alpha^3 (5k)^2 + \text{etc.},$$

et on aura donc

$$x^5 \equiv \alpha^5 \pmod{25}.$$

On trouvera de la même manière $\pm y^5 \equiv \beta^5$, $z^5 \equiv \gamma^5 \pmod{25}$, et comme on a aussi $2^m A \equiv H \pmod{25}$, on trouvera, en ayant égard à l'équation citée,

$$\alpha^5 + \beta^5 \equiv H\gamma^5 \pmod{25}.$$

Si maintenant, en substituant dans cette congruence, successivement pour α, β, toutes les combinaisons que l'on peut former avec les nombres positifs moindres que 5, et pour γ les valeurs correspondantes également moindres que 5, données par la formule

$$\alpha + \beta \equiv H\gamma \pmod 5,$$

on trouve que la congruence $\alpha^5 + \beta^5 \equiv H\gamma^5 \pmod{25}$ ne peut subsister que lorsque γ est nul, on sera assuré que l'équation

$$x^5 \pm y^5 = 2^m A z^5$$

ne peut avoir lieu, à moins qu'on ne suppose z divisible par 5. On pourra donc, dans ce cas, mettre $5z$ à la place de z, ce qui change notre équation

en celle-ci:

$$x^5 \pm y^5 = 2^m 5^5 A z^5,$$

qui rentre évidemment dans le théorème II, et par conséquent est impossible. Or, ce cas a lieu toutes les fois que le nombre H est un des huit nombres suivans, 3, 4, 9, 12, 13, 16, 21, 22, comme on peut s'en assurer par un calcul très simple. Nous avons donc ainsi ce nouveau théorème:

Théorème III.

„Les nombres m et A étant soumis aux mêmes restrictions que dans „l'énoncé du théorème II, si le nombre $2^m A$, étant divisé par 25, donne un des „huit restes suivans, 3, 4, 9, 12, 13, 16, 21, 22, il sera impossible de trouver „deux nombres x et y premiers entre eux, tels que l'on ait $x^5 \pm y^5 = 2^m A z^5$."

Pour donner un exemple bien simple, considérons les deux équations suivantes: $x^5 \pm y^5 = 4z^5$, $x^5 \pm y^5 = 16z^5$.

Comme dans ces équations on peut, sans nuire à la généralité, supposer les nombres x et y premiers entre eux, il sera facile de voir qu'elles rentrent dans le théorème II. En effet, si l'on fait $A = 1$, et successivement $m = 2$, $m = 4$, on aura respectivement

$$2^m A = 4, \quad 2^m A = 16.$$

Il est donc prouvé que les deux équations précédentes sont impossibles.

Considérons encore l'équation

$$x^5 \pm y^5 = z^5,$$

qui est une de celles que Fermat a assurées être impossibles. Par des considérations semblables à celles qui nous ont servi pour établir le théorème précédent, on peut s'assurer que cette équation ne saurait subsister, à moins qu'une des indéterminées x, y, z, ne soit divisible par 5. Soit z l'indéterminée divisible par 5, car il est évident qu'on peut faire en sorte qu'une quelconque des indéterminées se trouve toute seule dans un membre. D'un autre côté, si l'on suppose ces indéterminées premières entre elles, l'une d'elles sera paire et les deux autres seront impaires. Si z était paire, on pourrait remplacer cette indéterminée par $2.5.z$, ce qui changerait l'équation précédente en celle-ci:

$$x^5 \pm y^5 = 2^5 5^5 z^5,$$

qui est impossible, puisqu'elle rentre évidemment dans le théorème II. Il ne resterait donc qu'à traiter le cas où l'indéterminée divisible par 5, serait impaire; mais la méthode exposée dans ce Mémoire paraît insuffisante pour ce cas, et je ne vois pas comment on pourrait compléter la démonstration du cas particulier du théorème de Fermat, dont il vient d'être question.

ADDITION AU MÉMOIRE PRÉCÉDENT.

(Cette Addition a été présentée à l'Académie, et paraphée par M. le secrétaire perpétuel Fourier, le 14 novembre 1825.)

Depuis que le Mémoire précédent a été présenté à l'Académie, M. Legendre a publié un second supplément à sa Théorie des nombres, dans lequel il démontre l'impossibilité de l'équation

$$x^5 \pm y^5 = z^5.$$

Le cas de l'indéterminée divisible en même temps par 2 et par 5, est traité dans cet ouvrage comme dans le Mémoire précédent, et l'auteur prouve ensuite l'impossibilité de l'autre cas au moyen d'une analyse nouvelle, quoique du même genre que celle qui sert pour le premier cas. L'objet de cette addition est d'établir deux théorèmes nouveaux sur les équations indéterminées du cinquième degré, et qui comprennent, comme cas particulier, le théorème de Fermat pour les cinquièmes puissances. Pour y parvenir, je m'appuie sur les résultats obtenus dans ce qui précède, et je fais usage d'une analyse semblable à celle dont M. Legendre s'est servi dans l'ouvrage cité, et que je présente de manière à montrer la grande analogie qu'elle a avec la méthode exposée dans le mémoire précédent.

Les nombres P et Q, dont le premier est supposé n'être pas divisible par 5, étant impairs tous les deux, et n'ayant pas de diviseur commun, le nombre $P^2 - 5Q^2$ sera de la forme $8k+4$, et l'on pourra faire

$$P^2 - 5Q^2 = 4L,$$

L étant un nombre impair et non-divisible par 5. Si nous multiplions membre par membre l'équation précédente et celle-ci,

$$3^2-5.1^2=4,$$

nous aurons

$$(3P\pm5Q)^2-5(P\pm3Q)^2=16L.$$

Comme les nombres P et Q sont impairs tous les deux, il est évident qu'en déterminant convenablement le signe, les expressions

$$\frac{3P\pm5Q}{4},\qquad\frac{P\pm3Q}{4},$$

seront entières l'une et l'autre; faisant en conséquence

$$\frac{3P\pm5Q}{4}=P',\qquad\frac{\pm(P\pm3Q)}{4}=Q',$$

le signe en dehors de la parenthèse étant choisi de manière à donner une valeur positive pour Q', l'équation obtenue plus haut se changera en celle-ci, $P'^2-5Q'^2=L$, et l'on s'assurera facilement que l'on a

$$P+Q\sqrt5=(P'\pm Q'\sqrt5)(3\pm\sqrt5),$$

les signes étant convenablement choisis, et que les nombres P' et Q' sont premiers entre eux, et de plus l'un pair, l'autre impair.

Supposons maintenant que le nombre L doive être une cinquième puissance. On satisfera à cette condition de la manière la plus générale en posant

$$P'+Q'\sqrt5=(M\pm N\sqrt5)^5(9\pm4\sqrt5)^p.$$

En substituant cette valeur dans la dernière équation, on aura celle-ci:

$$P+Q\sqrt5=(M\pm N\sqrt5)^5(9\pm4\sqrt5)^p(3\pm\sqrt5),$$

dans laquelle les signes sont indépendans, comme dans les deux équations précédentes. On peut faire $p=5k\pm r$, k étant entier et positif, et r ayant une de ces trois valeurs, 0, 1, 2, la quantité $(9\pm4\sqrt5)^p$ se décomposera ainsi en ces deux facteurs $(9\pm4\sqrt5)^{5k}$ et $(9\pm4\sqrt5)^{\pm r}$ dont le premier peut être omis parce qu'il rentre dans $(M\pm N\sqrt5)^5$. Si nous observons de plus qu'en vertu de l'équation

$$9\pm4\sqrt5=(9\mp4\sqrt5)^{-1},$$

on peut changer dans $(9\pm4\sqrt5)^{\pm r}$ simultanément les signes de r et du radical, nous pouvons supposer le signe de r positif, et l'équation donnée plus haut deviendra

$$P+Q\sqrt5=(M\pm N\sqrt5)^5(9\pm4\sqrt5)^r(3\pm\sqrt5).$$

L devant toujours être la cinquième puissance d'un nombre impair et non-divisible par 5, déterminons les conditions nécessaires pour que Q soit divisible par 5. Comme le coefficient de $\sqrt5$, dans le développement de $(M\pm N\sqrt5)^5$ est divisible par 5, et que la partie rationnelle de ce développement ne l'est pas, M n'étant pas divisible par 5, on conclut, comme dans la démonstration du théorème I, que pour que Q puisse être divisible par 5, il faut que le coefficient de $\sqrt5$, dans la valeur développée de $(9\pm4\sqrt5)^r(3\pm\sqrt5)$ le soit.

Or, en substituant pour r successivement les trois valeurs 0, 1, 2, on trouve que cela n'a lieu que dans le cas de $r=2$, les signes des radicaux dans les deux facteurs $(9\pm4\sqrt5)^r$ et $(3\pm\sqrt5)$ étant en même temps opposés. Si l'on fait attention que l'on a

$$\frac{(3\pm\sqrt5)^3}{2^3}=9\pm4\sqrt5\quad\text{et}\quad3\mp\sqrt5=\frac{4}{3\pm\sqrt5},$$

on trouvera que le produit précédent sera, dans le cas dont il s'agit, équivalent à

$$\frac{(3\pm\sqrt5)^5}{2^4},$$

valeur dont la substitution dans l'équation obtenue plus haut, la change en celle-ci:

$$P+Q\sqrt5=\frac{(M\pm N\sqrt5)^5(3\pm\sqrt5)^5}{2^4}.$$

Les nombres M et N étant l'un pair, l'autre impair, les nombres φ et ψ déterminés par l'équation

$$\varphi+\psi\sqrt5=(M\pm N\sqrt5)(3\pm\sqrt5)$$

seront impairs l'un et l'autre, et l'on aura

$$P+Q\sqrt5=\frac{(\varphi+\psi\sqrt5)^5}{2^4}$$

et par conséquent

$$P = \varphi\frac{(\varphi^4+2.5^2\varphi^2\psi^2+5^3\psi^4)}{2^4},$$

$$Q = 5\psi\frac{(\varphi^4+10\varphi^2\psi^2+5\psi^4)}{2^4}.$$

Pour que P et Q soient premiers entre eux, il faut que φ et ψ n'aient pas de diviseur commun, et que le premier de ces nombres ne soit pas divisible par 5, et réciproquement, si les nombres φ et ψ, dont le premier est supposé ne pas être divisible par 5, n'ont pas de diviseur commun, et sont impairs l'un et l'autre, les nombres P et Q seront entiers et premiers entre eux. En effet, le quart de la quantité $\varphi^4+10\varphi^2\psi^2+5\psi^4$, pouvant se mettre sous la forme

$$\left(\frac{\varphi^2+5\psi^2}{2}\right)^2-5(\psi^2)^2,$$

et cette dernière expression étant évidemment le quadruple d'un nombre impair, on voit que la valeur de Q est entière et impaire; la même chose se prouvera pour la valeur de P, et l'on s'assurera facilement que les nombres P et Q, qui sont impairs tous les deux, n'ont pas de diviseur commun. Nous avons donc ainsi ce théorème:

Théorème IV.

„Les nombres P et Q devant être premiers entre eux, et impairs l'un „et l'autre, et le dernier devant être divisible par 5, je dis que pour égaler le „binome P^2-5Q^2, au quadruple d'une cinquième puissance avec toute la géné„ralité convenable, il suffira de poser

$$P+Q\sqrt{5} = \frac{(\varphi+\psi\sqrt{5})^5}{2^4},$$

„les nombres indéterminés φ et ψ étant premiers entre eux, impairs l'un et „l'autre, et le premier de plus non-divisible par 5 (*).“

Voici maintenant le premier des théorèmes nouveaux que nous avons annoncés au commencement de cette addition.

(*) Ce théorème, comme le théorème I, a ses analogues pour beaucoup d'autres nombres premiers.

Théorème V.

„La lettre n désignant un nombre positif autre que 0 et 2, et le „nombre A n'étant divisible ni par 2 ni par 5, ni par aucun nombre premier „de l'une de ces deux formes $10k\pm1$, il sera impossible de trouver deux „nombres x et y premiers entre eux, et tels que

$$x^5\pm y^5 = 5^nAz^5 \quad (\gamma).“$$

Les nombres x et y peuvent être impairs tous les deux, ou l'un pair et l'autre impair. Dans le premier cas, z sera divisible par 2, et l'on pourra mettre $2z$ à la place de z, ce qui changera l'équation (γ) en celle-ci:

$$x^5\pm y^5 = 2^5 5^n Az^5,$$

qui est impossible puisqu'elle rentre évidemment dans le théorème II. Reste donc à prouver l'impossibilité du second cas où l'on suppose les nombres x, y, l'un pair, l'autre impair. Si nous faisons

$$x\pm y = p, \quad x\mp y = q,$$

nous aurons

$$2x = p+q, \quad \pm 2y = p-q,$$

et les nombres p et q seront premiers entre eux, et de plus impairs l'un et l'autre. En substituant les valeurs précédentes de $2x$ et $\pm 2y$ dans l'équation (γ), après en avoir multiplié les deux membres par 2^5, on aura

$$p(p^4+10p^2q^2+5q^4) = 2^4 5^n Az^5.$$

Comme p doit évidemment être divisible par 5, nous ferons $p = 5r$, ce qui donnera

$$5^2 r(q^4+2.5^2q^2r^2+5^3r^4) = 2^4 5^n Az^5.$$

Le nombre n est par hypothèse égal à l'unité ou plus grand que 2. Si n est égal à l'unité, il faudra, dans l'équation précédente, supposer z divisible par 5. On pourra donc, dans ce cas, mettre $5z$ à la place de z, ou, ce qui est la même chose, donner à 5 l'exposant 6, d'où l'on voit que l'on peut supposer dans tous les cas que $n>2$.

Si l'on met l'équation précédente sous cette forme

$$r(q^4+2.5^2q^2r^2+5^3r^4) = 2^4 5^{n-2} Az^5,$$

et qu'on fasse attention que $n>2$, et que q est premier à $p = 5r$, on voit que r doit être supposé divisible par 5.

Choisissons maintenant un nombre positif ν tel que $n+\nu-2$ soit divisible par 5 et un nombre B qui n'ait d'autre diviseur premier que le nombre A et tel que le produit AB soit une cinquième puissance. Multipliant la dernière équation par $5^{\nu}B$, nous aurons

$$5^{\nu}Br(q^4+2.5^2q^2r^2+5^3r^4) = 2^4 5^{n+\nu-2}ABz^5.$$

Le facteur trinome pouvant se mettre sous la forme $(q^2+5^2r^2)^2-5(10r^2)^2$ et les nombres $q^2+5^2r^2$, $10r^2$ n'ayant évidemment d'autre diviseur commun que 2, tous les diviseurs premiers impairs du facteur trinome seront d'une de ces formes $10k\pm1$, et le facteur trinome sera par conséquent premier à B. Il est évident qu'il est aussi premier à $5^{\nu}r$, et par conséquent à $5^{\nu}Br$.

Comme le facteur $5^{\nu}Br$ et le facteur trinome sont premiers entre eux, et que le premier de ces facteurs est impair, il faut en vertu de la dernière équation, dont le second membre est le produit de 2^4 et de la cinquième puissance d'un nombre impair, que $5^{\nu}Br$ soit une cinquième puissance, et le facteur trinome une cinquième puissance multipliée par 2^4.

Le quart du facteur trinome devant être le quadruple d'une cinquième puissance, et ce quart pouvant se mettre sous la forme

$$\left(\frac{q^2+5^2r^2}{2}\right)^2-5(5r^2)^2,$$

où les nombres $\frac{q^2+5^2r^2}{2}$, $5r^2$, sont évidemment premiers entre eux, impairs l'un et l'autre, et le dernier de plus divisible par 5, il suffira en vertu du théorème établi au commencement de cette addition, pour égaler le quart du facteur trinome au quadruple d'une cinquième puissance, de poser ces deux équations

$$\frac{q^2+5^2r^2}{2} = t\frac{(t^4+2.5^2t^2s^2+5^3s^4)}{2^4}$$

$$5r^2 = 5s\frac{(t^4+10t^2s^2+5s^4)}{2^4},$$

les nombres indéterminés t et s devant être supposés premiers entre eux, impairs l'un et l'autre, et le premier de plus non-divisible par 5. Comme t n'est pas divisible par 5, et que r l'est comme nous l'avons vu ci-dessus, il faut, en vertu de la dernière des équations précédentes, que s soit divisible par 5.

Nous avons vu plus haut que $5^{\nu}Br$ devait être une cinquième puissance. Le nombre $5^{2\nu}B^2r^2$, carré du précédent, devra donc être une puissance du même degré, et même du dixième degré.

Or, en multipliant par $2^4.5^{2\nu-1}B^{\nu}$ les deux membres de la dernière équation, on aura celle-ci:

$$2^4 5^{2\nu}B^{\nu}r^2 = 5^{2\nu}B^{\nu}s(t^4+10t^2s^2+5s^4).$$

Si donc nous faisons pour abréger $2\nu = h$, $B^2 = C$, tout se réduit à faire voir qu'il est impossible de trouver deux nombres t et s premiers entre eux, impairs l'un et l'autre, et dont le dernier s soit de plus divisible par 5, tels que le produit

$$5^h Cs(t^4+10t^2s^2+5s^4) \quad (\delta)$$

soit une cinquième puissance multipliée pas 2^4.

Il est facile de voir que le produit (δ) ne saurait être le produit de 2^4 et d'une cinquième puissance, à moins que $5^h Cs$ ne soit une cinquième puissance, et le facteur trinome une cinquième puissance multipliée par 2^4.

Le quart du facteur trinome devant être le quadruple d'une cinquième puissance, et ce quart pouvant se mettre sous la forme

$$\left(\frac{t^2+5s^2}{2}\right)^2-5(s^2)^2,$$

où les nombres $\frac{t^2+5s^2}{2}$, s^2 sont évidemment premiers entre eux, impairs l'un et l'autre, et le dernier de plus divisible par 5, il suffira, pour égaler le facteur trinome divisé par 4 au quadruple d'une cinquième puissance, de poser ces équations

$$\frac{t^2+5s^2}{2} = t'\frac{(t'^4+2.5^2t'^2s'^2+5^3s'^4)}{2^4}$$

$$s^2 = 5s'\frac{(t'^4+10t'^2s'^2+5s'^4)}{2^4},$$

les nombres t' et s' étant supposés premiers entre eux, impairs l'un et l'autre, et le premier t' de plus non-divisible par 5. Comme s est divisible par 5, et que t' ne l'est plus, il faut, d'après la dernière équation, que s' soit aussi divisible par 5. On conclut encore de la dernière équation, que $\frac{25}{16}s'^5 < s^2$ et par suite que s' est beaucoup plus petit que s.

Le nombre $5^h Cs$ devant être une cinquième puissance, $5^{2h}C^2s^2$ carré du nombre précédent, devra être une puissance du même degré, et même du dixième

degré. Or, en multipliant par $2^4 5^{2h} C^2$ les deux membres de la dernière équation, on aura celle-ci:

$$2^4 5^{2h} C^2 s^2 = 5^{2h+1} C^2 s'(t'^4 + 10t'^2 s'^2 + 5s'^4)$$

ou ce qui est la même chose, en faisant $2h+1 = h'$, $C^2 = C'$, dans le second membre,

$$2^4 5^{2h} C^2 s^2 = 5^{h'} C' s'(t'^4 + 10t'^2 s'^2 + 5s'^4), \quad (\vartheta')$$

équation dont les deux membres devront être des cinquièmes puissances multipliées par 2^4.

Le produit (ϑ') étant parfaitement semblable au produit (ϑ), et le nombre s' étant beaucoup plus petit que le nombre s, on conclura, comme dans la démonstration du théorème II du mémoire précédent, que le produit (ϑ) ne saurait être égal à une cinquième puissance, multipliée par 2^4, et que par conséquent l'équation (γ) ne saurait avoir lieu.

Le théorème de Fermat, pour le cas des cinquièmes puissances, est compris comme cas particulier dans le théorème que nous venons d'établir. En effet, l'équation $x^5 \pm y^5 = z^5$ ne pouvant avoir lieu, à moins qu'une des indéterminées, z par exemple, ne soit divisible par 5, nous pouvons mettre $5z$ à la place de z; ce qui donnera $x^5 \pm y^5 = 5^5 z^5$, équation impossible, puisqu'elle rentre dans le dernier théorème.

Un raisonnement tout-à-fait semblable à celui au moyen duquel nous avons établi le théorème III, en partant du théorème II, peut servir à déduire du théorème que nous venons de démontrer un nouveau théorème qui peut s'énoncer comme il suit:

Théorème VI.

„Le nombre A étant soumis aux mêmes restrictions que dans l'énoncé „du théorème V, et ce nombre donnant un des huit restes suivans, 3, 4, 9, „12, 13, 16, 21, 22, lorsqu'il est divisé par 25, il sera impossible de trouver „deux nombres x et y premiers entre eux, et tels que l'on ait $x^5 \pm y^5 = Az^5$."

FIN.

MÉMOIRE SUR L'IMPOSSIBILITÉ DE QUELQUES ÉQUATIONS INDÉTERMINÉES DU CINQUIÈME DEGRÉ.

PAR

Mr. LEJEUNE DIRICHLET,
PROFESSEUR EN MATHÉMATIQUES.

LU A L'ACADÉMIE ROYALE DES SCIENCES (INSTITUT DE FRANCE), LE 11 JUILLET 1825, PAR L'AUTEUR.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 3 S. 354—375.

MÉMOIRE SUR L'IMPOSSIBILITÉ DE QUELQUES ÉQUATIONS INDÉTERMINÉES DU CINQUIÈME DEGRÉ.

Lu à l'Académie royale des Sciences (Institut de France) le 11 juillet 1825, par l'auteur.

(D'APRÈS LE RAPPORT DE MM. LACROIX ET LEGENDRE, CE MÉMOIRE A ÉTÉ APPROUVÉ, ET DOIT ÊTRE IMPRIMÉ DANS LE RECUEIL DES MÉMOIRES DE SAVANTS ÉTRANGERS*)).

On sait que la théorie des équations indéterminées des degrés supérieurs au second, est encore très peu avancée; il est vrai qu'il y a une infinité d'équations de tous les degrés dont on peut démontrer l'impossibilité en faisant voir que quelles que soient les valeurs que l'on attribue aux indéterminées, les deux membres de l'équation proposée ne peuvent jamais donner le même reste lorsqu'on les divise par un certain nombre ou module; mais lorsqu'une équation ne peut pas être traitée par ce moyen, il devient difficile de prouver qu'elle est impossible, et on n'y est parvenu, jusqu'à présent, que pour un très petit nombre d'équations. Toutes ces équations sont très particulières, et d'une forme telle, que lorsqu'on cherche à les résoudre, on est naturellement conduit à une ou plusieurs formules quadratiques qu'il s'agit d'égaler à des puissances parfaites. On satisfait ensuite de la manière la plus générale à cette condition, en exprimant les indéterminées par d'autres, dont les premières deviennent des fonctions entières, et il se trouve, du moins dans tous les cas où la méthode dont il est question réussit, que les nouvelles indéterminées ou d'autres quantités qui en dépendent d'une manière très simple, satisfont également à une équation semblable à l'équation proposée. Comme les nouvelles indéterminées sont en même temps plus petites que les indéterminées primitives, l'impossibilité de l'équation proposée se trouve établie; car il est évident que si elle était possible, on aurait le moyen d'obtenir une suite décroissante et indéfinie de nombres entiers, ce qui implique contradiction. C'est de cette

*) Ce Mémoire n'a pas encore été publié jusqu'ici. (Note d. réd.)

manière que FERMAT et EULER ont prouvé l'impossibilité de plusieurs équations du troisième et du quatrième degré.

En essayant d'appliquer des considérations semblables à quelques équations du cinquième degré et d'une forme analogue à celles des équations traitées par FERMAT et EULER, on est arrêté tout aussitôt. La formule quadratique à laquelle on arrive, et qu'il faut égaler à une cinquième puissance, admet plusieurs solutions différentes, et parmi ces solutions, il n'y en a qu'une seule qui conduise à une équation semblable à l'équation proposée. En réfléchissant à cette difficulté, j'ai reconnu qu'elle pouvait être levée très simplement en assujettissant à quelques conditions le nombre déterminé qui entre dans l'équation. Il résulte d'un théorème exposé dans les préliminaires, que lorsque ces conditions se trouvent remplies, les différentes solutions dont la formule quadratique est susceptible, en général, doivent être rejetées, à l'exception d'une seule, qui est précisément celle de laquelle on déduit des nombres qui satisfont à une équation semblable à l'équation proposée. On parvient ainsi à établir l'impossibilité d'une classe assez étendue d'équations indéterminées du cinquième degré. Le premier membre de ces équations est la somme ou la différence de deux cinquièmes puissances, et le second membre est le produit d'une cinquième puissance et d'un nombre déterminé assujetti à différentes conditions. En attribuant à ce nombre des valeurs particulières compatibles avec ces conditions, on peut obtenir autant de théorèmes particuliers que l'on veut. Cette généralité de nos théorèmes est d'autant plus singulière, que les équations analogues du troisième et du quatrième degré, dont l'impossibilité a été démontrée jusqu'à présent, ne sont qu'en nombre fini et même très petit.

Théorème I.

„Soit l un nombre premier impair non-diviseur du nombre a et supposons que l'on ait:

$$\delta^2 - a\varepsilon^2 \equiv l, \tag{1}$$

on satisfera, comme on sait, à l'équation:

$$d^2 - ae^2 = l^n \tag{2}$$

par les nombres d et e que donne la formule:

$$(\delta + \varepsilon\sqrt{a})^n = d + e\sqrt{a}, \tag{3}$$

lorsqu'on y égale les parties rationnelles et les coefficients de $\sqrt{a}$; je dis de plus que les nombres d et e ainsi obtenus seront premiers entre eux*).“

Il est évident, par l'équation (2), que si les nombres d et e avaient un diviseur commun, ce ne pourrait être que le nombre l ou une puissance de ce nombre. Il suffira donc de faire voir que d n'est pas divisible par l. La formule (3) donne cette valeur de d:

$$d = \delta^n + \frac{n(n-1)}{1.2} a\delta^{n-2}\varepsilon^2 + \frac{n(n-1)(n-2)(n-3)}{1.2.3.4} a^2\delta^{n-4}\varepsilon^4 + \text{etc.}$$

D'un autre côté, on conclut de l'équation (1), en se servant du signe employé par M. GAUSS:

$$\delta^2 \equiv a\varepsilon^2, \quad \delta^4 \equiv a^2\varepsilon^4, \quad \delta^6 \equiv a^3\varepsilon^6, \quad \ldots \pmod{l},$$

et en multipliant respectivement par δ^{n-2}, δ^{n-4}, ...:

$$\delta^n \equiv a\delta^{n-2}\varepsilon^2, \quad \delta^n \equiv a^2\delta^{n-4}\varepsilon^4, \quad \ldots \pmod{l}.$$

En combinant ces congruences avec l'équation qui donne d, on aura:

$$d \equiv \delta^n\left(1 + \frac{n(n-1)}{1.2} + \frac{n(n-1)(n-2)(n-3)}{1.2.3.4} + \text{etc.}\right),$$

ou, ce qui est la même chose, la quantité entre les crochets étant le développement de $\frac{1}{2}[(1+1)^n + (1-1)^n]$ et par conséquent égale à 2^{n-1}:

$$d \equiv 2^{n-1}\delta^n \pmod{l}.$$

Il est maintenant facile de voir que d n'est pas divisible par l, car il faudrait pour cela que δ fût divisible par l; mais la seule inspection de l'équation (1) montre que cela est impossible, δ et ε étant évidemment premiers entre eux et a non divisible par l.

Théorème II.

„La lettre l désignant un nombre premier impair non-diviseur de a, si l'on suppose que l'on ait:

$$d^2 - ae^2 = l^n, \tag{4}$$

$$d'^2 - ae'^2 = l^n, \tag{5}$$

les nombres d et e, d' et e' étant premiers entre eux, je dis que l'on pourra

*) Si le nombre l, au lieu d'être premier, était un nombre impair quelconque et que les nombres δ et $a\varepsilon$ fussent premiers entre eux, les nombres d et α seraient également premiers entre eux, comme il est facile de s'en assurer par un raisonnement parfaitement semblable à celui dont nous faisons usage dans le texte.

trouver deux nombres t et u satisfaisant à l'équation:

$$t^2 - au^2 = 1 \tag{6}$$

et en outre tels que l'on ait:

$$(d' \pm e'\sqrt{a})(t \pm u\sqrt{a}) = d + e\sqrt{a}, \tag{7}$$

les signes étant convenablement choisis et les parties rationnelles et les coefficients de $\sqrt{a}$ égalés séparément."

Les équations (4) et (5) donnent immédiatement:

$$d^2 \equiv ae^2, \quad d'^2 \equiv ae'^2, \pmod{l^n};$$

on conclut de là en multipliant membre à membre:

$$d^2 d'^2 \equiv a^2 e^2 e'^2 \pmod{l^n},$$

et en transposant:

$$d^2 d'^2 - a^2 e^2 e'^2 \equiv (dd' + aee')(dd' - aee') \equiv 0 \pmod{l^n}.$$

On voit par cette congruence qu'un des nombres $dd' + aee'$, $dd' - aee'$ est divisible par l^n ou qu'ils sont l'un et l'autre divisibles par l *).

Mais il est facile de voir que ce dernier cas est impossible; en effet, si ces nombres étaient tous les deux divisibles par l, leur somme $2dd'$ le serait également; il faudrait donc, dans ce cas, qu'un des nombres d, d' fût divisible par l; mais on s'assurera facilement que cela ne saurait être, en ayant égard aux suppositions faites dans l'énoncé du théorème. L'expression $\frac{dd' \pm aee'}{l^n}$ avec le signe convenable sera donc un entier. Nous ferons, pour plus de simplicité, $i = \pm 1$, i étant choisi de manière à rendre entière l'expression précédente.

Si l'on multiplie membre à membre les équations (4) et (5), on aura celle-ci:

$$(dd' \pm aee')^2 - a(d' \pm de')^2 = e^{2n},$$

dans laquelle on peut prendre à volonté les signes supérieurs ou les signes inférieurs. On a donc aussi:

$$(dd' + iaee')^2 - a(d'e + ide')^2 = l^{2n}.$$

Le nombre $dd' + iaee'$ étant divisible par l^n, et a n'étant pas divisible par l,

*) Dans le cas de $n = 1$, la première hypothèse est comprise dans la seconde et a par conséquent nécessairement lieu, mais le même raisonnement prouverait toujours l'impossibilité de la seconde.

on voit, par l'équation précédente que $d'e + ide'$ est également divisible par l^n. Cela posé, je dis qu'on aura:

$$t = \frac{dd' + iaee'}{l^n}, \quad u = \frac{i'(d'e + ide')}{l^n},$$

i' étant 1, ou -1 selon que la quantité entre les parenthèses est positive ou négative. En effet, on aura en divisant les deux nombres de l'équation donnée plus haut par l^{2n}:

$$\left(\frac{dd' + iaee'}{l^n}\right)^2 - a\left(\frac{d'e + ide'}{l^n}\right)^2 = 1,$$

ou, ce qui est la même chose, $t^2 - au^2 = 1$, et on s'assurera facilement par la substitution que les valeurs précédentes de t et u satisfont aussi à l'équation (7), en y déterminant les signes de cette manière:

$$(d' - ie'\sqrt{a})(t + i'u\sqrt{a}) = d + e\sqrt{a}.$$

Remarque. Comme il est évident qu'on peut changer simultanément les signes de e', u, e dans l'équation:

$$(d' \pm e'\sqrt{a})(t \pm u\sqrt{a}) = d + e\sqrt{a},$$

on voit que l'on peut poser:

$$(d' \pm e'\sqrt{a})(t \pm u\sqrt{a}) = (d \pm e\sqrt{a}),$$

le signe de e étant à volonté et les signes de e' et u étant convenablement choisis.

Théorème III.

„La lettre l désignant un nombre premier impair non-diviseur de a, et k un nombre impair qui n'a pas de diviseur commun avec a et qui n'est pas divisible par l, si nous supposons que l'on ait ces deux équations $D^2 - aE^2 = l^n k$, $d^2 - ae^2 = l^n$, et que les nombres D et E, d et e soient premiers entre eux, je dis que l'on pourra trouver deux nombres D' et E', premiers entre eux, satisfaisant à l'équation $D'^2 - 5E'^2 = k$, et en outre tels que l'on ait:

$$(D' \pm E'\sqrt{a})(d \pm e\sqrt{a}) = D + E\sqrt{a},$$

les signes étant convenablement choisis et les parties rationnelles et les coefficients de $\sqrt{a}$ étant égalés séparément."

La démonstration de ce théorème est tellement semblable à celle du théorème II. que nous nous dispenserons de la développer ici.

Il y a ici une remarque semblable à faire et l'on voit très facilement que l'on peut poser:

$$(D'\pm E'\sqrt{a})(d\pm e\sqrt{a}) = D\pm E\sqrt{a},$$

le signe de E étant à volonté et les signes de E' et e étant convenablement choisis.

Les théorèmes que nous venons d'établir et qui peuvent être utiles dans plusieurs occasions, vont nous servir maintenant à établir une proposition relative à la manière de rendre le binôme P^2-5Q^2, dans lequel P et Q sont des nombres indéterminés soumis à la restriction d'être premiers entre eux, égal à une cinquième puissance. Cette proposition consiste en ce que, pour égaler le binôme P^2-5Q^2 de la manière la plus générale à une cinquième puissance impaire et non-divisible par 5, on n'a qu'à poser:

$$P+Q\sqrt{5} = (M\pm N\sqrt{5})^5(t\pm u\sqrt{5}),$$

M et N étant de nouvelles indéterminées soumises à la seule restriction d'être premières entre elles, l'une paire, l'autre impaire et la première de plus non-divisible par 5; et les lettres t et u désignant la solution générale de l'équation $t^2-5u^2 = 1$; ce qui veut dire que toutes les fois que, P et Q étant premiers entre eux, le binôme P^2-5Q^2 est une cinquième puissance impaire non-divisible par 5, il existe des nombres M et N premiers entre eux et tels qu'on ait:

$$P+Q\sqrt{5} = (M\pm N\sqrt{5})^5(t\pm u\sqrt{5}),$$

t et u satisfaisant à l'équation $t^2-5u^2 = 1$.

Pour nous assurer de la vérité de cette proposition, posons $P^2-5Q^2 = L$, L désignant une cinquième puissance impaire, non-divisible par 5 et voyons ce qui en résulte sur la nature des nombres P et Q. Désignons par l l'un quelconque des diviseurs premiers de L et soit l^{5n} la puissance la plus élevée de l, qui divise L, de sorte qu'en faisant $L = l^{5n}L'$, L' soit premier à l. Il résulte d'un théorème connu, que le nombre l qui divise P^2-5Q^2 sera lui-même de la forme $\vartheta^2-5\varepsilon^2$. Si nous posons maintenant:

$$(\vartheta+\varepsilon\sqrt{5})^n = d+e\sqrt{5}, \quad (\vartheta+\varepsilon\sqrt{5})^{5n} = D+E\sqrt{5},$$

d et e, D et E seront premiers entre eux en vertu du théorème I., et l'on aura l'équation:

$$(d+e\sqrt{5})^5 = D+E\sqrt{5}.$$

Si l'on applique ensuite le théorème III. aux équations:

$$D^2-5E^2 = l^{5n}, \quad P^2-5Q^2 = l^{5n}L',$$

qui se déduisent immédiatement de ce qui précède, on verra qu'il existe des nombres P' et Q', premiers entre eux et tels qu'on ait:

$$P'^2-5Q'^2 = L', \quad P+Q\sqrt{5} = (D\pm E\sqrt{5})(P'\pm Q'\sqrt{5}),$$

ou, ce qui revient au même, en remplaçant $D+E\sqrt{5}$ par $(d+e\sqrt{5})^5$:

$$P+Q\sqrt{5} = (d\pm e\sqrt{5})^5(P'\pm Q'\sqrt{5}).$$

L'équation $P'^2-5Q'^2 = L'$ à laquelle nous venons de parvenir, est entièrement analogue à l'équation $P^2-5Q^2 = L$, car le nombre L' que l'on obtient en divisant L par l^{5n} est une cinquième puissance, comme L. Supposons pour un instant que la proposition que nous cherchons à démontrer soit vraie pour l'équation $P'^2-5Q'^2 = L'$, et voyons comment on pourrait en conclure qu'elle a également lieu pour le binôme P^2-5Q^2. Dans la supposition que nous venons de faire, il existe des nombres M' et N' tels qu'on ait:

$$P+Q\sqrt{5} = (M'\pm N'\sqrt{5})^5(t\pm u\sqrt{5}).$$

En mettant cette valeur de $P'+Q'\sqrt{5}$ dans l'équation obtenue plus haut et dont le premier membre renferme $P+Q\sqrt{5}$, il viendra celle-ci:

$$P+Q\sqrt{5} = (M'\pm N'\sqrt{5})^5(d\pm e\sqrt{5})^5(t\pm u\sqrt{5}),$$

dans laquelle les signes dépendent de ceux qui se trouvent dans les deux équations dont la combinaison l'a produite. Si nous posons maintenant:

$$(M'\pm N'\sqrt{5})(d\pm e\sqrt{5}) = M\pm N\sqrt{5},$$

le signe de N étant $+$ ou $-$, selon que le coefficient de $\sqrt{5}$, dans la valeur développée du premier membre, est positif ou négatif, l'équation précédente se changera en celle-ci:

$$P+Q\sqrt{5} = (M\pm N\sqrt{5})^5(t\pm u\sqrt{5}),$$

qui est conforme à l'énoncé de la proposition dont nous nous occupons.

Ayant ainsi fait voir que la proposition en question est vraie pour le binôme P^2-5Q^2 égal à la cinquième puissance L, si elle est supposée avoir lieu pour le binôme $P'^2-5Q'^2$, égal à la cinquième puissance L', qui a un diviseur premier de moins que L, il ne reste, pour rendre la démonstration

complète, qu'à prouver la vérité de notre proposition pour le cas où le binôme P^2-5Q^2 est une cinquième puissance qui n'a qu'un seul diviseur premier l. Or, c'est ce qu'il est très facile de faire en s'appuyant sur le théorème II. En effet, dans le cas que nous venons d'énoncer, on a $P^2-5Q^2=l^{5n}$; d'un autre côté, le nombre l pouvant être mis sous la forme $\delta^2-5\varepsilon^2$, si l'on fait:

$$(\delta+\varepsilon\sqrt{5})^n=M+N\sqrt{5},\quad (\delta+\varepsilon\sqrt{5})^{5n}=D+E\sqrt{5},$$

on aura aussi:

$$D+E\sqrt{5}=(M+N\sqrt{5})^5,\quad D^2-5E^2=l^{5n},$$

D et E étant premiers entre eux en vertu du théorème I. Cela posé, il résulte immédiatement de l'application du théorème II. aux équations:

$$P^2-5Q^2=l^{5n},\quad D^2-5E^2=l^{5n},$$

qu'on a la relation:

$$P+Q\sqrt{5}=(D\pm E\sqrt{5})(t\pm u\sqrt{5}),$$

t et u satisfaisant à l'équation $t^2-5u^2=1$ et les signes étant convenablement choisis; ou, ce qui revient au même, en mettant $(M\pm N\sqrt{5})^5$ à la place de $D\pm E\sqrt{5}$:

$$P+Q\sqrt{5}=(M\pm N\sqrt{5})^5(t\pm u\sqrt{5}),$$

résultat conforme à l'énoncé de notre proposition. Il est ainsi prouvé que toutes les fois que P^2-5Q^2 est une cinquième puissance impaire, il existe des nombres M et N qui satisfont à la formule précédente. Quant à l'inverse de cette proposition, savoir qu'en attribuant dans la formule précédente à M et N des valeurs soumises aux seules restrictions déjà plusieurs fois énoncées, on obtiendra des nombres P et Q premiers entre eux et tels que P^2-5Q^2 soit une cinquième puissance, la démonstration en est tellement simple qu'il est inutile de nous y arrêter. — Au moyen de ce qui précède il sera facile d'établir le théorème que nous allons énoncer et qui servira de base aux propositions qui font l'objet principal de ce mémoire.

Théorème IV.

„Les nombres P et Q devant être premiers entre eux, l'un pair, l'autre impair, et le dernier devant être de plus divisible par 5, je dis que pour égaler le binôme P^2-5Q^2 de la manière la plus générale à une cinquième

puissance, il suffira de poser:

$$P+Q\sqrt{5}=(\varphi+\psi\sqrt{5})^5.$$

Les indéterminées φ et ψ étant premières entre elles, l'une paire, l'autre impaire, et la première de plus non-divisible par 5*).“

Pour égaler P^2-5Q^2 à une cinquième puissance, nous poserons, d'après ce qui vient d'être dit:

$$P+Q\sqrt{5}=(M\pm N\sqrt{5})^5(t\pm u\sqrt{5}).$$

Le nombre M n'étant pas divisible par 5, si nous faisons pour un instant:

$$(M+N\sqrt{5})^5=M'+N'\sqrt{5},$$

il sera facile de voir que N' est divisible par 5, et que M' ne l'est pas. En substituant l'expression précédente dans la valeur de $P+Q\sqrt{5}$, on aura:

$$P+Q\sqrt{5}=(M'\pm N'\sqrt{5})(t\pm u\sqrt{5}),$$

d'où l'on tire:

$$Q=\pm M'u\pm N't.$$

N' étant divisible par 5, et M' ne l'étant pas, il est évident que Q ne pourra être divisible par 5, qu'autant que u le sera. Les valeurs les plus petites qui satisfassent à l'équation:

$$t^2-5u^2=1,$$

sont celles-ci:

$$t=9,\quad u=4.$$

Les valeurs générales seront par conséquent données par cette formule:

$$t+u\sqrt{5}=(9+4\sqrt{5})^p,$$

dans laquelle p est un nombre entier, positif quelconque**); on tire de là

$$u=\frac{p}{1}9^{p-1}.4+\frac{p(p-1)(p-2)}{1.2.3}9^{p-3}.4^3.5+\text{etc.}$$

Tous les termes, à partir du second, étant divisibles par 5, quel que soit p, on voit que pour que u puisse être divisible par 5, il faut que le premier terme, et par conséquent aussi p, soit divisible par 5. Si nous faisons donc $p=5p'$, p' étant un entier, et que nous substituions la

*) Il n'est peut-être pas inutile de faire remarquer qu'il y a des théorèmes analogues pour beaucoup d'autres nombres premiers, et que pour les établir, on peut faire usage des mêmes considérations dont nous nous servons ici.

**) Voyez les Additions à l'Algèbre d'Euler (art. 75).

valeur de $t+u\sqrt{5}$ dans celle de $P+Q\sqrt{5}$, nous aurons:

$$P+Q\sqrt{5} = (M\pm N\sqrt{5})^5(9\pm 4\sqrt{5})^{5\nu},$$

résultat qui, par l'introduction des nouvelles indéterminées φ et ψ telles que l'on ait:

$$(M\pm N\sqrt{5})(9\pm 4\sqrt{5})^{\nu} = \varphi+\psi\sqrt{5},$$

se change en celui-ci:

$$P+Q\sqrt{5} = (\varphi+\psi\sqrt{5})^5.$$

La forme de la solution donnée par l'énoncé du théorème se trouvant ainsi justifiée, il ne reste plus qu'à déterminer la nature des indéterminées.

Comme on a:

$$P^2-5Q^2 = (\varphi^2-5\psi^2)^5,$$

et que les nombres P et Q sont respectivement divisibles par φ et ψ, on voit facilement que les indéterminées φ et ψ doivent être supposées premières entre elles, l'une paire, l'autre impaire, et la première de plus non-divisible par 5. On peut même ajouter que φ ou ψ sera impaire selon que P ou Q l'est. Réciproquement, si les indéterminées φ et ψ satisfont aux conditions précédentes, les nombres P et Q déterminés par la formule:

$$P+Q\sqrt{5} = (\varphi+\psi\sqrt{5})^5,$$

seront premiers entre eux, comme il est facile de s'en assurer. Ces préliminaires établis, nous pourrons nous occuper des théorèmes qui font l'objet principal de ce Mémoire. Le premier de ces théorèmes peut s'énoncer de la manière suivante.

Théorème V.

„Les nombres m et n étant positifs, plus grands que zéro, le second de plus différent de 2, et le nombre A n'étant divisible ni par 2 ni par 5, ni par aucun nombre premier de la forme $10k+1$, il sera impossible de trouver deux nombres x et y premiers entre eux, tels que:

$$(\alpha) \qquad x^5\pm y^5 = 2^m5^nAz^5.“$$

Supposons, contre l'énoncé du théorème, que l'équation soit possible. Comme le second membre est pair (m ayant été supposé >0), il faut que les nombres x et y, qui sont premiers entre eux, soient impairs l'un et l'autre. Si

nous faisons $x\pm y = 2p$, $x\mp y = 2q$, et par suite:

$$x = p+q, \quad \pm y = p-q,$$

les nombres p et q seront entiers, premiers entre eux, et de plus l'un pair, l'autre impair. En substituant les valeurs précédentes de x et $\pm y$ dans l'équation (α), on la changera en celle-ci:

$$2p(p^4+10p^2q^2+5q^4) = 2^m5^nAz^5.$$

Le premier membre ne peut être égal au second membre, qui est divisible par 5, qu'autant qu'on suppose p divisible par 5. Faisant donc $p = 5r$, nous aurons:

$$2.5^2r(q^4+2.5^2q^2r^2+5^3r^4) = 2^m5^nAz^5.$$

Le nombre n est, par hypothèse, égal à l'unité ou plus grand que 2. Si n est égal à l'unité, il faudra, dans l'équation précédente, supposer z divisible par 5. On pourra, dans ce cas, mettre $5z$ à la place de z, ou, ce qui est la même chose, donner à 5 l'exposant 6, d'où l'on voit que l'on peut supposer, dans tous les cas, $n>2$. Si l'on met maintenant l'équation précédente sous cette forme:

$$r(q^4+2.5^2q^2r^2+5^3r^4) = 2^{m-1}5^{n-2}Az^5,$$

et qu'on se rappelle que les nombres q et $p = 5r$ sont premiers entre eux, et de plus l'un pair l'autre impair, il sera facile de voir que le facteur trinôme est impair, non-divisible par 5 et premier à r; il faut donc que r soit divisible par 5, n étant >2. Choisissons actuellement deux nombres positifs, μ et ν, tels que*) $m+\mu-1$, $n+\nu-2$, soient divisibles par 5, et un nombre B qui n'ait d'autres diviseurs premiers que ceux du nombre A et tel que le produit AB soit une cinquième puissance. Si nous multiplions l'équation précédente par $2^\mu5^\nu B$, nous aurons:

$$2^\mu5^\nu Br(q^4+2.5^2q^2r^2+5^3r^4) = 2^{m+\mu-1}5^{n+\nu-2}ABz^5.$$

Le second membre de cette équation étant une cinquième puissance, le premier membre en sera pareillement une. Or je dis que les deux facteurs dans lesquels ce premier membre peut se décomposer, le facteur $2^\mu5^\nu Br$ et le facteur trinôme, sont premiers entre eux. En effet, nous avons déjà vu plus haut que le facteur trinôme est premier à $2^\mu5^\nu r$, et il résulte d'un autre

*) Si $m-1$ était divisible par 5, on choisirait pour μ une autre valeur que zéro pour éviter les exposants négatifs dans ce qui va suivre.

côté des théorèmes connus d'Euler sur la forme linéaire des diviseurs premiers de la formule $x^n \pm y^n$ (*Théorie des nombres*, *no.* 156) que le facteur trinôme, dans lequel q et r n'ont pas de diviseur commun, n'est divisible que par des nombres premiers de la forme $10k+1$, qui, d'après les suppositions faites dans l'énoncé du théorème, ne convient à aucun des diviseurs de A, et par conséquent aussi de B, B n'ayant pas d'autres diviseurs premiers que ceux du nombre A. Il faut donc que le nombre $2^\mu 5^\nu Br$ et le facteur trinôme soient des cinquièmes puissances l'un et l'autre.

Le facteur trinôme pouvant s'écrire de cette manière:

$$(q^2+5^3r^2)^2-5(10r^2)^2,$$

et les nombres $q^2+5^3r^2$, $10r^2$ étant premiers entre eux, le premier impair, le second pair et divisible par 5, il suffira, en vertu du théorème I., pour égaler le facteur trinôme avec toute la généralité convenable à une cinquième puissance, de poser ces deux équations:

$$\begin{aligned} q^2+5^3r^2 &= t(t^4+2.5^2t^2s^2+5^3s^4), \\ 10r^2 &= 5s(t^4+10t^2s^2+5s^4). \end{aligned}$$

Les nombres s et t doivent être supposés premiers entre eux, et de plus le premier pair, le second impair et non-divisible par 5. Il suit de là que s doit être divisible par 5; en effet t n'étant pas divisible par 5, le second membre de la seconde équation ne peut être divisible par 5^2 qu'autant que s est divisible par 5; mais le premier membre qui a r^2 pour facteur, est divisible par 5^2; donc s est divisible par 5.

Nous avons vu plus haut que $2^\mu 5^\nu Br$ devait être une cinquième puissance. Le nombre $2^{2\mu}5^{2\nu}B^2r^2$, carré du nombre précédent, devra donc être une puissance du même degré, et même du dixième degré. Or, en multipliant par $2^{2\mu-1}5^{2\nu-1}B^2$ les deux membres de la dernière équation, on aura celle-ci:

$$2^{2\mu}5^{2\nu}B^2r^2 = 2^{2\mu-1}5^{2\nu}B^2s(t^4+10t^2s^2+5s^4).$$

Si donc nous faisons pour abréger: $2\mu-1=g$, $2\nu=h$, $B^2=C$, tout se réduira à faire voir qu'il est impossible de trouver deux nombres s et t premiers entre eux, et dont le premier soit de plus pair et divisible par 5, tels que le produit:

$$(\beta) \qquad 2^g5^hCs(t^4+10t^2s^2+5s^4)$$

soit une cinquième puissance.

En ayant égard à la nature des diviseurs premiers de C, on s'assurera facilement que le facteur 2^g5^hCs et le facteur trinôme sont premiers entre eux. Il faudrait donc, pour que le produit (β) pût être une cinquième puissance, que chacun de ces facteurs en fût pareillement une. Le facteur trinôme peut s'écrire de cette manière:

$$(t^2+5s^2)^2-5(2s^2).$$

Comme les nombres t^2+5s^2 et $2s^2$ sont évidemment premiers entre eux, et de plus le premier impair et le second pair et divisible par 5, le théorème I. est applicable ici, et l'on pourra poser:

$$\begin{aligned} t^2+5s^2 &= t'(t'^4+2.5^2t'^2s'^2+5^3s'^4), \\ 2s^2 &= 5s'(t'^4+10t'^2s'^2+5s'^4). \end{aligned}$$

Les nombres s' et t' doivent être supposés premiers entre eux, et de plus le premier pair, le second impair et non-divisible par 5. Comme t' n'est pas divisible par 5, il est évident par la seconde équation, dont le premier membre renferme le facteur s^2 et est par conséquent divisible par 5^2, que s' doit être divisible par 5. Ainsi les nombres s' et t' sont premiers entre eux, de même que les nombres s et t, et le premier s' est en outre pair et divisible par 5 comme s.

Il est facile encore de voir que s' est plus petit que s; car on conclut immédiatement de la dernière équation $5^2s'^5<2s^2$ et par suite $s'<\sqrt[5]{\frac{2s^2}{25}}$.

On a vu plus haut que 2^g5^hCs devait être une cinquième puissance. Le nombre $2^{2g}5^{2h}C^2s^2$, carré du précédent, devra donc être une puissance du même degré. Or, en multipliant les deux membres de la dernière équation par $2^{2g-1}5^{2h}C^2$, on aura:

$$2^{2g}5^{2h}C^2s^2 = 2^{2g-1}5^{2h+1}C^2s'(t'^4+10t'^2s'^2+5s'^4),$$

ou, ce qui est la même chose, en faisant $2g-1=g'$, $2h+1=h'$, $C^2=C'$, dans le second membre:

$$(\beta') \qquad 2^{2g}5^{2h}C^2s^2 = 2^{g'}5^{h'}C's'(t'^4+10t'^2s'^2+5s'^4),$$

équation dont les deux membres doivent être des puissances du cinquième degré.

Nous voilà donc arrivé à un produit (β') semblable au produit (β), mais dans lequel le nombre s' est plus petit que le nombre s du produit (β), et ce produit (β') serait une cinquième puissance, si le produit (β) en était

une. En traitant le produit (β') comme nous avons traité le produit (β), on arriverait à un troisième produit (β''), dans lequel le nombre s'' serait plus petit que s', et l'on pourrait continuer ce procédé aussi loin que l'on voudrait. Il est facile de voir en outre que quelque loin que l'on prolonge les séries $s, s', s'', \ldots$; $t, t', t'', \ldots$, on ne pourra jamais rencontrer un terme égal à zéro; car il est évident que si l'on supposait nul un de ces termes, on conclurait en remontant que $s = 0$, cas évident, et qui d'ailleurs est exclu, puisque les nombres s et t ont été supposés premiers entre eux.

Si donc le produit (β) pouvait être une cinquième puissance, on pourrait obtenir, par l'analyse précédente, une suite indéfinie de nombres entiers positifs, dans laquelle chaque terme serait plus petit que le terme précédent, sans qu'aucun des termes fût nul; ce qui implique contradiction. On doit conclure de là que le produit (β) ne saurait être une puissance du cinquième degré.

Le théorème V. se trouvant ainsi établi, nous allons donner le moyen d'en déduire un autre plus général. Considérons l'équation:

$$x^5 \pm y^5 = 2^m A z^5,$$

dans laquelle nous supposons x et y premiers entre eux; $m > 0$, et A soumis aux mêmes restrictions que dans l'énoncé du théorème V. Soient α, β, γ des nombres positifs moindres que 5, et tels que $x \equiv \alpha$, $\pm y \equiv \beta$, $z \equiv \gamma$ (mod. 5), et soit encore H un nombre positif < 25 et tel que $2^m A \equiv H \pmod{25}$. Comme 5 est un nombre premier, on aura:

$$x^5 \equiv x, \quad y^5 \equiv y, \quad z^5 \equiv z \pmod 5.$$

On conclut de là, en ayant égard à l'équation posée plus haut:

$$x \pm y \equiv 2^m A z \pmod 5,$$

et partant:

$$\alpha + \beta \equiv H\gamma \pmod 5.$$

Comme α est le reste de x, on pourra poser $x = \alpha + 5k$, k étant un entier; on tire de là, en élevant les deux membres à la cinquième puissance:

$$x^5 = \alpha^5 + 5\alpha^4(5k) + \frac{5.4}{1.2}\alpha^3(5k)^2 + \text{etc.},$$

on aura donc:

$$x^5 \equiv \alpha^5 \pmod{25}.$$

On trouvera de la même manière $\pm y^5 \equiv \beta^5$, $z^5 \equiv \gamma^5 \pmod{25}$, et comme on a aussi $2^m A \equiv H \pmod{25}$, on obtiendra, en ayant égard à l'équation citée:

$$\alpha^5 + \beta^5 \equiv H\gamma^5 \pmod{25}.$$

Si maintenant, en substituant dans cette congruence successivement pour α, β toutes les combinaisons que l'on peut former avec les nombres positifs moindres que 5, et pour γ les valeurs correspondantes également moindres que 5, données par la formule:

$$\alpha + \beta \equiv H\gamma \pmod 5,$$

on trouve que la congruence $\alpha^5 + \beta^5 \equiv H\gamma^5 \pmod{25}$ ne peut subsister que lorsque γ est nul, on sera assuré que l'équation:

$$x^5 \pm y^5 = 2^m A z^5$$

ne peut avoir lieu, à moins qu'on ne suppose z divisible par 5. On pourra donc, dans ce cas, mettre $5z$ à la place de z, ce qui change notre équation en celle-ci:

$$x^5 \pm y^5 = 2^m 5^5 A z^5,$$

qui rentre évidemment dans le théorème II., et par conséquent est impossible. Or ce cas a lieu toutes les fois que le nombre H est un des huit nombres suivants 3, 4, 9, 12, 13, 16, 21, 22, comme on peut s'en assurer par un calcul très simple. Nous avons donc ainsi ce nouveau théorème:

Théorème VI.

„Les nombres m et A étant soumis aux mêmes restrictions que dans l'énoncé du théorème II., si le nombre $2^m A$, étant divisé par 25, donne un des huit restes suivants, 3, 4, 9, 12, 13, 16, 21, 22, il sera impossible de trouver deux nombres x et y premiers entre eux, tels que l'on ait $x^5 \pm y^5 = 2^m A z^5$."

Pour donner un exemple bien simple, considérons les deux équations:

$$x^5 \pm y^5 = 4z^5, \quad x^5 \pm y^5 = 16z^5.$$

Comme dans ces équations on peut, sans nuire à la généralité, supposer les nombres x et y premiers entre eux, il sera facile de voir qu'elles rentrent dans le théorème II. En effet, si l'on fait $A = 1$, et successivement $m = 2$, $m = 4$, on aura respectivement:

$$2^m A = 4, \quad 2^m A = 16.$$

Il est donc prouvé que les deux équations précédentes sont impossibles.

Considérons encore l'équation:

$$x^5 \pm y^5 = z^5,$$

qui est une de celles que FERMAT a assuré être impossibles. Par des considérations semblables à celles qui nous ont servi pour établir le théorème précédent, on peut s'assurer que cette équation ne saurait subsister, à moins qu'une des indéterminées x, y, z ne soit divisible par 5. Soit z l'indéterminée divisible par 5, car il est évident qu'on peut faire en sorte qu'une quelconque des indéterminées se trouve toute seule dans un membre. D'un autre côté, si l'on suppose ces indéterminées premières entre elles, l'une d'elles sera paire et les deux autres seront impaires. Si z était paire, on pourrait remplacer cette indéterminée par $2.5.z$, ce qui changerait l'équation précédente en celle-ci:

$$x^5 \pm y^5 = 2^5 5^5 z^5,$$

qui est impossible, puisqu'elle rentre évidemment dans le théorème II. Il ne resterait donc qu'à traiter le cas où l'indéterminée divisible par 5 serait impaire; mais la méthode exposée dans ce Mémoire paraît insuffisante pour ce cas, et je ne vois pas comment on pourrait compléter la démonstration du cas particulier du théorème de FERMAT, dont il vient d'être question.

ADDITION AU MÉMOIRE PRÉCÉDENT.

Depuis que le Mémoire précédent a été présenté à l'Académie, M. LEGENDRE a publié un second supplément à sa Théorie des Nombres, dans lequel il démontre l'impossibilité de l'équation:

$$x^5 \pm y^5 = z^5.$$

Le cas de l'indéterminée divisible en même temps par 2 et par 5, est traité dans cet ouvrage comme dans le Mémoire précédent, et l'auteur prouve ensuite l'impossibilité de l'autre cas au moyen d'une analyse nouvelle. L'objet de cette addition est d'établir deux théorèmes nouveaux sur les équations indéterminées du cinquième degré et qui comprennent, comme cas particulier, le théorème de FERMAT pour les cinquièmes puissances. J'y parviens en partant des résultats obtenus dans ce qui précède et en faisant usage d'une analyse qui diffère à plusieurs égards de celle de M. LEGENDRE et qui est entièrement analogue à la méthode exposée dans le Mémoire précédent. On a vu que le succès de l'analyse

que nous y avons employée, est fondé sur ce que, pour égaler à une cinquième puissance impaire le binôme P^2-5Q^2, dans lequel Q doit être divisible par 5, il suffit de poser:

$$P+Q\sqrt{5} = (\varphi+\psi\sqrt{5})^5,$$

parce que cette circonstance donne lieu à la reproduction continuelle de l'expression que nous avons appelée facteur trinôme. En traitant les nouvelles équations qui font l'objet de cette addition, on est également conduit au binôme P^2-5Q^2, Q étant toujours divisible par 5; mais il y a cette différence que les nombres P et Q, qui précédemment étaient l'un pair, l'autre impair, sont ici impairs tous les deux et que le binôme P^2-5Q^2, qui dans l'autre cas devait être une cinquième puissance impaire, doit être égalé ici au quadruple d'une pareille puissance. Or la formule qui satisfait de la manière la plus générale à cette dernière condition, est susceptible d'être rendue parfaitement semblable à celle qui sert à remplir la première; car j'ai remarqué qu'on peut la présenter de cette manière:

$$P+Q\sqrt{5} = \frac{(\varphi+\psi\sqrt{5})^5}{16},$$

expression qui ne se distingue du résultat qu'on vient de rappeler qu'en ce que les indéterminées φ et ψ, au lieu d'être l'une paire, l'autre impaire, doivent être impaires toutes les deux. Dès qu'on a fait cette remarque et qu'en traitant les nouvelles équations qui vont nous occuper, on est arrivé au binôme qu'il s'agit d'égaler au quadruple d'une cinquième puissance, on voit d'un seul coup d'oeil qu'on doit réussir à prouver l'impossibilité de ces équations, en faisant usage d'un procédé tout à fait analogue à la marche que nous avons suivie dans la démonstration du théorème V. — Nous allons maintenant entrer en matière en commençant par établir la proposition que nous avons déjà énoncée.

Les nombres P et Q, dont le premier est supposé n'être pas divisible par 5, étant impairs tous les deux, et n'ayant pas de diviseur commun, le nombre P^2-5Q^2 sera de la forme $8k+4$, et l'on pourra faire:

$$P^2-5Q^2 = 4L,$$

L étant un nombre impair et non-divisible par 5. Si nous multiplions membre à membre l'équation précédente et celle-ci:

$$3^2-5.1^2 = 4,$$

nous aurons:

$$(3P\pm5Q)^2-5(P\pm3Q)^2 = 16L.$$

Comme les nombres P et Q sont impairs tous les deux, il est évident qu'en déterminant convenablement le signe, les expressions:

$$\frac{3P\pm5Q}{4}, \quad \frac{P\pm3Q}{4}$$

seront entières l'une et l'autre; faisant en conséquence:

$$\frac{3P\pm5Q}{4}=P', \qquad \frac{\pm(P\pm3Q)}{4}=Q',$$

le signe en dehors de la parenthèse étant choisi de manière à donner une valeur positive pour Q', l'équation obtenue plus haut se changera en celle-ci: $P'^2-5Q'^2=L$, et l'on s'assurera facilement que l'on a:

$$P+Q\sqrt{5}=(P'\pm Q'\sqrt{5})(3\pm\sqrt{5}),$$

les signes étant convenablement choisis, et que les nombres P' et Q' sont premiers entre eux, et de plus l'un pair, l'autre impair.

Supposons maintenant que le nombre L doive être une cinquième puissance. On satisfera à cette condition de la manière la plus générale en posant:

$$P'+Q'\sqrt{5}=(M\pm N\sqrt{5})^5(9\pm4\sqrt{5})^p.$$

En substituant cette valeur dans la dernière équation, on aura celle-ci:

$$P+Q\sqrt{5}=(M\pm N\sqrt{5})^5(9\pm4\sqrt{5})^p(3\pm\sqrt{5}),$$

dans laquelle les signes sont indépendants, comme dans les deux équations précédentes. On peut faire $p=5k\pm r$, k étant entier et positif, et r ayant une des trois valeurs 0, 1, 2, la quantité $(9\pm4\sqrt{5})^p$ se décomposera ainsi en deux facteurs $(9\pm4\sqrt{5})^{5k}$ et $(9\pm4\sqrt{5})^{\pm r}$ dont le premier peut être omis parce qu'il rentre dans $(M\pm N\sqrt{5})^5$. Si nous observons de plus qu'en vertu de l'équation:

$$9\pm4\sqrt{5}=(9\mp4\sqrt{5})^{-1}$$

on peut changer dans $(9\pm4\sqrt{5})^{\pm r}$ simultanément les signes de r et du radical, nous pouvons supposer r positif, et l'équation donnée plus haut deviendra:

$$P+Q\sqrt{5}=(M\pm N\sqrt{5})^5(9\pm4\sqrt{5})^r(3\pm\sqrt{5}).$$

L devant toujours être la cinquième puissance d'un nombre impair et non-

divisible par 5, déterminons les conditions nécessaires pour que Q soit divisible par 5. Comme le coefficient de $\sqrt{5}$ dans le développement de $(M\pm N\sqrt{5})^5$ est divisible par 5, et que la partie rationnelle de ce développement ne l'est pas, M n'étant pas divisible par 5, on conclut, comme dans la démonstration du théorème IV., qu'il faut, pour que Q puisse être divisible par 5, que le coefficient de $\sqrt{5}$, dans la valeur développée de $(9\pm4\sqrt{5})^r(3\pm\sqrt{5})$ le soit.

Or, en substituant pour r successivement les trois valeurs 0, 1, 2, on trouve que cela n'a lieu que dans le cas de $r=2$, les signes des radicaux dans les deux facteurs $(9\pm4\sqrt{5})^r$ et $(3\pm\sqrt{5})$ étant en même temps opposés. Si l'on fait attention que l'on a:

$$\frac{(3\pm\sqrt{5})^3}{2^3}=9\pm4\sqrt{5} \quad \text{et} \quad 3\mp\sqrt{5}=\frac{4}{3\pm\sqrt{5}},$$

on trouvera que le produit précédent sera, dans le cas dont il s'agit, équivalent à:

$$\frac{(3\pm\sqrt{5})^5}{2^4},$$

valeur dont la substitution dans l'équation obtenue plus haut, la change en celle-ci:

$$P+Q\sqrt{5}=\frac{(M\pm N\sqrt{5})^5(3\pm\sqrt{5})^5}{2^4}.$$

Les nombres M et N étant l'un pair, l'autre impair, les nombres φ et ψ déterminés par l'équation:

$$\varphi+\psi\sqrt{5}=(M\pm N\sqrt{5})(3\pm\sqrt{5})$$

seront impairs l'un et l'autre, et l'on aura:

$$P+Q\sqrt{5}=\frac{(\varphi+\psi\sqrt{5})^5}{2^4}$$

et par conséquent:

$$P=\varphi\frac{(\varphi^4+2.5^2\varphi^2\psi^2+5^2\psi^4)}{2^4},$$

$$Q=5\psi\frac{(\varphi^4+10\varphi^2\psi^2+5\psi^4)}{2^4}.$$

Pour que P et Q soient premiers entre eux, il faut que φ et ψ n'aient pas de

diviseur commun, et que le premier de ces nombres ne soit pas divisible par 5, et réciproquement, si les nombres φ et ψ, dont le premier est supposé ne pas être divisible par 5, n'ont pas de diviseur commun et sont impairs l'un et l'autre, les nombres P et Q seront entiers et premiers entre eux. En effet, le quart de la quantité $\varphi^4+10\varphi^2\psi^2+5\psi^4$ pouvant se mettre sous la forme:

$$\left(\frac{\varphi^2+5\psi^2}{2}\right)^2-5(\psi^2)^2,$$

et cette dernière expression étant évidemment le quadruple d'un nombre impair, on voit que la valeur de Q est entière et impaire; la même chose se prouvera pour la valeur de P, et l'on s'assurera facilement que les nombres P et Q, qui sont impairs tous les deux, n'ont pas de diviseur commun. Nous avons donc ainsi ce théorème:

Théorème VII.

„Les nombres P et Q devant être premiers entre eux, impairs l'un et l'autre, et le dernier devant être divisible par 5, je dis que pour égaler le binôme P^2-5Q^2 au quadruple d'une cinquième puissance avec toute la généralité convenable, il suffira de poser:

$$P+Q\sqrt{5}=\frac{(\varphi+\psi\sqrt{5})^5}{2^4},$$

les nombres indéterminés φ et ψ étant premiers entre eux, impairs l'un et l'autre et le premier de plus non-divisible par 5*).“

Voici maintenant le premier des théorèmes nouveaux que nous avons annoncés au commencement de cette addition.

Théorème VIII.

„La lettre n désignant un nombre positif autre que 0 et 2, et le nombre A n'étant divisible ni par 2, ni par 5, ni par aucun nombre premier de la forme $10k+1$, il sera impossible de trouver deux nombres x et y premiers entre eux et tels que:

$$(\gamma) \qquad x^5\pm y^5=5^n Az^5.“$$

Les nombres x et y peuvent être impairs tous les deux, ou l'un pair

*) Ce théorème, comme le théorème IV, a ses analogues pour beaucoup d'autres nombres premiers.

et l'autre impair. Dans le premier cas, z sera divisible par 2, et l'on pourra mettre $2z$ à la place de z, ce qui changera l'équation (γ) en celle-ci:

$$x^5\pm y^5=2^5 5^n Az^5,$$

qui est impossible puisqu'elle rentre évidemment dans le théorème V. Reste donc à prouver l'impossibilité du second cas où l'on suppose les nombres x, y l'un pair, l'autre impair. Si nous faisons:

$$x\pm y=p, \quad x\mp y=q,$$

nous aurons:

$$2x=p+q, \quad \pm 2y=p-q,$$

et les nombres p et q seront premiers entre eux et de plus impairs l'un et l'autre. En substituant les valeurs précédentes de $2x$ et $\pm 2y$ dans l'équation (γ), après en avoir multiplié les deux membres par 2^5, on aura:

$$p(p^4+10p^2q^2+5q^4)=2^4 5^n Az^5.$$

Comme p doit évidemment être divisible par 5, nous ferons $p=5r$, ce qui donnera:

$$5^3 r(q^4+2.5^2q^2r^2+5^3r^4)=2^4 5^n Az^5.$$

Le nombre n est par hypothèse égal à l'unité ou plus grand que 2. Si n est égal à l'unité, il faudra, dans l'équation précédente, supposer z divisible par 5. On pourra donc, dans ce cas, mettre $5z$ à la place de z ou, ce qui est la même chose, donner à 5 l'exposant 6, d'où l'on voit que l'on peut supposer dans tous les cas $n>2$.

Si l'on met l'équation précédente sous cette forme:

$$r(q^4+2.5^2q^2r^2+5^3r^4)=2^4 5^{n-2} Az^5,$$

et qu'on fasse attention que $n>2$ et que q est premier à $p=5r$, on voit que r doit être supposé divisible par 5.

Choisissons maintenant un nombre positif ν tel que $n+\nu-2$ soit divisible par 5 et un nombre B qui n'ait d'autres diviseurs premiers que ceux du nombre A et tel que le produit AB soit une cinquième puissance. Multipliant la dernière équation par $5^\nu B$, nous aurons:

$$5^\nu Br(q^4+2.5^2q^2r^2+5^3r^4)=2^4 5^{n+\nu-2} ABz^5.$$

Tous les diviseurs du facteur trinôme, dans lequel q et r sont premiers

entre eux, étant de la forme $10k+1$, il est évident qu'il n'a aucun diviseur commun avec B; il n'est pas moins évident qu'il est aussi premier à $5^\nu r$, et par conséquent à $5^\nu Br$.

Comme le facteur $5^\nu Br$ et le facteur trinôme sont premiers entre eux et que le premier de ces facteurs est impair, il faut, en vertu de la dernière équation, dont le second membre est le produit de 2^4 et de la cinquième puissance d'un nombre impair, que $5^\nu Br$ soit une cinquième puissance, et le facteur trinôme une cinquième puissance multipliée par 2^4.

Le quart du facteur trinôme devant être le quadruple d'une cinquième puissance, et ce quart pouvant se mettre sous la forme:

$$\left(\frac{q^2+5^2r^2}{2}\right)^2-5(5r^2)^2,$$

où les nombres $\frac{q^2+5^2r^2}{2}$, $5r^2$ sont évidemment premiers entre eux, impairs l'un et l'autre et le dernier de plus divisible par 5, il suffira, en vertu du théorème établi au commencement de cette addition, pour égaler le quart du facteur trinôme au quadruple d'une cinquième puissance, de poser ces deux équations:

$$\frac{q^2+5^2r^2}{2} = t\,\frac{(t^4+2.5^2t^2s^2+5^3s^4)}{2^4},$$

$$5r^2 = 5s\,\frac{(t^4+10t^2s^2+5s^4)}{2^4},$$

les nombres indéterminés t et s devant être supposés premiers entre eux, impairs l'un et l'autre et le premier de plus non-divisible par 5. Comme t n'est pas divisible par 5 et que r l'est ainsi que nous l'avons vu ci-dessus, il faut, en vertu de la dernière des équations précédentes, que s soit divisible par 5.

Nous avons vu plus haut que $5^\nu Br$ devait être une cinquième puissance. Le nombre $5^{2\nu}B^2r^2$, carré du précédent, devra donc être une puissance du même degré, et même du dixième degré.

Or, en multipliant par $2^4 5^{2\nu-1}B^2$ les deux membres de la dernière équation, on aura celle-ci:

$$2^4 5^{2\nu}B^2r^2 = 5^{2\nu}B^2s(t^4+10t^2s^2+5s^4).$$

Si donc nous faisons pour abréger $2\nu = h$, $B^2 = C$, tout se réduit à

faire voir qu'il est impossible de trouver deux nombres t et s premiers entre eux, impairs l'un et l'autre, et dont le dernier s soit de plus divisible par 5, tels que le produit:

$$(\delta) \qquad 5^h Cs(t^4+10t^2s^2+5s^4)$$

soit une cinquième puissance multipliée par 2^4.

Il est facile de voir que l'expression (δ) ne saurait être le produit de 2^4 et d'une cinquième puissance, à moins que $5^h Cs$ ne soit une cinquième puissance, et le facteur trinôme une cinquième puissance multipliée par 2^4.

Le quart du facteur trinôme devant être le quadruple d'une cinquième puissance, et ce quart pouvant se mettre sous la forme:

$$\left(\frac{t^2+5s^2}{2}\right)^2-5(s^2)^2,$$

où les nombres $\frac{t^2+5s^2}{2}$, s^2 sont évidemment premiers entre eux, impairs l'un et l'autre, et le dernier de plus divisible par 5, il suffira, pour égaler le facteur trinôme divisé par 4 au quadruple d'une cinquième puissance, de poser ces équations:

$$\frac{t^2+5s^2}{2} = t'\,\frac{(t'^4+2.5^2t'^2s'^2+5^3s'^4)}{2^4},$$

$$s^2 = 5s'\,\frac{(t'^4+10t'^2s'^2+5s'^4)}{2^4},$$

les nombres t' et s' étant supposés premiers entre eux, impairs l'un et l'autre, et le premier t' de plus non-divisible par 5. Comme s est divisible par 5, et que t' ne l'est plus, il faut, d'après la dernière équation, que s' soit aussi divisible par 5. On conclut encore de la dernière équation qu'on a: $\frac{25}{16}s'^5 < s^2$ et par suite que s' est beaucoup plus petit que s.

Le nombre $5^h Cs$ devant être une cinquième puissance, $5^{2h}C^2s^2$, carré du nombre précédent, devra être une puissance du même degré et même du dixième degré. Or, en multipliant par $2^4 5^{2h}C^2$ les deux membres de la dernière équation, on aura celle-ci:

$$2^4 5^{2h}C^2s^2 = 5^{2h+1}C^2s'(t'^4+10t'^2s'^2+5s'^4)$$

ou, ce qui est la même chose, en faisant $2h+1 = h'$, $C^2 = C'$ dans le second

membre:

$$(\delta') \qquad 2^4 5^{25} C^2 s^2 = 5^N C' s' (t'^4 + 10 t'^2 s'^2 + 5 s'^4),$$

équation dont les deux membres devront être des cinquièmes puissances multipliées par 2^4.

Le produit (δ') étant parfaitement semblable au produit (δ), et le nombre s' étant beaucoup plus petit que le nombre s, on conclura, comme dans la démonstration du théorème V. du mémoire précédent, que le produit (δ) ne saurait être égal à une cinquième puissance, multipliée par 2^4, et que par conséquent l'équation (γ) ne saurait avoir lieu.

Le théorème de FERMAT, pour le cas des cinquièmes puissances, est compris comme cas particulier dans le théorème que nous venons d'établir. En effet, l'équation $x^5 \pm y^5 = z^5$ ne pouvant avoir lieu, à moins qu'une des indéterminées, z par exemple, ne soit divisible par 5, nous pouvons mettre $5z$ à la place de z; ce qui donnera $x^5 \pm y^5 = 5^5 z^5$, équation impossible, puisqu'elle rentre dans le dernier théorème.

Un raisonnement tout-à-fait semblable à celui au moyen duquel nous avons établi le théorème VI., en partant du théorème V., peut servir à déduire du théorème que nous venons de démontrer un nouveau théorème qui peut s'énoncer comme il suit:

Théorème IX.

„Le nombre A étant soumis aux mêmes restrictions que dans l'énoncé du théorème VIII., et ce nombre donnant un des huit restes suivants, 3, 4, 9, 12, 13, 16, 21, 22, lorsqu'il est divisé par 25, il sera impossible de trouver deux nombres x et y premiers entre eux, et tels que l'on ait $x^5 \pm y^5 = Az^5$."

DE

FORMIS LINEARIBUS,

IN QUIBUS CONTINENTUR DIVISORES PRIMI QUARUMDAM FORMULARUM GRADUUM SUPERIORUM

COMMENTATIO,

QUAM

AD VENIAM DOCENDI

AB AMPLISSIMO PHILOSOPHORUM ORDINE IN REGIA UNIVERSITATE LITTERARUM VRATISLAVIENSI IMPETRANDAM

CONSCRIPSIT

GUSTAVUS LEJEUNE DIRICHLET,
PHILOSOPHIAE DOCTOR.

Vratislaviae, Typis Kupferianis.

DE FORMIS LINEARIBUS, IN QUIBUS CONTINENTUR DIVISORES PRIMI QUARUNDAM FORMULARUM GRADUUM SUPERIORUM.

Constat e doctrina de residuis quadraticis seu theoria divisorum formularum secundi gradus, divisores primos talium formularum in certis formis linearibus contineri, et esse formas lineares ab illis diversas, in quibus non-divisores sint comprehensi, ita ut ad absolvendam quaestionem, utrum primus datus formulam datam metiatur necne, sufficiat examinare, num primus in aliqua priorum an posteriorum formarum contineatur. Longe aliter res sese habet in formulis gradus superioris, quarum divisores a non-divisoribus simili modo discerni non possunt, et quibus adhibenda sunt criteria ab illis, quae in doctrina de residuis quadraticis proponuntur, longe diversa. Ratio divisores formularum gradus superioris a non-divisoribus distinguendi ut exemplo illustretur, contemplemur formulam quarti gradus x^4-3. Ex simplicissimis arithmeticae superioris principiis deducitur, hac formula proposita, solos primos formae $12n+1$ criterium altioris generis requirere, de reliquis autem ope notae doctrinae de residuis quadraticis rem diiudicari posse. Talis formae si proponitur primus, et quaeritur, utrum formulae x^4-3 sit divisor necne, hoc criterio erit utendum. Redigatur primus sub formam t^2+3u^2, quod semper et unico quidem modo fieri posse constat. Tum numerus t, quem nec per 2 nec per 3 divisibilem fore est perspicuum, erit formae $12n\pm1$, vel formae $12n\pm5$. Si prior casus locum habet, primus erit divisor formulae x^4-3, sin posterior, non erit. Est aliud criterium ad eandem quaestionem decidendam idoneum, quod tamen, ut elegantiorem habeat formam, non referendum est ad formulam x^4-3, sed ad hanc x^4+3, quae posterior priori tam arcte est coniuncta, ut, si numerum aliquem posterioris divisorem esse vel non esse scimus, inde statim concludi possit, utrum idem numerus priorem metiatur necne. Quod alterum criterium si adhibere velis, numerus primus propositus in duo quadrata est resolvendus. Quadratorum, quae haec decompositio suppeditat, alterum manifesto erit par, alterum

impar, nec minus facile est perspectu, alterum horum quadratorum idque unum tantum per 3 fore divisibile. Quibus ita praeparatis, criterium hoc modo exhiberi licet:

„Si quadratum par per 3 est divisibile, primus metietur formulam x^4+3, sin impar, non metietur."

Demonstrationes theorematum modo propositorum invenies in commentationibus nonnullis, in quibus theoriam generalem divisorum formulae $\alpha x^4+\beta x^2+\gamma$ struere conabor et quarum prima nuper lucem vidit in cel. Crellii ephemeridibus mathematicis (Recherches sur les diviseurs premiers d'une classe de formules du quatrième degré. Premier Mémoire). Theoremata praecedentia hoc loco nonnisi in hunc finem sunt prolata, ut exemplo aliquo appareat, quantum formulae gradus superioris a formulis quadraticis differre inveniantur, si in divisorum primorum indolem inquiritur. Quae diversitas quamquam in genere valere videtur, sunt tamen formulae particulares cuiusvis fere gradus, quae respectu divisorum simili se habent modo, quo formulae secundi gradus, eoque ut ex forma lineari, in qua continetur primus, cognosci possit, num formulam huius generis metiatur. Ad hoc genus referendae sunt formulae in expressione $x^n\pm 1$ comprehensae, de quibus ill. Euler instituit disquisitiones non minus insignes, quod ratiocinandi methodus, qua vir summus est usus, eximia simplicitate gaudet, quam quod theoremata, quae eius ope stabiliuntur, latissime patent. Quibus ill. Euleri disquisitionibus incumbens, incidi in novam quandam formularum speciem, quae, quod ad divisores attinet, similes habent proprietates, ut in sequentibus sum expositurus.

Cum pars disquisitionum sequentium nonnullis theorematum Eulerianorum modo laudatorum sit superstruenda, utile duximus, theoremata, quibus nobis opus erit, hoc loco in conspectum producere. Demonstrationes brevitatis causa omittimus, lectorem ad ill. Euleri dissertationes vel ill. Legendre opus egregium ablegantes, qui et haec et reliqua Euleri inventa arithmetica summa cum perspicuitate exposuit.

Theorema I. Si p est primus impar, omnes divisores primi formulae $\frac{x^p-1}{x-1}$ in forma lineari $2mp+1$ continentur, et vice versa quivis primus in hac forma comprehensus formulae est divisor.

Theorema II. Si α est potestas numeri 2, divisores formulae $x^\alpha+1$ continentur in forma $2m\alpha+1$, et vice versa quivis primus huius formae formulam metitur.

Formulae, de quarum divisoribus in sequentibus disquisitionem instituemus, originem trahunt ex evolutione potestatis $(x+\sqrt{b})^n$, ubi n et b sunt integri dati (posterior non-quadratus), x autem designat integrum indeterminatum. Ponamus, evolutione perfecta, prodire $U+V\sqrt{b}$, ubi tam U quam V a quantitate irrationali $\sqrt{b}$ liberi supponuntur, ita ut habeamus:

$$(x+\sqrt{b})^n = U+V\sqrt{b}, \quad (x-\sqrt{b})^n = U-V\sqrt{b},$$

$$(1) \qquad V = nx^{n-1} + \frac{n(n-1)(n-2)}{1.2.3}x^{n-3}b + \frac{n(n-1)(n-2)(n-3)(n-4)}{1.2.3.4.5}x^{n-5}b^2 + \cdots$$

Propositum est nobis, definire numeros primos, per quos V fit divisibilis, si ipsi x omnes valores integri tam positivi quam negativi successive tribuuntur. Excipiuntur tantum valores ad ipsum b non primi, quippe qui theorematum concinnitatem turbent. Caeterum facillime perspicitur, casum, ubi x cum ipso b divisorem communem habere statuitur, ad casum, ubi x et b inter se sunt primi, reduci posse.

Ut initium huius disquisitionis faciamus, demonstremus, ipsos U et V nullum divisorem communem (numero 2 excepto) habere posse, quotiescunque x valorem ad ipsum b primum nanciscitur. Ad hanc rem probandam, a suppositione contrarii proficiscimur. Sit igitur δ primus utrumque ipsorum U et V metiens. Si prima aequationum (1) in secundam multiplicatur, prodibit haec:

$$(x^2-b)^n = U^2 - bV^2,$$

ex cuius inspectione concluditur, primum δ ipsius x^2-b esse divisorem, quod, si signo ab ill. Gauss introducto utimur, hoc modo designabimus:

$$x^2 \equiv b \pmod{\delta},$$

ex qua congruentia hae novae deducuntur:

$$x^4 \equiv b^2, \quad x^6 \equiv b^3, \quad x^8 \equiv b^4, \quad \ldots \pmod{\delta}.$$

Si iam in expressione (1) ipsius V loco ipsorum b, b^2, b^3, ... valores secundum modulum δ illis resp. congruos x^2, x^4, x^6, ... substituerimus, obtinebimus congruentiam:

$$V \equiv x^{n-1}\left(n + \frac{n(n-1)(n-2)}{1.2.3} + \frac{n(n-1)(n-2)(n-3)(n-4)}{1.2.3.4.5} + \cdots\right) \pmod{\delta},$$

quam, cum expressionem uncinis inclusam esse $\frac{1}{2}((1+1)^n-(1-1)^n)$ sive 2^{n-1} facillime perspiciatur, hoc quoque modo exhibere possumus:

$$V \equiv 2^{n-1}x^{n-1} \pmod{\delta}.$$

Sequitur ex hac congruentia, primum imparem δ, quem ipsius V divisorem esse supposuimus, etiam esse divisorem ipsius x. Supra autem vidimus, numerum

x^2-b per ϑ esse divisibilem, ϑ metietur igitur utrumque ipsorum x et b, quod est contra suppositionem, numeros x et b inter se esse primos. Concludendum est igitur, suppositionem, ipsos U et V habere divisorem communem imparem, constare non posse.

His praemissis, in indolem divisorum primorum formulae V inquiramus. Quamquam methodus, qua in hac disquisitione utemur, pro quovis valore ipsius n applicari potest, hoc loco, ne haec dissertatio nimis longa fiat, duos tantum casus examini subiciemus, quorum prior locum habet, quando n est primus impar, posterior, quando n est potestas numeri 2.

Sit igitur primo n numerus primus impar, quem per litteram p designabimus, et k primus impar ab ipso p diversus formulam V metiens. Iam duo casus sunt distinguendi, prout b ipsius k est residuum aut non-residuum quadraticum.

Casu priore datur numerus μ huic congruentiae $\mu^2 \equiv b \pmod{k}$ satisfaciens. Primus k, quem formulae V divisorem esse statuimus, eandem metietur, si loco ipsius b valorem secundum modulum k congruum μ^2 substituerimus.

Formula V, quae primam et secundam aequationum (1) comparando hoc modo exhiberi posse invenitur:

$$\frac{(x+\sqrt{b})^p-(x-\sqrt{b})^p}{2\sqrt{b}},$$

substitutione, quam diximus, perfecta, in hanc abibit:

$$\frac{(x+\mu)^p-(x-\mu)^p}{2\mu},$$

in qua expressione neutrum numerorum $x+\mu$ et $x-\mu$ per k divisibilem esse dico. Si enim alter esset, alter non esset, $(x+\mu)^p-(x-\mu)^p$ per k non foret divisibilis. Utrumque autem per k divisibilem esse non posse hoc modo demonstratur. Tum enim k metiretur etiam utrumque ipsorum:

$$\tfrac{1}{2}((x+\mu)+(x-\mu)) \quad \text{et} \quad \tfrac{1}{2}((x+\mu)-(x-\mu)),$$

id est utrumque numerorum x et μ, et quoniam $\mu^2 \equiv b \pmod{k}$ est, k foret quoque divisor ipsius b. Numeri x et b haberent igitur divisorem communem k contra ea quae supposuimus.

Cum neuter ipsorum $x+\mu$ et $x-\mu$ per k sit divisibilis, congruentiae:

$$(x-\mu)y \equiv x+\mu \pmod{k}$$

satisfieri poterit per numerum y.

Quodsi iam in valore ipsius $2\mu V$ loco ipsius $x+\mu$ numerum congruum $y(x-\mu)$ substituerimus, habebimus hanc expressionem per k divisibilem

$$(x-\mu)^p(y^p-1),$$

et cum $x-\mu$, ut supra vidimus, per k non sit divisibilis, y^p-1 ipsius k multiplum esse concluditur. Iam dico, numerum $y-1$ per k divisibilem non esse; si enim k ipsum $y-1$ metiretur, haberemus $y \equiv 1 \pmod{k}$ et congruentia $(x-\mu)y \equiv x+\mu \pmod{k}$ in hanc transiret $2\mu \equiv 0 \pmod{k}$, id est, μ seu b per k foret divisibilis. Sequitur autem ex inspectione formulae V, k ipsius b divisorem esse non posse, nisi vel k ipsi p sit aequalis, vel ipsum x metiatur; quorum casuum utrumque supra exclusimus. Concluditur iam ope theorematis I, primum k esse formae $2mp+1$.

Habemus igitur theorema: „Nullus primus, cuius residuum est b, formulam V metiri potest, nisi in forma $2mp+1$ contineatur.“ Haec propositio etiam inversa valet et demonstrari potest, quemvis primum formae $2mp+1$ formulae V esse divisorem. Cuius propositionis demonstrationem, cum nulli difficultati sit obnoxia, brevitatis causa omittimus.

Pergimus iam ad primos, quorum non-residuum est b, quorumque relatio ad formulam V (quatenus formulae sunt divisores aut non-divisores) per theoremata sequentia definitur:

„Si primus, cuius non-residuum est b, simul est formae $2mp-1$, formulae V erit divisor.“

„Nullus primus k, cuius non-residuum est b, formulam V metiri potest, nisi in forma $2mp-1$ contineatur.“

Prius horum theorematum iam olim ab ill. Lagrange propositum et demonstratum est in commentatione in collectione academica (Nouveaux Mémoires de Berlin, année 1775) conservata, ubi eius ope propositiones nonnullae particulares ad doctrinam de residuis quadraticis pertinentes stabiliuntur. Theorema et demonstratio, qua a viro summo munitum est, exstant etiam in opere egregio „Disquisitiones arithmeticae“, quod cum in manibus omnium versetur, qui analysi Diophantaeae operam navant, demonstrationem hoc loco adicere opus non esse duximus. —

Theorema posterius, quod est prius inversum, a nemine hucusque, quantum scio, est prolatum. Demonstratio minus obvia absolvitur per ratiocinia iis simillima, quibus iam alio loco (Mémoire sur l'impossibilité de quelques équations du cinquième degré) in argumento longe diverso usus sum.

Contemplemur formulam $(x+\sqrt{b})^{k+1}$ et ponamus ex eius evolutione oriri $M+N\sqrt{b}$, ubi M et N a quantitate irrationali $\sqrt{b}$ sunt liberi. Valorem ipsius

N, qui obtinetur, si $k+1$ loco ipsius n in expressione (1) ipsius V substituitur, brevitatis causa non apponimus. Perspicuum est, coefficientes omnium terminorum ipsius N per k esse divisibiles, coefficientibus primi et ultimi termini exceptis.

Qui termini quum sint $(k+1)x^k$ et $(k+1)xb^{\frac{k-1}{2}}$, invenitur:

$$N \equiv (k+1)(x^k+xb^{\frac{k-1}{2}}) \pmod{k}.$$

Constat, numerum b, quem ipsius k non-residuum esse supposuimus, satisfacturum esse congruentiae $b^{\frac{k-1}{2}} \equiv -1 \pmod{k}$, et cum habeamus quoque $x^k \equiv x \pmod{k}$, concluditur:

$$x^k+xb^{\frac{k-1}{2}} \equiv 0 \pmod{k}.$$

N igitur per k erit divisibilis, quicunque valor ipsi x tribuatur.

Ponamus iam, formulam V pro valore determinato ipsius x divisibilem fieri per primum k, cuius non-residuum est b, talemque primum esse formae $2mp-1$ demonstrare conemur.

Cum V per k sit divisibilis, formula U non erit divisibilis, quippe quam formulam ad V primam esse vidimus, dummodo ipsi x valor ad valorem ipsius b primus tribuatur, quod semper fieri supposuimus. Demonstrandum iam est, primum k esse formae $2mp-1$ seu $k+1$ per p esse divisibilem.

Numerus $k+1$ si per p non esset divisibilis, darentur numeri integri g et h positivi ita comparati, ut esset $g(k+1)-hp=1$.

Revertamur nunc ad contemplationem formulae $M+N\sqrt{b}$, in qua N per k divisibilem esse vidimus, eamque ad potestatem g^{mi} gradus elevemus. Quae potestas si per $M'+N'\sqrt{b}$ designatur, facillime perspicitur N' per N ideoque per k esse divisibilem; M' autem per k non divisibilem esse sequitur ex eo, quod $M'+N'\sqrt{b}$ est potestas ipsius $x+\sqrt{b}$ (cuius potestatis exponens est $g(k+1)$), quam ob rem M' et N' divisorem communem habere non possunt. Eodem modo probatur, si ponatur $(U+V\sqrt{b})^h = U'+V'\sqrt{b}$, V' per k divisibilem fore, U' autem non fore. Ex comparatione aequationum:

$$(x+\sqrt{b})^{g(k+1)} = M'+N'\sqrt{b}, \quad (x+\sqrt{b})^{hp} = U'+V'\sqrt{b}, \quad g(k+1)-hp = 1$$

deducitur haec:

$$(x+\sqrt{b})(U'+V'\sqrt{b}) = M'+N'\sqrt{b},$$

quae, multiplicatione perfecta et partibus rationalibus et coefficientibus ipsius $\sqrt{b}$ separatim aequatis, has novas suppeditat:

$$M' = U'x+bV', \quad N' = V'x+U'.$$

Manifestum est, posteriorem harum aequationum locum habere non posse, cum N' et V' ipsius k sint multipla, U' autem per k non sit divisibilis. Concludendum igitur est, suppositionem, a qua profecti sumus, constare non posse, et $k+1$ re vera per p esse divisibilem, seu quod est idem, k esse formae $2mp-1$, q. e. d.

Si ea, quae hucusque docuimus, cum doctrina nota de residuis quadraticis iunguntur, assignari poterunt formae lineares, in quibus divisores primi formulae V includuntur.

Quod ut exemplis illustretur, sit $p=5$ et $b=-1$; quo casu V invenitur esse $5x^4-10x^2+1$.

Sequitur ex iis, quae supra demonstravimus, primos, quorum residuum est -1, ipsius V divisores esse non posse, nisi sint formae $10m+1$, constatque e doctrina de residuis quadraticis primos, quorum residuum est -1, in forma $4n+1$ contineri. Numeri autem simul in utraque formarum $10m+1$, $4n+1$ inclusi sunt formae $20h+1$, in qua igitur continetur quisque primus, cuius residuum est -1, et qui simul formulam V metitur.

Ad divisores primos ipsius V, quorum non-residuum est -1, quod attinet, simili modo invenitur, omnes tales primos in forma $20h-1$ comprehensos esse.

Formula duplex $20h\pm1$ suppeditat igitur omnes primos expressionem $5x^4-10x^2+1$ metientes et vice versa quivis primus in altera formarum $20h+1$, $20h-1$ inclusus ipsius V erit divisor.

Exemplum secundum praebebunt suppositiones $p=7$, $b=2$; quo casu erit:

$$V = 7x^6+70x^4+84x^2+8.$$

Primi, quorum residuum est 2, continentur in formis $8m+1$, $8m+7$; huiusmodi autem primi formulam V metiri non possunt, nisi sint formae $14n+1$, quam cum praecedentibus comparando inveniuntur formae $56h+1$, $56h+15$, in quibus includuntur primi, qui ipsius V sunt divisores et quorum simul residuum est 2.

Primi expressionis V divisores, quorum non-residuum est 2, in formis $56h+13$, $56h+27$ comprehensi esse inveniuntur.

Formulae $56h+1$, 13, 15, 27 suppeditant igitur omnes primos, quadrinomium $7x^6+70x^4+84x^2+8$ metientes, et vice versa quivis primus in una harum formarum contentus quadrinomii erit divisor.

Sunt casus particulares ob theorematum elegantiam attentionem peculiarem merentes. Hos casus, qui locum habent, quoties b ipsi p positive vel negative sumpto aequatur, iam fusius tractabimus.

Sit primo $b = p$; et primus p formae $4n+1$ esse supponatur. Notum est, primos, quorum residuum est $b = p$, in $\frac{1}{2}(p-1)$ huiusmodi formis linearibus contineri:

$$(2) \qquad mp+1, \quad mp+\alpha, \quad mp+\alpha', \quad mp+\alpha'', \quad \ldots,$$

ubi numeri $1, \alpha, \alpha', \alpha'', \ldots$, quos positivos ipsoque p minores supponere licet, omnes inter se erunt diversi et e divisione quadratorum $1, 2^2, 3^2, \ldots (\frac{1}{2}(p-1))^2$ per primum p oriuntur, inter quos numeros constat numerum $p-1$ occurrere, quoties p est formae $4n+1$. Primi autem, quorum non-residuum est b, continentur in $\frac{1}{2}(p-1)$ aliis formis linearibus:

$$(3) \qquad mp+\beta, \quad mp+\beta', \quad mp+\beta'', \quad \ldots,$$

ubi numeri $\beta, \beta', \beta'', \ldots$, qui ipso p minores supponuntur, tam inter se quam ab illis $1, \alpha, \alpha', \alpha'', \ldots$ erunt diversi, ita ut numerus $p-1$ inter ipsos $\beta, \beta', \beta'', \ldots$ occurrere non possit.

Supra demonstravimus, primum, cuius residuum est b, et qui igitur in aliqua formarum (2) continetur, ipsius V divisorem esse non posse, nisi sit formae $mp+1$, quae est eadem ac prima formarum (2) et cum nulla reliquarum constare potest. Sequitur inde, primos, quorum residuum est $b = p$, et qui simul formulam V metiuntur, in forma $mp+1$ comprehensos esse, et vice versa etc.

Quod ad primos attinet, quorum non-residuum est $b = p$, et qui igitur in aliqua formarum (3) continentur, sequitur ex iis, quae supra stabilivimus, tales primos formulae V divisores esse non posse, nisi simul in forma $mp-1$ seu, quod est idem, in forma $mp+p-1$ includantur. Haec autem forma cum nulla formarum (3) constare potest, quia nullus numerorum $\beta, \beta', \beta'', \ldots$ ipsi $p-1$ est aequalis.

Probatum igitur est, nullum primum, cuius non-residuum sit $b = p$, ipsius V esse divisorem, omnesque primos formulam V metientes in forma $mp+1$ esse comprehensos.

Si casus, ubi $b = -p$, p designante primum formae $4m+1$, simili modo examinatur, invenitur, nullum primum, nisi in altera formarum $4mp \pm 1$ contineatur, formulae V divisorem esse posse, et vice versa quemvis primum in altera harum formarum inclusum re vera formulam V metiri.

Casus tertius locum habet, quando $b = p$, et p est formae $4m+3$. Hoc

casu primi formulam V metientes in formis $4mp+1$, $4mp+2p-1$ comprehensi esse inveniuntur.

Superest, ut casum quartum examini subiciamus. Primus p hoc casu est formae $4m+3$, et b ipsi p negative sumpto est aequalis. Si considerationes, quibus in casibus praecedentibus usi sumus, ad casum praesentem applicaverimus, perveniemus ad hoc theorema:

„Nullus primus formulam V, in qua $b = -p$ et p primum formae $4m+3$ designat, metiri potest, nisi in altera formarum $mp+1$, $mp-1$ contineatur et vice versa omnes primi in his formis comprehensi formulae V erunt divisores.“

Quoties casus quartus locum habet, formula V duorum factorum rationalium productum esse invenitur, in quorum indolem iam profundius est inquirendum, ut decidatur, utrius eorum primus formulam metiens sit divisor.

Constat e theoria divisionis circuli, quae ill. Gauss debetur, expressionem $4\frac{t^p-u^p}{t-u}$, quoties p sit primus formae $4n+3$, redigi posse sub formam R^2+pS^2, ubi R et S sunt functiones rationales integrae ipsius x. Formula $4\frac{t^p-u^p}{t-u}$ manifesto est functio symmetrica ipsorum t et u, atque e demonstratione, qua vir summus theorema modo memoratum munivit, facillime deducitur, R esse functionem, quae valorem oppositum nanciscitur, ipsis t et u inter se mutatis. Cum S sit functio symmetrica gradus $\frac{p-1}{2}$, erit summa plurium aggregatorum huius formae:

$$at^m u^{k-m} + at^{k-m} u^m,$$

ubi $k = \frac{p-1}{2}$ et $m < \frac{k}{2}$ supponere licet; tale aggregatum etiam hoc modo exhiberi potest:

$$at^m u^m (t^{k-2m} + u^{k-2m}).$$

Quodsi in hac expressione loco ipsorum t et u resp. $x+\sqrt{-p}$ et $x-\sqrt{-p}$ substituuntur, $t^m u^m$ obtinebit valorem $(x^2+p)^m$, qui est functio par ipsius x (quo verbo brevitatis causa functionem designamus, in qua singuli exponentes sunt numeri pares). Alter factor $t^{k-2m}+u^{k-2m}$, cum exponens $k-2m$ sit impar, per eandem substitutionem mutabitur in functionem integram imparem ipsius x, id est, in functionem, in qua singuli exponentes sunt numeri impares. Aggregati illius valor post substitutionem erit igitur functio impar ipsius x.

Quoniam ea, quae modo diximus, valent de quovis aggregatorum, e quibus constat S, sequitur, S per eandem substitutionem mutatum iri in func-

tionem imparem ipsius x. Hanc functionem, cuius coefficientes singulos pares esse facillime perspicitur, per $2S'$ designabimus.

Simili modo invenitur, formulam R, si loco ipsorum t et u resp. $x+\sqrt{-p}$ et $x-\sqrt{-p}$ substituantur, nacturam esse valorem, e duobus factoribus constantem, quorum prior est $\sqrt{-p}$, posterior functio rationalis par ipsius x. Posteriorem si per $2R'$ denotamus, $2R'\sqrt{-p}$ erit valor, quem R per substitutionem obtinet.

Si iam in formula R^2+pS^2 loco ipsorum R et S resp. $2R'\sqrt{-p}$ et $2S'$ substituuntur, prodibit idem valor, quem nanciscitur $4\frac{t^p-u^p}{t-u}$, loco ipsorum t et u resp. $x+\sqrt{-p}$ et $x-\sqrt{-p}$ substitutis. Habemus igitur:

$$2\frac{(x+\sqrt{-p})^p-(x-\sqrt{-p})^p}{\sqrt{-p}} = 4pS'^2-4pR'^2,$$

et cum etiam sit:

$$V = \frac{(x+\sqrt{-p})^p-(x-\sqrt{-p})^p}{2\sqrt{-p}},$$

concluditur esse:

$$V = p(S'+R')(S'-R').$$

Demonstratum est igitur, formulam $\frac{V}{p}$ in duos factores rationales decomponi posse, quoties $b=-p$ et primus p sit formae $4n+3$.

Cum R' sit functio par, S' autem functio impar ipsius x, manifestum est, signo ipsius x mutato, factorem priorem $S'+R'$ transiturum esse in $R'-S'$, id est, in posteriorem negative sumptum et vice versa posteriorem $S'-R'$, eadem mutatione perfecta, fore $-S'-R'$, id est, priori negative sumpto aequalem.

His ita stabilitis, sit k primus formulae V divisor et α valor ipsi x tribuendus, ut V per k fiat divisibilis. Iam dico, $R'+S'$ per k fore divisibilem, si x valorem idoneum obtineat. Cum enim k metiatur formulam $V=p(R'+S')(R'-S')$, ubi $x=\alpha$ supponitur, aut $R'+S'$ aut $R'-S'$ per k erit divisibilis.

Si casus prior locum habet, α erit valor quaesitus; sin posterior, sequitur e praecedentibus $R'+S'$ per k fore divisibilem, si x ipsi $-\alpha$ aequetur; hoc igitur casu valor idoneus erit $-\alpha$.

Simili modo demonstratur, valorem ipsius x ita assumi posse, ut $R'-S'$ per k fiat divisibilis.

Quivis igitur primus formulam V metiens erit divisor utriusque factorum $R'+S'$, $R'-S'$, ubi vix est monendum, hos factores non pro eodem valore

ipsius x per k fore divisibiles, sed pro valoribus oppositis, id est, pro valoribus signo tantum discrepantibus.

Ut praecedentia exemplis nonnullis illustrentur, ponamus primo $p=7$. Factores ipsius V hoc casu inveniuntur esse:

$$x^3-7x^2+7x+7, \quad x^3+7x^2+7x-7,$$

qui manifesto respectu divisorum inter se non sunt diversi. Divisores primi harum formularum omnes in forma $7n\pm1$ continentur, et vice versa quivis primus in hac forma comprehensus formularum erit divisor.

Sit secundo $p=11$. Factores quinti gradus, quorum productum hoc casu est V, sunt hi:

$x^5+11x^4-2.11.x^3-2.11^2.x^2-3.11^2.x-11^2$, $x^5-11x^4-2.11.x^3+2.11^2.x^2-3.11^2.x+11^2$,

quarum formularum neutra per primum erit divisibilis, nisi in forma $11n\pm1$ contineatur, et vice versa quivis primus etc.

Hucusque supposuimus, numerum n in formulis (1) esse primum imparem. Considerabimus iam casum, ubi n numeri 2 est potestas. Theoremata ad hunc casum pertinentia non ad formulam V, sed ad formulam U sunt referenda. — Numerum n in sequentibus per α designabimus, et k erit primus impar formulam U metiens. Iam duo casus sunt distinguendi, prout b ipsius k est residuum vel non-residuum quadraticum. Si b ipsius k est residuum, datur numerus μ ita comparatus, ut sit $\mu^2\equiv b \pmod{k}$. Primus k, quem formulae U divisorem esse statuimus, eandem metietur, si μ^2 loco ipsius b substituerimus. Formula $2U$, quae, ut comparatio primae et secundae aequationum (1) docet, hoc quoque modo exhiberi potest:

$$2U = (x+\sqrt{b})^\alpha+(x-\sqrt{b})^\alpha,$$

substitutione modo indicata transibit in hanc $(x+\mu)^\alpha+(x-\mu)^\alpha$, quae manifesto per k divisibilis esse non potest, nisi k aut utrumque aut neutrum ipsorum $x+\mu$ et $x-\mu$ metiatur. Casum priorem locum habere non posse hoc modo demonstratur. Tum enim uterque numerorum:

$$\tfrac{1}{2}(x+\mu)+\tfrac{1}{2}(x-\mu), \quad \tfrac{1}{2}(x+\mu)-\tfrac{1}{2}(x-\mu),$$

seu uterque ipsorum x et μ per k esset divisibilis et quoniam est $b\equiv\mu^2 \pmod{k}$, k metiretur quoque ipsum b contra suppositionem, valores ipsi x tribuendos ad ipsum b esse primos.

Cum neuter ipsorum $x+\mu$, $x-\mu$ per k sit divisibilis, assignari potest numerus y huic congruentiae satisfaciens:

$$(x+\mu)y \equiv x-\mu \pmod{k}.$$

Quodsi iam in formula $2U$ loco ipsius $x-\mu$ valorem secundum mod. k congruum $y(x+\mu)$ substituerimus, obtinebimus hanc expressionem per k divisibilem $(x+\mu)^\alpha(y^\alpha+1)$, cuius factorem $y^\alpha+1$ igitur primus k metiri debet, unde ope theorematis II concluditur, k esse formae $2m\alpha+1$. Habemus itaque theorema:

„Omnes primi, quorum residuum est b, formulam U, in qua $n=\alpha$ est potestas numeri 2, metientes continentur in forma $2m\alpha+1$."

Haec propositio etiam inversa valet et simili modo demonstrari potest.

Progredimur ad considerationem primorum, quorum non-residuum quadraticum est b et de quibus hoc theorema valet:

„Si primus, cuius non-residuum est b, est formae $2m\alpha-1$, formulae U erit divisor, et vice versa nullus primus, cuius non-residuum est b, formulam metitur, nisi in forma $2m\alpha-1$ contineatur."

Demonstrationem partis prioris huius theorematis, cum iis, quae supra exposuimus, satis sit similis, lectori evolvendam relinquimus. Posterioris autem demonstrationem, quae nova artificia requirit, fusius explicabimus. Sit k primus, cuius non-residuum est b, formulam U pro valore determinato ipsius x metiens, demonstrandum est nobis, k esse formae $2m\alpha-1$, seu $k+1$ per 2α esse divisibilem. Ponamus $k+1$ per 2α non esse divisibilem, et quid inde sequatur, videamus. Si per β summam potestatem numeri 2 ipsum $k+1$ metientem designamus, $\frac{k+1}{\beta}$ erit numerus impar et $\frac{2\alpha}{\beta}$ vel 2 vel potestas ipsius 2. Numeri $\frac{k+1}{\beta}$, $\frac{2\alpha}{\beta}$ igitur divisorem communem non habent, unde sequitur, numeros integros positivos assignari posse ita comparatos, ut sit:

$$g\frac{k+1}{\beta}-\frac{2\alpha}{\beta}h=1,$$

quae aequatio hoc quoque modo exhiberi potest: $g(k+1)-2h\alpha=\beta$.

Supra vidimus, N in aequatione $M+N\sqrt{b}=(x+\sqrt{b})^{k+1}$ pro quovis valore ipsius x per k esse divisibilem. Expressionem $M+N\sqrt{b}$ ad potestatem g elevatam si per $M'+N'\sqrt{b}$ designamus, N' per N ideoque per k divisibilis erit, M' autem per k non divisibilem esse sequitur ex eo, quod $M'+N'\sqrt{b}$ manifesto est potestas ipsius $x+\sqrt{b}$, quam ob rem M' et N' divisorem communem imparem habere non possunt.

Habemus aequationem:

$$(x+\sqrt{b})^\alpha = U+V\sqrt{b},$$

in qua, cum U per k sit divisibilis, formula V non erit, quippe quae ad formulam U est prima. Ex aequatione praecedenti deducitur haec:

$$(x+\sqrt{b})^{2\alpha} = U^2+bV^2+2UV\sqrt{b}$$

seu, quod est idem, si brevitatis causa ponimus $U^2+bV^2=P$, $2UV=Q$:

$$(x+\sqrt{b})^{2\alpha} = P+Q\sqrt{b}.$$

Cum k ipsum b non metiatur, et U ipsius k sit multiplum, V autem non sit, concluditur, k ipsius Q esse divisorem, ipsius P autem non esse.

Iam si ponimus:

$$(P+Q\sqrt{b})^h = P'+Q'\sqrt{b},$$

ut supra demonstrari poterit, Q' ipsius k fore multiplum, P' autem non fore. —

E comparatione aequationum:

$$(x+\sqrt{b})^{g(k+1)} = M'+N'\sqrt{b},\quad (x+\sqrt{b})^{2h\alpha} = P'+Q'\sqrt{b},\quad g(k+1)-2h\alpha=\beta,$$

deducitur haec:

$$M'+N'\sqrt{b} = (P'+Q'\sqrt{b})(x+\sqrt{b})^\beta,$$

quae, si brevitatis causa ponimus $(x+\sqrt{b})^\beta = R+S\sqrt{b}$, hoc quoque modo exhiberi potest:

$$M'+N'\sqrt{b} = (P'+Q'\sqrt{b})(R+S\sqrt{b}).$$

Concluditur inde, multiplicando et partes rationales et coefficientes ipsius $\sqrt{b}$ separatim aequando, esse:

$$M'=P'R+bQ'S,\quad N'=P'S+Q'R.$$

Cum Q' et N' ipsius k sint multipla, k autem expressionem P' non metiatur, manifesto posterior aequationum praecedentium locum habere non potest, nisi S per k sit divisibilis.

Habemus aequationes:

$$(x+\sqrt{b})^\alpha = U+V\sqrt{b},\quad (x+\sqrt{b})^\beta = R+S\sqrt{b},$$

quarum comparatio hanc novam suppeditat:

$$U+V\sqrt{b} = (R+S\sqrt{b})^{\frac{\alpha}{\beta}},$$

ubi $\frac{\alpha}{\beta}$ est integer, quia $\frac{2\alpha}{\beta}$ est vel 2 vel potestas ipsius 2. Sequitur ex aequatione praecedenti, in qua exponens $\frac{\alpha}{\beta}$ est integer, V per S esse divisibilem; et cum k, ut supra vidimus, formulam S metiatur, concludendum est, k esse divisorem formulae V, quod est contra ea, quae supra stabilivimus. Demonstravimus enim, formulas U et V divisorem communem imparem habere non posse, unde sequitur, primum k, quem formulae U divisorem esse statuimus, formulam V metiri non posse. Probatum est igitur, suppositionem, a qua pro-

fecti sumus, constare non posse, sed $k+1$ re vera per $2a$ esse divisibilem seu k esse formae $2ma-1$.

Ecce quaedam exempla ad theoremata modo demonstrata referenda.

Sit $a=4$, quo casu U invenitur $x^4+6bx^2+b^2$, quae formula per nullum primum, cuius residuum quadraticum est b, erit divisibilis, nisi in forma $8m+1$ contentum, et per nullum primum, cuius non-residuum est b, nisi in forma $8m-1$ sit inclusus.

Ponamus $b=-3$, qua suppositione U erit x^4-18x^2+9. Constat autem e doctrina de residuis quadraticis, primos, quorum residuum sit -3, esse formae $3m+1$, primos, quorum non-residuum -3, esse formae $3m-1$. Quae si cum praecedentibus comparaveris, invenies: „formulam x^4-18x^2+9 per nullum primum esse divisibilem, nisi in altera formarum $24m\pm1$ contineatur, et vice versa, quemvis primum etc.“

Aliud exemplum praebebunt suppositiones $a=8$, $b=5$, quo casu valor formulae U erit $x^8+140x^6+1750x^4+3500x^2+625$, cuius expressionis divisores primi erunt formae $16m+1$ vel formae $16m-1$, prout 5 eorum est residuum vel non-residuum quadraticum. Quod si cum propositione nota: „primos, quorum residuum sit 5, esse formae $5m\pm1$, primos autem, quorum non-residuum sit 5, esse formae $5m\pm2$“ rite iunxeris, prodibit hoc theorema:

„Primi formulam $x^8+140x^6+1750x^4+3500x^2+625$ metientes continentur in formis $80m+1$, 47, 49, 63, et vice versa quivis primus in aliqua harum formarum comprehensus formulae erit divisor.“

RECHERCHES SUR LES DIVISEURS PREMIERS D'UNE CLASSE DE FORMULES DU QUATRIÈME DEGRÉ.

PAR

M. G. LEJEUNE DIRICHLET,
PROF. DE MATH. A BRESLAU.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 3 p. 35—69.

RECHERCHES SUR LES DIVISEURS PREMIERS D'UNE CLASSE DE FORMULES DU QUATRIÈME DEGRÉ.

1er Mémoire.

On trouve, dans les annonces littéraires de Gottingue (11 avril 1825), l'extrait d'un mémoire d'analyse indéterminée que M. Gauss a présenté à la Société Royale des Sciences de cette ville, mais qui n'a pas encore été imprimé. Ce mémoire est le premier d'une suite de mémoires que l'illustre auteur des *Disquisitiones arithmeticae* se propose de donner sur la théorie des résidus biquadratiques, et a pour objet de déterminer les caractères distinctifs des nombres premiers diviseurs de la formule x^4-2. L'auteur y établit deux théorèmes extrêmement élégants qui peuvent servir à décider, si un nombre premier, diviseur de x^2-2, divise ou ne divise pas la formule précédente. Ayant eu connaissance, dans le courant de l'année qui vient de finir, de l'extrait cité qui ne contient que les énoncés des deux théorèmes dont il vient d'être question, et de quelques propositions auxiliaires, j'eus le désir de démontrer de mon côté les beaux théorèmes découverts par M. Gauss. Les recherches que je fis dans cette vue me firent trouver une démonstration fondée sur des considérations extrêmement simples et probablement tout-à-fait différente de celle de M. Gauss, qui paraît exiger des recherches préliminaires très délicates et assez étendues. J'appliquai ensuite des considérations analogues à d'autres questions et particulièrement à la recherche des propriétés qui distinguent les diviseurs premiers de la formule $\alpha x^4+\beta x^2+\gamma$; et je parvins ainsi à un grand nombre de théorèmes intéressants. L'exposition rapide d'une partie des résultats auxquels ces recherches m'ont conduit, est l'objet du présent mémoire. Je commence par poser quelques définitions et par énoncer quelques théorèmes très faciles à établir et sur lesquels nous aurons à nous appuyer dans la suite.

1.

„Si l'on peut attribuer à l'indéterminée x une valeur telle que x^4-A devienne divisible par B, A sera dit résidu biquadratique par rapport à B.“

Il est facile de voir que, si un nombre A est résidu biquadratique par rapport à un nombre B, ou en d'autres termes, si B est diviseur de x^4-A, chaque facteur premier de B sera pareillement diviseur de x^4-A, et réciproquement, que si cette condition a lieu par rapport à tout facteur premier du nombre B, B sera lui-même diviseur de x^4-A. On peut donc se borner, lorsqu'il s'agit d'assigner tous les nombres qui divisent la formule x^4-A, à ne considérer que les nombres premiers.

Il n'est pas moins évident que, pour qu'un nombre divise la formule x^4-A, il est nécessaire que ce nombre soit diviseur de x^2-A. Il n'y a donc à examiner que les nombres premiers diviseurs de cette dernière formule, c'est-à-dire les nombres premiers par rapport auxquels A est résidu quadratique. On peut ajouter que, relativement à ceux de ces derniers qui sont de la forme $4n+3$, la question ne présente aucune difficulté; car on s'assure par un raisonnement très simple que tout nombre premier $4n+3$, diviseur de x^2-A, divise aussi la formule x^4-A.

Soit p un nombre premier $4n+1$, diviseur de x^2-A, A désignant un nombre positif ou négatif, non-divisible par p; on a, comme l'on sait, $A^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. On conclut de là, $A^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p}$ et l'on prouve facilement que le signe supérieur ou inférieur aura lieu, selon que p divise ou ne divise pas la formule x^4-A. On peut donc énoncer ce théorème:

„A désignant un nombre résidu quadratique par rapport au nombre premier $p=4n+1$, on aura $A^{\frac{p-1}{4}} \equiv 1$ ou $A^{\frac{p-1}{4}} \equiv -1 \pmod{p}$. Dans le premier cas, A sera résidu biquadratique par rapport à p, dans le second, A sera non-résidu biquadratique par rapport à p.“

Si l'on applique ce théorème au cas où $A=-1$, on trouvera que -1 est résidu biquadratique par rapport aux nombres premiers $8n+1$, et au contraire non-résidu relativement à ceux de la forme $8n+5$. Du théorème précédent on déduit facilement cet autre, dans l'énoncé duquel on suppose, comme dans tout ce qui suivra, que p soit un nombre premier $4n+1$, et que A et A' désignent des nombres non-divisibles par p et qui sont l'un et l'autre des résidus quadratiques par rapport à p.

„Si les nombres A et A' sont tous les deux des résidus biquadratiques ou tous les deux des non-résidus biquadratiques par rapport à p, le produit AA' sera résidu biquadratique par rapport à p; si, au contraire, l'un des nombres A et A' est résidu, l'autre non-résidu biquadratique relativement à p, AA' sera non-résidu biquadratique par rapport à p.“

En faisant $A'=-1$, et en ayant égard à ce qui précède, on verra que, si p est de la forme $8n+1$, A sera en même temps que $-A$ résidu ou non-résidu biquadratique, et qu'au contraire, si p est de la forme $8n+5$, l'un des nombres A et $-A$ sera résidu, l'autre non-résidu biquadratique par rapport à p.

2.

Après avoir établi ces préliminaires, nous allons nous occuper de la recherche des caractères qui distinguent les diviseurs premiers de la formule x^4-2. On sait que les diviseurs premiers de x^2-2 sont de l'une de ces deux formes: $8n+1$, $8n+7$, et que réciproquement tout nombre premier de l'une de ces formes divise la formule x^2-2. D'après ce que nous avons dit dans le paragraphe précédent, nous n'avons pas besoin d'avoir égard à la dernière de ces deux formes, et il suffira de considérer les nombres premiers $8n+1$. Soit p un nombre premier de cette espèce, et posons, comme il est permis de le faire, $p=t^2+2u^2$, où u sera pair, t impair. Faisons $u=2^\nu kk'k''\ldots$, 2^ν étant la puissance la plus élevée de 2 qui divise u, et k, k', k'', ... désignant des nombres premiers impairs, dont plusieurs peuvent être égaux entre eux. L'équation $t^2+2u^2=p$ donne immédiatement $t^2 \equiv p \pmod{k}$. Le nombre p est donc résidu quadratique par rapport à k, ce que nous écrirons ainsi: $\left(\frac{p}{k}\right)=1$, en adoptant la notation employée par M. Legendre. On se rappelle que, si c désigne un nombre premier et M un nombre quelconque, non divisible par c, cet illustre géomètre se sert du signe $\left(\frac{M}{c}\right)$, pour désigner le reste que l'on obtient, en divisant par c la puissance $M^{\frac{c-1}{2}}$, reste que l'on sait être égal à 1 ou -1, selon que M est ou n'est pas résidu quadratique par rapport à c. En appliquant à la relation $\left(\frac{p}{k}\right)=1$, le théorème connu sous le nom de loi de réciprocité (*theorema fundamentale* de M. Gauss), on aura, p étant

de la forme $4n+1$, $\left(\frac{k}{p}\right)=1$. On trouve de la même manière:

$$\left(\frac{k'}{p}\right)=1, \quad \left(\frac{k''}{p}\right)=1, \quad \text{etc.}$$

D'un autre côté, comme p est de la forme $8n+1$, on a aussi $\left(\frac{2}{p}\right)=1$, et par conséquent $\left(\frac{2^r}{p}\right)=1$. Multipliant cette dernière relation par toutes les précédentes, il viendra:

$$\left(\frac{2^r kk'k''\ldots}{p}\right)=\left(\frac{u}{p}\right)=1.$$

Considérons maintenant les facteurs simples du nombre impair t, que nous partagerons en deux classes. La première classe comprendra les diviseurs premiers de l'une de ces deux formes: $8n+1$, $8n+7$, et les nombres qui en font partie seront désignés par g, g', g'', ...; la seconde classe se composera de nombres h, h', h'', ..., contenus dans ces deux formes: $8n+3$, $8n+5$. On a d'abord:

$$t=gg'g''\ldots\times hh'h''\ldots,$$

et l'on conclura ensuite de l'équation $p=t^2+2u^2$:

$$\left(\frac{2p}{g}\right)=1, \quad \left(\frac{2p}{g'}\right)=1, \quad \left(\frac{2p}{g''}\right)=1, \quad \text{etc.}$$
$$\left(\frac{2p}{h}\right)=1, \quad \left(\frac{2p}{h'}\right)=1, \quad \left(\frac{2p}{h''}\right)=1, \quad \text{etc.}$$

D'un autre côté, on a en vertu de théorèmes connus:

$$\left(\frac{2}{g}\right)=1, \quad \left(\frac{2}{g'}\right)=1, \quad \left(\frac{2}{g''}\right)=1, \quad \text{etc.}$$
$$\left(\frac{2}{h}\right)=-1, \quad \left(\frac{2}{h'}\right)=-1, \quad \left(\frac{2}{h''}\right)=-1, \quad \text{etc.}$$

Si l'on compare maintenant ces relations aux précédentes, on trouvera:

$$\left(\frac{p}{g}\right)=1, \quad \left(\frac{p}{g'}\right)=1, \quad \left(\frac{p}{g''}\right)=1, \quad \text{etc.}$$
$$\left(\frac{p}{h}\right)=-1, \quad \left(\frac{p}{h'}\right)=-1, \quad \left(\frac{p}{h''}\right)=-1, \quad \text{etc.}$$

L'application de la loi de réciprocité à ces dernières relations donnera celles-ci:

$$\left(\frac{g}{p}\right)=1, \quad \left(\frac{g'}{p}\right)=1, \quad \left(\frac{g''}{p}\right)=1, \quad \text{etc.}$$
$$\left(\frac{h}{p}\right)=-1, \quad \left(\frac{h'}{p}\right)=-1, \quad \left(\frac{h''}{p}\right)=-1, \quad \text{etc.}$$

d'où il suit, en multipliant:

$$\left(\frac{gg'g''\ldots\times hh'h''\ldots}{p}\right)=\left(\frac{t}{p}\right)=\pm 1,$$

où il faudra prendre le signe supérieur ou inférieur, selon que les nombres h, h', h'', ... sont en nombre pair ou impair. Or, il est facile de voir, par l'équation $t=gg'g''\ldots\times hh'h''\ldots$, que le premier cas aura lieu, lorsque t est de l'une de ces formes: $8n+1$, $8n+7$, le second, lorsque t est contenu dans l'une de celles-ci: $8n+3$, $8n+5$. On a donc:

$$\left(\frac{t}{p}\right)=1, \quad \text{lorsque} \quad t=8n+1 \quad \text{ou} \quad 8n+7,$$
$$\left(\frac{t}{p}\right)=-1, \quad \text{lorsque} \quad t=8n+3 \quad \text{ou,} \quad 8n+5.$$

Reprenons l'équation $t^2+2u^2=p$ et mettons-la sous la forme d'une congruence:

$$t^2\equiv -2u^2 \pmod{p}.$$

En élevant les deux membres à la puissance $\frac{p-1}{4}$, on aura $\left(\frac{p-1}{4}\text{ étant pair}\right)$:

$$t^{\frac{p-1}{2}}\equiv 2^{\frac{p-1}{4}}u^{\frac{p-1}{2}} \pmod{p},$$

ou, ce qui revient au même, ayant prouvé que $\left(\frac{u}{p}\right)=1$:

$$t^{\frac{p-1}{2}}\equiv 2^{\frac{p-1}{4}} \pmod{p}.$$

On voit donc que ± 2 (on peut mettre le double signe attendu que $p=8n+1$) est ou n'est pas résidu biquadratique par rapport à p, selon que l'on a $\left(\frac{t}{p}\right)=1$ ou $\left(\frac{t}{p}\right)=-1$. En comparant ce résultat à ce qui précède, on aura ce théorème:

„p désignant un nombre premier $8n+1$, si l'on fait $p=t^2+2u^2$, je dis que ± 2 sera ou ne sera pas résidu biquadratique par rapport à p, selon que t est de l'une de ces formes: $8n+1$, $8n+7$ ou de l'une de celles-ci: $8n+3$, $8n+5$."

C'est le premier des deux théorèmes de M. Gauss, dont il a été question dans le préambule de ce mémoire. Le second de ces théorèmes est relatif à la décomposition du nombre p en deux carrés, et peut être facilement déduit de celui qui vient d'être établi.

Faisons $p=\varphi^2+\psi^2$ (où ψ est supposé divisible par 4) et égalons cette valeur de p à celle que nous venons de considérer.

Nous aurons ainsi:

$$p = t^2+2u^2 = \varphi^2+\psi^2,$$

et en transposant:

$$t^2-\psi^2 = (t+\psi)(t-\psi) = \varphi^2-2u^2.$$

Comme φ est impair, le plus grand diviseur commun de φ et u sera impair; désignons-le par m et faisons $\varphi = m\varphi'$, $u = mu'$. La substitution de ces valeurs dans l'équation précédente la changera en celle-ci:

$$(t+\psi)(t-\psi) = m^2(\varphi'^2-2u'^2).$$

On voit que le nombre impair $t+\psi$ est composé de deux facteurs E et K, dont le premier divise m^2, le second $\varphi'^2-2u'^2$, et qu'il en est de même de $t-\psi$ dont nous désignerons les facteurs par F et L, L pouvant être négatif. Nous avons donc les équations:

$$t+\psi = EK, \quad t-\psi = FL,$$
$$m^2 = EF, \quad \varphi'^2-2u'^2 = KL.$$

Il est facile de s'assurer que les nombres E et F sont premiers entre eux. En effet, soit δ un diviseur premier de E, et supposons que δ divise en même temps F. Le nombre δ serait diviseur commun de $t+\psi$ et $t-\psi$, et diviserait par conséquent le nombre t, qui est la demi-somme des précédents. D'un autre côté, de ce que δ est diviseur premier de E, il suit successivement, en ayant égard aux équations $EF = m^2$, $u = mu'$, que m^2, m et u sont multiples de δ. Les nombres t et u auraient donc le diviseur commun δ, et $p = t^2+2u^2$ ne serait pas un nombre premier.

Le produit des nombres E et F, qui sont premiers entre eux, étant un carré, chacun d'eux est aussi un carré. Faisons $E = e^2$, et nous aurons $t+\psi = e^2K$. Le carré impair e^2 est de la forme $8n+1$, et K, comme diviseur impair de $\varphi'^2+2u'^2$ (où φ' et u' sont premiers entre eux), de l'une de celles-ci: $8n+1$, $8n+7$. Le nombre $t+\psi$ sera donc lui-même de l'une des formes $8n+1$, $8n+7$. Le nombre ψ que nous savons être divisible par 4, sera de la forme $8n$ ou de celle-ci: $8n+4$. Il suit, de ce qui précède, que, dans le premier cas, t sera de l'une de ces deux formes: $8n+1$, $8n+7$, dans le second de l'une de celles-ci: $8n+3$, $8n+5$. En comparant ce résultat au théorème précédent, on aura cet autre théorème:

„p désignant un nombre premier $8n+1$, et ayant fait $p = \varphi^2+\psi^2$ (où ψ est supposé divisible par 4), ± 2 sera ou ne sera pas résidu biquadratique par rapport à p, selon que ψ est de la forme $8n$ ou de celle-ci: $8n+4$."

Il y a un troisième théorème propre à décider si ± 2 est ou n'est pas résidu biquadratique relativement à un nombre premier $p = 8n+1$, et qui peut s'énoncer comme il suit:

„Ayant fait d'une manière quelconque $p = t^2-2u^2$, ± 2 sera ou ne sera pas résidu biquadratique par rapport à p, selon que t est de l'une des formes $8n+1$, $8n+3$, ou de l'une de celles-ci: $8n+5$, $8n+7$."

Nous ne nous arrêterons pas à démontrer ce théorème que l'on peut établir d'une manière directe et par des considérations analogues à celles sur lesquelles est fondée la démonstration du premier des deux théorèmes précédents. On peut aussi le déduire de chacun des précédents à-peu-près comme on vient de passer du premier au second.

3.

Nous allons maintenant passer à des considérations plus générales. Soit b un nombre premier $4n+3$, p un nombre premier $4n+1$ susceptible d'être mis sous la forme t^2-bu^2, et proposons-nous de décider si $-b$ est ou n'est pas résidu biquadratique par rapport à p. Il est facile de voir que, si p peut être mis sous la forme t^2-bu^2, on peut toujours le faire de manière que u soit pair, et par conséquent t impair*). Faisons donc $p = t^2-bu^2$, et posons $u = 2^r kk'k''\ldots$, k, k', k'', $\ldots$ étant les facteurs impairs simples de u. On conclut immédiatement de l'équation précédente:

$$\left(\frac{p}{k}\right) = 1, \quad \left(\frac{p}{k'}\right) = 1, \quad \left(\frac{p}{k''}\right) = 1, \quad \text{etc.}$$

L'application de la loi de réciprocité donne ensuite, p étant de la forme $4n+1$:

$$\left(\frac{k}{p}\right) = 1, \quad \left(\frac{k'}{p}\right) = 1, \quad \left(\frac{k''}{p}\right) = 1, \quad \text{etc.}$$

Multipliant ces relations entre elles et avec la relation identique $\left(\frac{2^r}{p}\right) = \left(\frac{2^r}{p}\right)$,

*) Pour prouver que cela est toujours possible, nous allons faire voir que, si l'on a $t^2-bu^2 = p$, t étant pair, il est facile de déduire des valeurs de t et de u, d'autres nombres t' (impair) et u' qui satisfassent également à l'équation $t'^2-bu'^2 = p$. Soient r et s les moindres nombres tels que $r^2-bs^2 = 1$, je dis que r sera pair. En effet, on sait que, si b désigne un nombre premier $4n+3$, l'équation $\rho^2-b\sigma^2 = \pm 2$ est toujours possible, et que, ρ et σ étant supposés les plus petits nombres qui y satisfassent, on a $r = b\sigma^2+1$, $s = \rho\sigma$ (*Théorie des Nombres*, no. 44. 45). Il suit de là et de ce que les nombres ρ et σ sont évidemment impairs l'un et l'autre, que r est un nombre pair. Cela posé, si l'on multiplie entre elles les équations $r^2-bs^2 = 1$, $t^2-bu^2 = p$, il viendra $(rt\pm bsu)^2-b(ru\pm st)^2 = p$, et l'on verra facilement que $rt\pm bsu$ est un nombre impair.

on aura ce résultat:

$$(\alpha) \qquad \left(\frac{u}{p}\right) = \left(\frac{2^\nu}{p}\right).$$

Décomposons actuellement le nombre impair t en ses facteurs simples et partageons ces facteurs en deux classes. Ceux de la première classe seront désignés par $g, g', g'', \ldots$, et sont tels que:

$$(\beta) \qquad \left(\frac{-b}{g}\right) = 1, \quad \left(\frac{-b}{g'}\right) = 1, \quad \left(\frac{-b}{g''}\right) = 1, \quad \text{etc.}$$

Quant à ceux qui forment la seconde classe et que nous désignerons par $h, h', h'', \ldots$, ils sont tels que:

$$(\beta') \qquad \left(\frac{-b}{h}\right) = -1, \quad \left(\frac{-b}{h'}\right) = -1, \quad \left(\frac{-b}{h''}\right) = -1, \quad \text{etc.}$$

Le produit de tous ces nombres est égal à t, c'est-à-dire que:

$$t = gg'g''\ldots \times hh'h''\ldots .$$

L'inspection de l'équation $t^2 - bu^2 = p$ donne ces résultats:

$$\left(\frac{-bp}{g}\right) = 1, \quad \left(\frac{-bp}{g'}\right) = 1, \quad \left(\frac{-bp}{g''}\right) = 1, \quad \text{etc.}$$

$$\left(\frac{-bp}{h}\right) = 1, \quad \left(\frac{-bp}{h'}\right) = 1, \quad \left(\frac{-bp}{h''}\right) = 1, \quad \text{etc.}$$

La comparaison de ces relations avec les précédentes donnera ensuite:

$$\left(\frac{p}{g}\right) = 1, \quad \left(\frac{p}{g'}\right) = 1, \quad \left(\frac{p}{g''}\right) = 1, \quad \text{etc.}$$

$$\left(\frac{p}{h}\right) = -1, \quad \left(\frac{p}{h'}\right) = -1, \quad \left(\frac{p}{h''}\right) = -1, \quad \text{etc.}$$

Appliquant maintenant la loi de réciprocité, il viendra:

$$\left(\frac{g}{p}\right) = 1, \quad \left(\frac{g'}{p}\right) = 1, \quad \left(\frac{g''}{p}\right) = 1, \quad \text{etc.}$$

$$\left(\frac{h}{p}\right) = -1, \quad \left(\frac{h'}{p}\right) = -1, \quad \left(\frac{h''}{p}\right) = -1, \quad \text{etc.}$$

Multipliant ces relations entre elles, on aura:

$$\left(\frac{gg'g''\ldots \times hh'h''}{p}\right) = \left(\frac{t}{p}\right) = \pm 1,$$

le signe supérieur ou inférieur ayant lieu, selon que les nombres $h, h', h'', \ldots$ sont en nombre pair ou impair. D'un autre côté, si l'on applique la loi de réciprocité aux relations (β) et (β'), il viendra, b étant de la forme $4n+3$:

$$\left(\frac{g}{b}\right) = 1, \quad \left(\frac{g'}{b}\right) = 1, \quad \left(\frac{g''}{b}\right) = 1, \quad \text{etc.}$$

$$\left(\frac{h}{b}\right) = -1, \quad \left(\frac{h'}{b}\right) = -1, \quad \left(\frac{h''}{b}\right) = -1, \quad \text{etc.}$$

égalités qui, étant multipliées entre elles, donneront celle-ci:

$$\left(\frac{gg'g''\ldots \times hh'h''}{b}\right) = \left(\frac{t}{b}\right) = \pm 1,$$

où il faut prendre le signe supérieur ou inférieur, selon que les nombres $h, h', h'', \ldots$ sont en nombre pair ou impair.

La comparaison de ce résultat avec celui que nous avons obtenu, il n'y a qu'un instant, fait voir qu'on a toujours:

$$(\gamma) \qquad \left(\frac{t}{p}\right) = \left(\frac{t}{b}\right).$$

Reprenons maintenant l'équation $p = t^2 - bu^2$, et mettons-la sous la forme d'une congruence:

$$t^2 \equiv bu^2 \pmod{p}.$$

On tire de là, en élevant les deux membres à la puissance $\frac{p-1}{4}$:

$$t^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{4}} u^{\frac{p-1}{2}} \pmod{p}.$$

La formule (α), qui est celle-ci: $\left(\frac{u}{p}\right) = \left(\frac{2^\nu}{p}\right)$, 2^ν désignant la puissance la plus élevée qui divise u, peut être présentée d'une autre manière. Il faut pour cela distinguer deux cas, selon que p est de la forme $8n+1$ ou de celle-ci: $8n+5$. Si p est un nombre premier $8n+1$, on a, comme on sait, $\left(\frac{2}{p}\right) = 1$, et par conséquent $\left(\frac{2^\nu}{p}\right) = 1$; la formule dont il s'agit se change donc dans ce cas en celle-ci: $\left(\frac{u}{p}\right) = 1$. Si p est un nombre premier $8n+5$, le nombre ν est $= 1$; car si ν était plus grand que l'unité, u^2 serait divisible par 8, et $p = t^2 - bu^2$ serait de la forme $8n+1$. Comme d'ailleurs dans ce cas $\left(\frac{2}{p}\right) = -1$, la formule (α) se changera en celle-ci: $\left(\frac{u}{p}\right) = -1$. Les deux cas que nous venons d'examiner sont compris dans la formule $\left(\frac{u}{p}\right) = (-1)^{\frac{p-1}{4}}$, qui équivaut à cette congruence: $u^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \pmod{p}$. En substituant la valeur qu'elle donne

pour $u^{\frac{p-1}{2}}$ dans la congruence obtenue plus haut, on aura:

$$t^{\frac{p-1}{2}} \equiv (-b)^{\frac{p-1}{4}} \pmod{p},$$

résultat qui montre que $-b$ sera ou ne sera pas résidu biquadratique par rapport à p, selon que t est ou n'est pas résidu quadratique par rapport à p. Si l'on compare maintenant ce résultat avec celui qui est contenu dans la formule (γ), on arrivera au théorème que nous allons énoncer:

„Désignons par b un nombre premier $4n+3$, et par p un nombre premier $4n+1$, susceptible d'être mis sous la forme t^2-bu^2. Ayant fait $p = t^2-bu^2$ (où t est supposé impair), je dis que $-b$ sera ou ne sera pas résidu biquadratique par rapport à p, selon que t est ou n'est pas résidu quadratique par rapport à b."

4.

Nous allons maintenant déduire de ce théorème un autre, au moyen duquel on peut décider plus promptement encore, si $-b$ est ou n'est pas résidu biquadratique par rapport à p. Conservons les notations précédentes et faisons $p = \varphi^2+\psi^2$ (où ψ est supposé pair). En égalant cette valeur de p à celle que nous avons considérée précédemment, on aura:

$$p = t^2-bu^2 = \varphi^2+\psi^2,$$

et en transposant:

$$t^2-\psi^2 = (t+\psi)(t-\psi) = \varphi^2+bu^2.$$

Il y a maintenant deux cas à distinguer, selon que φ est ou n'est pas divisible par b. Nous commençons par l'examen du dernier de ces deux cas. Soit m le plus grand commun diviseur de φ et u qui sera impair (φ étant impair) et non-divisible par b, et posons $\varphi = m\varphi'$, $u = mu'$. La substitution de ces valeurs dans la dernière équation, la changera en celle-ci:

$$(t+\psi)(t-\psi) = m^2(\varphi'^2+bu'^2).$$

Il est évident, par cette équation, que $t+\psi$ est composé de deux facteurs E et K dont le premier divise m^2, le second $\varphi'^2+bu'^2$, et qu'il en est de même de $t-\psi$. Désignant les facteurs de ce dernier nombre par F et L, nous aurons ces équations:

$$t+\psi = EK, \qquad t-\psi = FL,$$
$$m^2 = EF, \quad \varphi'^2+bu'^2 = KL.$$

Il est très facile de s'assurer que les nombres E et F sont premiers entre eux. En effet, soit δ un facteur simple quelconque de E (qui sera nécessairement impair, E étant lui même impair) et supposons que δ divise aussi F. L'inspection des équations précédentes fait voir que δ serait, dans cette supposition, diviseur commun de $t+\psi$ et $t-\psi$, et diviserait par conséquent le nombre t, qui est la demi-somme des précédents. Mais on voit d'un autre côté que δ, comme diviseur premier de E, divise m^2, et par conséquent m et u (u étant $= mu'$). Les nombres t et u auraient donc, dans cette supposition, le facteur commun δ, ce qui est absurde, $p = t^2-bu^2$ étant un nombre premier. Il est donc prouvé que E et F ne sauraient avoir de diviseur commun, et comme le produit de ces nombres est un carré, chacun d'eux est pareillement un carré. On a donc:

$$\left(\frac{E}{b}\right) = 1, \quad \left(\frac{F}{b}\right) = 1.$$

Quant aux nombres K et L, ils sont de même tels qu'on ait:

$$\left(\frac{K}{b}\right) = 1, \quad \left(\frac{L}{b}\right) = 1.$$

En effet, on voit par la dernière équation (p. 74) que ces nombres divisent l'un et l'autre la formule $\varphi'^2+bu'^2$ (où φ' et bu' sont premiers entre eux) et l'on sait par un théorème connu qui se déduit facilement de la loi de réciprocité (*Théorie des Nombres*, no. 197) que tout diviseur impair R d'une pareille formule est tel que $\left(\frac{R}{b}\right) = 1$. Multipliant la première des dernières relations par la troisième, la seconde par la quatrième, il viendra:

$$\left(\frac{EK}{b}\right) = 1, \quad \left(\frac{FL}{b}\right) = 1,$$

ou, ce qui est la même chose:

$$(\delta) \qquad \left(\frac{t+\psi}{b}\right) = 1, \quad \left(\frac{t-\psi}{b}\right) = 1.$$

En examinant d'une manière semblable le cas de φ divisible par b, on trouvera que, dans ce cas, l'un des nombres $t+\psi$ et $t-\psi$ est divisible par b, et que l'autre est, comme dans le cas dont nous venons de nous occuper, résidu quadratique par rapport à b, de sorte qu'en désignant par $t\pm\psi$ celui de ces nombres qui est divisible par b, on a:

$$(\delta') \qquad t\pm\psi \equiv 0 \pmod{b}, \quad \left(\frac{t\mp\psi}{b}\right) = 1.$$

Il résulte du théorème énoncé à la fin du paragraphe précédent que, pour décider si $-b$ est ou n'est pas résidu biquadratique par rapport à p, tout se réduit à la question de savoir si t est ou n'est pas résidu quadratique par rapport à b. Nous pouvons maintenant faire voir, au moyen des résultats que nous venons d'obtenir, que cette dernière question peut être décidée sans connaître t, c'est-à-dire sans qu'il soit nécessaire de mettre p sous la forme t^2-bu^2. Supposons d'abord φ non-divisible par b. Les relations (δ), qui ont lieu dans ce cas, peuvent être présentées de cette manière, en observant que b est un nombre premier $4n+3$:

$$\left(\frac{\psi+t}{b}\right)=1, \quad \left(\frac{\psi-t}{b}\right)=-1.$$

On tire immédiatement de l'équation $p=t^2-bu^2$: $t^2\equiv p \pmod{b}$, résultat qui fait voir qu'en résolvant la congruence $\chi^2\equiv p \pmod{b}$, et désignant par χ l'une de ses racines prise au hasard, on aura $t\equiv\chi$, ou $t\equiv-\chi \pmod{b}$. Dans le premier cas, on a:

$$\left(\frac{t}{b}\right)=\left(\frac{\chi}{b}\right), \quad \left(\frac{\chi+\psi}{b}\right)=1,$$

car il est évident que les expressions $\left(\frac{t}{b}\right)$ et $\left(\frac{t+\psi}{b}\right)$ ne changent pas en mettant à la place de t un autre nombre χ qui ne diffère de t que par un multiple de b. En multipliant les dernières relations entre elles, il viendra:

$$\left(\frac{t}{b}\right)=\left(\frac{\chi(\chi+\psi)}{b}\right).$$

Considérons maintenant l'autre cas dans lequel $t\equiv-\chi \pmod{b}$. On aura alors:

$$\left(\frac{t}{b}\right)=-\left(\frac{\chi}{b}\right), \quad \left(\frac{\psi+\chi}{b}\right)=-1,$$

la dernière de ces relations résultant de la formule $\left(\frac{\psi-t}{b}\right)=-1$, si l'on met à la place de $-t$ le nombre χ qui n'en diffère que par un multiple de b. En multipliant les relations précédentes entre elles, on trouvera, comme plus haut:

$$\left(\frac{t}{b}\right)=\left(\frac{\chi(\chi+\psi)}{b}\right).$$

Nous sommes donc arrivés à ce résultat remarquable: Si φ n'est pas divisible par b, on pourra décider très simplement si l'on a:

$$\left(\frac{t}{b}\right)=1 \quad \text{ou} \quad \left(\frac{t}{b}\right)=-1.$$

Il suffira de chercher un nombre qui satisfasse à la congruence $\chi^2\equiv p \pmod{b}$; ayant trouvé un pareil nombre χ, on aura toujours:

$$\left(\frac{t}{b}\right)=\left(\frac{\chi(\chi+\psi)}{b}\right).$$

Venons maintenant au cas où φ est divisible par b. Les relations (δ') qui ont lieu alors, sont:

$$t\pm\psi\equiv 0 \pmod{b}, \quad \left(\frac{t\mp\psi}{b}\right)=1.$$

On peut dans la dernière de ces relations ajouter à $t\mp\psi$ un multiple quelconque de b. Si l'on y ajoute le nombre $t\pm\psi$ qui, en vertu de la première, est divisible par b, il viendra $\left(\frac{2t}{b}\right)=1$, résultat qui entraîne cet autre: $\left(\frac{t}{b}\right)=\left(\frac{2}{b}\right)$.

En combinant ce résultat avec un théorème connu, on verra que, dans le cas de φ divisible par b, on a $\left(\frac{t}{b}\right)=1$ ou $\left(\frac{t}{b}\right)=-1$, selon que t est de la forme $8n+7$ ou de celle-ci: $8n+3$.

En comparant ce qui vient d'être prouvé au théorème établi à la fin du dernier paragraphe, on verra qu'on peut décider, indépendamment de la connaissance du nombre t, si $-b$ est ou n'est pas résidu biquadratique par rapport à p. Le résultat auquel on parvient ainsi ne contenant plus aucune trace du nombre t, on est porté à croire qu'il ne suppose pas la possibilité de l'équation $t^2-bu^2=p$, d'où le nombre t tire son origine, et qu'il est généralement vrai pour toutes les valeurs de b et p, telles que $\left(\frac{b}{p}\right)=1$. C'est en effet ce qui a lieu, comme on peut le prouver, en examinant, au lieu de l'équation $t^2-bu^2=p$, l'équation plus générale $t^2\pm Mu^2=p$, où M désigne le produit d'un nombre quelconque de nombres premiers différents, et en combinant ensuite les résultats de cet examen avec le théorème suivant, de la vérité duquel on ne saurait douter, mais dont la démonstration rigoureuse ne laisse pas que de présenter des difficultés:

„c désignant un nombre premier quelconque et p un nombre premier $4n+1$, tel que $\left(\frac{c}{p}\right)=1$, on pourra toujours déterminer un nombre δ, composé de facteurs simples tous moindres que c et tel que l'équation $t^2\pm c\delta u^2=p$, soit résoluble."

Quoi qu'il en soit, on peut remarquer que le théorème que nous allons énoncer est rigoureusement prouvé, par ce qui précède, pour toutes les valeurs

de b, telles que la formule t^2-bu^2 n'ait que le seul diviseur quadratique $\pm(t^2-bu^2)$. En jetant les yeux sur la première des tables ajoutées à la *Théorie des Nombres*, on voit que tous les nombres premiers $4n+3$, moindres que 136 (limite de la table) se trouvent dans ce cas, en exceptant le seul nombre 79. Il serait facile, en suivant la marche que nous venons d'indiquer, de prouver la vérité du théorème pour cette valeur ou pour toute autre valeur particulière de b, quel que soit p; mais pour l'établir dans toute sa généralité, il faut d'abord prouver, comme nous l'avons déjà dit, qu'on peut toujours satisfaire à la condition que nous avons énoncée, il n'y a qu'un instant.

Théorème I.

„b désignant un nombre premier $4n+3$, et p un nombre premier $4n+1$ tel que $\left(\frac{b}{p}\right)=1$, si l'on fait $p=\varphi^2+\psi^2$ (où ψ est supposé pair) on aura cette règle pour décider si $-b$ est ou n'est pas résidu biquadratique par rapport à p: Si φ est divisible par b, $-b$ sera ou ne sera pas résidu biquadratique, selon que b est de la forme $8n+7$ ou de celle-ci: $8n+3$. Si φ n'est pas divisible par b, on cherchera un nombre χ tel qu'on ait $\chi^2\equiv p \pmod{b}$. Cela posé, $-b$ sera ou ne sera pas résidu biquadratique par rapport à p, selon que l'on a $\left(\frac{\chi(\chi+\psi)}{b}\right)=1$ ou $\left(\frac{\chi(\chi+\psi)}{b}\right)=-1$.“

En faisant successivement $b=3$, $b=7$ etc., on obtiendra les théorèmes particuliers suivants qui sont analogues au second des théorèmes de M. Gauss et que l'on doit regarder comme rigoureusement prouvés par les considérations que nous avons exposées dans ce paragraphe et dans le précédent.

„p désignant un nombre premier $12n+1$, si l'on fait $p=\varphi^2+\psi^2$ (où ψ est supposé pair) l'un des nombres φ et ψ sera nécessairement divisible par 3. Cela posé, je dis que -3 sera ou ne sera pas résidu biquadratique par rapport à p, selon que c'est ψ ou φ qui est divisible par 3.“

„p désignant un nombre premier de l'une de ces formes: $28n+1$, $28n+9$, $28n+25$, si l'on fait $p=\varphi^2+\psi^2$, je dis que -7 sera résidu biquadratique par rapport à p, si l'un des nombres φ et ψ est divisible par 7, et que -7 sera non-résidu biquadratique par rapport à p, si ni l'un ni l'autre de ces nombres n'est divisible par 7.“

etc.

5.

Désignons par a un nombre premier $4n+1$, et par p un nombre premier également $4n+1$, et de plus susceptible d'être mis sous la forme t^2-au^2. Nous pouvons donc faire $p=t^2-au^2$ où le nombre t, comme il est facile de le voir, est nécessairement impair. On trouvera, comme dans le paragraphe 3, que, si l'on désigne par 2^r la puissance la plus élevée de 2 qui divise u, on a $\left(\frac{u}{p}\right)=\left(\frac{2^r}{p}\right)$, relation que l'on changera ensuite, comme a l'endroit cité, en celle-ci: $\left(\frac{u}{p}\right)=(-1)^{\frac{p-1}{4}}$.

Décomposons actuellement le nombre impair t en ses facteurs simples, en posant $t=gg'g''\ldots\times hh'h''\ldots$, où les nombres premiers g, g', g'', etc., h, h', h'', etc. sont tels que:

$$(s)\qquad \begin{cases} \left(\frac{-a}{g}\right)=1, & \left(\frac{-a}{g'}\right)=1, & \left(\frac{-a}{g''}\right)=1, \text{ etc.} \\ \left(\frac{-a}{h}\right)=-1, & \left(\frac{-a}{h'}\right)=-1, & \left(\frac{-a}{h''}\right)=-1, \text{ etc.} \end{cases}$$

L'équation $t^2-au^2=p$ donne immédiatement:

$$\left(\frac{-ap}{g}\right)=1, \quad \left(\frac{-ap}{g'}\right)=1, \quad \left(\frac{-ap}{g''}\right)=1, \text{ etc.}$$
$$\left(\frac{-ap}{h}\right)=1, \quad \left(\frac{-ap}{h'}\right)=1, \quad \left(\frac{-ap}{h''}\right)=1, \text{ etc.}$$

Comparant ces relations aux précédentes il viendra:

$$\left(\frac{p}{g}\right)=1, \quad \left(\frac{p}{g'}\right)=1, \quad \left(\frac{p}{g''}\right)=1, \text{ etc.}$$
$$\left(\frac{p}{h}\right)=-1, \quad \left(\frac{p}{h'}\right)=-1, \quad \left(\frac{p}{h''}\right)=-1, \text{ etc.}$$

L'application de la loi de réciprocité donnera ensuite, p étant de la forme $4n+1$:

$$\left(\frac{g}{p}\right)=1, \quad \left(\frac{g'}{p}\right)=1, \quad \left(\frac{g''}{p}\right)=1, \text{ etc.}$$
$$\left(\frac{h}{p}\right)=-1, \quad \left(\frac{h'}{p}\right)=-1, \quad \left(\frac{h''}{p}\right)=-1, \text{ etc.}$$

d'où l'on conclut en multipliant:

$$\left(\frac{gg'g''\ldots\times hh'h''\ldots}{p}\right)=\left(\frac{t}{p}\right)=\pm 1,$$

le signe supérieur ou inférieur ayant lieu selon que les nombres premiers h,

h', h'', ... sont en nombre pair ou impair. On peut énoncer ce résultat d'une manière un peu différente, en disant que $\left(\frac{t}{p}\right)$ est égal au produit des seconds membres des relations (ε).

On peut, dans les relations (ε), changer partout $-a$ en a, pourvu qu'en même temps on change le signe des seconds membres de celles de ces relations où il se trouve un nombre premier g, g', g'', ..., h, h', h'', ... de la forme $4n+3$. On aura ainsi:

$$(\zeta)\qquad \begin{cases} \left(\frac{a}{g}\right)=\pm 1, \quad \left(\frac{a}{g'}\right)=\pm 1, \quad \left(\frac{a}{g''}\right)=\pm 1, \quad \text{etc.} \\ \left(\frac{a}{h}\right)=\pm 1, \quad \left(\frac{a}{h'}\right)=\pm 1, \quad \left(\frac{a}{h''}\right)=\pm 1, \quad \text{etc.} \end{cases}$$

En comparant le second membre de chacune de ces relations avec le second membre de la relation correspondante du tableau (ε), on trouvera autant de changements de signe qu'il y a de nombres premiers $4n+3$ parmi les nombres g, g', g'', ..., h, h', h'', ...

Le nombre des changements sera donc pair, lorsque parmi les nombres g, g', g'', ..., h, h', h'', ... il s'en trouve un nombre pair de la forme $4n+3$. Dans ce cas qui aura lieu toutes les fois que $t=gg'g''\ldots\times hh'h''\ldots$ est de la forme $4n+1$, le produit des seconds membres des relations (ζ) sera donc le même que le produit des seconds membres des relations (ε).

D'un autre côté, on peut, en vertu de la loi de réciprocité, renverser les premiers membres des relations (ζ), sans qu'il soit nécessaire de changer le signe d'aucun des seconds membres de ces relations. Le produit de toutes les expressions renversées, c'est-à-dire $\left(\frac{gg'g''\ldots\times hh'h''\ldots}{a}\right)$ ou $\left(\frac{t}{a}\right)$, est donc égal au produit des seconds membres des relations (ζ) et par conséquent aussi, d'après ce qu'on a vu précédemment, égal au produit des seconds membres des relations (ε). Or, ayant prouvé plus haut que ce dernier produit est égal à $\left(\frac{t}{p}\right)$, on a:

$$\left(\frac{t}{p}\right)=\left(\frac{t}{a}\right).$$

Ce résultat est relatif au cas où t est de la forme $4n+1$; si l'on examine d'une manière semblable le cas de $t=4n+3$, on trouvera qu'on a alors:

$$\left(\frac{t}{p}\right)=-\left(\frac{t}{a}\right).$$

Ces deux cas sont compris dans la formule suivante à laquelle nous réunissons un résultat obtenu plus haut:

$$(\eta)\qquad \left(\frac{t}{p}\right)=(-1)^{\frac{t-1}{2}}\left(\frac{t}{a}\right), \quad \left(\frac{u}{p}\right)=(-1)^{\frac{p-1}{4}}.$$

L'équation $t^2-au^2=p$ donne successivement:

$$t^2\equiv au^2, \quad t^{\frac{p-1}{2}}\equiv a^{\frac{p-1}{4}}u^{\frac{p-1}{2}} \pmod{p},$$

d'où l'on voit que a sera ou ne sera pas résidu biquadratique relativement à p, selon que l'on a $\left(\frac{t}{p}\right)=\left(\frac{u}{p}\right)$ ou $\left(\frac{t}{p}\right)=-\left(\frac{u}{p}\right)$. En mettant à la place de $\left(\frac{t}{p}\right)$ et $\left(\frac{u}{p}\right)$ les valeurs données par les expressions (η), on pourra remplacer les conditions précédentes par celles qui suivent:

(θ) a sera ou ne sera pas résidu biquadratique par rapport à p, selon que l'on a:

$$\left(\frac{t}{a}\right)=(-1)^{\frac{t-1}{2}+\frac{p-1}{4}} \quad \text{ou} \quad \left(\frac{t}{a}\right)=-(-1)^{\frac{t-1}{2}+\frac{p-1}{4}},$$

résultat que nous ne nous arrêterons pas à démontrer.

Posons maintenant $p=\varphi^2+\psi^2$ (où ψ est supposé pair) et égalons cette valeur de p à celle que nous avons considérée précédemment. Nous aurons ainsi $p=t^2-au^2=\varphi^2+\psi^2$ d'où l'on conclut en transposant:

$$t^2-\psi^2=(t+\psi)(t-\psi)=\varphi^2+au^2.$$

Il y a maintenant deux cas à distinguer, selon que φ est ou n'est pas divisible par a. Commençons par celui où φ n'est pas divisible par a. Soit m le plus grand commun diviseur de φ et de u, qui sera nécessairement impair et non divisible par a, et faisons $\varphi=m\varphi'$, $u=mu'$, valeurs dont la substitution dans l'équation obtenue plus haut la change en celle-ci:

$$(t+\psi)(t-\psi)=m^2(\varphi'^2+au'^2).$$

Cette équation fait voir que $t+\psi$ est composé de deux facteurs dont l'un divise m^2, l'autre $\varphi'^2+au'^2$, et qu'il en est de même de $t-\psi$. Si nous désignons les facteurs de $t+\psi$ par E et K et ceux de $t-\psi$ par F et L, nous aurons:

$$t+\psi=EK, \qquad t-\psi=FL,$$
$$m^2=EF, \quad \varphi'^2+au'^2=KL.$$

On s'assurera, comme dans le paragraphe 4, que les nombres E et F sont premiers entre eux. Il suit de là et de l'équation $m^2=EF$ que chacun de ces nombres est un carré, de sorte que:

$$\left(\frac{E}{a}\right)=1, \quad \left(\frac{F}{a}\right)=1.$$

La différence des nombres impairs $t+\psi$ et $t-\psi$ étant 2ψ et par conséquent divisible par 4, on voit que ces deux nombres sont ou l'un et l'autre de la forme $4n+1$, ou l'un et l'autre de la forme $4n+3$. Comme, d'un autre côté, les nombres E et F sont l'un et l'autre de la forme $4n+1$ (ces nombres étant des carrés impairs), il suit des équations $t+\psi = EK$, $t-\psi = FL$, que les nombres K et L sont ou l'un et l'autre de la forme $4n+1$ ou l'un et l'autre de la forme $4n+3$ et que le premier ou le second de ces cas a lieu, selon que les nombres $t+\psi$ et $t-\psi$ sont l'un et l'autre de la forme $4n+1$, ou l'un et l'autre de la forme $4n+3$. Distinguons maintenant deux cas, selon que p est de la forme $8n+1$ ou de celle-ci: $8n+5$. On voit, par l'équation $p^2 = \varphi^2+\psi^2$, que, dans le premier cas, ψ est divisible par 4, d'où il suit que $t+\psi$ et $t-\psi$ sont alors l'un et l'autre de la forme $4n+1$ ou l'un et l'autre de la forme $4n+3$, selon que t est de la forme $4n+1$, ou de celle-ci: $4n+3$. Le contraire a lieu dans le cas de $p = 8n+5$ et les résultats relatifs à ces deux cas peuvent être compris dans cet énoncé:

Les nombres $t+\psi$ et $t-\psi$, et par conséquent aussi les nombres K et L, sont l'un et l'autre de la forme $4n+1$ ou de celle-ci: $4n+3$, selon que $(-1)^{\frac{p-1}{4}+\frac{t-1}{2}}$ est égal à 1 ou à -1.

Il résulte de l'équation $\varphi'^2+au'^2 = KL$ que les nombres K et L sont diviseurs de la formule $\varphi'^2+au'^2$ (où φ' et au' sont premiers entre eux et où a désigne un nombre premier $4n+1$). Or, on sait que, si R désigne un diviseur impair d'une telle formule, on a:

$$\left(\frac{R}{a}\right) = 1, \quad \text{ou} \quad \left(\frac{R}{a}\right) = -1,$$

selon que R est de la forme $4n+1$ ou de la forme $4n+3$. (*Théorie des Nombres*, no. 196.)

Appliquant ce théorème aux nombres K et L, il viendra:

$$\left(\frac{K}{a}\right) = \left(\frac{L}{a}\right) = (-1)^{\frac{p-1}{4}\cdot\frac{t-1}{2}},$$

d'où l'on conclura ensuite, en multipliant par les expressions $\left(\frac{E}{a}\right) = 1, \left(\frac{F}{a}\right) = 1$, trouvées plus haut:

$$\left(\frac{t+\psi}{a}\right) = \left(\frac{t-\psi}{a}\right) = (-1)^{\frac{p-1}{4}+\frac{t-1}{2}},$$

ou, ce qui revient au même, a étant un nombre premier $4n+1$:

$$\left(\frac{\psi+t}{a}\right) = \left(\frac{\psi-t}{a}\right) = (-1)^{\frac{p-1}{4}+\frac{t-1}{2}}.$$

Si l'on compare ce qui vient d'être prouvé au résultat (θ), obtenu plus haut, on verra que a est ou n'est pas résidu biquadratique relativement à p, selon que l'on a:

$$\left(\frac{\psi+t}{a}\right) = \left(\frac{\psi-t}{a}\right) = \left(\frac{t}{a}\right),$$

ou:

$$\left(\frac{\psi+t}{a}\right) = \left(\frac{\psi-t}{a}\right) = -\left(\frac{t}{a}\right).$$

L'équation $p = t^2-au^2$ fait voir que, si l'on désigne par χ l'une quelconque des deux racines de la congruence $\chi^2 \equiv p \pmod{a}$, on a $t \equiv \chi$ ou $t \equiv -\chi \pmod{a}$. Il suit de là, a étant de la forme $4n+1$, $\left(\frac{t}{a}\right) = \left(\frac{\chi}{a}\right)$. D'un autre côté, comme en vertu de ce qui précède $\left(\frac{\psi+t}{a}\right) = \left(\frac{\psi-t}{a}\right)$, on voit qu'on a toujours:

$$\left(\frac{\psi+\chi}{a}\right) = \left(\frac{\psi+t}{a}\right) = \left(\frac{\psi-t}{a}\right).$$

On conclut de là, en ayant égard à ce qui a été dit il n'y a qu'un instant, que le nombre a sera résidu biquadratique par rapport à p, lorsqu'on a $\left(\frac{\chi+\psi}{a}\right) = \left(\frac{\chi}{a}\right)$ ou, ce qui est la même chose, lorsque $\left(\frac{\chi(\chi+\psi)}{a}\right) = 1$, et que a sera non-résidu biquadratique relativement à p, lorsqu'on a $\left(\frac{\chi+\psi}{a}\right) = -\left(\frac{\chi}{a}\right)$, ou, ce qui revient au même, lorsque $\left(\frac{\chi(\chi+\psi)}{a}\right) = -1$.

Ce résultat est relatif au cas où φ n'est pas divisible par a. Reste à examiner le cas de φ divisible par a. En traitant ce cas d'une manière semblable, on trouve que, lorsqu'il a lieu, l'un des nombres $t+\psi$, $t-\psi$ (nous le désignerons par $t\pm\psi$) est divisible par a et que, comme dans le premier cas, l'autre $t\mp\psi$ est tel que:

$$\left(\frac{t\mp\psi}{a}\right) = (-1)^{\frac{p-1}{4}+\frac{t-1}{2}},$$

ou, ce qui revient au même, en ajoutant à $t\mp\psi$ le nombre $t\pm\psi$, multiple de a:

$$\left(\frac{2t}{a}\right) = (-1)^{\frac{p-1}{4}+\frac{t-1}{2}}.$$

En comparant ceci à ce qui a été prouvé plus haut (θ), on trouvera que, dans le cas de φ divisible par a, a est ou n'est pas résidu biquadratique relativement à p, selon que l'on a $\left(\frac{2}{a}\right) = 1$, ou $\left(\frac{2}{a}\right) = -1$, ou, ce qui est la

même chose, d'après un théorème connu, selon que a est de la forme $8n+1$ ou de la forme $8n+5$.

Il en est des résultats que nous venons d'obtenir comme de ceux que nous avons établis dans le paragraphe 4; ils ont encore lieu quand même p ne pourrait être mis sous la forme t^2-au^2, et supposent uniquement que les nombres premiers $a=4n+1$, et $p=4n+1$, soient tels que $\left(\frac{a}{p}\right)=1$. Pour les démontrer dans cette extension, il suffira de suivre la marche qui a été indiquée vers la fin du paragraphe 4, et de s'appuyer sur la proposition auxiliaire, dont il y est question et à l'énoncé de laquelle on a donné la généralité nécessaire pour qu'elle puisse servir de base, en même temps, à la démonstration du théorème général à la fin du paragraphe 4 et à celle du théorème que nous allons énoncer. Ces deux théorèmes n'en forment proprement qu'un, et en procédant, comme on l'a dit à l'endroit cité, c'est-à-dire en appliquant à l'équation $t^2 \pm Mu^2 = p$, où M désigne le produit d'un nombre quelconque de nombres premiers différents, des considérations analogues à celles qu'on a employées dans ce paragraphe et dans les précédents, on démontrera simultanément ces deux théorèmes, ou plutôt on arrivera à un théorème dans l'énoncé duquel ils se trouvent réunis.

Théorème II.

„a désignant un nombre premier $4n+1$, et p un autre nombre premier $4n+1$, tel que $\left(\frac{a}{p}\right)=1$, si l'on fait $p=\varphi^2+\psi^2$ (où ψ est supposé pair), on pourra décider de la manière suivante, si a est ou n'est pas résidu biquadratique par rapport à p. Si φ est divisible par a, a sera ou ne sera pas résidu biquadratique relativement à p, selon que a est de la forme $8n+1$ ou de celle-ci: $8n+5$. Si φ n'est pas divisible par a, on cherchera un nombre χ tel qu'on ait $\chi^2 \equiv p \pmod{a}$. Cela posé, a sera ou ne sera pas résidu biquadratique par rapport à p, selon que l'on a $\left(\frac{\chi(\chi+\psi)}{a}\right)=1$ ou $\left(\frac{\chi(\chi+\psi)}{a}\right)=-1$.“

En faisant successivement $a=5$, $a=13$, on aura les théorèmes particuliers suivants qu'on doit regarder comme rigoureusement prouvés par ce qui précède, la formule t^2-au^2 n'ayant, pour ces valeurs de a, d'autre diviseur quadratique que celui-ci: t^2-au^2, ou en d'autres termes, tout diviseur de t^2-au^2 étant lui-même de la forme t^2-au^2.

„p désignant un nombre premier de l'une des formes $20n+1$, $20n+9$, si l'on fait $p=\varphi^2+\psi^2$ (où ψ est supposé pair) on s'assure facilement que l'un des nombres φ, ψ est multiple de 5. Cela posé, je dis que 5 sera ou ne sera pas résidu biquadratique relativement à p, selon que c'est ψ ou φ qui est divisible par 5.“

etc.

En indiquant plus haut une méthode qui pourrait servir à établir dans toute leur généralité les théorèmes I et II, nous avons dit qu'en suivant cette méthode on se trouvait dans la nécessité de s'appuyer sur une proposition subsidiaire qu'il paraît assez difficile de démontrer en toute rigueur. En réfléchissant à cet inconvénient, j'ai reconnu qu'il était très facile d'y remédier en modifiant un peu la marche tracée plus haut. Cette modification est extrêmement légère et consiste en ce qu'au lieu de considérer les équations $t^2-bu^2=p$, $t^2-au^2=p$, qui peuvent n'être pas possibles quoiqu'on ait $\left(\frac{b}{p}\right)=1$, $\left(\frac{a}{p}\right)=1$, il faut appliquer des considérations du genre des précédentes aux équations plus générales $t^2-bu^2=ps^2$, $t^2-au^2=ps^2$ (on remplace avec avantage la dernière par celle-ci: $t^2+au^2=ps$, qui peut être traitée plus simplement), auxquelles on peut toujours satisfaire, lorsque les conditions $\left(\frac{b}{p}\right)=1, \left(\frac{a}{p}\right)=1$ ont lieu, comme il résulte du beau théorème que M. Legendre a donné pour juger de la possibilité ou de l'impossibilité de l'équation $ax^2+\beta y^2=\gamma z^2$ (*Théorie des Nombres*, no. 27).

La démonstration ainsi modifiée, outre qu'elle est entièrement rigoureuse, a encore l'avantage d'une plus grande simplicité, comme tout lecteur qui a bien saisi l'esprit des considérations précédentes pourra en juger, en développant cette démonstration d'après l'indication qu'on vient d'en donner.

Addition au mémoire précédent.

Quoique l'indication que nous avons donnée à la fin du mémoire précédent sur la marche à suivre pour établir d'une manière entièrement rigoureuse les théorèmes I et II de notre mémoire, puisse suffire à tout lecteur familiarisé avec l'analyse indéterminée, nous croyons ne pas faire une chose inutile, en développant avec détail, dans cette addition, les démonstrations des théorèmes dont il s'agit, ces démonstrations étant susceptibles d'être beaucoup

simplifiées au moyen de quelques considérations qui peuvent ne pas se présenter de suite à l'esprit. Nous commençons par la démonstration du premier des théorèmes cités.

Désignons par p un nombre premier $4n+1$, par b un nombre premier $4n+3$, tel que $\left(\frac{b}{p}\right)=1$, et considérons l'équation:

$$(\alpha') \qquad t^2-bu^2=ps^2.$$

D'après le théorème déjà cité (*Théorie des Nombres*, no. 27), les conditions nécessaires pour que cette équation soit possible sont celles-ci: $\left(\frac{b}{p}\right)=1$ et $\left(\frac{p}{b}\right)=1$. Or, de ces conditions la première a lieu par hypothèse et quant à la seconde, il suit du théorème connu sous le nom de loi de réciprocité, qu'elle a toujours lieu lorsque la première est satisfaite. L'équation est donc résoluble. Il est évident qu'on peut supposer que les nombres t, u, s, qui y satisfont, sont premiers entre eux, comparés deux à deux. L'équation étant dans cet état, ces trois nombres seront l'un pair, les deux autres impairs, et on s'assure facilement que s ne saurait être pair. Le nombre s étant impair, les nombres t, u seront l'un pair, l'autre impair et il y aurait deux cas à examiner selon que t est pair ou impair. Mais quoique ces deux cas soient susceptibles d'être traités par la même analyse, il est plus simple de n'en considérer qu'un seul, celui de t impair par exemple, et de montrer que l'autre peut y être facilement ramené. Faisons donc voir qu'il est toujours permis de supposer t impair dans l'équation $t^2-bu^2=ps^2$. Si t était pair dans l'équation (α'), on déduirait des nombres t, u, par le moyen indiqué dans la note relative au commencement du paragraphe 3 du mémoire précédent, d'autres nombres t' (impair), u' (pair) tels que $t'^2-bu'^2=ps^2$. Nous pourrons donc considérer t comme impair dans tout ce qui va suivre.

Décomposons les nombres t et u en leurs facteurs simples, en faisant:

$$t=ll'l''\ldots, \quad u=2^\nu kk'k''\ldots,$$

l, l', l'', ... et k, k', k'', ... désignant des nombres premiers impairs. La seule inspection de l'équation (α') donne:

$$\left(\frac{p}{k}\right)=1, \quad \left(\frac{p}{k'}\right)=1, \quad \left(\frac{p}{k''}\right)=1, \quad \ldots.$$

On aura ensuite, en appliquant la loi de réciprocité, p étant un nombre premier $4n+1$:

$$\left(\frac{k}{p}\right)=1, \quad \left(\frac{k'}{p}\right)=1, \quad \left(\frac{k''}{p}\right)=1, \quad \ldots.$$

Faisant le produit de toutes ces expressions et de la formule identique $\left(\frac{2^\nu}{p}\right)=\left(\frac{2}{p}\right)^\nu$, il viendra:

$$\left(\frac{2^\nu kk'k''\ldots}{p}\right)=\left(\frac{u}{p}\right)=\left(\frac{2}{p}\right)^\nu.$$

Le nombre p est de l'une des deux formes $8n+1$, $8n+5$. Si p est de la première forme, on a, en vertu d'un théorème connu, $\left(\frac{2}{p}\right)=1$, et par conséquent aussi $\left(\frac{2^\nu}{p}\right)=1$. Donc $\left(\frac{u}{p}\right)=1$. Si p est de la forme $8n+5$, le nombre u sera impairement pair, de sorte que $\nu=1$, et comme on a, d'un autre côté, pour les nombres premiers $p=8n+5$, $\left(\frac{2}{p}\right)=-1$, il viendra $\left(\frac{u}{p}\right)=-1$. Les deux cas dont il vient d'être question sont compris dans la formule:

$$(\beta') \qquad \left(\frac{u}{p}\right)=(-1)^{\frac{p-1}{4}}.$$

Reprenons l'équation (α') de laquelle nous tirons immédiatement:

$$\left(\frac{-b}{l}\right)=\left(\frac{p}{l}\right), \quad \left(\frac{-b}{l'}\right)=\left(\frac{p}{l'}\right), \quad \left(\frac{-b}{l''}\right)=\left(\frac{p}{l''}\right), \quad \ldots.$$

Comme p est un nombre premier $4n+1$, et b un nombre premier $4n+3$, on trouvera en appliquant la loi de réciprocité:

$$\left(\frac{l}{b}\right)=\left(\frac{l}{p}\right), \quad \left(\frac{l'}{b}\right)=\left(\frac{l'}{p}\right), \quad \left(\frac{l''}{b}\right)=\left(\frac{l''}{p}\right), \quad \ldots.$$

La multiplication donnera ensuite:

$$\left(\frac{ll'l''\ldots}{b}\right)=\left(\frac{ll'l''\ldots}{p}\right),$$

ou, ce qui revient au même:

$$(\gamma') \qquad \left(\frac{t}{b}\right)=\left(\frac{t}{p}\right).$$

En mettant l'équation (α') sous la forme d'une congruence, on aura:

$$t^2 \equiv bu^2 \pmod{p}.$$

On conclut de là, en élevant les deux membres à la puissance $\frac{p-1}{4}$:

$$t^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{4}} u^{\frac{p-1}{2}} \pmod{p},$$

ou, ce qui revient au même, en remplaçant $u^{\frac{p-1}{2}}$ par sa valeur $(-1)^{\frac{p-1}{4}}$ donnée par la formule (β'):

$$t^{\frac{p-1}{2}} \equiv (-b)^{\frac{p-1}{4}} \pmod{p}.$$

Cette dernière congruence fait voir que $-b$ est ou n'est pas résidu biquadratique relativement à p, selon que l'on a $\left(\frac{t}{p}\right)=1$, ou $\left(\frac{t}{p}\right)=-1$. Si l'on compare ce résultat à la formule (γ'), on obtiendra cet énoncé:

(δ') $-b$ est ou n'est pas résidu biquadratique par rapport à p, selon que l'on a $\left(\frac{t}{b}\right)=1$ ou $\left(\frac{t}{b}\right)=-1$.

Décomposons actuellement le nombre premier p en deux carrés, en posant $p=\varphi^2+\psi^2$ (où ψ est supposé pair) et mettons cette valeur de p dans l'équation (α'). Il viendra ainsi:

$$t^2-bu^2=s^2\varphi^2+s^2\psi^2,$$

et l'on aura ensuite en transposant:

$$t^2-\psi^2s^2=(t+\psi s)(t-\psi s)=s^2\varphi^2+bu^2.$$

Les nombres s, t, u étant deux à deux premiers entre eux, on voit par l'équation (α') que s ne saurait être divisible par b. Nous distinguerons maintenant deux cas selon que φ est ou n'est pas divisible par b, et nous examinerons d'abord le dernier de ces deux cas. Si nous désignons par m le plus grand diviseur commun de φ et u, m sera impair et non-divisible par b comme φ. Posons $\varphi=m\varphi'$, $u=mu'$ et substituons ces valeurs dans la dernière équation. Il viendra ainsi:

$$(t+\psi s)(t-\psi s)=m^2(s^2\varphi'^2+bu'^2).$$

Comme $s\varphi'$ et bu' sont premiers entre eux, d'après ce qui précède, il suit d'un théorème connu, conséquence très simple de la loi de réciprocité (*Théorie des Nombres* no. 197), que tout diviseur R du facteur binôme du second membre qui est évidemment impair, est tel que $\left(\frac{R}{b}\right)=1$.

La dernière équation fait voir que chacun des nombres $t+\psi s$, $t-\psi s$ est composé de deux facteurs, l'un diviseur de m^2, l'autre diviseur de $s^2\varphi'^2+bu'^2$. Si nous désignons ces 4 facteurs par E, F, K et L, nous aurons les équations:

$$t+\psi s=EK, \quad m^2=EF,$$
$$t-\psi s=FL, \quad \varphi^2s'^2+bu'^2=KL.$$

Il est facile de s'assurer que les nombres E et F, qui sont impairs l'un et l'autre, comme diviseurs de m^2, sont premiers entre eux. En effet, si ces nombres étaient divisibles l'un et l'autre par un même nombre premier ϑ, ϑ diviserait chacun des nombres $t+\psi s$, $t-\psi s$ et par conséquent aussi leur demi-somme et leur demi-différence, c'est-à-dire les nombres t et ψs. D'un autre

côté, comme ϑ divise m^2, il divisera aussi le nombre φ, φ étant égal à $m\varphi'$; il suit de là et de ce que $\varphi^2+\psi^2$ est égal au nombre premier p, que ψ n'est pas divisible par b. Il faudrait donc, d'après ce qui précède, que ϑ fût diviseur commun de t et s, ce qui est impossible, ces nombres étant premiers entre eux. Donc les nombres E et F sont premiers entre eux, et comme leur produit est un carré, chacun d'eux sera pareillement un carré. On a donc:

$$\left(\frac{E}{b}\right)=1, \quad \left(\frac{F}{b}\right)=1.$$

On a aussi:

$$\left(\frac{K}{b}\right)=1, \quad \left(\frac{L}{b}\right)=1,$$

K et L étant des diviseurs de $s^2\varphi'^2+bu'^2$. On conclut de là, en multipliant:

$$\left(\frac{EK}{b}\right)=1, \quad \left(\frac{FL}{b}\right)=1,$$

ou, ce qui est la même chose:

$$\left(\frac{t+\psi s}{b}\right)=1, \quad \left(\frac{t-\psi s}{b}\right)=1.$$

Si l'on fait attention que b est un nombre premier $4n+3$, on pourra présenter de cette autre manière la dernière de ces relations:

$$\left(\frac{\psi s-t}{b}\right)=-1.$$

Cela étant, on voit qu'on peut les comprendre l'une et l'autre dans cette formule:

(ε') $$\left(\frac{\psi s\pm t}{b}\right)=\pm 1,$$

où les signes sont à volonté, mais les mêmes dans les deux membres.

Comme on a $\left(\frac{p}{b}\right)=1$, la congruence $\chi^2\equiv p \pmod{b}$ est possible et a, comme l'on sait, deux racines entre les limites $-\frac{1}{2}b$ et $\frac{1}{2}b$. Désignons par χ l'une de ces racines prise au hasard. L'équation (α') donne cette congruence: $t^2\equiv ps^2 \pmod{b}$. Si l'on compare celle-ci à la précédente, on aura $t^2\equiv\chi^2s^2 \pmod{b}$. On conclut de là $\pm t\equiv\chi s \pmod{b}$, le signe étant tantôt positif, tantôt negatif et dépendant du choix que l'on aura fait entre les deux racines de la congruence $\chi^2\equiv p \pmod{b}$. Les signes étant à volonté dans la formule (ε'), on peut supposer qu'ils y sont les mêmes que dans celle-ci: $\pm t\equiv\chi s \pmod{b}$. Remplaçant $\pm t$ par le nombre χs qui ne diffère de $\pm t$ que par un multiple de b, il viendra:

$$\left(\frac{\psi s+\chi s}{b}\right)=\pm 1.$$

D'un autre côté, si l'on se rappelle que b est de la forme $4n+3$, on tirera de la formule $\pm t \equiv \chi s \pmod{b}$: $\pm\left(\frac{t}{b}\right) = \left(\frac{\chi s}{b}\right)$. Si l'on multiplie cette égalité par la précédente, on aura, les signes étant les mêmes dans ces deux formules:

$$\left(\frac{\chi(\chi+\psi)}{b}\right)\left(\frac{s^2}{b}\right) = \left(\frac{t}{b}\right)$$

ou, ce qui revient au même:

$$\left(\frac{\chi(\chi+\psi)}{b}\right) = \left(\frac{t}{b}\right).$$

Si l'on compare cette formule avec ce qui a été prouvé plus haut (δ'), on obtiendra ce résultat:

(ζ') $-b$ est ou n'est pas résidu biquadratique par rapport à p, selon que l'on a $\left(\frac{\chi(\chi+\psi)}{b}\right) = 1$ ou $\left(\frac{\chi(\chi+\psi)}{b}\right) = -1$.

Cette proposition est relative au cas où φ n'est pas divisible par b. Examinons maintenant le cas de φ divisible par b. Soient b^{1+k} et b^k respectivement les puissances les plus élevées de b qui divisent φ et u (k et h pouvant être nuls), soit de plus m le plus grand commun diviseur de $\frac{\varphi}{b^{1+k}}$ et $\frac{u}{b^k}$. Si nous faisons $\varphi = b^{1+k}m\varphi'$, $u = b^k m u'$, les nombres φ' et u', dont le premier est impair, le second pair, seront premiers entre eux, et non-divisibles par b, et m sera impair et non-divisible par b. La substitution des valeurs précédentes donne cette équation:

$$(t+\psi s)(t-\psi s) = m^2[b^{2k+2}(s\varphi')^2 + b^{2h+1}u'^2].$$

Il faut maintenant distinguer deux cas selon que l'on a $k \geqq h$ ou $k < h$. Dans le premier, le facteur binôme du second membre peut être mis sous cette forme:

$$b^{2h+1}[u'^2 + b(b^{k-h}s\varphi')^2],$$

où il faut remarquer que les nombres u' et $b^{k-h}s\varphi'$ sont premiers entre eux. Dans le cas de $k < h$, on mettra le facteur binôme sous la forme suivante:

$$b^{2k+2}[(s\varphi')^2 + b(b^{h-k-1}u')^2],$$

où les nombres $s\varphi'$ et $b^{h-k-1}u'$ sont premiers entre eux. On voit donc que le facteur binôme est toujours le produit d'une puissance de b et d'une expression impaire telle que g^2+bh^2, dans laquelle g et bh sont premiers entre eux. Désignant par b^r la puissance de b dont il s'agit, on pourra donc écrire la dernière équation de cette manière:

$$(t+\psi s)(t-\psi s) = m^2 b^r (g^2+bh^2).$$

Les nombres $t+\psi s$, $t-\psi s$ ne sauraient être divisibles l'un et l'autre par b, puisqu'alors leur demi-somme qui est t, le serait aussi, ce qu'on a vu plus haut être impossible. Si l'on désigne par $t \pm \psi s$ celui de ces deux nombres qui est divisible par b, on aura $t \pm \psi s \equiv 0 \pmod{b}$ et je dis que l'autre $t \mp \psi s$ est tel que $\left(\frac{t \mp \psi s}{b}\right) = 1$. En effet $t \mp \psi s$ est composé de deux facteurs E et K dont le premier E divise m^2, le second g^2+bh^2.

Or, on s'assure, comme dans le cas de φ non-divisible par b, que E est un carré, de sorte qu'on a $\left(\frac{E}{b}\right) = 1$. On a aussi $\left(\frac{K}{b}\right) = 1$, K étant diviseur de g^2+bh^2. On conclut de là en multipliant:

$$\left(\frac{EK}{b}\right) = \left(\frac{t \mp \psi s}{b}\right) = 1.$$

Il est permis d'augmenter $t \mp \psi s$ dans cette formule d'un multiple quelconque de b. Ajoutant le nombre $t \pm \psi s$ qu'on a vu être un tel multiple, il viendra $\left(\frac{2t}{b}\right) = 1$ ou, ce qui revient au même: $\left(\frac{t}{b}\right) = \left(\frac{2}{b}\right)$, résultat dont la comparaison avec un théorème connu fait voir que dans le cas de φ divisible par b, on a $\left(\frac{t}{b}\right) = 1$ ou $\left(\frac{t}{b}\right) = -1$, selon que b est de la forme $8n+7$ ou de celle-ci: $8n+3$. Si l'on combine ceci avec le résultat obtenu plus haut (δ'), on trouve que, lorsque φ est multiple de b:

$-b$ est ou n'est pas résidu biquadratique par rapport à p, selon que b est de la forme $8n+7$ ou de celle-ci: $8n+3$.

En réunissant ce dernier résultat à celui auquel nous sommes parvenu plus haut (ζ'), on aura le théorème I énoncé à la fin du paragraphe 4 du mémoire précédent, théorème qui se trouve ainsi établi d'une manière très simple et entièrement rigoureuse.

Occupons-nous maintenant de la démonstration du théorème II. Désignons, comme dans tout ce qui précède, par a un nombre premier $4n+1$ et par p un autre nombre premier également de la forme $4n+1$ et tel que $\left(\frac{a}{p}\right) = 1$. On conclut de là, en appliquant la loi de réciprocité, qu'on a aussi $\left(\frac{p}{a}\right) = 1$. Ces conditions ayant lieu, il suit du théorème déjà cité plusieurs

fois, que l'équation:

$$(\eta') \qquad t^2+au^2 = ps^2,$$

peut être résolue. Si l'on suppose que les nombres t, u, s, comparés deux à deux, n'ont pas de diviseur commun, s sera impair et les deux autres seront l'un pair, l'autre impair, comme il est très facile de le voir. Il est évident en outre que, si l'équation est dans cet état, u n'est pas divisible par p, s ne l'est pas par a, et t n'est divisible ni par a ni par p.

Décomposons les nombres t et u en leurs facteurs simples, en faisant $u = 2^\nu kk'k''\ldots$, $t = 2^\mu ll'l''\ldots$, $k, k', k''\ldots$ et $l, l', l''\ldots$ désignant des nombres premiers impairs, et l'un des nombres μ, ν étant égal à zéro.

L'équation (η') donne d'abord:

$$\left(\frac{p}{k}\right)=1, \quad \left(\frac{p}{k'}\right)=1, \quad \left(\frac{p}{k''}\right)=1, \quad \ldots$$

d'où l'on conclut ensuite en appliquant la loi de réciprocité:

$$\left(\frac{k}{p}\right)=1, \quad \left(\frac{k'}{p}\right)=1, \quad \left(\frac{k''}{p}\right)=1, \quad \ldots.$$

Faisant le produit des équations précédentes et de l'équation identique $\left(\frac{2^\nu}{p}\right)=\left(\frac{2^\nu}{p}\right)$, il viendra:

$$\left(\frac{2^\nu kk'k''\ldots}{p}\right)=\left(\frac{u}{p}\right)=\left(\frac{2^\nu}{p}\right).$$

Il résulte encore de l'équation (η'), qu'on a:

$$\left(\frac{a}{l}\right)=\left(\frac{p}{l}\right), \quad \left(\frac{a}{l'}\right)=\left(\frac{p}{l'}\right), \quad \left(\frac{a}{l''}\right)=\left(\frac{p}{l''}\right), \quad \ldots.$$

Comme les nombres premiers a et p sont l'un et l'autre de la forme $4n+1$, on conclut de là, en vertu de la loi de réciprocité:

$$\left(\frac{l}{a}\right)=\left(\frac{l}{p}\right), \quad \left(\frac{l'}{a}\right)=\left(\frac{l'}{p}\right), \quad \left(\frac{l''}{a}\right)=\left(\frac{l''}{p}\right), \quad \ldots.$$

Multipliant entre elles toutes ces relations, il viendra l'équation:

$$\left(\frac{ll'l''\ldots}{a}\right)=\left(\frac{ll'l''\ldots}{p}\right),$$

qui, si l'on multiplie ses deux membres par $\left(\frac{2^\mu}{a}\right)\left(\frac{2^\mu}{p}\right)$, se change en celle-ci:

$$\left(\frac{t}{a}\right)\left(\frac{2^\mu}{p}\right)=\left(\frac{t}{p}\right)\left(\frac{2^\mu}{a}\right).$$

Distinguons actuellement deux cas, selon que u est pair ou impair. Si

u est pair, t est impair; on a donc alors $\mu = 0$, et la dernière égalité se réduit à celle-ci:

$$\left(\frac{t}{a}\right)=\left(\frac{t}{p}\right).$$

Quant à la relation $\left(\frac{u}{p}\right)=\left(\frac{2^\nu}{p}\right)$, il est facile de voir qu'elle équivaut, dans ce cas, à celle-ci:

$$\left(\frac{u}{p}\right)=(-1)^{\frac{p-1}{4}}.$$

Pour s'en convaincre, il suffit de remarquer que, si p est de la forme $8n+1$, on a $\left(\frac{2}{p}\right)=1$, et par conséquent aussi $\left(\frac{2^\nu}{p}\right)=1$, et que, si p a la forme $8n+5$, ν est égal à l'unité et qu'on a pour tout nombre premier $p = 8n+5$, $\left(\frac{2}{p}\right)=-1$.

Passons à l'autre cas qui est celui de t pair et u impair. On a alors $\nu = 0$, ce qui réduit l'équation $\left(\frac{u}{p}\right)=\left(\frac{2^\nu}{p}\right)$ à $\left(\frac{u}{p}\right)=1$.

Si les nombres p et a sont l'un et l'autre de la forme $8n+1$, ou l'un et l'autre de la forme $8n+5$, on a $\left(\frac{2}{a}\right)=\left(\frac{2}{p}\right)$ et par conséquent aussi $\left(\frac{2^\mu}{a}\right)=\left(\frac{2^\mu}{p}\right)$, et l'égalité $\left(\frac{t}{p}\right)\left(\frac{2^\mu}{a}\right)=\left(\frac{t}{a}\right)\left(\frac{2^\mu}{p}\right)$ se change en celle-ci: $\left(\frac{t}{p}\right)=\left(\frac{t}{a}\right)$. Si, au contraire, les nombres a, p sont l'un de la forme $8n+1$, l'autre de la forme $8n+5$, on a $\left(\frac{2}{a}\right)=-\left(\frac{2}{p}\right)$. D'un autre côté, l'équation (η') fait voir que, dans ce cas, le nombre t est impairement pair, de sorte que $\mu = 1$. On a donc alors $\left(\frac{t}{p}\right)=-\left(\frac{t}{a}\right)$. Ces deux résultats sont compris dans la formule:

$$\left(\frac{t}{p}\right)=\left(\frac{t}{a}\right)(-1)^{\frac{a-1}{4}+\frac{p-1}{4}}.$$

Si nous réunissons tout ce que nous venons de prouver, nous aurons cet énoncé:

Si u est pair, on a $\left(\frac{t}{p}\right)=\left(\frac{t}{a}\right)$, $\left(\frac{u}{p}\right)=(-1)^{\frac{p-1}{4}}$; si u est impair, on a $\left(\frac{t}{p}\right)=\left(\frac{t}{a}\right)(-1)^{\frac{p-1}{4}+\frac{a-1}{4}}$, $\left(\frac{u}{p}\right)=1$.

En comparant ce résultat avec la congruence $t^{\frac{p-1}{2}} \equiv (-a)^{\frac{p-1}{4}} u^{\frac{p-1}{2}} \pmod{p}$, qui se déduit immédiatement de l'équation (η'), on trouvera ce théorème:

Si u est pair, a est ou n'est pas résidu biquadratique par rapport à p, selon que l'on a:

$$\left(\frac{t}{a}\right)=1 \quad \text{ou} \quad \left(\frac{t}{a}\right)=-1;$$

(ϑ') si u est impair, a est ou n'est pas résidu biquadratique relativement à p, selon que l'on a:

$$\left(\frac{t}{a}\right)=(-1)^{\frac{a-1}{4}} \quad \text{ou} \quad \left(\frac{t}{a}\right)=-(-1)^{\frac{a-1}{4}}.$$

Décomposons p en deux carrés, en posant $p=\varphi^2+\psi^2$ (ψ étant supposé pair). La substitution de cette valeur dans l'équation (η') donnera:

$$(t+\psi s)(t-\psi s)=\varphi^2 s^2-au^2.$$

Nous distinguerons maintenant deux cas selon que φ est ou n'est pas divisible par a.

Premier cas: φ n'est pas divisible par a.

Comme φ est impair et non-divisible par a, le plus grand commun diviseur de φ et de u, que nous désignerons par m, sera aussi impair et non-divisible par a. Si nous faisons $\varphi=m\varphi'$, $u=mu'$, l'équation précédente se changera en celle-ci:

$$(t+\psi s)(t-\psi s)=m^2(\varphi'^2 s^2-au'^2);$$

s est premier à au et par conséquent aussi à au', φ' est également premier à au'; donc $\varphi' s$ et au' n'ont pas de diviseur commun. Cela étant, il suit d'un théorème connu (*Théorie des Nombres* no. 197) que tout diviseur impair R de $s^2\varphi'^2-au'^2$ est tel qu'on a $\left(\frac{R}{a}\right)=1$.

Désignant par E, K, F et L quatre indéterminées, nous pourrons remplacer la dernière équation par celles que je vais écrire:

$$t+\psi s=EK, \qquad m^2=EF,$$
$$t-\psi s=FL, \quad (s\varphi')^2-au'^2=KL.$$

On s'assure facilement que les nombres impairs E et F sont premiers entre eux. Il suit de là que chacun d'eux est un carré, de sorte qu'on a:

$$\left(\frac{E}{a}\right)=1, \quad \left(\frac{F}{a}\right)=1.$$

Il faut maintenant considérer successivement le cas de u pair et celui de u impair. Si u est pair, $u'=\frac{u}{m}$ le sera pareillement, et comme $s\varphi'$ est toujours impair, $(s\varphi')^2-au'^2$ sera également impair. Les nombres K et L seront donc

dans ce cas impairs l'un et l'autre, et comme ils divisent le binôme précédent, on aura:

$$\left(\frac{K}{a}\right)=1, \quad \left(\frac{L}{a}\right)=1.$$

Multipliant ces relations par celles que nous venons d'écrire, il viendra:

$$\left(\frac{EK}{a}\right)=\left(\frac{t+\psi s}{a}\right)=1, \quad \left(\frac{FL}{a}\right)=\left(\frac{t-\psi s}{a}\right)=1.$$

Comme a est un nombre premier $4n+1$, il est permis d'écrire la formule $\left(\frac{t-\psi s}{a}\right)=1$ de cette autre manière: $\left(\frac{\psi s-t}{a}\right)=1$. On a donc, dans le cas de u pair, $\left(\frac{\psi s\pm t}{a}\right)=1$, le double signe étant à volonté.

Passons au cas où u est impair. Le nombre $u'=\frac{u}{m}$ sera également impair dans ce cas, et comme les carrés impairs $(s\varphi')^2$, u'^2 sont de la forme $8n+1$, on voit que le binôme $(s\varphi')^2-au'^2$ sera de la forme $8n$ ou de la forme $8n+4$, selon que a est de la forme $8n+1$ ou de celle-ci: $8n+5$. Il est facile de s'assurer que, si a est de la forme $8n+1$, on a $\left(\frac{K}{a}\right)=1$, $\left(\frac{L}{a}\right)=1$. En effet, si l'on fait $K=2^\beta K'$, 2^β étant la puissance la plus élevée de 2 qui divise K, K' sera un diviseur impair de $(s\varphi')^2-au'^2$ et l'on aura $\left(\frac{K'}{a}\right)=1$. D'un autre côté, on sait, par un théorème connu, que tout nombre premier $a=8n+1$, est tel que $\left(\frac{2}{a}\right)=1$. On conclut de là $\left(\frac{2^\beta}{a}\right)=1$, et multipliant ensuite par $\left(\frac{K'}{a}\right)=1$, il viendra $\left(\frac{K}{a}\right)=1$. On prouve d'une manière toute semblable qu'on a aussi $\left(\frac{L}{a}\right)=1$. Multipliant ces relations par les suivantes: $\left(\frac{E}{a}\right)=1$, $\left(\frac{F}{a}\right)=1$, obtenues plus haut, il viendra:

$$\left(\frac{EK}{a}\right)=\left(\frac{t+\psi s}{a}\right)=1, \quad \left(\frac{FL}{a}\right)=\left(\frac{t-\psi s}{a}\right)=1.$$

Il est facile de voir que ces résultats, qui ont lieu lorsque u est impair et qu'en même temps a est de la forme $8n+1$, peuvent être réunis dans la formule $\left(\frac{\psi s\pm t}{a}\right)=1$, où le double signe est à volonté.

Le nombre u étant toujours impair, supposons a de la forme $8n+5$. Le produit KL, qui équivaut au binôme $(s\varphi')^2-au'^2$, étant alors de la forme $8n+4$, et les nombres K et L étant évidemment pairs l'un et l'autre, chacun

d'eux sera de la forme $4n+2$, de sorte qu'en faisant $K=2K'$, $L=2L'$, K' et L' seront impairs; et comme ces derniers nombres sont en outre diviseurs de $(s\varphi')^2-au'^2$, il suit de ce qui a été dit plus haut, qu'on a $\left(\frac{K'}{a}\right)=1$, $\left(\frac{L'}{a}\right)=1$. Mais on a, d'un autre côté, a étant de la forme $8n+5$, $\left(\frac{2}{a}\right)=-1$. Multipliant par les égalités précédentes, il viendra d'abord $\left(\frac{K}{a}\right)=-1$, $\left(\frac{L}{a}\right)=-1$, et si l'on multiplie ensuite avec les égalités $\left(\frac{E}{a}\right)=1$, $\left(\frac{F}{a}\right)=1$, trouvées plus haut, on aura:

$$\left(\frac{EK}{a}\right)=\left(\frac{t+\psi s}{a}\right)=-1, \quad \left(\frac{FL}{a}\right)=\left(\frac{t-\psi s}{a}\right)=-1.$$

Ces résultats, qui sont relatifs au cas où u est impair et où le nombre a est de la forme $8n+5$, sont compris dans la double formule:

$$\left(\frac{\psi s\pm t}{a}\right)=-1.$$

En résumant tout ce qui précède, on aura cet énoncé:

„Si u est pair, on a $\left(\frac{\psi s\pm t}{a}\right)=1$: si, au contraire, u est impair, on a $\left(\frac{\psi s\pm t}{a}\right)=(-1)^{\frac{a-1}{4}}$, le double signe étant à volonté dans l'un et l'autre cas."

On a vu plus haut (ϑ') que, lorsque u est pair, a est ou n'est pas résidu biquadratique par rapport à p, selon que l'on a $\left(\frac{t}{a}\right)=1$, ou $\left(\frac{t}{a}\right)=-1$. D'un autre côté, il résulte de ce qui précède, qu'on a, dans ce même cas, $\left(\frac{\psi s\pm t}{a}\right)=1$. On conclut de là que, si u est pair, a est ou n'est pas résidu biquadratique relativement à p, selon que l'on a:

$$\left(\frac{t}{a}\right)=\left(\frac{\psi s\pm t}{a}\right) \quad \text{ou} \quad \left(\frac{t}{a}\right)=-\left(\frac{\psi s\pm t}{a}\right).$$

On a également vu plus haut (ϑ') que, lorsque u est impair, a est ou n'est pas résidu biquadratique par rapport à p, selon que l'on a:

$$\left(\frac{t}{a}\right)=(-1)^{\frac{a-1}{4}} \quad \text{ou} \quad \left(\frac{t}{a}\right)=-(-1)^{\frac{a-1}{4}}.$$

D'un autre côté, l'énoncé précédent fait voir, qu'on a, dans le cas de u impair, $\left(\frac{\psi s\pm t}{a}\right)=(-1)^{\frac{a-1}{4}}$. En comparant ces deux résultats, on conclut que, lorsque

u est impair, a est ou n'est pas résidu biquadratique relativement à p, selon que l'on a:

$$\left(\frac{t}{a}\right)=\left(\frac{\psi s\pm t}{a}\right) \quad \text{ou} \quad \left(\frac{t}{a}\right)=-\left(\frac{\psi s\pm t}{a}\right).$$

La conclusion étant la même dans le cas de u pair et dans celui de u impair, on peut énoncer ce théorème:

„Si a est résidu biquadratique relativement à p, on a $\left(\frac{t}{a}\right)=\left(\frac{\psi s\pm t}{a}\right)$; si, au contraire, a n'est pas résidu biquadratique par rapport à p, on a $\left(\frac{t}{a}\right)=-\left(\frac{\psi s\pm t}{a}\right)$, le double signe étant à volonté dans l'un et l'autre cas."

Comme on a $\left(\frac{p}{a}\right)=1$, la congruence $\chi^2\equiv p \pmod a$ sera possible et aura, comme on sait, deux racines entre les limites $-\frac{1}{2}a$ et $\frac{1}{2}a$. Supposons que χ désigne indistinctement l'une ou l'autre de ces racines. On tire immédiatement de l'équation (η'): $t^2\equiv ps^2 \pmod a$, congruence dont la comparaison avec la précédente donne $t^2\equiv\chi^2 s^2$, $\pm t\equiv\chi s \pmod a$, le signe supérieur ayant lieu pour l'une et le signe inférieur pour l'autre des deux racines de la congruence $\chi^2\equiv p \pmod a$. Si a est résidu biquadratique relativement à p, on a, comme on l'a vu il n'y a qu'un instant, $\left(\frac{t}{a}\right)=\left(\frac{\psi s\pm t}{a}\right)$. Le double signe étant à volonté dans cette formule, nous pouvons le supposer égal à celui qui se trouve dans la congruence $\pm t\equiv\chi s \pmod a$. Si nous remplaçons $\pm t$ par χs, il viendra:

$$\left(\frac{t}{a}\right)=\left(\frac{\psi s+\chi s}{a}\right)=\left(\frac{\psi+\chi}{a}\right)\left(\frac{s}{a}\right).$$

D'un autre côté, on tire de la congruence $\pm t\equiv\chi s \pmod a$ en se rappelant que a est de la forme $4n+1$: $\left(\frac{t}{a}\right)=\left(\frac{\chi}{a}\right)\left(\frac{s}{a}\right)$. Si l'on multiplie maintenant membre par membre cette équation et la précédente, on aura $\left(\frac{t^2}{a}\right)=\left(\frac{\chi}{a}\right)\left(\frac{\chi+\psi}{a}\right)\left(\frac{s^2}{a}\right)$ ou ce qui revient au même: $\left(\frac{\chi(\chi+\psi)}{a}\right)=1$, résultat qui a lieu lorsque a est résidu biquadratique relativement à p. On trouverait de la même manière que, si a n'est pas résidu biquadratique par rapport à p, on a $\left(\frac{\chi(\chi+\psi)}{a}\right)=-1$.

Ces résultats sont relatifs au cas où φ n'est pas divisible par a. Resterait à traiter le cas ou φ est divisible par a. L'analyse qu'il faut appliquer

à ce second cas, étant entièrement semblable à celle que nous avons exposée avec détail dans ce qui précède, nous nous dispenserons de la développer ici, et nous nous bornerons à énoncer la conclusion à laquelle elle conduit:

„Si φ est divisible par a, a est ou n'est pas résidu biquadratique par rapport à p, selon que a est de la forme $8n+1$ ou de celle-ci: $8n+5$."

Ce résultat et celui qui précède constituent le théorème II énoncé dans le dernier paragraphe du mémoire précédent.

On a sans doute remarqué que les énoncés des théorèmes I et II sont tels qu'il n'y entre que la racine ψ du carré pair ψ^2 que l'on obtient en décomposant p en deux carrés. Il serait facile de modifier ces énoncés de manière à ce qu'ils ne renfermassent plus que la racine φ du carré impair. On y parviendrait en suivant une marche entièrement semblable à celle que nous avons exposée dans ce qui précède.

Les résultats (ϑ') et (ϑ'), sur lesquels nous nous sommes appuyé pour établir les théorèmes I et II, renferment eux-mêmes une infinité de théorèmes intéressants analogues au premier des théorèmes de M. Gauss. On déduit, par exemple, de l'énoncé (ϑ'), en y supposant $a = 5$:

„p désignant un nombre premier $20n+1$, si l'on fait $p = t^2+5u^2$, 5 sera ou ne sera pas résidu biquadratique relativement à p, selon que u est pair ou impair; au contraire, si p désigne un nombre premier $20n+9$ et qu'on fasse de même $p = t^2+5u^2$, 5 sera ou ne sera pas résidu biquadratique par rapport à p, selon que u est impair ou pair."

Les théorèmes (ϑ') et (ϑ') se rapportent aux équations:

$$t^2-bu^2 = ps^2, \quad t^2+au^2 = ps^2.$$

On trouverait par des considérations du même genre des résultats analogues relatifs aux équations $t^2+bu^2 = ps^2$, $t^2-au^2 = ps^2$.

En traitant la première de ces équations et faisant ensuite, pour donner un exemple, $b = 3$, on aurait ce théorème particulier:

„p désignant un nombre premier $12n+1$, si l'on fait $p = t^2+3u^2$, t sera un nombre impair. Cela posé, je dis que 3 sera ou ne sera pas résidu biquadratique par rapport à p, selon que t est de la forme $12n\pm1$ ou de celle-ci: $12n\pm5$."

DÉMONSTRATIONS NOUVELLES DE QUELQUES THÉORÈMES RELATIFS AUX NOMBRES.

PAR

M. G. LEJEUNE DIRICHLET,
PROF. DE MATH.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 3 p. 390—393.

DÉMONSTRATIONS NOUVELLES DE QUELQUES THÉORÈMES RELATIFS AUX NOMBRES.

Parmi les différentes démonstrations que les géomètres ont successivement données du théorème de WILSON, celle que M. GAUSS a exposée dans ses „*Disquisitiones arithmeticae, art.* 77“ et qui est fondée sur la considération des nombres correspondants (*numeri socii*), est sans contredit la plus simple. En généralisant un peu la définition des nombres correspondants et en suivant ensuite une marche analogue à celle de M. GAUSS, on peut démontrer simultanément le théorème de WILSON et deux autres propositions qui sont d'un grand usage dans la théorie des nombres. C'est ce que nous allons faire voir en peu de mots.

La lettre p désignant un nombre premier, EULER qui le premier s'est servi de cette considération, nomme correspondants deux nombres m et n, l'un et l'autre moindres que p et tels que leur produit mn donne l'unité pour reste lorsqu'il est divisé par p.

Généralisons cette définition et appelons correspondants deux nombres m et n moindres que p et dont le produit mn donne le même reste qu'un nombre déterminé a que nous supposons n'être pas divisible par p. Cela posé, considérons la suite:

(1) $$1,\ 2,\ 3,\ \ldots,\ p-1.$$

Il est facile de voir que, si m désigne l'un quelconque des nombres qui composent cette suite, ce nombre m aura son correspondant n et n'en aura qu'un. Cela résulte immédiatement de ce que la congruence $my \equiv a \pmod{p}$, dans laquelle ni m ni a ne sont divisibles par p, a toujours une racine y moindre que p et n'en a qu'une.

Il peut arriver que n soit égal à m. On a alors $m^2 \equiv a \pmod{p}$, ce qui fait voir que ce cas ne peut avoir lieu qu'autant qu'il existe un carré

donnant le même reste que a, ou, en d'autres termes, qu'autant que a est résidu quadratique par rapport à p. Distinguons actuellement deux cas selon que a est ou n'est pas résidu quadratique par rapport à p et commençons par le dernier de ces deux cas.

Soit, dans ce cas, m l'un quelconque des nombres (1) et n son correspondant. On aura $mn \equiv a \pmod{p}$ et n sera différent de m. Après avoir ôté les nombres m, n de la suite (1), il restera $p-3$ nombres. Désignons par m' l'un quelconque de ces $p-3$ nombres restants et par n' son correspondant: n' sera différent de m' et l'on aura $m'n' \equiv a \pmod{p}$. En continuant de procéder ainsi, on épuisera la suite (1) et l'on formera $\frac{1}{2}(p-1)$ groupes composés chacun de deux nombres correspondants; car chaque nombre n'ayant qu'un correspondant qui est mis de côté en même temps que lui, on ne peut jamais, pour former un nouveau groupe, avoir besoin d'un des nombres déjà mis de côté.

Le produit de deux nombres composant un groupe donnant le même reste que a, et les groupes étant au nombre de $\frac{1}{2}(p-1)$, on voit que le produit des nombres dont l'ensemble des groupes est formé, c'est-à-dire le produit des nombres compris dans la série (1), donne le même reste que le nombre a élevé à la puissance $\frac{1}{2}(p-1)$. On a donc dans le cas que nous venons d'examiner:

$$1.2.3\ldots(p-1) \equiv a^{\frac{1}{2}(p-1)} \pmod{p}. \tag{2}$$

Passons au second cas qui a lieu lorsque a est résidu quadratique de p. Il existe dans ce cas un carré k^2 (dont la racine k peut être supposée $< p$) tel que $k^2 \equiv a \pmod{p}$. Le carré du nombre $p-k$, qui est également moindre que p, donne aussi le même reste que a lorsqu'il est divisé par p. Les nombres k et $p-k$ étant ôtés de la suite (1), il n'y restera aucun nombre x tel que $x^2 \equiv a \pmod{p}$. Car si parmi les nombres restants il y en avait un satisfaisant à cette condition, $x^2-k^2=(x+k)(x-k)$ serait divisible par p; il faudrait donc qu'un des facteurs $x+k$, $x-k$ le fût pareillement; or c'est ce qui est manifestement impossible, x étant plus petit que p et différent de k et $p-k$. — Cela posé, on voit, comme dans le cas déjà examiné, que les $p-3$ nombres qui restent dans la suite (1) après en avoir ôté k et $p-k$, se correspondent deux à deux, d'où l'on conclut comme précédemment que le produit de ces nombres donne le même reste que $a^{\frac{1}{2}(p-3)}$. Il suit de là que le produit de tous les nombres qui composent la suite (1) donne le même reste

que $a^{\frac{1}{2}(p-3)}k(p-k)$, et comme, d'après ce qu'on a vu plus haut, on a $k(p-k) \equiv -k^2 \equiv -a \pmod{p}$, il vient ce résultat:

$$1.2.3\ldots(p-1) \equiv -a^{\frac{1}{2}(p-1)} \pmod{p}.$$

Ce résultat et celui que nous avons obtenu plus haut, peuvent être réunis dans la formule suivante:

$$1.2.3\ldots(p-1) \equiv \mp a^{\frac{1}{2}(p-1)} \pmod{p}, \tag{3}$$

dans laquelle il faut prendre le signe supérieur ou inférieur, selon que le nombre a est ou n'est pas résidu quadratique de p. Si nous posons $a=1$, le signe supérieur aura lieu, l'unité étant un carré et par conséquent résidu quadratique de tout nombre. Nous avons donc:

$$1.2.3\ldots(p-1) \equiv -1 \pmod{p},$$

congruence qui constitue le théorème de Wilson.

Remplaçons le premier membre de la formule (3) par le nombre -1 qui n'en diffère, comme nous venons de le voir, que d'un multiple de p, et changeons ensuite les signes des deux membres: il viendra ainsi:

$$a^{\frac{1}{2}(p-1)} \equiv \pm 1 \pmod{p},$$

congruence dans laquelle il faudra choisir le signe $+$ ou le signe $-$, selon que a est ou n'est pas résidu quadratique de p. Le théorème que cette formule renferme, et qui a été découvert par Euler, est d'une grande importance dans la théorie des résidus. — On fera disparaître le double signe dans la dernière congruence en élevant ses deux membres au carré. On trouve ainsi:

$$a^{p-1} \equiv 1 \pmod{p},$$

ce qui est le théorème de Fermat.

Ce dernier théorème peut être démontré très simplement de la manière suivante, sans qu'il soit nécessaire de rien supposer de ce qui précède.

Les nombres a et p conservant leur signification, considérons les $p-1$ multiples de a que voici:

$$a,\ 2a,\ 3a,\ \ldots,\ (p-1)a.$$

Il est facile de voir que deux de ces nombres ne sauraient donner le même reste quand on les divise par p; car si les restes provenant des multiples ma et na étaient égaux, $ma-na=(m-n)a$ serait divisible par p, ce qui est impossible, a n'étant pas divisible par p, et $m-n$ étant $< p$ sans

pouvoir être zéro. Les restes que l'on obtient en divisant par p les $p-1$ multiples de a, étant tous différents entre eux et aucun de ces restes ne pouvant être nul, comme on le voit facilement, ces restes doivent coïncider avec les nombres de la série 1, 2, 3, ..., $p-1$, quand on fait abstraction de l'ordre dans lequel ils se suivent. Il suit de là que le produit des $p-1$ multiples de a, doit donner le même reste que le produit $1.2.3...(p-1)$.

La différence de ces produits est donc un multiple de p. Or cette différence pouvant facilement se mettre sous la forme:

$$(a^{p-1}-1)(1.2.3...(p-1))$$

et $1.2.3...(p-1)$ n'étant pas divisible par p, on en conclut que $a^{p-1}-1$ est multiple de p, ou, ce qui est la même chose, que a^{p-1} étant divisé par p donne l'unité pour reste.

QUESTION D'ANALYSE INDÉTERMINÉE.

PAR

M. G. LEJEUNE DIRICHLET,
PROF. DE MATH.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 3 p. 407—408.

QUESTION D'ANALYSE INDÉTERMINÉE.

La lettre p désignant un nombre premier impair, on sait, par le théorème de Wilson, que le produit $1.2.3...(p-1)$, augmenté de l'unité, est divisible par p. On peut substituer au produit précédent celui que l'on obtient en remplaçant ses $\frac{1}{2}(p-1)$ derniers facteurs qui sont:

$$p-1,\ p-2,\ \ldots,\ \tfrac{1}{2}(p+1),$$

par les nombres:

$$-1,\ -2,\ \ldots,\ -\tfrac{1}{2}(p-1),$$

qui en diffèrent respectivement de p. On voit ainsi que l'expression:

$$\pm[1.2.3...\tfrac{1}{2}(p-1)]^2+1,$$

dans laquelle il faut prendre le signe supérieur ou inférieur, selon que $\frac{1}{2}(p-1)$ est pair ou impair, est toujours un multiple de p. Or $\frac{1}{2}(p-1)$ est pair ou impair, selon que p est de la forme $4n+1$ ou de celle-ci: $4n+3$. On a donc pour tout nombre premier $p=4n+1$:

$$[1.2.3...\tfrac{1}{2}(p-1)]^2+1$$

égal à un multiple de p, et pour tout nombre premier $p=4n+3$:

$$-[1.2.3...\tfrac{1}{2}(p-1)]^2+1,$$

ou ce qui revient au même:

$$[1.2.3...\tfrac{1}{2}(p-1)]^2-1$$

égal à un multiple de p.

Ces deux corollaires du théorème de Wilson sont dus à Lagrange, qui les a énoncés dans le beau mémoire où il a le premier démontré le théorème qu'on vient de nommer. Le dernier de ces corollaires donne lieu à une question que nous croyons pouvoir proposer à l'attention des géomètres qui s'occupent de la théorie des nombres.

La différence:

$$[1.2.3...\tfrac{1}{2}(p-1)]^2-1$$

étant divisible par p (p désignant un nombre premier $4n+3$) et cette différence pouvant se décomposer dans les deux facteurs:

$$1.2.3...\tfrac{1}{2}(p-1)+1, \quad 1.2.3...\tfrac{1}{2}(p-1)-1,$$

il s'ensuit que l'expression:

$$1.2.3...\tfrac{1}{2}(p-1)\pm 1$$

avec le signe convenable est un multiple de p. On demande une règle qui fasse connaître le signe convenable, sans qu'il soit nécessaire de chercher, par des multiplications successives, le reste que l'on obtient en divisant le produit $1.2.3...\frac{1}{2}(p-1)$ par p. Il est facile de voir que la question proposée revient à celle de savoir si $1.2.3...\frac{1}{2}(p-1)$ est ou n'est pas résidu quadratique de p.

NOTE SUR LES INTÉGRALES DÉFINIES.

PAR

M. G. LEJEUNE DIRICHLET,
PROF. DE MATH.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 4 p. 94—98.

NOTE SUR LES INTÉGRALES DÉFINIES.

Quoique les intégrales qui font l'objet de cette note, soient comprises en grande partie parmi celles dont MM. Poisson et Cauchy et d'autres savants ont déterminé les valeurs dans ces derniers temps, je me flatte que cette nouvelle manière d'y parvenir pourra intéresser les géomètres par son extrême simplicité. Le procédé dont je fais usage, est fondé sur la propriété connue des intégrales doubles, d'être indépendantes de l'ordre dans lequel les deux intégrations sont effectuées. C'est une extension de la méthode dont MM. Laplace et Poisson ont fait un emploi si heureux dans la théorie des intégrales définies. Mais si l'on doit convenir que la méthode dont il s'agit a acquis son importance principale par les applications ingénieuses que les géomètres cités en ont faites, la justice exige aussi d'attribuer à Euler la première idée de faire servir la propriété énoncée des intégrales doubles à l'évaluation des intégrales définies simples*).

Si l'on désigne par k et m deux constantes positives, et que l'on adopte la notation de M. Legendre, on aura par le simple changement de ky en y:

$$(1) \qquad \int e^{-ky} y^{m-1} dy = \frac{\int e^{-y} y^{m-1} dy}{k^m} = \frac{\Gamma(m)}{k^m},$$

les limites étant zéro et l'infini positif. Euler a été conduit par l'induction à remplacer la constante réelle k par une quantité de la forme $k+\theta\sqrt{-1}$, la partie réelle étant toujours positive, sans quoi l'intégrale deviendrait infinie. Il a obtenu de cette manière l'équation suivante:

$$\int_0^\infty e^{-(k+\theta\sqrt{-1})y} y^{m-1} dy = \frac{\Gamma(m)}{(k+\theta\sqrt{-1})^m},$$

*) *Novi Comment. acad. Petrop. tom. XVI.*

qui a été verifiée depuis par M. Poisson*). L'équation précédente a non seulement lieu pour des valeurs réelles et positives de m, mais elle subsiste encore quand même m serait imaginaire, pourvu qu'alors la partie réelle de m fût toujours positive. C'est ce qu'on peut démontrer facilement par le même procédé qui a servi à la vérifier dans le cas de m réelle. Si donc nous désignons par p une quantité soumise à la seule restriction d'avoir sa partie réelle positive, nous avons:

$$\int_0^\infty e^{-(k+\theta\sqrt{-1})y} y^{p-1} dy = \frac{\Gamma(p)}{(k+\theta\sqrt{-1})^p}. \tag{2}$$

Si l'on remplace dans cette dernière formule la quantité réelle quelconque θ par $x+l$, x et l étant des quantités réelles quelconques, et qu'on écrive ensuite simplement k à la place de $k+l\sqrt{-1}$, il viendra celle-ci:

$$\int_0^\infty e^{-(k+x\sqrt{-1})y} y^{p-1} dy = \frac{\Gamma(p)}{(k+x\sqrt{-1})^p}, \tag{3}$$

où x désigne une quantité réelle et k et p sont deux quantités soumises à la restriction d'avoir leurs parties réelles positives.

Outre la formule précédente, nous aurons encore besoin d'une autre formule dont on est redevable à M. Laplace. La constante α étant réelle et positive et b désignant une quantité soumise à la restriction d'avoir sa partie réelle positive, la formule dont nous parlons, est celle-ci:

$$\int_{-\infty}^{\infty} \frac{b^2+x^2}{\cos\alpha x} dx = \frac{\pi}{b} e^{-\alpha b}.$$

Nous l'écrirons d'une manière un peu différente, en remplaçant $\cos\alpha x$ par $e^{-\alpha x\sqrt{-1}}$, ce qui est permis, l'intégrale $\int_{-\infty}^{\infty} \frac{b^2+x^2}{\sin\alpha x} dx$, qui est composée d'éléments égaux deux à deux, mais de signes opposés, étant évidemment nulle. Nous

*) Pour éviter toute ambiguïté, il convient de fixer le sens de quelques signes. Les lettres k et θ désignent deux quantités réelles et la première de plus positive, la notation $l(k+\theta\sqrt{-1})$ servira à remplacer l'expression $l(r)+q\sqrt{-1}$, r étant la quantité positive $\sqrt{(k^2+\theta^2)}$ et q l'arc compris entre $-\frac{\pi}{2}$ et $\frac{\pi}{2}$ déterminé par l'équation $\operatorname{tg} q = \frac{\theta}{k}$. Les suppositions précédentes étant conservées, et q désignant une quantité quelconque réelle ou imaginaire, $(k+\theta\sqrt{-1})^q$ indiquera la quantité $e^{q(l(k+\theta\sqrt{-1})} = e^{q(l(r)+qq\sqrt{-1}}$. En vérifiant l'équation (2), on trouve que cette équation n'a lieu qu'autant qu'on attache à la notation $(k+\theta\sqrt{-1})^{-p}$ le sens que je viens de définir.

avons donc:

$$\int_{-\infty}^{\infty} \frac{e^{-ax\sqrt{-1}}}{b^2+x^2} dx = \frac{\pi}{b} e^{-ba}. \tag{4}$$

L'équation (3) subsistant pour toutes les valeurs réelles de x, on peut intégrer ses deux membres par rapport à cette quantité entre des limites quelconques, après les avoir multipliés par dx et par une fonction quelconque de x. Si l'on multiplie les deux membres par $\frac{e^{-cx\sqrt{-1}}}{b^2+x^2} dx$ (c étant réelle et positive et b conservant sa signification précédente) et qu'on intègre ensuite depuis $x = -\infty$ jusqu'à $x = \infty$, on aura:

$$\int_0^\infty e^{-ky} y^{p-1} \left(\int_{-\infty}^{\infty} \frac{e^{-(c+y)x\sqrt{-1}}}{b^2+x^2} dx \right) dy = \Gamma(p) \int_{-\infty}^{\infty} \frac{e^{-cx\sqrt{-1}}}{(k+x\sqrt{-1})^p} \cdot \frac{dx}{b^2+x^2}.$$

Comme $c+y$ est positive (y ne devant recevoir que des valeurs positives dans l'intégration relative à cette variable), on aura en vertu de la formule (4):

$$\int_{-\infty}^{\infty} \frac{e^{-(c+y)x\sqrt{-1}}}{b^2+x^2} dx = \frac{\pi}{b} e^{-bc} e^{-by}.$$

La substitution de cette valeur dans le premier membre le réduira à la quantité:

$$\frac{\pi e^{-bc}}{b} \int_0^\infty e^{-(b+k)y} y^{p-1} dy,$$

ou ce qui est la même chose d'après l'équation (2), la partie réelle de $b+k$ étant évidemment positive:

$$\frac{\pi \Gamma(p) e^{-bc}}{b(b+k)^p}.$$

Égalant cette quantité au second membre et effaçant le facteur $\Gamma(p)$ qui se trouvera commun aux deux membres, on aura définitivement:

$$\int_{-\infty}^{\infty} \frac{e^{-cx\sqrt{-1}}}{(k+x\sqrt{-1})^p} \cdot \frac{dx}{b^2+x^2} = \frac{\pi e^{-bc}}{b(b+k)^p}. \tag{5}$$

En particularisant les constantes de cette formule, on obtiendra toutes celles dont il est question dans le Mémoire sur les intégrales définies que M. Poisson a inséré dans le 18ième cahier du Journal de l'École Polytechnique.

J'accentue maintenant les lettres k et p dans l'équation (3), je multiplie ses deux membres par la quantité qui se trouve sous le signe $\int$ dans la formule (5) et je les intègre ensuite depuis $x = -\infty$ jusqu'à $x = \infty$.

On effectuera la double intégration comme on l'a fait pour obtenir l'équation (5) avec la seule différence qu'au lieu de s'appuyer sur la formule (4), il faudra s'appuyer sur l'équation (5).

Tout calcul fait, on trouvera:

$$\int_{-\infty}^{\infty} \frac{e^{-cx\sqrt{-1}}}{b^2+x^2} \cdot \frac{1}{(k+x\sqrt{-1})^p} \cdot \frac{1}{(k'+x\sqrt{-1})^{p'}} dx = \frac{\pi e^{-bc}}{b} \cdot \frac{1}{(b+k)^p} \cdot \frac{1}{(b+k')^{p'}}.$$

En continuant de procéder ainsi, on arrivera à cette formule:

$$(6) \quad \left\{ \begin{array}{l} \displaystyle\int_{-\infty}^{\infty} \frac{e^{-cx\sqrt{-1}}}{b^2+x^2} \cdot \frac{1}{(k+x\sqrt{-1})^p} \cdot \frac{1}{(k'+x\sqrt{-1})^{p'}} \cdot \frac{1}{(k''+x\sqrt{-1})^{p''}} \cdots dx \\ \qquad = \dfrac{\pi e^{-bc}}{b} \cdot \dfrac{1}{(b+k)^p} \cdot \dfrac{1}{(b+k')^{p'}} \cdot \dfrac{1}{(b+k'')^{p''}} \cdots \end{array} \right.$$

dans laquelle les facteurs:

$$\frac{1}{(k+x\sqrt{-1})^p}, \quad \frac{1}{(k'+x\sqrt{-1})^{p'}}, \quad \frac{1}{(k''+x\sqrt{-1})^{p''}}, \quad \ldots$$

sont en nombre quelconque. Il faut se rappeler que c désigne une quantité positive et que b, k, p, k', p', k'', p'', ... ou du moins les parties réelles de ces quantités sont également positives.

La formule (6) fournit un grand nombre de conséquences; je me contenterai d'en indiquer une seule.

Si l'on désigne par h une quantité positive supérieure à l'unité, ou une quantité imaginaire ayant pour partie réelle une telle quantité, et par x une quantité réelle quelconque, la partie réelle de la quantité $l(h+x\sqrt{-1})$ sera positive*). On pourra par conséquent la mettre à la place de $k+0\sqrt{-1}$ dans la formule (2). On aura ainsi, en remplaçant de plus p par q (q étant une quantité du même genre, c'est-à-dire soumise aux mêmes restrictions que p):

*) Soit $h = m+n\sqrt{-1}$, m et n étant réelles et m de plus positive et > 1, la partie réelle de $l(h+x\sqrt{-1})$ ou ce qui revient au même, de $l[m+(n+x)\sqrt{-1}]$ sera $\frac{1}{2}l[m^2+(n+x)^2]$, valeur qui sera toujours positive, attendu que la quantité $m^2+(n+x)^2$ ne pourra jamais s'abaisser au-dessous de la quantité positive m^2, et à fortiori pas au dessous de l'unité, m étant > 1.

$$(7) \quad \int_0^{\infty} e^{-y(h+x\sqrt{-1})} y^{q-1} dy = \frac{\Gamma(q)}{[l(h+x\sqrt{-1})]^q},$$

ou si l'on écrit simplement $\frac{1}{(h+x\sqrt{-1})^y}$ à la place de $e^{-y(h+x\sqrt{-1})}$:

$$\int_0^{\infty} \frac{y^{q-1}}{(h+x\sqrt{-1})^y} dy = \frac{\Gamma(q)}{[l(h+x\sqrt{-1})]^q}.$$

Je multiplie les deux membres de cette dernière équation par la quantité qui se trouve sous le signe $\int$ dans l'équation (6) et je les intègre ensuite depuis $x = -\infty$ jusqu'à $x = \infty$:

$$\int_0^{\infty} y^{q-1} dy \left(\int_{-\infty}^{\infty} \frac{e^{-cx\sqrt{-1}}}{b^2+x^2} \cdot \frac{1}{(h+x\sqrt{-1})^y} \cdot \frac{1}{(k+x\sqrt{-1})^p} \cdot \frac{1}{(k'+x\sqrt{-1})^{p'}} \cdots dx \right)$$
$$= \Gamma(q) \int_{-\infty}^{\infty} \frac{e^{-cx\sqrt{-1}}}{b^2+x^2} \left(\frac{1}{(k+x\sqrt{-1})^p} \cdot \frac{1}{(k'+x\sqrt{-1})^{p'}} \cdots \right) \frac{dx}{[l(h+x\sqrt{-1})]^q}.$$

L'intégrale relative à x du premier membre s'obtient au moyen de la formule (6), y étant positive. En l'effectuant, le premier membre se réduira à:

$$\frac{\pi e^{-bc}}{b} \cdot \frac{1}{(b+k)^p} \cdot \frac{1}{(b+k')^{p'}} \cdot \frac{1}{(b+k'')^{p''}} \cdots \int_0^{\infty} \frac{y^{q-1}}{(b+h)^y} dy.$$

Si l'on met dans cette quantité à la place de l'intégrale sa valeur:

$$\frac{\Gamma(q)}{[l(b+h)]^q},$$

qu'on l'égale au second membre de l'équation précédente et qu'on efface le facteur commun $\Gamma(q)$, on aura:

$$(8) \quad \left\{ \begin{array}{l} \displaystyle\int_{-\infty}^{\infty} \frac{e^{-cx\sqrt{-1}}}{b^2+x^2} \left(\frac{1}{(k+x\sqrt{-1})^p} \cdot \frac{1}{(k'+x\sqrt{-1})^{p'}} \cdots \right) \frac{dx}{[l(h+x\sqrt{-1})]^q} \\ \qquad = \dfrac{\pi e^{-bc}}{b} \left(\dfrac{1}{(b+k)^p} \cdot \dfrac{1}{(b+k')^{p'}} \cdots \right) \dfrac{1}{[l(b+h)]^q}. \end{array} \right.$$

Si l'on accentue les lettres h et q dans la formule (7), qu'on multiplie les deux membres par la quantité qui se trouve sous le signe $\int$ dans l'équation (8) et qu'on les intègre ensuite depuis $x = -\infty$ jusqu'à $x = \infty$, on arrivera à une formule semblable à la formule (8), dans laquelle il y aura sous le signe $\int$ deux facteurs de la forme:

$$\frac{1}{[l(h+x\sqrt{-1})]^q}, \quad \frac{1}{[l(h'+x\sqrt{-1})]^{q'}}.$$

On pourra introduire de cette manière un nombre quelconque de ces facteurs, ce qui donnera la formule

$$(9)\quad \left\{\begin{array}{l} \displaystyle\int_{-\infty}^{\infty} \frac{e^{-cx\sqrt{-1}}}{b^2+x^2}\left(\frac{1}{(k+x\sqrt{-1})^p}\cdot\frac{1}{(k'+x\sqrt{-1})^{p'}}\cdots\right)\left(\frac{1}{[l(h+x\sqrt{-1})]^q}\cdot\frac{1}{[l(h'+x\sqrt{-1})]^{q'}}\cdots\right)dx \\ \qquad = \dfrac{\pi e^{-bc}}{b}\left(\dfrac{1}{(b+k)^p}\cdot\dfrac{1}{(b+k')^{p'}}\cdots\right)\left(\dfrac{1}{[l(b+h)]^q}\cdot\dfrac{1}{[l(b+h')]^{q'}}\cdots\right) \end{array}\right.$$

dans laquelle on suppose c positive, les parties réelles des quantités b; k, k', k'', ...; p, p', p'', ...; q, q', q'', ...; h, h', h'', ... également positives, et en outre les parties réelles des quantités de la dernière série h, h', h'', ... supérieures à l'unité.

SUR LA CONVERGENCE DES SÉRIES TRIGONOMÉTRIQUES QUI SERVENT A REPRÉSENTER UNE FONCTION ARBITRAIRE ENTRE DES LIMITES DONNÉES.

PAR

M. G. LEJEUNE DIRICHLET,
PROF. DE MATH.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 4 p. 157—169.

SUR LA CONVERGENCE DES SÉRIES TRIGONOMÉTRIQUES QUI SERVENT A REPRÉSENTER UNE FONCTION ARBITRAIRE ENTRE DES LIMITES DONNÉES.

Les séries de sinus et de cosinus, au moyen desquelles on peut représenter une fonction arbitraire dans un intervalle donné, jouissent entre autres propriétés remarquables de celle d'être convergentes. Cette propriété n'avait pas échappé au géomètre illustre qui a ouvert une nouvelle carrière aux applications de l'analyse, en y introduisant la manière d'exprimer les fonctions arbitraires dont il est question; elle se trouve énoncée dans le Mémoire qui contient ses premières recherches sur la chaleur. Mais personne, que je sache, n'en a donné jusqu'à présent une démonstration générale. Je ne connais sur cet objet qu'un travail dû à M. Cauchy et qui fait partie des Mémoires de l'Académie des sciences de Paris pour l'année 1823. L'auteur de ce travail avoue lui-même que sa démonstration se trouve en défaut pour certaines fonctions pour lesquelles la convergence est pourtant incontestable. Un examen attentif du Mémoire cité m'a porté à croire que la démonstration qui y est exposée n'est pas même suffisante pour les cas auxquels l'auteur la croit applicable. Je vais, avant d'entrer en matière, énoncer en peu de mots les objections auxquelles la démonstration de M. Cauchy me paraît sujette. La marche que ce géomètre célèbre suit dans cette recherche, exige que l'on considère les valeurs que la fonction $\varphi(x)$ qu'il s'agit de développer, obtient, lorsqu'on y remplace la variable x par une quantité de la forme $u+v\sqrt{-1}$. La considération de ces valeurs semble étrangère à la question et l'on ne voit d'ailleurs pas bien ce que l'on doit entendre par le résultat d'une pareille substitution lorsque la fonction dans laquelle elle a lieu, ne peut pas être exprimée par une formule analytique. Je présente cette objection avec d'autant plus de confiance, que l'auteur me semble partager mon opinion sur ce point. Il insiste en effet dans plusieurs de ses ouvrages sur la nécessité de définir

d'une manière précise le sens que l'on attache à une pareille substitution même lorsqu'elle est faite dans une fonction d'une loi analytique régulière; on trouve surtout dans le Mémoire qu'il a inséré dans le 19ième cahier du Journal de l'École Polytechnique pag. 567 et suiv., des remarques sur les difficultés que font naître les quantités imaginaires placées sous des signes de fonctions arbitraires. Quoi qu'il en soit de cette première observation, la démonstration de M. CAUCHY donne encore lieu à une autre objection qui paraît ne laisser aucun doute sur son insuffisance. La considération des quantités imaginaires conduit l'auteur à un résultat sur le décroissement des termes de la série, qui est loin de prouver que ces termes forment une suite convergente. Le résultat dont il s'agit peut être énoncé comme il suit, en supposant que l'intervalle considéré s'étend depuis zéro jusqu'à 2π.

„Le rapport du terme dont le rang est n, à la quantité $A\frac{\sin nx}{n}$ (A désignant une constante determinée, dépendante des valeurs extrêmes de la fonction) diffère de l'unité prise positivement d'une quantité qui diminue indéfiniment, à mesure que n devient plus grand."

De ce résultat et de ce que la série qui a $A\frac{\sin nx}{n}$ pour terme général, est convergente, l'auteur conclut que la série trigonométrique générale l'est également. Mais cette conclusion n'est pas permise, car il est facile de s'assurer que deux séries (du moins lorsque, comme il arrive ici, les termes n'ont pas tous le même signe) peuvent être l'une convergente, l'autre divergente, quoique le rapport de deux termes de même rang diffère aussi peu que l'on veut de l'unité prise positivement lorsque les termes sont d'un rang très avancé.

On en voit un exemple très simple dans les deux séries, ayant l'une pour terme général $\frac{(-1)^n}{\sqrt{n}}$, et l'autre $\frac{(-1)^n}{\sqrt{n}}\left(1+\frac{(-1)^n}{\sqrt{n}}\right)$. La première de ces séries est convergente, la seconde au contraire est divergente, car en la soustrayant de la première on obtient la série divergente:

$$-1-\tfrac{1}{2}-\tfrac{1}{3}-\tfrac{1}{4}-\tfrac{1}{5}-\text{ etc.}$$

et cependant le rapport de deux termes correspondants, qui est $1\pm\frac{1}{\sqrt{n}}$, converge vers l'unité à mesure que n croît.

Je vais maintenant entrer en matière, en commençant par l'examen des cas les plus simples, auxquels tous les autres peuvent être ramenés. Désignons

par h un nombre positif inférieur ou tout au plus égal à $\frac{\pi}{2}$ et par $f(\beta)$ une fonction de β qui reste continue entre les limites 0 et h; j'entends par là une fonction qui a une valeur finie et déterminée pour toute valeur de β comprise entre 0 et h, et en outre telle que la différence $f(\beta+\varepsilon)-f(\beta)$ diminue sans limite lorsque ε devient de plus en plus petit. Supposons encore que la fonction reste toujours positive entre les limites 0 et h et qu'elle décroisse constamment depuis 0 jusqu'à h, en sorte que si p et q désignent deux nombres compris entre 0 et h, $f(p)-f(q)$ ait toujours un signe opposé à celui de $p-q$. Cela posé, considérons l'intégrale:

$$(1) \qquad \int_0^h \frac{\sin i\beta}{\sin\beta} f(\beta)\,d\beta$$

dans laquelle i est une quantité positive, et voyons ce que cette intégrale deviendra à mesure que i croît. Pour cela partageons-la en plusieurs autres prises la première depuis $\beta=0$ jusqu'à $\beta=\frac{\pi}{i}$, la seconde depuis $\beta=\frac{\pi}{i}$ jusqu'à $\beta=\frac{2\pi}{i}$, et ainsi de suite, l'avant-dernière ayant pour limites $(r-1)\frac{\pi}{i}$ et $\frac{r\pi}{i}$, et la dernière $\frac{r\pi}{i}$ et h, $\frac{r\pi}{i}$ désignant le plus grand multiple de $\frac{\pi}{i}$ qui soit contenu dans h. Il est facile de voir que ces intégrales nouvelles, dont le nombre est $r+1$, sont alternativement positives et négatives, la fonction placée sous le signe d'intégration étant évidemment toujours positive entre les limites de la première, négative entre les limites de la seconde et ainsi de suite. Il n'est pas moins facile de se convaincre que chacune d'elles est plus petite que la précédente, abstraction faite du signe. En effet ν désignant un entier $< r$, les expressions:

$$\int_{(\nu-1)\frac{\pi}{i}}^{\frac{\nu\pi}{i}} \frac{\sin i\beta}{\sin\beta} f(\beta)\,d\beta \quad \text{et} \quad \int_{\frac{\nu\pi}{i}}^{(\nu+1)\frac{\pi}{i}} \frac{\sin i\beta}{\sin\beta} f(\beta)\,d\beta$$

représentent deux intégrales consécutives. Remplaçons dans la seconde β par $\frac{\pi}{i}+\beta$; elle se changera ainsi en celle-ci:

$$\int_{(\nu-1)\frac{\pi}{i}}^{\frac{\nu\pi}{i}} \frac{\sin(i\beta+\pi)}{\sin\left(\beta+\frac{\pi}{i}\right)} f\left(\beta+\frac{\pi}{i}\right) d\beta$$

ou ce qui revient au même:

$$-\int_{(\nu-1)\frac{\pi}{i}}^{\nu\frac{\pi}{i}} \frac{\sin i\beta}{\sin\left(\beta+\frac{\pi}{i}\right)} f'\left(\beta+\frac{\pi}{i}\right) d\beta.$$

Les deux intégrales qu'il s'agit de comparer ayant ainsi les mêmes limites, on voit sans peine que la seconde a une valeur numérique inférieure à celle de la première. Il suffit pour cela de remarquer qu'il suit de la supposition faite sur la fonction $f(\beta)$:

$$f\left(\frac{\pi}{i}+\beta\right)<f(\beta),$$

et que d'un autre côté:

$$\sin\left(\frac{\pi}{i}+\beta\right)>\sin\beta,$$

les arcs β et $\frac{\pi}{i}+\beta$ étant l'un et l'autre moindres que $\frac{\pi}{2}$, car il en résulte l'inégalité:

$$\frac{f(\beta)}{\sin\beta}>\frac{f\left(\beta+\frac{\pi}{i}\right)}{\sin\left(\beta+\frac{\pi}{i}\right)},$$

qui ayant lieu pour toutes les valeurs de β intermédiaires entre les limites $(\nu-1)\frac{\pi}{i}$ et $\frac{\nu\pi}{i}$, fait voir, comme nous l'avons dit, que chaque intégrale est plus grande que celle qui la suit, abstraction faite du signe. Cette circonstance a lieu à fortiori, lorsqu'on compare l'avant-dernière à la dernière, attendu que la différence des limites $\frac{r\pi}{i}$ et h de la dernière est inférieure à $\frac{\pi}{i}$, différence commune des limites de toutes les autres.

Examinons actuellement un peu plus en détail l'intégrale du rang ν, qui est:

$$\int_{(\nu-1)\frac{\pi}{i}}^{\nu\frac{\pi}{i}} \frac{\sin i\beta}{\sin\beta} f(\beta) d\beta.$$

Comme la fonction de β qui se trouve sous le signe f est le produit des facteurs $\frac{\sin i\beta}{\sin\beta}$ et $f(\beta)$, qui sont l'un et l'autre des fonctions continues de

β entre les limites de l'intégration, et comme d'un autre côté le premier de ces facteurs conserve toujours le même signe entre ces mêmes limites, on conclura, en vertu d'un théorème connu, que l'intégrale considérée est égale à l'intégrale du premier facteur multipliée par une quantité comprise entre la valeur la plus grande et la valeur la plus petite de l'autre facteur. Le second facteur décroissant depuis la première limite jusqu'à la seconde, la quantité dont il s'agit est comprise entre $f\left(\frac{(\nu-1)\pi}{i}\right)$ et $f\left(\frac{\nu\pi}{i}\right)$. En la désignant par ϱ_ν, notre intégrale sera équivalente à:

$$\varrho_\nu \int_{(\nu-1)\frac{\pi}{i}}^{\nu\frac{\pi}{i}} \frac{\sin i\beta}{\sin\beta} d\beta.$$

L'intégrale que renferme encore cette expression, dépend à la fois de ν et de i. Elle est positive ou négative selon que $\nu-1$ est pair ou impair; nous la désignerons désormais par K_ν, abstraction faite du signe. Nous aurons bientôt besoin de connaître la limite vers laquelle elle converge, lorsque, ν restant invariable, i devient de plus en plus grand. Pour découvrir cette limite, remplaçons β par $\frac{\gamma}{i}$, γ étant une nouvelle variable. Nous aurons ainsi:

$$\int_{(\nu-1)\pi}^{\nu\pi} \frac{\sin\gamma}{i\sin\left(\frac{\gamma}{i}\right)} d\gamma.$$

Sous cette forme, il est évident qu'elle converge vers la limite:

$$\int_{(\nu-1)\pi}^{\nu\pi} \frac{\sin\gamma}{\gamma} d\gamma,$$

que pour abréger nous désignerons par k_ν, abstraction faite du signe.

On sait que l'intégrale $\int_0^\infty \frac{\sin\gamma}{\gamma} d\gamma$ a une valeur finie et égale à $\frac{\pi}{2}$. Cette intégrale peut être partagée en une infinité d'autres, prises la première depuis $\gamma=0$ jusqu'à $\gamma=\pi$, la seconde depuis $\gamma=\pi$ jusqu'à $\gamma=2\pi$, et ainsi de suite. Ces nouvelles intégrales sont alternativement positives et négatives, chacune d'elles a une valeur numérique inférieure à celle de la précédente, et celle du rang ν est k_ν, abstraction faite du signe. La proposition qu'on vient de citer, revient donc à dire que la suite infinie:

(2) $$k_1-k_2+k_3-k_4+k_5-\text{ etc.}$$

est convergente et a une somme égale à $\frac{\pi}{2}$.

Les termes de cette suite allant toujours en décroissant, il suit d'une proposition connue que la somme des n premiers termes est supérieure ou inférieure à $\frac{\pi}{2}$, selon que n est impair ou pair, et que cette somme qu'on peut désigner par S_n, diffère de $\frac{\pi}{2}$ d'une quantité moindre que le terme suivant k_{n+1}.

Reprenons actuellement l'intégralè (1) et cherchons à déterminer la limite vers laquelle elle converge lorsque i croît indéfiniment. En faisant ainsi croître le nombre i, les intégrales dans lesquelles nous avons décomposé l'intégrale (1), changeront sans cesse de valeur en même temps que leur nombre augmentera; il s'agit de connaître le résultat de ce double changement lorsqu'il continue indéfiniment. Pour cela, prenons un nombre entier m (qu'il soit supposé pair pour plus de simplicité) et supposons que le nombre m reste invariable pendant que i croît. Le nombre r, qui croît sans cesse avec i, finira bientôt par surpasser le nombre invariable m, quelque grand qu'on l'ait choisi.

Cela posé, partageons en deux groupes les intégrales dont la somme est équivalente à l'intégrale (1). Le premier groupe comprendra les m premières de ces intégrales, et le second sera composé de toutes les suivantes. On aura pour la somme du premier groupe:

(3) $$K_1\varrho_1-K_2\varrho_2+K_3\varrho_3-K_4\varrho_4+\cdots-K_m\varrho_m$$

et le second, dont le nombre des termes croît sans cesse avec i, a pour premiers termes:

(4) $$K_{m+1}\varrho_{m+1}-K_{m+2}\varrho_{m+2}+\cdots$$

Considérons séparément ces deux groupes. Le nombre i croissant indéfiniment, la somme (3) convergera vers une limite qu'il est facile de déterminer. En effet, les quantités $\varrho_1, \varrho_2, \ldots, \varrho_m$ qui sont comprises la première entre $f(0)$ et $f\left(\frac{\pi}{i}\right)$, la seconde entre $f\left(\frac{\pi}{i}\right)$ et $f\left(\frac{2\pi}{i}\right)$, et la dernière entre $f\left(\frac{(m-1)\pi}{i}\right)$ et $f\left(\frac{m\pi}{i}\right)$ convergent chacune vers la limite $f(0)$, lorsque, m restant invariable, i croît sans cesse. D'un autre côté nous avons vu que les quantités:

$$K_1,\ K_2,\ \ldots,\ K_m$$

convergent dans les mêmes circonstances respectivement vers les limites:

$$k_1,\ k_2,\ \ldots,\ k_m.$$

Donc la somme (3) converge vers la limite:

$$(k_1-k_2+k_3-\cdots-k_m)f(0) = S_m f(0),$$

ce qui veut dire que la différence entre la somme (3) et $S_m f(0)$ finira toujours, abstraction faite du signe, par être constamment inférieure à ω, ω désignant une quantité positive aussi petite que l'on veut.

Considérons pareillement la somme (4), dont le nombre des termes augmente sans cesse. Ses termes étant alternativement positifs et negatifs, et chacun d'eux ayant une valeur numérique inférieure à celle du terme précédent, comme nous l'avons vu plus haut, en considérant les intégrales que ces termes représentent, il suit d'un principe connu*) que cette somme, quel que soit le nombre de ses termes, est positive comme son premier terme $K_{m+1}\varrho_{m+1}$ et a une valeur inférieure à celle de ce terme. Or ce premier terme convergeant vers la limite $k_{m+1}f(0)$, il s'ensuit que la somme (4) finira toujours par être inférieure à $k_{m+1}f(0)$ augmenté d'une quantité positive ω' aussi petite que l'on veut. En combinant ce résultat avec celui que nous avons obtenu sur la somme (3), il n'y a qu'un instant, on verra que l'intégrale (1) qui est la somme des expressions (3) et (4) finira toujours par différer de $S_m f(0)$ d'une quantité moindre, abstraction faite du signe, que $\omega+\omega'+k_{m+1}f(0)$, ω et ω' étant deux nombres d'une petitesse arbitraire. D'un autre côté S_m diffère de $\frac{\pi}{2}$ d'une quantité numériquement inférieure à k_{m+1}; donc l'intégrale finira toujours par différer de $\frac{\pi}{2}f(0)$ d'une quantité moindre que $\omega+\omega'+2k_{m+1}f(0)$, abstraction faite du signe.

Comme m peut être choisi tellement grand que k_{m+1} soit moindre que toute grandeur donnée, il s'ensuit que l'intégrale (1) finira toujours, lorsque i croît sans limite, par différer constamment de $\frac{\pi}{2}f(0)$ d'une quantité moindre, abstraction faite du signe, qu'un nombre aussi petit que l'on veut. Il est ainsi

*) Le principe sur lequel nous nous appuyons peut être énoncé de cette manière.
Les lettres $A, A', A'', \ldots$ désignant des quantités positives en nombre quelconque et telles que:

$$A > A' > A'' > \text{ etc.},$$

la quantité:

$$A-A'+A''-A'''+\text{ etc.}$$

est positive et inférieure à A. Cela résulte immédiatement de ce que la quantité précédente peut être mise sous l'une et l'autre de ces deux formes:

$$(A-A')+(A''-A''')+\text{ etc.},$$
$$A-(A'-A'')-(A'''-A^{IV})-\text{ etc.}$$

prouvé, que l'intégrale (1) converge vers la limite $\frac{\pi}{2}f(0)$ pour des valeurs croissantes de i.

Supposons maintenant que la fonction $f(\beta)$, au lieu d'être toujours décroissante depuis 0 jusqu'à h, soit constante et égale à l'unité. On pourra dans ce cas déterminer la limite vers laquelle converge l'intégrale (1) par les mêmes considérations que nous venons d'employer; c'est ce qu'on voit tout de suite, en se rappelant que la démonstration précédente est fondée sur ce que les intégrales, dans lesquelles nous avons décomposé l'intégrale (1), forment une suite décroissante. Or ce décroissement tient à deux choses, au décroissement du facteur $f(\beta)$ et à l'accroissement du diviseur $\sin\beta$. Si $f(\beta)$ devient un nombre constant, l'accroissement de $\sin\beta$ suffira toujours pour rendre chaque intégrale de la série plus petite que la précédente. On trouvera ainsi, en supposant toujours h positive et tout au plus égale à $\frac{\pi}{2}$, que l'intégrale $\int_0^h \frac{\sin i\beta}{\sin\beta}d\beta$ converge vers la limite $\frac{\pi}{2}$. Il suit de là que l'intégrale $\int_0^h c\frac{\sin i\beta}{\sin\beta}d\beta$, dans laquelle c est une constante positive ou négative, converge vers la limite $c\frac{\pi}{2}$.

Nous avons supposé que la fonction $f(\beta)$ était décroissante et positive entre les limites 0 et h. La première circonstance ayant toujours lieu, c'est-à-dire la fonction étant telle que $f(p)-f(q)$ ait un signe contraire à celui de $p-q$ pour des valeurs p et q comprises entre 0 et h, supposons que $f(\beta)$ ne soit pas toujours positive. On prendra alors une constante positive c assez grande pour que $c+f(\beta)$ conserve toujours un signe positif depuis $\beta=0$ jusqu'à $\beta=h$. L'intégrale $\int_0^h f(\beta)\frac{\sin i\beta}{\sin\beta}d\beta$ étant égale à la différence de celles-ci:

$$\int_0^h [c+f(\beta)]\frac{\sin i\beta}{\sin\beta}d\beta \quad \text{et} \quad \int_0^h c\frac{\sin i\beta}{\sin\beta}d\beta,$$

sa limite sera la différence des limites vers lesquelles convergent ces dernières. Or ces dernières rentrent dans les cas précédemment examinés ($c+f(\beta)$ étant une fonction décroissante et positive) et convergent vers les limites $[c+f(0)]\frac{\pi}{2}$ et $c\frac{\pi}{2}$, d'où il suit que la première converge vers la limite $\frac{\pi}{2}f(0)$.

Considérons actuellement une fonction $f(\beta)$ croissante depuis 0 jusqu'à h. Dans ce cas $-f(\beta)$ sera une fonction décroissante. L'intégrale

$\int_0^h -f(\beta)\frac{\sin i\beta}{\sin\beta}d\beta$ convergera donc vers la limite $-\frac{\pi}{2}f(0)$, et par conséquent l'intégrale $\int_0^h f(\beta)\frac{\sin i\beta}{\sin\beta}d\beta$ vers la limite $\frac{\pi}{2}f(0)$.

En réunissant ces résultats, on aura cet énoncé:

(5) „Quelle que soit la fonction $f(\beta)$, pourvu qu'elle reste continue entre les limites 0 et h (h étant positive et tout au plus égale à $\frac{\pi}{2}$), et qu'elle croisse ou qu'elle décroisse depuis la première de ces limites jusqu'à la seconde, l'intégrale $\int_0^h f(\beta)\frac{\sin i\beta}{\sin\beta}d\beta$ finira par différer constamment de $\frac{\pi}{2}f(0)$ d'une quantité moindre que tout nombre assignable, lorsqu'on y fait croître i au delà de toute limite positive."

Désignons par g un nombre positif différent de zéro et inférieur à h, et supposons que la fonction reste continue et croisse ou décroisse depuis g jusqu'à h. L'intégrale $\int_g^h f(\beta)\frac{\sin i\beta}{\sin\beta}d\beta$ convergera alors vers une limite qu'il est facile de découvrir. On pourrait y parvenir par des considérations analogues à celles que nous avons appliquées à l'intégrale (1); mais il est plus simple de ramener ce nouveau cas à ceux que nous avons considérés dans ce qui précède. La fonction n'étant donnée que depuis g jusqu'à h, reste entièrement arbitraire pour les valeurs de β comprises entre 0 et g. Supposons que l'on entende par $f(\beta)$, pour les valeurs de β comprises entre 0 et g, une fonction continue et croissante ou décroissante depuis 0 jusqu'à g, selon que $f(\beta)$ croît ou décroît depuis g jusqu'à h; supposons encore que $f(g-\varepsilon)$ diffère infiniment peu de $f(g+\varepsilon)$, si ε décroît sans limite; ayant satisfait d'une manière quelconque à ces conditions, ce qu'on peut toujours faire d'une infinité de manières, la fonction $f(\beta)$ remplira depuis 0 jusqu'à h les conditions exprimées dans l'énoncé (5). Les intégrales:

$$\int_0^g f(\beta)\frac{\sin i\beta}{\sin\beta}d\beta \quad \text{et} \quad \int_0^h f(\beta)\frac{\sin i\beta}{\sin\beta}d\beta$$

convergeront donc l'une et l'autre vers la limite $\frac{\pi}{2}f(0)$. D'où l'on conclut que l'intégrale $\int_g^h f(\beta)\frac{\sin i\beta}{\sin\beta}d\beta$, qui est la différence des précédentes, a zéro pour limite.

Ce nouveau résultat peut être réuni en un seul énoncé avec celui que nous avons obtenu plus haut. On aura ainsi:

(6) „La lettre h désignant une quantité positive tout au plus égale à $\frac{\pi}{2}$, et g une quantité également positive et en outre inférieure à h, l'intégrale:

$$\int_g^h f(\beta)\frac{\sin i\beta}{\sin\beta}d\beta$$

dans laquelle la fonction $f(\beta)$ est continue entre les limites de l'intégration et a une marche toujours croissante ou toujours décroissante depuis $\beta = g$ jusqu'à $\beta = h$, convergera vers une certaine limite, lorsque le nombre i devient de plus en plus grand. Cette limite est égale à zéro, le seul cas excepté où g a une valeur nulle, dans ce cas elle a la valeur $\frac{\pi}{2}f(0)$."

Il est évident que ce résultat ne serait que légèrement modifié, si la fonction $f(\beta)$ présentait une solution de continuité pour $\beta = g$ et $\beta = h$, c'est-à-dire si $f(g)$ était différent de $f(g+\varepsilon)$ et $f(h)$ de $f(h-\varepsilon)$, ε désignant une quantité infiniment petite et positive, pourvu qu'alors les valeurs $f(g)$ et $f(h)$ ne fussent pas infinies. Il faudrait seulement dans ce cas remplacer $f(0)$ par $f(\varepsilon)$ dans l'énoncé précédent, ce qu'on peut faire encore même quand il n'y a pas de solution de continuité, attendu qu'alors $f(\varepsilon)$ est égale à $f(0)$.

Nous sommes maintenant en état de prouver la convergence des séries périodiques qui expriment des fonctions arbitraires entre des limites données. La marche que nous allons suivre nous conduira à établir la convergence de ces séries et à déterminer en même temps leurs valeurs. Soit $\varphi(x)$ une fonction de x, ayant une valeur finie et déterminée pour chaque valeur de x comprise entre $-\pi$ et π, et supposons qu'il s'agisse de développer cette fonction en une série de sinus et de cosinus d'arcs multiples de x. La série qui résout cette question, est, comme l'on sait:

$$(7)\qquad \frac{1}{2\pi}\int\varphi(\alpha)d\alpha+\frac{1}{\pi}\left\{\begin{array}{l}\cos x\int\varphi(\alpha)\cos\alpha\,d\alpha+\cos 2x\int\varphi(\alpha)\cos 2\alpha\,d\alpha+\cdots\\ \sin x\int\varphi(\alpha)\sin\alpha\,d\alpha+\sin 2x\int\varphi(\alpha)\sin 2\alpha\,d\alpha+\cdots\end{array}\right\},$$

les intégrales qui déterminent les coefficients constants, étant prises depuis

$\alpha = -\pi$ jusqu'à $\alpha = \pi$, et x désignant une quantité quelconque comprise entre $-\pi$ et π (*Théorie de la Chaleur*, No. 232 et suiv.).

Considérons les $2n+1$ premiers termes de cette série (n étant un nombre entier) et voyons vers quelle limite converge la somme de ces termes, lorsque n devient de plus en plus grand. Cette somme peut être mise sous la forme suivante:

$$\frac{1}{\pi}\int_{-\pi}^{+\pi}\varphi(\alpha)d\alpha[\tfrac{1}{2}+\cos(\alpha-x)+\cos 2(\alpha-x)+\cdots+\cos n(\alpha-x)],$$

ou en sommant la suite de cosinus:

$$(8)\qquad \frac{1}{\pi}\int_{-\pi}^{+\pi}\varphi(\alpha)\frac{\sin(n+\frac{1}{2})(\alpha-x)}{2\sin\frac{1}{2}(\alpha-x)}d\alpha.$$

Tout se réduit maintenant à déterminer la limite dont cette intégrale approche sans cesse, lorsque n croît indéfiniment. Pour cela nous la partagerons en deux autres prises l'une depuis $-\pi$ jusqu'à x, l'autre depuis x jusqu'à π. Si l'on remplace dans la première α par $x-2\beta$, et dans la seconde α par $x+2\beta$, β étant une nouvelle variable, ces deux intégrales se changeront en celles-ci, abstraction faite du facteur $\frac{1}{\pi}$:

$$(9)\qquad \int_0^{\frac{1}{2}(\pi+x)}\frac{\sin(2n+1)\beta}{\sin\beta}\varphi(x-2\beta)d\beta \quad\text{et}\quad \int_0^{\frac{1}{2}(\pi-x)}\frac{\sin(2n+1)\beta}{\sin\beta}\varphi(x+2\beta)d\beta.$$

Considérons la seconde de ces deux intégrales. La quantité x étant inférieure ou tout au plus égale à π, abstraction faite du signe, $\frac{1}{2}(\pi-x)$ ne pourra tomber hors des limites 0 et π. Si $\frac{1}{2}(\pi-x)=0$, ce qui a lieu lorsque $x=\pi$, l'intégrale est nulle quel que soit n; dans tous les autres cas elle convergera pour des valeurs croissantes de n vers une limite que nous allons déterminer. Supposons d'abord $\frac{1}{2}(\pi-x)$ inférieure ou tout au plus égale à $\frac{\pi}{2}$, et remarquons que la fonction $\varphi(x+2\beta)$ peut présenter plusieurs solutions de continuité depuis $\beta=0$ jusqu'à $\beta=\frac{1}{2}(\pi-x)$, et qu'elle peut aussi avoir plusieurs maxima et minima dans ce même intervalle. Désignons par l, l', l'', ..., $l^{(\nu)}$, rangées selon l'ordre de leur grandeur, les différentes valeurs de β qui présentent l'une ou l'autre de ces circonstances, et décomposons notre intégrale en plusieurs autres prises respectivement entre les limites:

$$0 \text{ et } l,\quad l \text{ et } l',\quad l' \text{ et } l'',\quad \ldots,\quad l^{(\nu)} \text{ et } \tfrac{1}{2}(\pi-x).$$

Toutes ces intégrales se trouveront dans le cas de l'énoncé (6). Elles convergeront donc toutes vers la limite zéro à mesure que n croît, à l'exception de la première qui converge vers la limite $\frac{\pi}{2}\varphi(x+\varepsilon)$, ε étant un nombre infiniment petit et positif. Si $\frac{1}{2}(\pi-x)$ était supérieure à $\frac{1}{2}\pi$, ce qui arrivera lorsque x a une valeur négative, on partagerait l'intégrale en deux autres, l'une prise depuis $\beta=0$ jusqu'à $\beta=\frac{1}{2}\pi$, l'autre depuis $\beta=\frac{1}{2}\pi$ jusqu'à $\beta=\frac{1}{2}(\pi-x)$. La première de ces nouvelles intégrales se trouvera dans le même cas que celle que nous venons de considérer, elle convergera donc vers la limite $\frac{\pi}{2}\varphi(x+\varepsilon)$. Quant à la seconde, on peut la changer en celle-ci, en y remplaçant β par $\pi-\gamma$, γ étant une nouvelle variable:

$$\int_{\frac{1}{2}(\pi+x)}^{\frac{1}{2}\pi}\varphi(x+2\pi-2\gamma)\frac{\sin(2n+1)(\pi-\gamma)}{\sin(\pi-\gamma)}\,d\gamma,$$

ou ce qui revient au même, n étant un entier:

$$\int_{\frac{1}{2}(\pi+x)}^{\frac{1}{2}\pi}\varphi(x+2\pi-2\gamma)\frac{\sin(2n+1)\gamma}{\sin\gamma}\,d\gamma.$$

Elle a ainsi une forme analogue à celle de la précédente; en la décomposant comme précédemment en plusieurs autres, on verra qu'elle converge vers la limite zéro, le seul cas excepté, où $\frac{1}{2}(\pi+x)$ a une valeur nulle, c'est-à-dire lorsque $x=-\pi$; dans ce cas elle approche continuellement de la limite $\varphi(\pi-\varepsilon)$, ε ayant toujours la même signification. En résumant tout ce qui précède, on trouvera que la seconde des intégrales (9) est nulle lorsque $x=\pi$, qu'elle converge vers la limite $\frac{\pi}{2}[\varphi(\pi-\varepsilon)+\varphi(-\pi+\varepsilon)]$ lorsque $x=-\pi$, et que dans tous les autres cas elle approche continuellement de la limite $\frac{\pi}{2}\varphi(x+\varepsilon)$.

La première des intégrales (9) est entièrement analogue à la seconde; en y appliquant des considérations semblables, on trouvera qu'elle est nulle lorsque $x=-\pi$, qu'elle converge vers la limite $\frac{\pi}{2}[\varphi(\pi-\varepsilon)+\varphi(-\pi+\varepsilon)]$ lorsque $x=\pi$ et que dans tous les autres cas elle a pour limite $\frac{\pi}{2}\varphi(x-\varepsilon)$. Connaissant ainsi les limites de chacune des intégrales (9), il est facile de

trouver la limite dont l'intégrale (8) approche sans cesse, lorsque n devient de plus en plus grand; il suffit pour cela de se rappeler que cette intégrale est égale à la somme des intégrales (9) divisée par π. Or, l'intégrale (8) étant équivalente à la somme des $2n+1$ premiers termes de la série (7), il est prouvé que cette série est convergente, et l'on trouve au moyen des résultats précédents qu'elle est égale à:

$$\tfrac{1}{2}[\varphi(x+\varepsilon)+\varphi(x-\varepsilon)]$$

pour toute valeur de x comprise entre $-\pi$ et π, et que pour chacune des valeurs extrêmes π et $-\pi$, elle est égale à:

$$\tfrac{1}{2}[\varphi(\pi-\varepsilon)+\varphi(-\pi+\varepsilon)].$$

L'exposé précédent embrasse tous les cas; il se simplifie lorsque la valeur de x qu'on considère n'est pas une de celles qui présentent une solution de continuité. En effet les quantités $\varphi(x+\varepsilon)$ et $\varphi(x-\varepsilon)$ étant alors l'une et l'autre équivalentes à $\varphi(x)$, on voit que la série a pour valeur $\varphi(x)$.

Les considérations précédentes prouvent d'une manière rigoureuse que, si la fonction $\varphi(x)$, dont toutes les valeurs sont supposées finies et déterminées, ne présente qu'un nombre fini de solutions de continuité entre les limites $-\pi$ et π, et si en outre elle n'a qu'un nombre déterminé de maxima et de minima entre ces mêmes limites, la série (7), dont les coefficients sont des intégrales définies dépendantes de la fonction $\varphi(x)$, est convergente et a une valeur généralement exprimée par:

$$\tfrac{1}{2}[\varphi(x+\varepsilon)+\varphi(x-\varepsilon)],$$

où ε désigne un nombre infiniment petit. Il nous resterait à considérer les cas où les suppositions que nous avons faites sur le nombre des solutions de continuité et sur celui des valeurs maxima et minima cessent d'avoir lieu. Ces cas singuliers peuvent être ramenés à ceux que nous venons de considérer. Il faut seulement, pour que la série (8) présente un sens lorsque les solutions de continuité sont en nombre infini, que la fonction $\varphi(x)$ remplisse la condition suivante.

Il est nécessaire qu'alors la fonction $\varphi(x)$ soit telle que, si l'on désigne par a et b deux quantités quelconques comprises entre $-\pi$ et π, on puisse toujours placer entre a et b d'autres quantités r et s assez rapprochées pour que la fonction reste continue dans l'intervalle de r à s. On sentira

facilement la nécessité de cette restriction en considérant que les différents termes de la série sont des intégrales définies et en remontant à la notion fondamentale des intégrales. On verra alors que l'intégrale d'une fonction ne signifie quelque chose qu'autant que la fonction satisfait à la condition précédemment énoncée. On aurait un exemple d'une fonction qui ne remplit pas cette condition, si l'on supposait $\varphi(x)$ égale à une constante déterminée c lorsque la variable x obtient une valeur rationnelle, et égale à une autre constante d, lorsque cette variable est irrationnelle. La fonction ainsi définie a des valeurs finies et déterminées pour toute valeur de x, et cependant on ne saurait la substituer dans la série, attendu que les différentes intégrales qui entrent dans cette série, perdraient toute signification dans ce cas. La restriction que je viens de préciser, et celle de ne pas devenir infinie, sont les seules auxquelles la fonction $\varphi(x)$ soit sujette et tous les cas qu'elles n'excluent pas peuvent être ramenés à ceux que nous avons considérés dans ce qui précède. Mais la chose, pour être faite avec toute la clarté qu'on peut désirer, exige quelques détails liés aux principes fondamentaux de l'analyse infinitésimale et qui seront exposés dans une autre note, où je m'occuperai aussi de quelques autres propriétés assez remarquables de la série (7).

Berlin, Janvier 1829.

ÜBER DIE DARSTELLUNG GANZ WILLKÜRLICHER FUNCTIONEN DURCH SINUS- UND COSINUSREIHEN.

VON

G. LEJEUNE DIRICHLET.

Repertorium der Physik, unter Mitwirkung der Herren Lejeune Dirichlet, Jacobi, Neumann, Riess, Strehlke, herausgegeben von Heinrich Wilhelm Dove und Ludwig Moser. Bd. I, 1837, S. 152—174.

ÜBER DIE DARSTELLUNG GANZ WILLKÜRLICHER FUNCTIONEN DURCH SINUS- UND COSINUSREIHEN.

Die merkwürdigen Reihen, welche in einem bestimmten Intervalle Functionen darstellen, welche ganz gesetzlos sind oder in verschiedenen Theilen dieses Intervalls ganz verschiedenen Gesetzen folgen, haben seit der Begründung der mathematischen Wärmelehre durch FOURIER so zahlreiche Anwendungen in der analytischen Behandlung physikalischer Probleme gefunden, dass es zweckmässig erscheint, die für die folgenden Bände dieses Werkes bestimmten Auszüge aus den neuesten Arbeiten über einige Theile der mathematischen Physik durch die Entwickelung einiger der wichtigsten dieser Reihen einzuleiten.

§. 1.

Man denke sich unter a und b zwei feste Werthe und unter x eine veränderliche Grösse, welche nach und nach alle zwischen a und b liegenden Werthe annehmen soll. Entspricht nun jedem x ein einziges, endliches y, und zwar so, dass, während x das Intervall von a bis b stetig durchläuft, $y = f(x)$ sich ebenfalls allmählich verändert, so heisst y eine stetige oder continuirliche*) Function von x für dieses Intervall. Es ist dabei gar nicht nöthig, dass y in diesem ganzen Intervalle nach demselben Gesetze von x abhängig sei, ja man braucht nicht einmal an eine durch mathematische Operationen ausdrückbare Abhängigkeit zu denken. Geometrisch dargestellt, d. h. x und y als Abscisse und Ordinate gedacht, erscheint eine stetige Function als eine zusammenhängende Curve, von der jeder zwischen a und b enthaltenen Abscisse nur ein Punkt entspricht. Diese Definition schreibt den einzelnen Theilen der Curve kein gemeinsames Gesetz vor; man kann sich dieselbe aus den verschiedenartigsten Theilen zusammengesetzt oder ganz gesetzlos gezeichnet denken. Es

*) Da im Folgenden nur von stetigen Functionen die Rede sein wird, so kann der Zusatz ohne Nachtheil wegbleiben.

geht hieraus hervor, dass eine solche Function für ein Intervall als vollständig bestimmt nur dann anzusehen ist, wenn sie entweder für den ganzen Umfang desselben graphisch gegeben ist, oder mathematischen, für die einzelnen Theile desselben geltenden Gesetzen unterworfen wird. So lange man über eine Function nur für einen Theil des Intervalls bestimmt hat, bleibt die Art ihrer Fortsetzung für das übrige Intervall ganz der Willkür überlassen.

Es seien A und B die Endpunkte von a und b, und $\alpha\gamma\beta$ die der Function $f(x)$ entsprechende Curve, so ist klar, dass mit dieser Function auch der Flächenraum $A\alpha\gamma\beta B$ bestimmt ist, welcher von den Ordinaten $A\alpha$, $B\beta$, dem Stück AB der Abscissenachse und der Curve $\alpha\gamma\beta$ begrenzt wird, wenn er sich gleich nicht immer genau angeben lässt. Dieser Raum heisst bekanntlich auch das bestimmte Integral der Function $f(x)$, von a bis b oder zwischen den Grenzen a und b genommen, und wird durch $\int_a^b f(x)\,dx$ bezeichnet. Der Ursprung dieses Zeichens liegt in der Art, wie die Infinitesimalrechnung einen Flächenraum oder ein solches Integral betrachtet. Wird die Linie $AB = b-a$, in eine Anzahl n gleicher Theile zerlegt, deren gemeinschaftlicher Werth $= \frac{b-a}{n} = \delta$, und werden durch α und die Endpunkte der den Theilungspunkten 1, 2, 3, ... entsprechenden Ordinaten, Parallelen mit der Abscissenachse gezogen, so entstehen n Rechtecke, deren Summe:

$$\delta f(a)+\delta f(a+\delta)+\delta f(a+2\delta)+\cdots+\delta f(a+(n-1)\delta), \tag{1}$$

wie sich leicht streng beweisen lässt, und wie es auch schon die blosse Anschauung ergiebt, bei unaufhörlichem Wachsen der Anzahl n zuletzt in den Flächenraum $A\alpha\gamma\beta B$ übergeht, d. h. man kann n immer so gross wählen, dass die Summe (1) von diesem Raum um weniger verschieden sein wird, als eine noch so kleine, vorher bestimmte Grösse. Nimmt man $b-a$ und also auch δ als positiv an, so erscheinen offenbar die in (1) enthaltenen Rechtecke als positiv oder negativ, je nachdem sie auf der Seite der positiven oder der negativen y liegen. Umgekehrt verhält es sich, wenn $b-a$ negativ ist. Es geht also hieraus hervor, dass ein bestimmtes Integral $\int_a^b f(x)\,dx$ (wenn man dieses als den Grenzwerth betrachtet, welchen (1) für ein unendliches n annimmt) nur insofern als Flächenraum angesehen werden kann, als man bei letzterem die Theile, welche auf entgegengesetzten Seiten der Abscissenachse liegen, entgegengesetzt und zwar die auf der Seite der positiven y liegenden als positiv oder negativ nimmt, je nachdem b grösser oder kleiner als a ist.

§. 2.

Aus der Definition des bestimmten Integrals als Grenzwerth von (1) oder als Flächenraum mit der eben angegebenen Modification folgen fast unmittelbar mehrere Eigenschaften, die ich hier zusammenstelle, um mich im Folgenden leichter darauf berufen zu können; c bezeichnet, wie a und b, eine Constante.

$$\int_a^b f(x)\,dx = -\int_b^a f(x)\,dx, \tag{2}$$

$$\int_a^b cf(x)\,dx = c\int_a^b f(x)\,dx, \tag{3}$$

$$\int_a^b f(x)\,dx = \int_{a+c}^{b+c} f(x-c)\,dx, \tag{4}$$

$$\int_a^b f(x)\,dx = \frac{1}{c}\int_{ac}^{bc} f\left(\frac{x}{c}\right)dx, \tag{5}$$

$$\int_a^b [f(x)\pm F(x)]\,dx = \int_a^b f(x)\,dx \pm \int_a^b F(x)\,dx, \tag{6}$$

(7) Hat $f(x)$ zwischen $x=a$ und $x=b$ immer dasselbe Zeichen, so ist $\int_a^b f(x)\,dx$ positiv oder negativ, je nachdem jenes Zeichen dem von $b-a$ gleich oder entgegengesetzt ist.

(8) Das Integral $\int_a^b \varphi(x)F(x)\,dx$ liegt immer zwischen $M\int_a^b F(x)\,dx$ und $N\int_a^b F(x)\,dx$, wenn $F(x)$ innerhalb der Grenzen a und b sein Zeichen nicht ändert und M und N respective den grössten und kleinsten Werth*) bezeichnen, den $\varphi(x)$ in dem genannten Intervall erhält.

Dieser Satz, welcher im Folgenden häufig Anwendung findet, ist leicht aus den vorhergehenden abzuleiten. Nach den über M und N gemachten Vor-

*) Es ist wohl zu bemerken, dass hier bei der Vergleichung zweier Werthe hinsichtlich ihrer Grösse auf die Zeichen Rücksicht genommen wird; r heisst grösser als s, oder geschrieben: $r > s$, wenn die algebraische Differenz $r-s$ positiv ist.

aussetzungen bleiben:

$$M-\varphi(x), \quad \varphi(x)-N$$

zwischen $x=a$ und $x=b$ stets positiv;

$$[M-\varphi(x)]F(x), \quad [\varphi(x)-N]F(x)$$

sind daher in diesem Intervall entweder beide immer positiv oder beide immer negativ, woraus vermöge (7) folgt, dass die Integrale:

$$\int_a^b [M-\varphi(x)]F(x)dx, \quad \int_a^b [\varphi(x)-N]F(x)dx$$

gleiche Zeichen haben. Werden diese Integrale nach (6) und (3) in die Form:

$$M\int_a^b F(x)dx-\int_a^b \varphi(x)F(x)dx, \quad \int_a^b \varphi(x)F(x)dx-N\int_a^b F(x)dx$$

gebracht, so ist die Behauptung bewiesen.

(9) Liegt c zwischen a und b, so ist:

$$\int_a^b f(x)dx = \int_a^c f(x)dx+\int_c^b f(x)dx.$$

Dieser Satz sagt nichts anderes, als dass der Flächenraum $\int_a^b f(x)dx$ durch die der Abscisse c entsprechende Ordinate in zwei andere Flächenräume zerlegt wird. Man kann durch wiederholte Anwendung desselben jedes Integral in eine beliebige Anzahl anderer Integrale zerlegen.

Es geht z. B. daraus hervor,

(10) dass $\int_0^{\frac{\pi}{2}} \cos 2mx\,dx = 0$, wenn m irgend eine von 0 verschiedene ganze Zahl bezeichnet.

Zerlegt man nämlich diesen Flächenraum in $2m$ andere zwischen den Grenzen: 0 und $\frac{\pi}{4m}$, $\frac{\pi}{4m}$ und $\frac{2\pi}{4m}$, $\frac{2\pi}{4m}$ und $\frac{3\pi}{4m}$, ..., $\frac{(2m-1)\pi}{4m}$ und $\frac{2m\pi}{4m}$, so sieht man leicht, dass der erste dem zweiten, der dritte dem vierten u. s. w. gleich und entgegengesetzt ist.

Endlich ist für das Folgende noch die Kenntniss der Summe z der endlichen Reihe:

$$z = \cos\vartheta+\cos 2\vartheta+\cdots+\cos n\vartheta$$

erforderlich. Um zur Bestimmung derselben zu gelangen, multiplicire man die

Gleichung mit $2\cos\vartheta$ und verwandle die Cosinusproducte nach der bekannten Formel $2\cos\beta\cos\gamma = \cos(\beta-\gamma)+\cos(\beta+\gamma)$ in Summen. Man erhält so:

$$2z\cos\vartheta = 1+\cos\vartheta+\cos 2\vartheta+\cdots+\cos(n-1)\vartheta$$
$$+\cos 2\vartheta+\cos 3\vartheta+\cos 4\vartheta+\cdots+\cos(n+1)\vartheta.$$

Die Vergleichung der oberen Horizontalreihe mit der durch z bezeichneten Reihe ergiebt für dieselbe:

$$z+1-\cos n\vartheta;$$

eben so findet man für die untere:

$$z-\cos\vartheta+\cos(n+1)\vartheta.$$

Werden beide Werthe eingesetzt, so kommt:

$$2z\cos\vartheta = 2z+1-\cos\vartheta+\cos(n+1)\vartheta-\cos n\vartheta;$$

Bringt man $2z$ auf die andere Seite und dividirt durch $2(\cos\vartheta-1)$, so folgt:

$$z = -\frac{1}{2}+\frac{\cos n\vartheta-\cos(n+1)\vartheta}{2(1-\cos\vartheta)}.$$

Dieser Ausdruck für z wird vereinfacht, wenn man $2\sin^2\frac{1}{2}\vartheta$ für $1-\cos\vartheta$ und $2\sin\frac{1}{2}\vartheta\sin(n+\frac{1}{2})\vartheta$ für $\cos n\vartheta-\cos(n+1)\vartheta$ einführt und den gemeinschaftlichen Factor $2\sin\frac{1}{2}\vartheta$ wegässt. Man findet so:

$$(11) \qquad \cos\vartheta+\cos 2\vartheta+\cdots+\cos n\vartheta = -\frac{1}{2}+\frac{\sin(n+\frac{1}{2})\vartheta}{2\sin\frac{1}{2}\vartheta}.$$

§. 3.

Verschiedene Aufgaben der mathematischen Physik erfordern die Darstellung einer für das Intervall von 0 bis π ganz willkürlich gegebenen Function $f(x)$ durch eine unendliche Reihe von folgender Form:

$$a_1\sin x+a_2\sin 2x+a_3\sin 3x+\cdots,$$

wo $a_1, a_2, a_3, \ldots$ von x unabhängige Grössen bezeichnen. Der natürlichste Weg zu der verlangten Reihenentwicklung scheint der sogenannte Uebergang vom Endlichen zum Unendlichen zu sein. Man denke sich nämlich zunächst die Reihe aus einer endlichen Anzahl $(n-1)$ von Gliedern bestehend, d. h. man betrachte den Ausdruck:

$$a_1\sin x+a_2\sin 2x+\cdots+a_{n-1}\sin(n-1)x.$$

Die darin enthaltenen willkürlichen $n-1$ Coefficienten $a_1, a_2, \ldots, a_{n-1}$ lassen sich so bestimmen, dass dieser Ausdruck für eben so viele besondere Werthe von x, nämlich $\frac{\pi}{n}, \frac{2\pi}{n}, \ldots, (n-1)\frac{\pi}{n}$, der gegebenen Function $f(x)$

gleich wird. Lässt man, nachdem die Werthe der Coefficienten gefunden worden sind, n ohne Grenzen wachsen, so geht die endliche Reihe in eine unendliche über, die Werthe $\frac{\pi}{n}$, $\frac{2\pi}{n}$, ..., $(n-1)\frac{\pi}{n}$ rücken einander immer näher und erfüllen zuletzt das ganze Intervall von 0 bis π, so dass die Gleichheit der Function und der unendlichen Reihe für den ganzen Umfang desselben Statt findet.

Die Gleichsetzung der gegebenen Function $f(x)$ und der endlichen Reihe für die vorher angeführten besondern Werthe ergiebt folgende Bedingungen:

$$a_1\sin\frac{\pi}{n}+a_2\sin\frac{2\pi}{n}+\cdots+a_m\sin\frac{m\pi}{n}+\cdots+a_{n-1}\sin(n-1)\frac{\pi}{n}=f\left(\frac{\pi}{n}\right),$$

$$a_1\sin\frac{2\pi}{n}+a_2\sin\frac{4\pi}{n}+\cdots+a_m\sin\frac{2m\pi}{n}+\cdots+a_{n-1}\sin 2(n-1)\frac{\pi}{n}=f\left(\frac{2\pi}{n}\right),$$

$$a_1\sin\frac{3\pi}{n}+a_2\sin\frac{6\pi}{n}+\cdots+a_m\sin\frac{3m\pi}{n}+\cdots+a_{n-1}\sin 3(n-1)\frac{\pi}{n}=f\left(\frac{3\pi}{n}\right),$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$a_1\sin(n-1)\frac{\pi}{n}+\cdots+a_m\sin(n-1)\frac{m\pi}{n}+\cdots+a_{n-1}\sin(n-1)^2\frac{\pi}{n}=f\left((n-1)\frac{\pi}{n}\right).$$

Um aus diesen $n-1$ Gleichungen irgend einen der darin enthaltenen Coefficienten, z. B. a_m (wo m eine der Zahlen 1, 2, 3, ..., $n-1$) zu erhalten, multiplicire man diese Gleichungen der Reihe nach mit $2\sin\frac{m\pi}{n}$, $2\sin\frac{2m\pi}{n}$, $2\sin\frac{3m\pi}{n}$, ..., $2\sin(n-1)\frac{m\pi}{n}$ und addire nachher alle zusammen. Die so entstehende neue Gleichung wird a_m allein enthalten und zur Bestimmung dieser Grösse führen. Um sich hiervon zu überzeugen, betrachte man den Inbegriff aller Glieder, die in dieser Gleichung irgend einen Coefficienten a_h enthalten, wo h wie m eine in der Reihe 1, 2, 3, ..., $n-1$ enthaltene Zahl bezeichnet. Setzt man a_h als gemeinschaftlichen Factor heraus, so erhält man als Vereinigung aller dieser Glieder:

$$a_h\left(2\sin\frac{m\pi}{n}\sin\frac{h\pi}{n}+2\sin\frac{2m\pi}{n}\sin\frac{2h\pi}{n}+\cdots+2\sin(n-1)\frac{m\pi}{n}\sin(n-1)h\frac{\pi}{n}\right),$$

und man beweist leicht, dass der Ausdruck zwischen den Klammern der Null gleich ist, wenn h von m verschieden ist. Schreibt man nämlich statt der Sinusproducte Cosinusdifferenzen, so geht derselbe in folgende Differenz über:

$$(12)\quad\begin{cases}\cos(m-h)\frac{\pi}{n}+\cos 2(m-h)\frac{\pi}{n}+\cdots+\cos(n-1)(m-h)\frac{\pi}{n}\\ -\left(\cos(m+h)\frac{\pi}{n}+\cos 2(m+h)\frac{\pi}{n}+\cdots+\cos(n-1)(m+h)\frac{\pi}{n}\right).\end{cases}$$

Jede dieser Reihen lässt sich nach Formel (11) summiren. Wenn man dort $\vartheta=(m-h)\frac{\pi}{n}$ setzt und n in $n-1$ verwandelt, so findet man für die erste:

$$-\frac{1}{2}+\frac{\sin(n-\frac{1}{2})(m-h)\frac{\pi}{n}}{2\sin(m-h)\frac{\pi}{2n}}.$$

Erinnert man sich, dass für irgend eine ganze Zahl l:

$$\sin(l\pi-\gamma)=\mp\sin\gamma,$$

wo das obere oder das untere Zeichen gilt, je nachdem l gerade oder ungerade ist, so sieht man gleich, dass:

$$\sin(n-\tfrac{1}{2})(m-h)\frac{\pi}{n}=\sin\left((m-h)\pi-(m-h)\frac{\pi}{2n}\right)=\mp\sin(m-h)\frac{\pi}{2n},$$

und dass also die erste der Reihen (12):

$$\cos(m-h)\frac{\pi}{n}+\cos 2(m-h)\frac{\pi}{n}+\cdots+\cos(n-1)(m-h)\frac{\pi}{n}$$

den Werth -1 oder 0 hat, je nachdem $m-h$ gerade oder ungerade ist. Aehnlicherweise ergiebt sich für die zweite Reihe (12):

$$-\left(\cos(m+h)\frac{\pi}{n}+\cos 2(m+h)\frac{\pi}{n}+\cdots+\cos(n-1)(m+h)\frac{\pi}{n}\right)$$

der Werth $+1$ oder 0, je nachdem $m+h$ gerade oder ungerade ist. Bemerkt man nun, dass $m-h$ und $m+h$ entweder zugleich gerade oder zugleich ungerade sind, da ihre Summe $2m$ gerade ist, so sieht man auf der Stelle, dass der Ausdruck (12) verschwindet, wie es früher behauptet wurde.

Es ist nicht zu übersehen, dass das oben gefundene Resultat wesentlich voraussetzt, dass h von m verschieden ist. Für den Fall, wo $h=m$, erscheint der Ausdruck für die Summe der ersten der Reihen (12) in der Form $\frac{0}{0}$, und die vorige Bestimmung verliert ihre Gültigkeit. Man erhält aber in diesem Falle, da alle Glieder dieser Reihe der Einheit gleich werden, sogleich für ihre Summe $n-1$, während die zweite den Werth 1 annimmt, indem $m+h=2m$ in diesem Falle gerade ist. Der Ausdruck (12) verschwindet also für jedes h, welches von m verschieden ist, für $h=m$ hingegen erhält er den Werth n. Es geht daraus hervor, dass die Gleichung, deren Entstehung man oben näher angegeben hat, in der That nur den einzigen Coefficienten a_m enthält und von folgender sehr einfachen Form ist:

$$na_m=2\sin\frac{m\pi}{n}f\left(\frac{\pi}{n}\right)+2\sin\frac{2m\pi}{n}f\left(\frac{2\pi}{n}\right)+\cdots+2\sin(n-1)\frac{m\pi}{n}f\left(\frac{(n-1)\pi}{n}\right)$$

und folglich:

$$a_m = \frac{2}{n}\left[\sin\frac{m\pi}{n} f\left(\frac{\pi}{n}\right) + \sin\frac{2m\pi}{n} f\left(\frac{2\pi}{n}\right) + \cdots + \sin(n-1)\frac{m\pi}{n} f\left(\frac{(n-1)\pi}{n}\right)\right].$$

Nachdem die Coefficienten der endlichen Reihe gefunden worden sind, bleibt zu untersuchen, wie sich der Coefficient, welcher eine beliebige, aber bestimmte Stelle einnimmt, bei unaufhörlich wachsender Gliederzahl verändert, d. h. es bleibt der Werth auszumitteln, den der vorhergehende Ausdruck für a_m annimmt, wenn man n unendlich gross werden lässt, während m constant gedacht wird. Schreibt man den Ausdruck wie folgt:

$$a_m = \frac{2}{\pi}\left[\frac{\pi}{n}\sin\left(\frac{0m\pi}{n}\right) f\left(\frac{0\pi}{n}\right) + \frac{\pi}{n}\sin\left(\frac{m\pi}{n}\right) f\left(\frac{\pi}{n}\right) + \frac{\pi}{n}\sin\frac{2m\pi}{n} f\left(\frac{2\pi}{n}\right) + \cdots\right.$$
$$\left. \cdots + \frac{\pi}{n}\sin(n-1)\frac{m\pi}{n} f\left((n-1)\frac{\pi}{n}\right)\right],$$

so erhellt sogleich aus der Vergleichung der Summe zwischen den Klammern mit der Gleichung (1), dass für $n = \infty$ die Summe in das bestimmte Integral $\int_0^\pi \sin mx f(x)dx$ übergeht.

Die alsdann zu einer unendlichen gewordene Reihe stellt aber, wie früher bemerkt worden, die Function $f(x)$ für alle zwischen 0 und π gelegenen Werthe von x dar, und wir haben also für den ganzen Umfang des genannten Intervalls:

(13) $$f(x) = a_1\sin x + a_2\sin 2x + \cdots + a_m\sin mx + \cdots,$$

in welcher Reihe die Coefficienten nach der allgemeinen Gleichung:

$$a_m = \frac{2}{\pi}\int_0^\pi \sin mx f(x)dx$$

zu bestimmen sind.

Man kann durch ähnliche Betrachtungen zu einer Reihe gelangen, welche nur die Cosinus von x und dessen Vielfachen enthält, und die Function $f(x)$, wie die gefundene Sinusreihe, für dasselbe Intervall von 0 bis π darstellt. Kürzer erreicht man jedoch diesen Zweck, wenn man das schon gefundene Resultat (13) benutzt. Setzt man in demselben statt $f(x)$ das Product $2f(x)\sin x$, so erhält man:

$$2\sin x f(x) = a_1\sin x + a_2\sin 2x + \cdots + a_m\sin mx + \cdots,$$

wo:

$$a_m = \frac{2}{\pi}\int_0^\pi 2\sin mx\sin x f(x)dx.$$

Dieser Werth für a_m lässt sich auch so schreiben:

$$a_m = \frac{2}{\pi}\int_0^\pi \cos(m-1)x f(x)dx - \frac{2}{\pi}\int_0^\pi \cos(m+1)x f(x)dx,$$

oder, wenn man zur Abkürzung setzt:

$$\frac{2}{\pi}\int_0^\pi \cos hx f(x)dx = b_h,$$

wo h eine ganze positive Zahl mit Einschluss der Null bezeichnet:

$$a_m = b_{m-1} - b_{m+1}.$$

Nimmt man successive $m = 1, 2, 3, \ldots$ und substituirt in obige Reihe, so kommt:

$$2\sin x f(x) = (b_0 - b_2)\sin x + (b_1 - b_3)\sin 2x + (b_2 - b_4)\sin 3x + \cdots,$$

oder wenn man nach $b_0, b_1, b_2, \ldots$ ordnet:

$$2\sin x f(x) = b_0\sin x + b_1\sin 2x + b_2(\sin 3x - \sin x) + b_3(\sin 4x - \sin 2x) + \text{ etc.}$$

Durch Einführung der Producte $2\sin x\cos x$, $2\sin x\cos 2x$, ... an die Stelle von $\sin 2x$, $\sin 3x - \sin x$, ... wird die ganze Gleichung durch $2\sin x$ theilbar, und man erhält nach Entfernung dieses gemeinschaftlichen Factors:

(14) $$f(x) = \tfrac{1}{2}b_0 + b_1\cos x + b_2\cos 2x + \cdots + b_m\cos mx + \cdots$$

Diese Gleichung gilt wie die Gleichung (13), aus der sie abgeleitet ist, für alle Werthe zwischen 0 und π, und der allgemeine Coefficient b_m ist:

$$\frac{2}{\pi}\int_0^\pi \cos mx f(x)dx.$$

Obgleich die Reihen (13) und (14) beide eine ganz beliebige Function $f(x)$ für das Intervall von 0 bis π darstellen, so sind sie doch wesentlich von einander verschieden. Während die letztere wegen der bekannten Eigenschaft des Cosinus, für entgegengesetzte Werthe des Bogens gleich zu sein, durch die Verwandlung von x in $-x$ unverändert bleibt, nimmt die erstere in demselben Falle den entgegengesetzten Werth an, wie eben so leicht aus der Natur des Sinus erhellt. Man sieht hieraus leicht, dass man unter gewissen Umständen eine Function von x für das Intervall von $-\pi$ bis π durch die Reihe (14) oder (13) darstellen kann. Denkt man sich nämlich unter $f(x)$ eine von $x = 0$ bis $x = \pi$ ganz beliebig gegebene Function von x, und setzt diese Function oder Curve von $x = 0$ bis $x = -\pi$ so fort, dass immer:

$$f(-x) = f(x),$$

so wird diese Function von $x = \pi$ bis $x = -\pi$, durch die Reihe (14) ausgedrückt werden können, denn diese Reihe gilt immer von 0 bis π, und da sie bei der Verwandlung von x in $-x$ unverändert bleibt, welches nach der angegebenen Art der Fortsetzung auch bei der Function der Fall ist, so stellt sie diese auch von 0 bis $-\pi$ dar. Ganz auf dieselbe Weise überzeugt man sich, dass wenn man eine von 0 bis π beliebig gegebene Function so fortsetzt, dass:

$$f(-x) = -f(x),$$

für eine solche Function zwischen $x = -\pi$ und $x = \pi$ die Reihe (13) gilt. Auf diese einfache Bemerkung kann man eine Reihe gründen, welche die Reihen (13) und (14) als besondere Fälle in sich begreift und eine von $x = -\pi$ bis $x = \pi$ ganz willkürlich gegebene Function $\varphi(x)$ darzustellen geeignet ist. — Bringt man nämlich $\varphi(x)$ in die Form:

$$\frac{\varphi(x)+\varphi(-x)}{2} + \frac{\varphi(x)-\varphi(-x)}{2},$$

so hat der erste Theil $\frac{\varphi(x)+\varphi(-x)}{2}$ die Eigenschaft, durch Verwandlung von x in $-x$ unverändert zu bleiben, und ist also nach dem Vorhergehenden von $x = -\pi$ bis $x = \pi$ durch (14) ausdrückbar. Eben so lässt sich offenbar der zweite Theil $\frac{\varphi(x)-\varphi(-x)}{2}$ durch die Reihe (13) darstellen, und man hat also für den ganzen Umfang des Intervalls von $-\pi$ bis π, wenn man beide Theile vereinigt:

$$(15) \qquad \begin{cases} \varphi(x) = \frac{1}{2}b_0 + b_1\cos x + b_2\cos 2x + \cdots + b_m\cos mx + \cdots \\ \qquad + a_1\sin x + a_2\sin 2x + \cdots + a_m\sin mx + \cdots, \end{cases}$$

wo die Coefficienten durch die Gleichungen:

$$b_m = \frac{1}{\pi}\int_0^\pi \cos mx[(\varphi x)+\varphi(-x)]dx,$$

$$a_m = \frac{1}{\pi}\int_0^\pi \sin mx[\varphi(x)-\varphi(-x)]dx$$

zu bestimmen sind. Man kann diesen Ausdrücken eine einfachere Form geben. Es ist nämlich:

$$\int_0^\pi \cos mx[\varphi(x)+\varphi(-x)]dx = \int_0^\pi \cos mx\,\varphi(x)dx + \int_0^\pi \cos mx\,\varphi(-x)dx$$

und nach (5):

$$\int_0^\pi \cos mx\,\varphi(-x)dx = -\int_0^{-\pi} \cos mx\,\varphi(x)dx,$$

oder nach (2), $= \int_{-\pi}^{0} \cos mx\,\varphi(x)dx$, folglich:

$$b_m = \frac{1}{\pi}\left(\int_{-\pi}^{0} \cos mx\,\varphi(x)dx + \int_0^\pi \cos mx\,\varphi(x)dx\right)$$

oder nach (9):

$$b_m = \frac{1}{\pi}\int_{-\pi}^{+\pi} \cos mx\,\varphi(x)dx.$$

Ebenso ergiebt sich:

$$a_m = \frac{1}{\pi}\int_{-\pi}^{+\pi} \sin mx\,\varphi(x)dx.$$

§. 4.

Wie natürlich und wie befriedigend auch auf den ersten Blick der Gang erscheinen mag, welcher uns zu den Reihen des vorigen Paragraphen geführt hat, so findet man doch bald bei genauerer Erwägung, dass derselbe als strenger Beweis für die Gültigkeit dieser Reihen etwas zu wünschen übrig lässt. Es geht aus dem Begriff des bestimmten Integrals, wie dieser in (1) festgestellt wurde, unbestreitbar hervor, dass irgend ein Coefficient a_m, welcher in der endlichen Reihe eine bestimmte Stelle m einnimmt, bei unaufhörlichem Wachsen von n in das Integral $\frac{2}{\pi}\int_0^\pi \sin mx f(x)dx$ übergeht, allein man darf nicht vergessen, dass durch das Zunehmen von n zugleich immer mehr neue Glieder hinzukommen. Um die Richtigkeit der Reihe (13) zu beweisen, müsste man sich die Glieder der endlichen Reihe in zwei Gruppen zerfällt denken; die erste würde alle Glieder bis zu einer bestimmten unveränderlich gedachten Stellenzahl m, die zweite alle übrigen enthalten. Könnte man nun zeigen, dass, während die Coefficienten der Glieder der ersten Gruppe sich ins Unendliche den durch bestimmte Integrale ausgedrückten Werthen nähern, der Inbegriff aller Glieder der zweiten, deren Anzahl mit n unaufhörlich wächst, nie eine gewisse von m abhängige und zwar beliebig klein ausfallende Grenze überschreitet, wenn man das m gehörig gross wählte, so würde man die Gewissheit erlangen, dass die Reihe (13) convergirend ist und die Function $f(x)$ für das Intervall von 0 bis π wirklich darstellt. — Die Nothwendigkeit der eben angedeuteten Nachweisung, wenn man den Uebergang vom Endlichen zum Unendlichen zu einem ganz strengen Verfahren erheben will, wird im höchsten

Grade einleuchtend, wenn man der endlichen Reihe, von der man ausgeht, eine andere Form giebt. Betrachtet man eine Reihe von der Form:

$$a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1},$$

so lassen sich die Coefficienten ebenfalls leicht so bestimmen, dass die Reihe für n Werthe von x innerhalb eines beliebigen Intervalls einer ganz willkürlichen Function $f(x)$ gleich wird. Lässt man nach erlangter Bestimmung irgend eines Coefficienten n unendlich wachsen, während die Stellenzahl m der Coefficienten constant bleibt, so nähert sich der Coefficient unaufhörlich einem gewissen Endwerth, und man würde also durch das im vorigen Paragraphen befolgte Verfahren zu der falschen Folgerung verleitet, eine ganz gesetzlose oder stellenweise ganz anderen Gesetzen gehorchende Function lasse sich durch eine nach Potenzen der Veränderlichen x geordnete Reihe darstellen.

Die Betrachtungen, die dem Verfahren, welches uns die Reihe (13) geliefert hat, die gehörige Strenge geben würden, sind so zusammengesetzter Art, dass wir lieber einen andern Weg der Beweisführung einschlagen. Wir werden die Reihe (15), welche die beiden andern (13) und (14) als besondere Fälle in sich begreift, an und für sich untersuchen und, ohne etwas von dem Früheren vorauszusetzen, direct nachweisen, dass diese Reihe:

$$\begin{aligned}&\tfrac{1}{2}b_0+b_1\cos x+b_2\cos 2x+\cdots+b_m\cos mx+\cdots\\&\quad+a_1\sin x+a_2\sin 2x+\cdots+a_m\sin mx+\cdots,\end{aligned}$$

wenn man ihre Coefficienten durch die Gleichungen:

$$b_m=\frac{1}{\pi}\int_{-\pi}^{+\pi}\cos mx\varphi(x)dx,\qquad a_m=\frac{1}{\pi}\int_{-\pi}^{+\pi}\sin mx\varphi(x)dx$$

bestimmt, immer convergirt und für alle zwischen $-\pi$ und π enthaltenen Werthe von x der Function $\varphi(x)$ gleich ist.

Schreibt man in den vorhergehenden Integralen statt x einen andern Buchstaben α, was offenbar erlaubt ist, da ein bestimmtes Integral nur von der Natur der Function und den Werthen der Grenzen abhängig ist, und setzt die Werthe für die $2n+1$ ersten Coefficienten ein, so erhält man als Summe der $2n+1$ ersten Glieder der Reihe:

$$\begin{aligned}&\frac{1}{2\pi}\int_{-\pi}^{+\pi}d\alpha\varphi(\alpha)+\frac{1}{\pi}\cos x\int_{-\pi}^{+\pi}d\alpha\cos\alpha\varphi(\alpha)+\cdots+\frac{1}{\pi}\cos nx\int_{-\pi}^{+\pi}d\alpha\cos n\alpha\varphi(\alpha)\\&+\frac{1}{\pi}\sin x\int_{-\pi}^{+\pi}d\alpha\sin\alpha\varphi(\alpha)+\cdots+\frac{1}{\pi}\sin nx\int_{-\pi}^{+\pi}d\alpha\sin n\alpha\varphi(\alpha)\end{aligned}$$

oder nach (3) und (6):

$$\frac{1}{\pi}\int_{-\pi}^{+\pi}d\alpha\varphi(\alpha)[\tfrac{1}{2}+\cos(\alpha-x)+\cos 2(\alpha-x)+\cdots+\cos n(\alpha-x)]$$

oder endlich, wenn man die Cosinusreihe vermittelst der Formel (11) summirt:

$$\frac{1}{\pi}\int_{-\pi}^{+\pi}d\alpha\varphi(\alpha)\frac{\sin(2n+1)\frac{\alpha-x}{2}}{2\sin\frac{\alpha-x}{2}}.$$

Soll also die Reihe convergiren und den Werth $\varphi(x)$ haben, so muss der Unterschied zwischen $\varphi(x)$ und diesem Integral, welches die Summe ihrer $2n+1$ ersten Glieder ausdrückt, bei unaufhörlichem Zunehmen von n zuletzt kleiner werden als jede noch so klein gedachte Grösse. Es ist nöthig, der Untersuchung dieses Integrals in seiner ganzen Allgemeinheit die Behandlung einiger einfachen Fälle vorauszuschicken, auf welche sich alle übrigen zurückführen lassen.

§. 5.

Man betrachte zunächst das Integral:

$$\int_0^{\frac{\pi}{2}}\frac{\sin(2n+1)\beta}{\sin\beta}d\beta,$$

in welchem n wie vorher eine positive ganze Zahl bezeichnet. Setzt man statt $\frac{\sin(2n+1)\beta}{\sin\beta}$ den nach (11) äquivalenten Ausdruck:

$$1+2\cos 2\beta+2\cos 4\beta+\cdots+2\cos 2n\beta,$$

so erhellt nach (10), dass alle Glieder mit Ausnahme des ersten zwischen den angegebenen Grenzen integrirt verschwinden, und man findet:

$$\int_0^{\frac{\pi}{2}}\frac{\sin(2n+1)\beta}{\sin\beta}d\beta=\frac{\pi}{2}.$$

Setzt man zur Abkürzung $2n+1=k$ und zerlegt das Integral in $n+1$ andere zwischen den Grenzen 0 und $\frac{\pi}{k}$, $\frac{\pi}{k}$ und $\frac{2\pi}{k}$, …, $\frac{n\pi}{k}$ und $\frac{\pi}{2}$, so folgt nach (7), dass von diesen Integralen das erste positiv, das zweite negativ, das dritte positiv u. s. w. sein wird, da $\frac{\sin k\beta}{\sin\beta}$ innerhalb der Grenzen des ersten positiv, des zweiten negativ u. s. w. ist. Bezeichnet man das Integral des Ranges ν,

d. h. das von $\frac{(\nu-1)\pi}{k}$ bis $\frac{\nu\pi}{k}$ genommene, abgesehen von seinem Zeichen, mit ϱ_ν, so dass also:

$$\varrho_\nu = \mp\int_{\frac{(\nu-1)\pi}{k}}^{\frac{\nu\pi}{k}} \frac{\sin k\beta}{\sin\beta}\, d\beta,$$

wo das obere oder untere Zeichen gilt, je nachdem ν gerade oder ungerade ist, so folgt leicht aus (8), da $\mp\sin k\beta$ von $\frac{(\nu-1)\pi}{k}$ bis $\frac{\nu\pi}{k}$ stets positiv bleibt, dass ϱ_ν zwischen den beiden Producten liegt, welche man erhält, wenn man:

$$\int_{\frac{(\nu-1)\pi}{k}}^{\frac{\nu\pi}{k}} \mp\sin k\beta d\beta = \frac{2}{k}$$

mit dem grössten und kleinsten Werth multiplicirt, den der Factor $\frac{1}{\sin\beta}$ in dem genannten Intervall annimmt.

Das vorhergehende Integral ist nach (4):

$$= \int_0^{\frac{\pi}{k}} \mp\sin((\nu-1)\pi + k\beta)d\beta = \int_0^{\frac{\pi}{k}} \sin k\beta d\beta,$$

oder nach (5):

$$= \frac{1}{k}\int_0^{\pi} \sin\beta d\beta = \frac{A}{k},$$

wenn man zur Abkürzung den von k unabhängigen Werth $\int_0^{\pi}\sin\beta d\beta$ mit A bezeichnet.

Was den Factor $\frac{1}{\sin\beta}$ betrifft, so ist dieser um so kleiner, als β grösser ist. Sein grösster Werth ist daher $\frac{1}{\sin\frac{(\nu-1)\pi}{k}}$ und der kleinste $\frac{1}{\sin\frac{\nu\pi}{k}}$, so dass also:

$$\varrho_\nu > \frac{A}{k}\frac{1}{\sin\frac{\nu\pi}{k}} \quad \text{und} \quad \varrho_\nu < \frac{A}{k}\frac{1}{\sin\frac{(\nu-1)\pi}{k}}.$$

Für das letzte Integral ϱ_{n+1} gelten die Grenzen $\frac{A}{k}$ und $\frac{A}{k}\frac{1}{\sin\frac{n\pi}{k}}$, die sich auf dieselbe Weise ergeben. Vergleicht man die Grenzen, zwischen welchen

je zwei auf einander folgende Integrale liegen, so ergiebt sich auf der Stelle, dass $\varrho_1, \varrho_2, \varrho_3, \ldots, \varrho_{n+1}$ eine abnehmende Reihe bilden, d. h.:

$$\varrho_1 > \varrho_2 > \varrho_3 > \cdots > \varrho_{n+1}.$$

Das ursprüngliche, später in $n+1$ andre Integrale zerlegte Integral hatte den Werth $\frac{\pi}{2}$. Es findet also folgende Gleichung statt:

$$\frac{\pi}{2} = \varrho_1 - \varrho_2 + \varrho_3 - \varrho_4 + \cdots \pm \varrho_{n+1}.$$

Aus der Abnahme der Glieder $\varrho_1, \varrho_2, \ldots$ folgt leicht, wenn man die Reihe bei ihrem $2m^{\text{ten}}$ und $(2m+1)^{\text{ten}}$ Gliede abbricht (wo natürlich $2m < n$):

$$(16) \qquad \begin{cases} \frac{\pi}{2} > \varrho_1 - \varrho_2 + \varrho_3 - \cdots - \varrho_{2m}, \\ \frac{\pi}{2} < \varrho_1 - \varrho_2 + \varrho_3 - \cdots - \varrho_{2m} + \varrho_{2m+1}. \end{cases}$$

Um sich zu überzeugen, dass diese Ungleichheiten stattfinden, darf man nur bemerken, dass im ersten Falle die weggebrachten Glieder, wenn man sie paarweise vereinigt, $\varrho_{2m+1} - \varrho_{2m+2}, \varrho_{2m+3} - \varrho_{2m+4}, \ldots$, positive Differenzen geben, und dass man also etwas positives weglässt, und das Umgekehrte für den zweiten gilt.

Wir wenden uns jetzt zu der Betrachtung des Integrals:

$$\int_0^h \frac{\sin k\beta}{\sin\beta} f(\beta) d\beta = S,$$

wo h eine positive $\frac{\pi}{2}$ nicht übersteigende Constante und $f(\beta)$ eine stetige Function von β bezeichnet, welche, während β von 0 bis h wächst, immer positiv bleibt und nie zunimmt. Ich sage absichtlich, nie zunimmt, um den Fall nicht auszuschliessen, wo $f(\beta)$ stellenweise oder für das ganze Intervall constant bliebe. Der Buchstabe k ist nur zur Abkürzung für $2n+1$ eingeführt, und wir wollen untersuchen, wie sich S verändert, wenn n ohne Grenze wächst. Es sei $r\frac{\pi}{k}$ das grösste in h enthaltene Vielfache von $\frac{\pi}{k}$, wo offenbar die ganze Zahl r nicht grösser als n sein kann, und man zerlege das Integral in $r+1$ andere, zwischen den Grenzen 0 und $\frac{\pi}{k}$, $\frac{\pi}{k}$ und $\frac{2\pi}{k}$, $\ldots$, $\frac{r\pi}{k}$ und h, so sind diese Integrale wieder abwechselnd positiv und negativ. Bezeichnet man dasjenige, welches die ν^{te} Stelle einnimmt, abgesehen von seinem Zeichen,

mit R_ν, so dass also:

$$R_\nu = \mp\int_{\frac{(\nu-1)\pi}{k}}^{\frac{\nu\pi}{k}} \frac{\sin k\beta}{\sin\beta} f(\beta)\,d\beta.$$

wo wieder das obere oder das untere Zeichen gilt, je nachdem ν gerade oder ungerade ist, so hat man:

$$S = R_1 - R_2 + R_3 - \cdots \pm R_{r+1}.$$

Die positiven Werthe $R_1, R_2, R_3, \ldots$ bilden eine abnehmende Reihe, wie man sich leicht überzeugt, wenn man auf R_ν den Satz (8) anwendet. Man findet unter Berücksichtigung der über $f(\beta)$ gemachten Voraussetzung, dass:

$$R_\nu = \int_{\frac{(\nu-1)\pi}{k}}^{\frac{\nu\pi}{k}} \mp\frac{\sin k\beta}{\sin\beta} f(\beta)\,d\beta$$

zwischen den beiden Producten:

$$f\left(\frac{\nu\pi}{k}\right)\int_{\frac{(\nu-1)\pi}{k}}^{\frac{\nu\pi}{k}} \mp\frac{\sin k\beta}{\sin\beta}\,d\beta \quad \text{und} \quad f\left(\frac{(\nu-1)\pi}{k}\right)\int_{\frac{(\nu-1)\pi}{k}}^{\frac{\nu\pi}{k}} \mp\frac{\sin k\beta}{\sin\beta}\,d\beta$$

liegt, d. h. also:

$$R_\nu > \varrho_\nu f\left(\frac{\nu\pi}{k}\right), \quad R_\nu < \varrho_\nu f\left(\frac{(\nu-1)\pi}{k}\right)^*).$$

Vergleicht man die untere Grenze $\varrho_\nu f\left(\frac{\nu\pi}{k}\right)$ für R_ν mit der obern für $R_{\nu+1}$, welche $\varrho_{\nu+1} f\left(\frac{\nu\pi}{k}\right)$ ist, so folgt wegen $\varrho_\nu > \varrho_{\nu+1}$, dass auch $R_\nu > R_{\nu+1}$, wie vorher behauptet wurde. Bricht man die Reihe S bei R_{2m} und R_{2m+1} ab (wo $2m < r$), so ergeben sich die Ungleichheiten:

$$S > R_1 - R_2 + R_3 - \cdots - R_{2m},$$
$$S < R_1 - R_2 + R_3 - \cdots - R_{2m} + R_{2m+1}.$$

Die erste dieser Ungleichheiten wird nicht aufhören, richtig zu bleiben, wenn man statt der zu addirenden Glieder $R_1, R_3, \ldots$ ihre unteren Grenzen $\varrho_1 f\left(\frac{\pi}{k}\right), \varrho_3 f\left(\frac{3\pi}{k}\right), \ldots$ und statt der zu subtrahirenden $R_2, R_4, \ldots$ ihre oberen

*) Wäre $f\left(\frac{\nu\pi}{k}\right) = f\left(\frac{(\nu-1)\pi}{k}\right)$, so würden die beiden Grenzen zusammenfallen, und man muss um alle Fälle zu umfassen, mit dem Zeichen $t > w$ den Sinn verbinden, dass t nicht kleiner als w ist.

Grenzen $\varrho_2 f\left(\frac{\pi}{k}\right), \varrho_4 f\left(\frac{3\pi}{k}\right), \ldots$ setzt. Hierdurch und durch Anwendung des umgekehrten Verfahrens auf die untere Ungleichheit erhält man:

$$S > (\varrho_1 - \varrho_2) f\left(\frac{\pi}{k}\right) + (\varrho_3 - \varrho_4) f\left(\frac{3\pi}{k}\right) + \cdots + (\varrho_{2m-1} - \varrho_{2m}) f\left(\frac{(2m-1)\pi}{k}\right),$$
$$S < \varrho_1 f(0) - (\varrho_2 - \varrho_3) f\left(\frac{2\pi}{k}\right) - (\varrho_4 - \varrho_5) f\left(\frac{4\pi}{k}\right) - \cdots - (\varrho_{2m} - \varrho_{2m+1}) f\left(\frac{2m\pi}{k}\right).$$

Da die Differenzen $\varrho_1 - \varrho_2$, $\varrho_2 - \varrho_3$, $\varrho_3 - \varrho_4$, $\ldots$ positiv sind und die Function $f(\beta)$ nie zunimmt, so darf man offenbar in der ersten Ungleichheit $f\left(\frac{\pi}{k}\right)$, $f\left(\frac{3\pi}{k}\right), \ldots$ und in der zweiten $f\left(\frac{2\pi}{k}\right), f\left(\frac{4\pi}{k}\right), \ldots$ mit $f\left(\frac{2m\pi}{k}\right)$ vertauschen. Es ist also:

$$S > (\varrho_1 - \varrho_2 + \varrho_3 - \cdots - \varrho_{2m}) f\left(\frac{2m\pi}{k}\right),$$
$$S < \varrho_1 f(0) - (\varrho_2 - \varrho_3 + \varrho_4 - \cdots - \varrho_{2m+1}) f\left(\frac{2m\pi}{k}\right).$$

Die Zahl $2m$ ist kleiner als r, und also um so mehr kleiner als n, so dass die Resultate (16) stattfinden.

Die dort gefundenen Ungleichheiten lassen sich in die Form bringen:

$$\varrho_2 - \varrho_3 + \cdots + \varrho_{2m} > \varrho_1 - \frac{\pi}{2}, \quad \varrho_1 - \varrho_2 + \cdots - \varrho_{2m} > \frac{\pi}{2} - \varrho_{2m+1}.$$

Vergleicht man diese, nachdem man von beiden Seiten der ersten ϱ_{2m+1} abgezogen hat, mit den vorher erhaltenen Grenzen für S, so ergeben sich folgende höchst einfache Resultate:

$$S > \frac{\pi}{2} f\left(\frac{2m\pi}{k}\right) - \varrho_{2m+1} f\left(\frac{2m\pi}{k}\right),$$
$$S < \frac{\pi}{2} f\left(\frac{2m\pi}{k}\right) + \varrho_{2m+1} f\left(\frac{2m\pi}{k}\right) + \varrho_1 \left[f(0) - f\left(\frac{2m\pi}{k}\right)\right].$$

Unser Zweck war, die allmähliche Veränderung des Integrals:

$$S = \int_0^k \frac{\sin k\beta}{\sin\beta} f(\beta)\,d\beta$$

zu untersuchen, wenn man in demselben $k = 2n+1$ nimmt und die ganze Zahl n über jede Grenze hinaus wachsen lässt. Diese Frage wird auf der Stelle durch die eben gefundenen Ausdrücke beantwortet. Nach dem Früheren ist die darin enthaltene gerade Zahl $2m$ für ein bestimmtes n insofern noch willkürlich, als sie

jeden r nicht übersteigenden Werth haben kann, wo r wie früher das grösste in $\frac{h}{\pi}k = \frac{h}{\pi}(2n+1)$ enthaltene Ganze bezeichnet. Da hiernach r offenbar gleichzeitig mit n über jede Grenze hinaus wächst, so darf auch $2m$ jede Grenze überschreiten.

Denkt man sich nun das gleichzeitige Wachsen von $2m$ und n so, dass dabei $\frac{2m}{k}$ successive jeden Grad von Kleinheit erreicht, so werden die für S gefundenen Grenzen zuletzt zusammenfallen. Betrachtet man zunächst die untere Grenze:

$$\frac{\pi}{2} f\left(\frac{2m\pi}{k}\right) - \varrho_{2m+1} f\left(\frac{2m\pi}{k}\right),$$

so wird unter der angegebenen Voraussetzung ihr erstes Glied zuletzt in $\frac{\pi}{2}f(0)$ übergehen; was das zweite betrifft, so liegt der Factor ϱ_{2m+1} nach Obigem zwischen:

$$\frac{\Delta}{k}\frac{1}{\sin\frac{2m\pi}{k}} \quad \text{und} \quad \frac{\Delta}{k}\frac{1}{\sin\frac{(2m+1)\pi}{k}}.$$

Schreibt man diese in folgender Form:

$$\frac{\Delta}{2m\pi}\frac{\frac{2m\pi}{k}}{\sin\frac{2m\pi}{k}} \quad \text{und} \quad \frac{\Delta}{(2m+1)\pi}\frac{(2m+1)\frac{\pi}{k}}{\sin(2m+1)\frac{\pi}{k}},$$

so ist leicht zu sehen, dass beide zuletzt verschwinden. Durch das unaufhörliche Wachsen von m nähert sich $\frac{\Delta}{2m\pi}$ der Null, während $\frac{\frac{2m\pi}{k}}{\sin\frac{2m\pi}{k}}$ wegen des Abnehmens von $\frac{2m\pi}{k}$ sich der Einheit nähert. Das Product wird also Null, und dasselbe gilt von dem zweiten. Es geht hieraus hervor, dass die untere Grenze für S zuletzt mit $\frac{\pi}{2}f(0)$ zusammenfällt. Die beiden ersten Glieder in der oberen Grenze sind den schon untersuchten ganz ähnlich, und es bleibt uns nur noch das dritte $\varrho_i\left[f(0) - f\left(\frac{2m\pi}{k}\right)\right]$ zu betrachten. Der zweite Factor nähert sich offenbar der Null, und dieses Glied wird also verschwinden, wenn der erste nicht über jede Grenze hinaus wächst. Dass dieses

aber nicht der Fall ist, folgt sogleich aus den beiden Ungleichheiten:

$$\varrho_i < \frac{\pi}{2} + \varrho_2, \quad \varrho_2 < \frac{\Delta}{k}\frac{1}{\sin\frac{\pi}{k}},$$

von denen die erste aus (16) hervorgeht, wenn man dort $m = 1$ setzt. Beide mit einander verglichen ergeben:

$$\varrho_i < \frac{\pi}{2} + \frac{\Delta}{k}\frac{1}{\sin\frac{\pi}{k}},$$

und der Werth von:

$$\frac{\Delta}{k}\frac{1}{\sin\frac{\pi}{k}} \quad \text{oder} \quad \frac{\Delta}{\pi}\frac{\frac{\pi}{k}}{\sin\frac{\pi}{k}}$$

nähert sich durch das Wachsen von k dem Werthe $\frac{\Delta}{\pi}$.

Es ist somit streng bewiesen, dass die beiden Grenzen, zwischen denen S eingeschlossen ist, bei unaufhörlichem Wachsen von n zuletzt mit $\frac{\pi}{2}f(0)$ zusammenfallen, welcher Werth also auch der des Integrals:

$$\int_0^h \frac{\sin k\beta}{\sin\beta} f(\beta)\,d\beta$$

für ein unendlich grosses n ist.

Wir haben bisher vorausgesetzt, dass die Function $f(\beta)$, während β von 0 bis h wächst, nie zunimmt und ausserdem stets positiv bleibt. Behält man die erste Bedingung bei, d. h. setzt man voraus, dass für irgend zwei zwischen 0 und h fallende Werthe p und q die Differenz $f(p) - f(q)$ immer negativ oder Null ist, wenn $p - q$ positiv ist, ohne damit die zweite Annahme zu verbinden, dass $f(\beta)$ nicht negativ wird, so findet der vorige Satz ebenfalls noch statt. Nimmt man nämlich eine positive Constante c, welche so gross ist, dass $f(\beta) + c$ nicht negativ wird, so ist der Satz auf $f(\beta) + c$ anwendbar, d. h. das Integral:

$$\int_0^h [f(\beta) + c]\frac{\sin k\beta}{\sin\beta}\,d\beta$$

wird für ein unendlich grosses n:

$$\frac{\pi}{2}[f(0) + c].$$

Zugleich ist klar, dass dieses Integral die Summe von folgenden ist:

$$\int_0^h f(\beta)\frac{\sin k\beta}{\sin\beta}d\beta, \quad \int_0^h c\frac{\sin k\beta}{\sin\beta}d\beta,$$

von denen das zweite in demselben Falle $\frac{\pi}{2}c$ wird. (Es ist nämlich bei der vorigen Behandlung der Fall mit eingeschlossen worden, wo die positive Function im ganzen Intervall constant war). Also muss das erste durch unaufhörliches Wachsen von n zuletzt den Werth $\frac{\pi}{2}f(0)$ annehmen.

Denkt man sich jetzt eine Function $f(\beta)$, die, während β von 0 bis h wächst, nie abnimmt, so wird $-f(\beta)$ nie zunehmen. Man hat also, wenn n unendlich wächst:

$$\int_0^h -f(\beta)\frac{\sin k\beta}{\sin\beta}d\beta = -\frac{\pi}{2}f(0)$$

und folglich:

$$\int_0^h f(\beta)\frac{\sin k\beta}{\sin\beta}d\beta = \frac{\pi}{2}f(0).$$

Die vorhergehenden Resultate lassen sich in folgenden Satz zusammenfassen:

(17) Ist $f(\beta)$ eine stetige Function von β, die, während β von 0 bis h wächst $\left(\text{wo die Constante } h>0 \text{ und } \leq\frac{\pi}{2}\right)$, nie vom Abnehmen ins Zunehmen oder umgekehrt übergeht, so wird das Integral:

$$\int_0^h \frac{\sin(2n+1)\beta}{\sin\beta}f(\beta)d\beta,$$

wenn man darin der ganzen Zahl n immer grössere positive Werthe beilegt, zuletzt immerfort weniger als jede angebbare Grösse von $\frac{\pi}{2}f(0)$ verschieden sein.

Die Constante h bleibe den vorigen Bestimmungen unterworfen und man denke sich unter g eine zweite Constante, welche kleiner als h und zugleich positiv und von Null verschieden sei. Ist $f(\beta)$ eine für das Intervall von g bis h gegebene stetige Function von β, die, wenn β von g bis h wächst, nie vom Abnehmen ins Zunehmen oder umgekehrt übergeht, so lässt sich nach dem vorigen Satz leicht ermitteln, was aus dem Integral:

$$\int_g^h \frac{\sin(2n+1)\beta}{\sin\beta}f(\beta)d\beta$$

wird, wenn man n unendlich werden lässt. Da nämlich $f(\beta)$ bloss von $\beta=g$ bis $\beta=h$ gegeben ist, so bleibt die Art der Fortsetzung dieser Function über das genannte Intervall hinaus ganz willkürlich. Denkt man sich $f(\beta)$ für alle Werthe von β zwischen 0 und g incl. constant, und zwar $=f(g)$, so hat man eine von $\beta=0$ bis $\beta=h$ stetige Function, welche in diesem ganzen Intervall nie vom Abnehmen ins Zunehmen oder umgekehrt übergeht, und auf welche daher der vorige Satz anwendbar ist. Es wird daher das Integral:

$$\int_0^h \frac{\sin(2n+1)\beta}{\sin\beta}f(\beta)d\beta,$$

wenn man $n=\infty$ setzt, $=\frac{\pi}{2}f(0)=\frac{\pi}{2}f(g)$ sein. Zerlegt man dasselbe Integral in die folgenden:

$$\int_0^g \frac{\sin(2n+1)\beta}{\sin\beta}f(\beta)d\beta+\int_g^h \frac{\sin(2n+1)\beta}{\sin\beta}f(\beta)d\beta$$

so wird auch das erste $=\frac{\pi}{2}f(0)=\frac{\pi}{2}f(g)$ nach dem vorigen Satz, also muss das zweite für ein unendliches n verschwinden. Es gilt also der Satz:

(18) Sind g und h Constanten, welche den Bedingungen genügen $g>0$, $\frac{\pi}{2}\geq h>g$, und geht die Function $f(\beta)$, wenn β von g bis h wächst, nie vom Abnehmen ins Zunehmen oder umgekehrt über, so wird das Integral:

$$\int_g^h \frac{\sin(2n+1)\beta}{\sin\beta}f(\beta)d\beta$$

für ein unendlich grosses n der Null gleich.

Vermittelst der Sätze (17) und (18) ist es nun leicht, die zu Ende des §. 4. aufgestellte Behauptung zu beweisen.

§. 6.

Die Summe der $2n+1$ ersten Glieder der zu untersuchenden Reihe war durch das Integral:

$$\frac{1}{\pi}\int_{-\pi}^{+\pi} d\beta\varphi(\beta)\frac{\sin(2n+1)\frac{\beta-x}{2}}{2\sin\frac{\beta-x}{2}}$$

ausgedrückt. Wir haben früher vorausgesetzt, dass die Function $\varphi(\beta)$ für das ganze Intervall von $\beta = -\pi$ bis $\beta = \pi$ stetig ist; wir können aber, ohne die folgende Untersuchung im Geringsten zu erschweren, die Annahme machen, dass $\varphi(\beta)$ für einzelne Werthe von β eine plötzliche Veränderung erleidet, ohne jedoch unendlich zu werden. Die Curve, deren Abscisse β und deren Ordinate $\varphi(\beta)$ ist, besteht alsdann aus mehreren Stücken, deren Zusammenhang über den Punkten der Abscissenaxe, die jenen besonderen Werthen von β entsprechen, unterbrochen ist, und für jede solche Abscisse finden eigentlich zwei Ordinaten statt, wovon die eine dem dort endenden und die andere dem dort beginnenden Curvenstück angehört. Es wird im Folgenden nöthig sein, diese beiden Werthe von $\varphi(\beta)$ zu unterscheiden, und wir werden sie durch $\varphi(\beta-0)$ und $\varphi(\beta+0)$ bezeichnen. Um unnütze, die folgende Darstellung verlängernde Unterscheidungen zu vermeiden, bemerke man, dass dieselbe Bezeichnung auch für die Werthe von β gelten kann, für welche keine Unterbrechung der Stetigkeit stattfindet, wo dann natürlich $\varphi(\beta-0)$ und $\varphi(\beta+0)$ beide mit $\varphi(\beta)$ gleichbedeutend sind.

Das obige Integral lässt sich nach (9) in die folgenden zerlegen:

$$\frac{1}{\pi}\int_{-\pi}^{x} d\beta\varphi(\beta)\frac{\sin(2n+1)\frac{\beta-x}{2}}{2\sin\frac{\beta-x}{2}}, \quad \frac{1}{\pi}\int_{x}^{\pi} d\beta\varphi(\beta)\frac{\sin(2n+1)\frac{\beta-x}{2}}{2\sin\frac{\beta-x}{2}}.$$

oder nach (4):

$$\frac{1}{\pi}\int_{-(\pi+x)}^{0} d\beta\varphi(x+\beta)\frac{\sin(2n+1)\frac{\beta}{2}}{2\sin\frac{\beta}{2}}, \quad \frac{1}{\pi}\int_{0}^{\pi-x} d\beta\varphi(x+\beta)\frac{\sin(2n+1)\frac{\beta}{2}}{2\sin\frac{\beta}{2}}.$$

Wendet man (3) auf beide an und nachher noch (2) und (5) auf das erste, so kommt:

$$(19)\quad \frac{1}{\pi}\int_{0}^{\frac{\pi+x}{2}} d\beta\varphi(x-2\beta)\frac{\sin(2n+1)\beta}{\sin\beta}, \quad \frac{1}{\pi}\int_{0}^{\frac{\pi-x}{2}} d\beta\varphi(x+2\beta)\frac{\sin(2n+1)\beta}{\sin\beta}.$$

Wir betrachten jetzt das zweite dieser Integrale, abgesehen von dem constanten Factor $\frac{1}{\pi}$. Da x zwischen $-\pi$ und $+\pi$ liegt, so liegt $\frac{\pi-x}{2}$ zwischen 0 und π. Ist $\frac{\pi-x}{2} = 0$, was für $x = \pi$ der Fall ist, so ist das Integral für jedes n Null und erfordert keine weitere Untersuchung. Nehmen wir zunächst an, $\frac{\pi-x}{2}$ sei nicht grösser als $\frac{\pi}{2}$. Man bezeichne mit $e_1, e_2, \ldots, e_\nu$, wie sie der Grösse nach auf einander folgen, die Werthe von β, für welche *erstens* $\varphi(x+2\beta)$ innerhalb des Intervalls von $\beta = 0$ bis $\beta = \frac{\pi-x}{2}$ eine Unterbrechung der Stetigkeit erleidet und *zweitens* vom Zunehmen ins Abnehmen oder vom Abnehmen ins Zunehmen übergeht, und zerlege das Integral in andere zwischen den Grenzen 0 und e_1, e_1 und e_2, $\ldots$, e_ν und $\frac{\pi-x}{2}$ genommen. Auf alle diese neuen Integrale, mit Ausnahme des ersten, ist der Satz (18) offenbar anwendbar, da innerhalb der Grenze eines jeden die Function keine Unterbrechung der Stetigkeit erleidet und nicht vom Abnehmen ins Zunehmen oder umgekehrt übergeht: alle nähern sich daher ins Unendliche der Null, wenn man n über alle Grenzen hinaus wachsen lässt. Das erste hingegen erfüllt die Bedingungen (17) und geht bei unaufhörlichem Wachsen von n zuletzt in den Werth $\frac{\pi}{2}\varphi(x+0)$ über. Also wird das Integral:

$$\int_{0}^{\frac{\pi-x}{2}} d\beta\varphi(x+2\beta)\frac{\sin(2n+1)\beta}{\sin\beta}$$

für $n = \infty$ den Werth $\frac{\pi}{2}\varphi(x+0)$ annehmen.

Liegt $\frac{\pi-x}{2}$ über $\frac{\pi}{2}$ oder ist x negativ, so zerlege man das vorige Integral in zwei andere zwischen den Grenzen 0 und $\frac{\pi}{2}$, $\frac{\pi}{2}$ und $\frac{\pi-x}{2}$. Auf das erste dieser neuen Integrale bleibt das vorige Verfahren anwendbar, und dasselbe wird also $\frac{\pi}{2}\varphi(x+0)$, wenn man n unendlich gross werden lässt. Das andere:

$$\int_{\frac{\pi}{2}}^{\frac{\pi-x}{2}} d\beta\varphi(x+2\beta)\frac{\sin(2n+1)\beta}{\sin\beta}$$

kann nach (4) und (5) in die Form gebracht werden:

$$-\int_{\frac{\pi}{2}}^{\frac{(\pi+x)}{2}} d\beta\varphi(x+2\pi-2\beta)\frac{\sin(2n+1)(\pi-\beta)}{\sin(\pi-\beta)}.$$

Wendet man (2) an, und setzt $\sin\beta$ statt $\sin(\pi-\beta)$ und $\sin(2n+1)\beta$ statt $\sin(2n+1)(\pi-\beta)$ (da n eine ganze Zahl ist), so geht das Integral über in:

$$\int_{\frac{\pi+x}{2}}^{\frac{\pi}{2}} \varphi(x+2\pi-2\beta)\frac{\sin(2n+1)\beta}{\sin\beta}\,d\beta.$$

Da x, wie vorher gesagt wurde, in diesem Falle negativ ist und also zwischen 0 und $-\pi$ liegt, so ist $\frac{\pi+x}{2}$ positiv und von Null verschieden, den einzigen Fall ausgenommen, wo $x=-\pi$. Zerlegt man das Integral in andere, zwischen deren Grenzen $\varphi(x+2\pi-2\beta)$ weder eine Unterbrechung der Continuität erleidet noch aus dem Zunehmen ins Abnehmen oder umgekehrt übergeht, so werden alle diese Integrale nach (18) für $n=\infty$ der Null gleich. Dieses Resultat gilt nicht, wenn $\frac{\pi+x}{2}=0$ und also $x=-\pi$, da alsdann auf das erste der durch Zerlegung entstehenden Integrale nicht der Satz (18) sondern der Satz (17) angewendet werden muss. Dieses erste Integral ist alsdann (wegen $x=-\pi$):

$$\int_0^{\varepsilon} d\beta\,\varphi(x+2\pi-2\beta)\frac{\sin(2n+1)\beta}{\sin\beta} = \int_0^{\varepsilon} d\beta\,\varphi(\pi-2\beta)\frac{\sin(2n+1)\beta}{\sin\beta}$$

und wird also für $n=\infty$ den Werth $\frac{\pi}{2}\varphi(\pi-0)$ erhalten, während alle übrigen verschwinden.

Vereinigt man die verschiedenen für das zweite Integral (19) gefundenen Resultate, so ergiebt sich, dass dieses Integral durch unaufhörliches Wachsen der darin enthaltenen ganzen Zahl n für jedes zwischen $-\pi$ und $+\pi$ gelegene x in den Werth $\frac{1}{2}\varphi(x+0)$ übergeht. Für $x=\pi$ und $x=-\pi$ erleidet das Resultat eine Ausnahme; in dem erstern Falle ist das Integral Null, im andern wird es $\frac{1}{2}[\varphi(\pi-0)+\varphi(-\pi+0)]$. Aus einer ganz ähnlichen Untersuchung des ersten Integrals (19) folgt, dass dasselbe für $n=\infty$ im Allgemeinen $\frac{1}{2}\varphi(x-0)$ wird, aber in den besondern Fällen, $x=-\pi$ und $x=\pi$, respective Null und $\frac{1}{2}[\varphi(\pi-0)+\varphi(-\pi+0)]$.

Erinnert man sich nun, dass die beiden Integrale (19) zusammengenommen die Summe der $2n+1$ ersten Glieder der Reihe darstellen:

$$(20)\qquad \begin{cases} \frac{1}{2}b_0+b_1\cos x+b_2\cos 2x+\cdots+b_m\cos mx+\cdots \\ \quad +a_1\sin x+a_2\sin 2x+\cdots+a_m\sin mx+\cdots, \end{cases}$$

wo die Coefficienten durch die Gleichungen:

$$b_m=\frac{1}{\pi}\int_{-\pi}^{+\pi} d\beta\,\varphi(\beta)\cos m\beta, \quad a_m=\frac{1}{\pi}\int_{-\pi}^{+\pi} d\beta\,\varphi(\beta)\sin m\beta$$

zu bestimmen sind, so geht aus dem Vorhergehenden ganz streng hervor, dass diese Reihe immer convergirt, d. h. dass es immer einen gewissen Werth giebt, von dem die Summe der $2n+1$ ersten Glieder der Reihe, wenn n über alle Grenzen hinaus wachsend gedacht wird, zuletzt immerfort um weniger als jede angebbare Grösse verschieden sein wird, und dass dieser Werth oder die Summe der unendlichen Reihe, wenn x zwischen $-\pi$ und π liegt, durch $\frac{1}{2}[\varphi(x+0)+\varphi(x-0)]$, für $x=\pi$ und $x=-\pi$ aber durch $\frac{1}{2}[\varphi(\pi-0)+\varphi(-\pi+0)]$ dargestellt wird.

Dieses Resultat umfasst alle Fälle; ist x keiner von den besondern Werthen, für welche die Stetigkeit von $\varphi(x)$ unterbrochen wird, so sind $\varphi(x+0)$ und $\varphi(x-0)$ einander gleich, und der Werth der Reihe wird also $\varphi(x)$. Wo eine Unterbrechung der Stetigkeit eintritt und also die Function $\varphi(x)$ eigentlich zwei Werthe hat, stellt die Reihe, welche ihrer Natur nach für jedes x einwerthig ist, die halbe Summe dieser Werthe dar. An den Grenzen des Intervalls von $-\pi$ bis $+\pi$, d. h. für diese Werthe selbst, ist die Summe der unendlichen Reihe gleich der halben Summe der beiden Werthe $\varphi(\pi)$ und $\varphi(-\pi)$. Man sieht daraus, dass die Reihe die Function $\varphi(x)$ an den Grenzen des Intervalls nur dann richtig darstellt, wenn $\varphi(\pi)=\varphi(-\pi)$ ist.

Wir haben schon früher bemerkt, dass die eben untersuchte Reihe (20) oder (15) die Reihen (13) und (14) als specielle Fälle in sich begreift. Man braucht sich nur die Function $\varphi(x)$ für den halben Umfang des Intervalls, nämlich $x=0$ bis $x=\pi$, als ganz beliebig gegeben zu denken und für die Werthe zwischen 0 und $-\pi$ fortgesetzt zu denken, wie es die Gleichungen $\varphi(-x)=\varphi(x)$ oder $\varphi(-x)=-\varphi(x)$ vorschreiben, um respective zu (14) und (13) zu gelangen. Ich will dies noch mit zwei Worten für den ersten Fall zeigen, weil sich aus dieser Ableitung eine Eigenschaft der Reihe (14) ergiebt, welche bei der frühern Behandlung nicht hervortrat.

Setzt man die von 0 bis π beliebige Function $\varphi(x)$ nach der Gleichung $\varphi(-x)=\varphi(x)$ fort, so ist klar, dass für $x=0$ keine Unterbrechung der Stetigkeit eintreten und dass $\varphi(-\pi)=\varphi(\pi)$ sein wird. Die Reihe (20) wird also $\varphi(0)$ für $x=0$, und $\varphi(\pi)$ für $x=\pi$. Die Gleichungen für die Coefficienten

werden durch Zerlegung der darin enthaltenen Integrale:

$$b_m = \frac{1}{\pi}\int_{-\pi}^{0} d\beta\varphi(\beta)\cos m\beta + \frac{1}{\pi}\int_{0}^{\pi} d\beta\varphi(\beta)\cos m\beta,$$

$$a_m = \frac{1}{\pi}\int_{-\pi}^{0} d\beta\varphi(\beta)\sin m\beta + \frac{1}{\pi}\int_{0}^{\pi} d\beta\varphi(\beta)\sin m\beta.$$

Wendet man auf die beiden von $-\pi$ bis 0 genommenen Integrale nach einander (5) und (2) an und berücksichtigt, dass:

$$\varphi(-\beta) = \varphi(\beta), \quad \cos(-m\beta) = \cos m\beta, \quad \sin(-m\beta) = -\sin m\beta,$$

so erhält man:

$$b_m = \frac{2}{\pi}\int_{0}^{\pi} d\beta\varphi(\beta)\cos m\beta, \quad a_m = 0.$$

Die von $x = 0$ bis $x = \pi$ ganz beliebig gegebene Function $\varphi(x)$ wird also durch die Reihe:

$$\tfrac{1}{2}b_0 + b_1\cos x + b_2\cos 2x + \cdots + b_m\cos mx + \cdots$$

dargestellt, welche auch für die das Intervall begrenzenden Werthe 0 und π noch gültig ist. Es versteht sich dabei von selbst, dass, wenn $\varphi(x)$ zwischen 0 und π eine Unterbrechung der Stetigkeit erleidet, die Reihe für jeden solchen Werth von x die halbe Summe der entsprechenden Werthe von $\varphi(x)$ ausdrückt. Auf ganz ähnliche Weise gelangt man zu der Reihe (13) und findet, dass diese im Allgemeinen für $x = 0$ und $x = \pi$ nicht mehr richtig ist, was sich aber in diesem Fall ganz von selbst versteht, da die Reihe, wie auch ihre Coefficienten beschaffen sein mögen, für die genannten Werthe verschwindet.

SOLUTION D'UNE QUESTION RELATIVE A LA THÉORIE MATHÉMATIQUE DE LA CHALEUR.

PAR

M. G. LEJEUNE DIRICHLET,
PROF. DE MATH.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 5 p. 287—295.

SOLUTION D'UNE QUESTION RELATIVE A LA THÉORIE MATHÉMATIQUE DE LA CHALEUR.

La question qui va nous occuper et qui a pour objet de déterminer les états successifs d'une barre primitivement échauffée d'une manière quelconque et dont les deux extrémités sont entretenues à des températures données en fonction du temps, a déjà été résolue par M. Fourier dans un Mémoire inséré dans le Vol. VIII de la collection de l'Académie Royale des Sciences de Paris. La méthode dont cet illustre géomètre a fait usage dans cette recherche est une espèce singulière de passage du fini à l'infini, et offre un nouvel exemple de la fécondité de ce procédé analytique qui avait déjà conduit l'auteur à tant de résultats remarquables dans son grand ouvrage sur la théorie de la chaleur. J'ai traité la même question par une analyse dont la marche diffère beaucoup de celle de M. Fourier et qui donne lieu à l'emploi de quelques artifices de calcul, qui paraissent pouvoir être utiles dans d'autres recherches.

Pour simplifier les calculs, nous supposerons l'unité linéaire qui est arbitraire, tellement choisie que la longueur de la barre soit égale à π, cette lettre désignant à l'ordinaire le rapport du diamètre à la circonférence. Soit x la distance d'un point quelconque de la barre à l'une de ses extrémités, que nous nommerons la première extrémité. La température du point x à l'instant t est une fonction u de x et de t, et c'est cette fonction qui fait l'objet de la question. Soit $F(t)$ la fonction donnée de t qui exprime la température à laquelle la première extrémité est entretenue, et soit de même $f(t)$ la température de la sesonde extrémité, $F(t)$ et $f(t)$ étant des fonctions arbitraires dont les valeurs sont données pour toute valeur positive de t, et désignons enfin par $\varphi(x)$ la température initiale du point dont l'abscisse est x.

En faisant abstraction du rayonnement latéral, la fonction u doit satisfaire à cette équation aux différences partielles $\frac{\partial u}{\partial t} = k\frac{\partial^2 u}{\partial x^2}$ dans laquelle k désigne un coefficient dépendant des propriétés spécifiques de la substance dont la barre est formée.

Pour plus de simplicité, nous supposerons égal à l'unité le coefficient k qu'il sera facile de rétablir à la fin du calcul, de sorte que l'équation précédente se changera en celle-ci:

$$\frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2}. \tag{1}$$

Cela posé, la fonction cherchée doit évidemment remplir les quatre conditions suivantes:

(2)
1°. Elle doit satisfaire à l'équation (1) quels que soient x et t.
2°. Pour $x = 0$, elle doit se réduire à la fonction donnée $F(t)$.
3°. Pour $x = \pi$, elle doit se réduire à la fonction $f(t)$ également donnée.
4°. Lorsque t est nul, elle doit coïncider dans toute l'étendue de la barre, c'est-à-dire tant que x est inférieur à π, avec la fonction $\varphi(x)$ qui exprime les températures initiales.

La question que nous avons à résoudre se partage naturellement en deux autres. On fera d'abord abstraction de la quatrième condition et l'on cherchera une fonction v de x et de t uniquement assujettie à remplir les 3 premières. Il y a une infinité de fonctions qui satisfont à ces 3 conditions, et qui diffèrent entre elles en ce qu'elles se réduisent à des fonctions de x différentes entre elles par la supposition de $t = 0$; mais il suffit d'en obtenir une seule. Une pareille fonction v étant trouvée, on y fera $t = 0$, ce qui la réduira à une fonction $\chi(x)$ de x. On formera ensuite la différence $\varphi(x) - \chi(x)$ et l'on cherchera la fonction entièrement déterminée w de x et de t, qui satisfait à l'équation (1), s'évanouit pour $x = 0$ et $x = \pi$ quel que soit t, et se réduit à $\varphi(x) - \chi(x)$ lorsqu'on y fait $t = 0$.

Cette seconde question est résolue depuis longtemps, c'est celle de la détermination du mouvement de la chaleur dans une barre dont l'état initial est exprimé par $\varphi(x) - \chi(x)$ et dont les extrémités sont entretenues à la température zéro. Les deux fonctions v et w dont il vient d'être question, étant

ajoutées, formeront une nouvelle fonction de x et de t, qui remplit l'ensemble des conditions (2). En effet, chacune d'elles satisfaisant à l'équation (1), leur somme y satisfera également. La première se réduisant à $F(t)$ pour $x = 0$, et la seconde s'évanouissant dans cette même supposition, leur somme remplira évidemment la seconde des conditions (2). Il en est de même de la troisième de ces conditions. Quant à la quatrième, il est également manifeste qu'elle est satisfaite par la somme $v + w$ que nous venons de former, v se réduisant à $\chi(x)$ et w à $\varphi(x) - \chi(x)$, lorsqu'on y suppose le temps nul. La somme $v + w$ est donc la fonction cherchée u.

La marche que nous venons d'indiquer revient à assujettir les deux extrémités d'une barre, l'une à la température $F(t)$, l'autre à la température $f(t)$, sans supposer arbitraire l'état initial de cette barre, à considérer une seconde barre dont les extrémités sont entretenues à la température zéro et dont l'état initial est la différence entre l'état initial arbitraire $\varphi(x)$ et celui de la première barre, et à ajouter ensuite les expressions qui expriment les états variables de ces deux barres.

La recherche de la fonction v peut à son tour se décomposer en deux autres questions plus simples; car il est évident que pour obtenir une fonction qui remplisse les 3 premières des conditions (2), il suffit de chercher d'abord une expression v' qui soit assujettie à la première et à la troisième de ces conditions et qui s'évanouisse pour $x = 0$, et de déterminer ensuite une seconde expression v'' qui remplisse la première et la seconde, et devienne égale à zéro lorsqu'on y suppose $x = \pi$; la somme $v' + v''$ de ces expressions satisfera manifestement aux 3 premières des conditions (2), et pourra par conséquent être prise pour v.

Quant à ces nouvelles fonctions v' et v'', il est facile de voir qu'elles peuvent être obtenues de la même manière, c'est-à-dire que l'une d'elles, la première v' par exemple, étant trouvée, l'autre v'' s'en déduira immédiatement. Il suffira pour cela, de changer en $F(t)$ la fonction arbitraire $f(t)$ que renferme cette expression v' et d'y remplacer en même temps x par $\pi - x$. Il est évident que l'expression v' ainsi modifiée satisfera toujours à l'équation (1) et que pour $x = 0$, $x = \pi$ elle se réduira respectivement à $F(t)$ et à zéro; elle pourra donc être prise pour v''.

Toute la difficulté du problème que nous nous sommes proposé de résoudre, se réduit donc à la recherche d'une fonction v' de x et de t, qui rem-

plisse les 3 conditions de satisfaire à l'équation (1), de s'évanouir pour $x = 0$, et de se réduire à $f(t)$ lorsqu'on y fait $x = \pi$.

On satisfait à l'équation:

$$\frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2}$$

par une solution particulière de cette forme:

$$r\cos\alpha t + s\sin\alpha t, \tag{3}$$

α désignant une quantité constante mais arbitraire, et r et s étant des fonctions de x et de α sans t. En effet, différentiant l'expression précédente une fois par rapport à t, et deux fois par rapport à x, et égalant les deux résultats, il viendra:

$$\frac{\partial^2 r}{\partial x^2}\cos\alpha t + \frac{\partial^2 s}{\partial x^2}\sin\alpha t = \alpha s\cos\alpha t - \alpha r\sin\alpha t,$$

équation qui aura évidemment lieu quels que soient x et t, si les fonctions r et s sont telles que l'on ait:

$$\frac{\partial^2 r}{\partial x^2} = \alpha s, \quad \frac{\partial^2 s}{\partial x^2} = -\alpha r. \tag{4}$$

Ces équations différentielles simultanées étant linéaires et a coefficients constants, il sera facile d'en trouver les intégrales complètes, et comme ces équations sont l'une et l'autre du second ordre, les valeurs générales de r et de s renfermeront chacune deux constantes arbitraires. Ces 4 constantes peuvent servir à assujettir chacune des fonctions r et s à deux conditions. Supposons qu'on les choisisse de manière à avoir $r = 0$, $s = 0$ lorsque $x = 0$, et $r = 1$, $s = 0$ lorsqu'on fait $x = \pi$. Désignant par R et S les valeurs de r et s ainsi particularisées, nous aurons l'expression:

$$R\cos\alpha t + S\sin\alpha t \tag{5}$$

qui, outre qu'elle satisfait à l'équation:

$$\frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2}$$

jouit encore de la double propriété de s'évanouir pour $x = 0$, et de se réduire à $\cos\alpha t$, lorsqu'on y fait $x = \pi$. L'expression précédente étant multipliée par $\psi(\alpha)d\alpha$, $\psi(\alpha)$ désignant une fonction entièrement arbitraire de α, et intégrée

depuis $\alpha = 0$ jusqu'à $\alpha = \infty$, donnera cette nouvelle fonction de x et de t:

$$\int_0^\infty (R\cos\alpha t + S\sin\alpha t)\psi(\alpha)d\alpha,$$

qui satisfera également à l'équation:

$$\frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2},$$

s'évanouira pour $x = 0$, et deviendra:

$$\int_0^\infty \psi(\alpha)\cos\alpha t\, d\alpha,$$

lorsqu'on y fait $x = \pi$. La fonction $\psi(\alpha)$ étant arbitraire, on peut la choisir de manière que l'intégrale précédente devienne égale à la fonction donnée $f(t)$, pour toute valeur positive de t. La fonction $\psi(\alpha)$ qui remplit cette condition, est d'après le théorème connu de M. Fourier (*Théorie de la chaleur*, art. 346, pag. 431) celle que donne l'équation:

$$\psi(\alpha) = \frac{2}{\pi}\int_0^\infty \cos\alpha\mu f(\mu)d\mu,$$

dans laquelle μ est une variable auxiliaire qui disparaît par l'intégration définie. Si l'on substitue cette valeur de $\psi(\alpha)$ dans l'expression obtenue plus haut, on aura cette nouvelle expression:

$$\frac{2}{\pi}\int_0^\infty\int_0^\infty (R\cos\alpha t + S\sin\alpha t)f(\mu)\cos\alpha\mu\, d\alpha d\mu, \tag{6}$$

qui remplit les 3 conditions de satisfaire à l'équation:

$$\frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2},$$

de s'évanouir pour $x = 0$, et de devenir $f(t)$ pour $x = \pi$. Cette expression peut donc être prise pour v'. Si l'on change ensuite x en $\pi - x$, et $f(\mu)$ en $F(\mu)$ dans l'expression précédente, on aura une nouvelle expression, que l'on pourra prendre pour v'', et il ne restera plus qu'à former la troisième partie w de la solution.

Cette troisième partie exprime, comme nous l'avons vu plus haut, les états successifs d'une barre dont les deux extrémités sont entretenues à la température zéro et dont l'état initial est $\varphi(x) - \chi(x)$, $\varphi(x)$ étant une fonction

primitivement donnée et $\chi(x)$ désignant la fonction de x, à laquelle se réduit la somme $v'+v''=v$, lorsqu'on y fait $t=0$. Quoique, d'après ce que nous avons dit plus haut, il suffise pour la solution de notre problème, d'obtenir une quelconque des fonctions en nombre infini qui remplissent les 3 premières des conditions (2), le choix de cette fonction n'est pas indifférent. Le calcul se simplifie d'une manière remarquable, lorsque l'on prend pour v une fonction telle que l'on puisse prévoir, quelle est la fonction $\chi(x)$ à laquelle elle se réduit pour $t=0$; car alors on pourra former immédiatement la troisième partie w, dans la composition de laquelle entre cette fonction $\chi(x)$. La valeur de v précédemment obtenue ne présente pas cette facilité, mais il est facile d'en obtenir une qui remplisse cet objet, en modifiant un peu l'analyse que nous venons d'employer. C'est ce que nous allons faire voir en reprenant ce que nous avons dit depuis que nous sommes parvenu à l'expression (5).

La variable t étant remplacée dans cette expression par $t-\mu$, μ désignant une nouvelle arbitraire indépendante de α, x et t, elle ne cessera pas de satisfaire à l'équation:

$$\frac{\partial u}{\partial t}=\frac{\partial^2 u}{\partial x^2}$$

et de s'évanouir pour $x=0$, quelle que soit la valeur positive ou négative de t, mais pour $x=\pi$ elle se réduira à $\cos\alpha(t-\mu)$.

Multipliant l'expression ainsi modifiée par $\frac{1}{\pi}f(\mu)d\alpha d\mu$ et intégrant depuis $\mu=0$, $\alpha=0$, jusqu'à $\mu=\infty$, $\alpha=\infty$, on aura cette nouvelle fonction de x et de t:

$$(7)\qquad \frac{1}{\pi}\int_0^\infty\int_0^\infty (R\cos\alpha(t-\mu)+S\sin\alpha(t-\mu))f(\mu)d\alpha d\mu,$$

qui satisfait encore à l'équation:

$$\frac{\partial u}{\partial t}=\frac{\partial^2 u}{\partial x^2},$$

s'évanouit pour $x=0$, et se réduit à:

$$\frac{1}{\pi}\int_0^\infty\int_0^\infty \cos\alpha(t-\mu)f(\mu)d\alpha d\mu,$$

lorsqu'on y fait $x=\pi$. La valeur de cette intégrale double est connue par le

théorème de M. Fourier et l'intégration relative à μ ne s'étendant que depuis $\mu=0$ jusqu'à $\mu=\infty$, cette valeur est $f(t)$ lorsque t est positif, et égale à zéro lorsque le temps t devient négatif. La formule (7) exprime donc les états variables d'une barre dont les deux extrémités ont été entretenues à la température zéro pendant tout le temps infini antérieur à l'instant qui répond à $t=0$, et dont la seconde extrémité est entretenue à la température $f(t)$ à partir de cette époque, la première conservant toujours la température zéro. Or il est évident qu'une barre dont les deux extrémités ont été assujetties à la température zéro pendant un temps infini, a acquis dans tous ses points cette même température zéro. Donc, l'expression (7) doit s'évanouir pour toute valeur de x inférieure à π, lorsqu'on y fait $t=0$. Il serait d'ailleurs facile d'obtenir cette même conséquence par le seul examen de l'expression (7) et sans aucune considération physique.

Prenant l'expression (7) pour v' et l'expression qui s'en déduit par le changement de $f(\mu)$ en $F(\mu)$ et de x en $\pi-x$, pour v'', la somme $v'+v''$ s'évanouira pour $t=0$; la fonction $\chi(x)$ sera nulle et la troisième partie w sera l'expression des états variables d'une barre dont les deux extrémités sont assujetties à la température zéro et dont l'état initial est exprimé par la fonction connue $\varphi(x)$. Cette troisième partie w est donnée par la formule suivante, dans laquelle le signe Σ se rapporte à toutes les valeurs positives et entières de i:

$$\frac{2}{\pi}\Sigma e^{-i^2t}\sin ix\int_0^\pi \varphi(\mu)\sin i\mu d\mu,$$

(*Théorie de la chaleur*, art. 252, pag. 436).

La valeur de v' (7) est sous une forme assez compliquée. Il en est de même de la seconde partie v''. Ces deux expressions se simplifient beaucoup lorsqu'on leur donne une forme analogue à celle de la troisième, c'est-à-dire, lorsqu'on les développe en séries de sinus des arcs multiples de x. Ce développement est évidemment permis, la variable x ne devant recevoir que des valeurs inférieures à π dans l'expression v' (7) et dans l'expression analogue v''. Pour transformer la fonction (7) en une pareille série, il suffira de développer R et S qui renferment seules la variable x. Faisons donc:

$$(8)\qquad R=\Sigma b_i\sin ix,\quad S=\Sigma c_i\sin ix$$

le signe Σ se rapportant comme précédemment aux valeurs positives et entières

de i. Les coefficients b_i et c_i qui ne peuvent dépendre que de α, seront donnés par ces intégrales définies, d'après la théorie connue des séries de sinus:

$$(9) \qquad b_i = \frac{2}{\pi}\int_0^\pi R \sin ix\,dx, \quad c_i = \frac{2}{\pi}\int_0^\pi S \sin ix\,dx.$$

On peut obtenir les valeurs de ces deux intégrales définies sans être obligé de résoudre les équations différentielles (4).

Pour y parvenir, nous remplacerons dans les expressions précédentes de b_i et c_i, R et S par les différentielles secondes $-\frac{1}{\alpha}\cdot\frac{\partial^2 S}{\partial x^2}$, $\frac{1}{\alpha}\cdot\frac{\partial^2 R}{\partial x^2}$ qui leur sont respectivement égales en vertu des équations (4) dont R et S sont des intégrales particulières. Intégrant ensuite deux fois par parties les expressions de b_i et c_i, et observant qu'à la première limite $x = 0$, $\sin ix$, R et S sont nulles, et qu'à la seconde limite $x = \pi$, on a $\sin i\pi = 0$, $R = 1$, $S = 0$, il viendra:

$$b_i = \frac{2}{\pi}\cdot\frac{i^2}{\alpha}\int_0^\pi S \sin ix\,dx,$$

$$c_i = -\frac{2}{\pi}\cdot\frac{i\cos i\pi}{\alpha} - \frac{2i^2}{\pi\alpha}\int_0^\pi R \sin ix\,dx.$$

Mais d'après les équations (9) les deux intégrales précédentes sont respectivement équivalentes à $\frac{\pi}{2}b_i$, $\frac{\pi}{2}c_i$. La substitution de ces valeurs donne ces deux relations entre b_i et c_i:

$$b_i = \frac{i^2}{\alpha}c_i, \quad c_i = -\frac{2}{\pi}\cdot\frac{i\cos i\pi}{\alpha} - \frac{i^2}{\alpha}b_i,$$

d'où l'on tire:

$$b_i = -\frac{2}{\pi}\cdot\frac{i^2\cos i\pi}{\alpha^2+i^4}, \quad c_i = -\frac{2}{\pi}\cdot\frac{i\alpha\cos i\pi}{\alpha^2+i^4}.$$

Mettant ces valeurs des coefficients b_i et c_i dans R et S (8), substituant ensuite R et S ainsi transformées dans l'expression (7) et intervertissant l'ordre des signes Σ et f, l'expression (7) deviendra:

$$(10) \quad -\frac{1}{\pi}\int_0^\infty f(\mu)\,d\mu\,\Sigma\,\frac{2i\cos i\pi\sin ix}{\pi}\left(\int_0^\infty \frac{i^2\cos\alpha(t-\mu)}{\alpha^2+i^4}\,d\alpha + \int_0^\infty \frac{\alpha\sin\alpha(t-\mu)}{\alpha^2+i^4}\,d\alpha\right).$$

Les deux intégrales relatives à α que renferme cette expression sont faciles à

obtenir par les formules connues. On a, comme l'on sait:

$$\int_0^\infty \frac{b\cos\alpha l}{b^2+\alpha^2}\,d\alpha = \frac{\pi}{2}e^{\mp bl}, \quad \int_0^\infty \frac{\alpha\sin\alpha l}{\alpha^2+b^2}\,d\alpha = \pm\frac{\pi}{2}e^{\mp bl},$$

b désignant une quantité positive, et le signe supérieur ou le signe inférieur ayant lieu selon que l est positif ou négatif. En comparant ces résultats avec les intégrales précédentes, on voit que ces deux intégrales ont l'une et l'autre la valeur $\frac{\pi}{2}e^{-i^2(t-\mu)}$ lorsque $t-\mu$ est positif, et que lorsque $t-\mu$ est négatif, elles ont respectivement les valeurs:

$$\frac{\pi}{2}e^{i^2(t-\mu)}, \quad -\frac{\pi}{2}e^{i^2(t-\mu)},$$

qui ne diffèrent que par les signes. Donc, la somme de ces intégrales est $\pi e^{-i^2(t-\mu)}$ ou nulle, selon que $t-\mu$ est positif ou négatif. Il suit de là que la série contenue dans la formule (10) peut être remplacée par:

$$(11) \qquad 2\,\Sigma ie^{-i^2(t-\mu)}\cos i\pi\sin ix,$$

lorsque $t-\mu$ est positif, c'est-à-dire tant que μ est inférieur à t, et qu'elle se réduit à zéro, lorsque μ surpasse t. La fonction de μ qui doit être intégrée depuis $\mu = 0$ jusqu'à $\mu = \infty$, et dont la série en question est facteur, s'évanouit donc aussi pour toutes les valeurs de μ supérieures à t.

On pourra donc n'intégrer que depuis $\mu = 0$ jusqu'à $\mu = t$; changeant ainsi la limite supérieure de l'intégrale (10) et remplaçant la série qui y entre par l'expression (11), qui lui est équivalente tant que $\mu < t$, c'est-à-dire dans toute l'étendue de l'intégration, l'expression (10) prendra cette forme très simple:

$$-\frac{2}{\pi}\int_0^t f(\mu)\,d\mu\,\Sigma ie^{-i^2(t-\mu)}\cos i\pi\sin ix,$$

ou ce qui revient au même, en intervertissant l'ordre des signes $\int$ et Σ:

$$-\frac{2}{\pi}\Sigma ie^{-i^2t}\cos i\pi\sin ix\int_0^t e^{i^2\mu}f(\mu)\,d\mu.$$

Ayant ainsi obtenu la première partie v' de la solution, on en déduira la seconde v'' en changeant x en $\pi - x$ et $f(\mu)$ en $F(\mu)$. Si l'on ajoute ensuite v' et v'' à la troisième partie w déjà formée plus haut, on obtiendra l'expression suivante de la température variable u du point dont l'abscisse est x:

$$u = -\frac{2}{\pi}\Sigma i e^{-i^2 t}\cos i\pi \sin ix \int_0^t e^{i^2\mu} f(\mu)\,d\mu$$

$$-\frac{2}{\pi}\Sigma i e^{-i^2 t}\sin ix \int_0^t e^{i^2\mu} F(\mu)\,d\mu$$

$$+\frac{2}{\pi}\Sigma e^{-i^2 t}\sin ix \int_0^\pi \varphi(\mu)\sin i\mu\,d\mu.$$

Cette expression diffère un peu par la forme du résultat que M. FOURIER a donné. Pour la faire coïncider avec la formule que l'on trouve dans le Mémoire déjà cité, il faut remplacer l'intégrale qui entre dans la première partie v' de u par cette expression que donne l'intégration par parties:

$$\frac{e^{i^2 t} f(t) - f(0)}{i^2} - \frac{1}{i^2}\int_0^t e^{i^2\mu} f'(\mu)\,d\mu,$$

$f'(\mu)$ désignant la fonction dérivée de $f(\mu)$.

La première partie v' se change ainsi en:

$$-\frac{2}{\pi} f(t)\Sigma \frac{\cos i\pi \sin ix}{i} + \frac{2}{\pi}\Sigma e^{-i^2 t}\cos i\pi \frac{\sin ix}{i}\left(f(0) + \int_0^t e^{i^2\mu} f'(\mu)\,d\mu\right).$$

Mettant maintenant à la place de $\Sigma \frac{\cos i\pi \sin ix}{i}$ sa valeur connue $-\frac{1}{2}x$, v' prendra cette forme:

$$\frac{x}{\pi} f(t) + \frac{2}{\pi}\Sigma e^{-i^2 t}\cos i\pi \frac{\sin ix}{i}\left(f(0) + \int_0^t e^{i^2\mu} f'(\mu)\,d\mu\right).$$

Si l'on transforme v'' d'une manière analogue et que l'on ajoute ensuite les 3 parties v', v'' et w, on aura l'expression de la température u, telle que M. FOURIER l'a donnée.

DÉMONSTRATION D'UNE PROPRIÉTÉ ANALOGUE A LA LOI DE RÉCIPROCITÉ QUI EXISTE ENTRE DEUX NOMBRES PREMIERS QUELCONQUES.

PAR

M. G. LEJEUNE DIRICHLET,
PROF. DE MATH.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 9 p. 379—389.

DÉMONSTRATION D'UNE PROPRIÉTÉ ANALOGUE A LA LOI DE RÉCIPROCITÉ QUI EXISTE ENTRE DEUX NOMBRES PREMIERS QUELCONQUES.

Dans un mémoire qui vient d'être publié dans le recueil de la Société Royale de Gottingue, M. Gauss a étendu le domaine de l'analyse indéterminée aux expressions de la forme $t+u\sqrt{-1}$, t et u désignant des nombres entiers positifs ou négatifs. Ce grand géomètre a reconnu que les expressions de cette espèce se rapprochent entièrement par leurs propriétés des nombres entiers réels qu'elles comprennent d'ailleurs comme cas particulier. L'analogie qui existe à cet égard est telle que les énoncés des théorèmes connus relatifs aux entiers réels peuvent être transportés pour la plupart presque littéralement dans la théorie des nombres ainsi généralisée. Il n'en est pas de même des démonstrations qui paraissent présenter de nouvelles difficultés si l'on excepte les théorèmes très simples qui dérivent immédiatement des notions fondamentales. L'induction appliquée à des questions d'un ordre plus élevé, a fait connaître à M. Gauss une proposition qui ne le cède, ni en simplicité ni en élégance, au théorème si célèbre sous le nom de loi de réciprocité. Quant à la démonstration de ce nouveau théorème, que l'illustre auteur juge sujette à de grandes difficultés, il la renvoie à un autre mémoire où elle sera exposée avec celle d'une autre proposition plus générale. Je me propose de démontrer dans ce mémoire le théorème dont il s'agit par des considérations fort simples et qui mériteront peut-être de fixer un instant l'attention parce qu'elles sont également applicables à d'autres questions*).

*) On peut, au lieu des expressions de la forme $t+u\sqrt{-1}$, considérer celles de la forme plus générale $t+u\sqrt{a}$, a étant sans diviseur carré. Les expressions de ce genre, considérées sous le même point de vue, donnent lieu à des théorèmes analogues à celui qui fait l'objet de ce mémoire et susceptibles d'une démonstration toute semblable.

J'entre en matière en énonçant quelques définitions et en démontrant plusieurs propositions préliminaires, qui se trouvent déjà pour la plupart dans le mémoire cité plus haut.

§. 1.

Une expression de la forme $g+h\sqrt{-1}$, g et h désignant des entiers réels, sans excepter zéro, sera dite un nombre entier complexe. Il résulte de là que les entiers réels sont des cas particuliers des entiers complexes. Cette définition posée, il n'est besoin d'aucune explication pour indiquer le sens que l'on doit attacher aux mots divisibilité et congruence. De même que tout nombre réel est divisible par ± 1, tout nombre complexe doit être considéré comme contenant les facteurs ± 1, $\pm\sqrt{-1}$. Un nombre complexe sera dit premier lorsqu'il ne peut être décomposé en deux facteurs différents l'un et l'autre de ± 1 et $\pm\sqrt{-1}$. Voyons d'après cela comment on peut reconnaître si un nombre complexe $g+h\sqrt{-1}$ est premier ou non. Pour cela nous distinguerons deux cas selon que les deux termes g, h du nombre complexe sont ou ne sont pas l'un et l'autre différents de zéro. Le second de ces deux cas semble se subdiviser; le terme subsistant pouvant être réel ou le produit de $\sqrt{-1}$ et d'un nombre réel. Mais il est facile de voir que cela revient au même, car si $h\sqrt{-1}$ est premier, h l'est pareillement et réciproquement. Or, pour qu'un nombre réel q, considéré comme complexe, soit premier, il faut d'abord qu'il le soit aussi sous le point de vue ordinaire. Mais cela ne suffit pas; il doit en outre, abstraction faite du signe, être de la forme $4n+3$; car s'il avait la forme $4n+1$ qui entraîne toujours celle-ci: c^2+d^2, il serait décomposable dans les facteurs $c+d\sqrt{-1}$ et $c-d\sqrt{-1}$. Réciproquement, tout nombre premier réel q qui, abstraction faite du signe, est de la forme $4n+3$, doit être aussi considéré comme premier dans la théorie des nombres complexes; car si l'on avait:

$$q = (c+d\sqrt{-1})(e+f\sqrt{-1}),$$

on aurait aussi:

$$q = (c-d\sqrt{-1})(e-f\sqrt{-1})$$

et par conséquent, en multipliant:

$$q^2 = (c^2+d^2)(e^2+f^2),$$

équation impossible, q ne pouvant être diviseur de la somme de deux carrés.

Considérons, en second lieu, le cas où aucun des deux termes de l'expression $g+h\sqrt{-1}$ ne s'évanouit. Pour qu'elle représente alors un nombre premier complexe, il est nécessaire et suffisant que g^2+h^2 soit un nombre premier réel. Pour le faire voir, supposons $g+h\sqrt{-1}$ décomposable dans les deux facteurs $c+d\sqrt{-1}$ et $e+f\sqrt{-1}$, $g-h\sqrt{-1}$ sera le produit de $c-d\sqrt{-1}$ et de $e-f\sqrt{-1}$, et l'on trouve:

$$g^2+h^2 = (c^2+d^2)(e^2+f^2),$$

c'est-à-dire g^2+h^2 égal à un nombre composé. Réciproquement si g^2+h^2 est un nombre réel composé, $g+h\sqrt{-1}$ est un nombre complexe également composé. La chose est évidente lorsque g, h ont un facteur commun; si un pareil facteur n'existe pas, g^2+h^2 n'a que des diviseurs premiers réels $4n+1$. Soit $p = c^2+d^2$ un de ces diviseurs, on aura:

$$g^2 \equiv -h^2; \quad c^2 \equiv -d^2 \pmod{p}$$

et par suite, en multipliant et transposant:

$$(cg+dh)(cg-dh) \equiv 0 \pmod{p},$$

d'où l'on conclut que $\frac{cg\pm dh}{p}$, avec le signe convenable, est entier. On a d'un autre côté:

$$p(g^2+h^2) = (cg\pm dh)^2+(ch\mp dg)^2,$$

équation qui exige évidemment que $\frac{ch\mp dg}{p}$ soit entier en même temps que $\frac{cg\pm dh}{p}$, les signes supérieurs et inférieurs se correspondant. Cela posé, il est évident que le quotient:

$$\frac{g+h\sqrt{-1}}{c\pm d\sqrt{-1}} = \frac{cg\pm dh}{p} + \frac{ch\mp dg}{p}\sqrt{-1}$$

est un entier complexe et $g+h\sqrt{-1}$ par conséquent un nombre composé. Il est donc prouvé que, si g^2+h^2 est un nombre premier réel, $g+h\sqrt{-1}$ est un nombre premier complexe, et réciproquement.

Il résulte de cette discussion qu'il y a des nombres premiers de deux espèces différentes. Ceux de la première espèce se réduisent à un seul terme, et ne sont autre chose, abstraction faite du signe ou du facteur $\pm\sqrt{-1}$, que

des nombres premiers réels de la forme $4n+3$. Pour plus de simplicité, nous les supposerons toujours débarrassés du facteur $\sqrt{-1}$.

Ceux de la seconde espèce tirent leur origine des nombres premiers réels composés de deux carrés qui, à l'exception de 2, sont tous de la forme $4n+1$. Si l'on désigne par $c+d\sqrt{-1}$ un nombre premier de cette espèce (à l'exception de $\pm(1+\sqrt{-1})$, $\pm(1-\sqrt{-1})$ qui proviennent du nombre 2), il est évident que les entiers réels c, d sont l'un pair, l'autre impair. Cela posé, nous considérerons, pour plus d'uniformité, dans ce qui va suivre, d comme pair, ce qui est permis, car si d est impair, on n'a qu'à multiplier par $\sqrt{-1}$, ce qui donne le nombre $-d+c\sqrt{-1}$, qui est également premier et tellement lié au précédent que la connaissance des propriétés de l'un suffit pour juger de celles de l'autre.

Nous terminons ces préliminaires par la démonstration d'un théorème, dont nous aurons besoin dans la suite. Les termes réels A et B du nombre complexe $A+B\sqrt{-1}$ étant supposés premiers entre eux (ce qui exclut le cas où l'un d'eux serait nul) et $g+h\sqrt{-1}$ étant un nombre complexe quelconque, je dis qu'il existe toujours un nombre s entier réel et tel qu'on ait:

$$s \equiv g+h\sqrt{-1} \pmod{A+B\sqrt{-1}}.$$

En effet, la congruence en question revient à cette équation:

$$s-g-h\sqrt{-1} = (g+\psi\sqrt{-1})(A+B\sqrt{-1})$$

ou à celles-ci:

$$s-g = A\varphi-B\psi, \quad -h = A\psi+B\varphi.$$

La dernière est évidemment possible, A et B n'ayant pas de diviseur commun, et il est également manifeste que la première donnera ensuite une valeur entière pour s.

§. 2.

Ces préliminaires posés, nous arrivons au véritable objet de ce mémoire, qui est de considérer les nombres complexes, en tant qu'ils sont ou ne sont pas résidus quadratiques les uns des autres. D'après la définition connue on dit que le nombre $\alpha+\beta\sqrt{-1}$ est ou n'est pas résidu quadratique de $A+B\sqrt{-1}$, selon qu'il existe ou qu'il n'existe pas d'expression $x+y\sqrt{-1}$, telle que $(x+y\sqrt{-1})^2-\alpha-\beta\sqrt{-1}$ soit divisible par $A+B\sqrt{-1}$. Pour décider si un

nombre complexe est ou n'est pas résidu quadratique d'un nombre complexe composé, il suffit, comme lorsqu'il s'agit de nombres réels, de considérer les différents facteurs simples du diviseur. Nous supposerons donc, dans ce qui va suivre, que le diviseur ou module $A+B\sqrt{-1}$ est un nombre premier. Pour commencer par le cas le plus simple, considérons un nombre premier q de première espèce, et proposons-nous de déterminer si $\alpha+\beta\sqrt{-1}$, expression que nous supposons non-divisible par q et dans laquelle β peut être nul, est ou n'est pas résidu quadratique de q. Attribuant dans l'expression $t+u\sqrt{-1}$, à chacune des lettres t et u, les valeurs 0, 1, 2, 3, ..., $q-1$, et excluant la combinaison 0, 0, on aura q^2-1 nombres dont nous désignerons l'ensemble par (k). Cela posé, distinguons deux cas, selon que $\alpha+\beta\sqrt{-1}$ est ou n'est pas résidu*) de q, et commençons par l'examen du dernier. L'ensemble (k) peut être partagé, dans ce cas, en groupes composés chacun de deux nombres tels que leur produit soit $\equiv\alpha+\beta\sqrt{-1} \pmod{q}$. En effet, soit $r+s\sqrt{-1}$ l'un quelconque des nombres (k) et $r'+s'\sqrt{-1}$ celui qui doit former un groupe avec lui. Il faut donc qu'on ait:

$$(r+s\sqrt{-1})(r'+s'\sqrt{-1}) \equiv \alpha+\beta\sqrt{-1} \pmod{q},$$

c'est-à-dire:

$$rr'-ss' \equiv \alpha, \quad rs'+sr' \equiv \beta \pmod{q}.$$

On peut remplacer ces congruences par celles-ci:

$$(r^2+s^2)r' \equiv \alpha r+\beta s, \quad (r^2+s^2)s' \equiv \beta r-\alpha s \pmod{q}.$$

Comme r^2+s^2 ne peut être divisible par q, qui est un nombre premier $4n+3$, ces congruences sont possibles et leur résolution donnera pour r' et s' un système unique de valeurs positives et moindres que q. Il est évident d'ailleurs, par ce qu'on a supposé, qu'on ne saurait avoir à la fois $r'=0$, $s'=0$, ni $r'=r$, $s'=s$, ce qui suffit pour montrer la possibilité de distribuer la suite (k) en groupes tels que nous les avons définis. Or ces groupes dont chacun est composé de deux nombres tels que leur produit soit $\equiv\alpha+\beta\sqrt{-1} \pmod{q}$, étant évidemment au nombre de $\frac{1}{2}(q^2-1)$, il s'ensuit que le produit des nombres (k), que nous désignerons par K, satisfait à la congruence:

$$(\alpha+\beta\sqrt{-1})^{\frac{1}{2}(q^2-1)} \equiv K \pmod{q}.$$

*) Comme les résidus quadratiques ou du second degré sont les seuls dont il soit question dans ce mémoire, nous supprimerons, pour abréger, le mot quadratique.

Venons maintenant au cas où $\alpha+\beta\sqrt{-1}$ est résidu de q. Il existe alors dans la suite (k) deux nombres tels que le carré de chacun d'eux soit $\equiv \alpha+\beta\sqrt{-1} \pmod{q}$. Si l'on désigne l'un d'eux par $r+s\sqrt{-1}$, l'autre sera $q-r+(q-s)\sqrt{-1}$. Ayant ôté ces deux nombres de la suite (k), les nombres restants pourront se partager en groupes, d'où l'on conclut que leur produit est $\equiv (\alpha+\beta\sqrt{-1})^{\frac{1}{2}(q^2-3)} \pmod{q}$. Comme on a, d'un autre côté:

$$(r+s\sqrt{-1})(q-r+(q-s)\sqrt{-1}) \equiv -(r+s\sqrt{-1})^2 \equiv -(\alpha+\beta\sqrt{-1}) \pmod{q},$$

il viendra en multipliant:

$$(\alpha+\beta\sqrt{-1})^{\frac{1}{2}(q^2-1)} \equiv -K \pmod{q}.$$

Les deux cas que nous venons de considérer, sont compris dans cet énoncé:

„On a:

$$(\alpha+\beta\sqrt{-1})^{\frac{1}{2}(q^2-1)} \equiv \mp K \pmod{q},$$

le signe supérieur ou inférieur ayant lieu selon que $\alpha+\beta\sqrt{-1}$ est ou n'est pas résidu de q."

Le signe supérieur devant évidemment être choisi lorsque $\alpha = 1$, $\beta = 0$, il s'ensuit qu'on a:

$$K \equiv -1 \pmod{q},$$

ce qui est analogue au théorème de WILSON. On peut, d'après cela, remplacer K par -1 dans l'avant-dernière congruence ce qui donne cet énoncé très simple:

I. „On a:

$$(\alpha+\beta\sqrt{-1})^{\frac{1}{2}(q^2-1)} \equiv +1 \quad \text{ou} \quad (\alpha+\beta\sqrt{-1})^{\frac{1}{2}(q^2-1)} \equiv -1 \pmod{q}$$

selon que $\alpha+\beta\sqrt{-1}$ est ou n'est pas résidu de q."

Si l'on désigne par $\alpha'+\beta'\sqrt{-1}$ une seconde expression non-divisible par q, on conclut immédiatement de ce théorème que le produit:

$$(\alpha+\beta\sqrt{-1})(\alpha'+\beta'\sqrt{-1})$$

est résidu de q, lorsque chacun de ses deux facteurs est résidu ou non-résidu, et qu'au contraire, ce produit est non-résidu, lorsque ses facteurs sont l'un résidu, l'autre non-résidu de q. En étendant ce résultat à un plus grand nombre de facteurs, on trouve cette proposition:

II. „Le produit d'un nombre quelconque de facteurs est ou n'est pas résidu du nombre premier q, selon que parmi ces facteurs il y a un nombre pair ou impair de non-résidus de q."

Ce théorème a également lieu pour les nombres premiers de seconde espèce, comme on le verra plus loin.

Il y a un théorème plus simple que le théorème I et qui remplit le même objet. Pour l'établir, considérons successivement les deux cas où $\alpha+\beta\sqrt{-1}$ est et où ce nombre n'est pas résidu de q. Dans le premier de ces cas, on a:

$$\alpha+\beta\sqrt{-1} \equiv (t+u\sqrt{-1})^2 \pmod{q}$$

et par conséquent aussi:

$$\alpha-\beta\sqrt{-1} \equiv (t-u\sqrt{-1})^2 \pmod{q}$$

d'où l'on conclut en multipliant et en élevant ensuite à la puissance $\frac{1}{2}(q-1)$:

$$(\alpha^2+\beta^2)^{\frac{1}{2}(q-1)} \equiv (t^2+u^2)^{q-1} \equiv 1 \pmod{q}$$

ou ce qui revient au même, en se servant du signe très commode employé par M. LEGENDRE:

$$\left(\frac{\alpha^2+\beta^2}{q}\right) = 1.$$

Supposons en second lieu que $\alpha+\beta\sqrt{-1}$ soit non-résidu de q. On prendra alors deux nombres (réels) α' et β' tels que $\alpha'^2+\beta'^2+1$ soit divisible par q. (L'existence de pareils nombres résulte d'un théorème connu d'EULER. *Théorie des nombres.* 3ième édit. vol. I. pag. 213.)

Cela posé, on aura:

$$\alpha'^2+\beta'^2 \equiv -1 \pmod{q},$$

et par conséquent:

$$\left(\frac{\alpha'^2+\beta'^2}{q}\right) = -1.$$

On conclut de là que $\alpha'+\beta'\sqrt{-1}$ est non-résidu de q; car pour qu'il fût résidu, il faudrait, d'après ce qu'on a vu dans le premier cas, qu'on eût:

$$\left(\frac{\alpha'^2+\beta'^2}{q}\right) = 1.$$

Le produit:

$$(\alpha+\beta\sqrt{-1})(\alpha'+\beta'\sqrt{-1}) = \alpha\alpha'-\beta\beta'+(\alpha\beta'+\beta\alpha')\sqrt{-1}$$

sera donc résidu, et l'on aura:

$$\left(\frac{(\alpha\alpha'-\beta\beta')^2+(\alpha\beta'+\beta\alpha')^2}{q}\right) = 1.$$

Or cette expression pouvant être mise sous la forme:

$$\left(\frac{\alpha^2+\beta^2}{q}\right)\left(\frac{\alpha'^2+\beta'^2}{q}\right) = 1,$$

on en conclut, en faisant attention à l'équation:

$$\left(\frac{\alpha'^2+\beta'^2}{q}\right) = -1,$$

qu'on a:

$$\left(\frac{\alpha^2+\beta^2}{q}\right) = -1.$$

Les deux résultats que nous venons d'obtenir, peuvent se réunir dans cet énoncé:

III. „L'expression $\alpha+\beta\sqrt{-1}$, qui est supposée n'être pas divisible par le nombre premier q (de première espèce), est ou n'est pas résidu de q, selon que l'on a:

$$\left(\frac{\alpha^2+\beta^2}{q}\right) = +1 \quad \text{ou} \quad \left(\frac{\alpha^2+\beta^2}{q}\right) = -1.\text{“}$$

Il résulte de là comme corollaire, en faisant successivement $\beta = 0$, $\alpha = 0$, que tout nombre réel α est résidu de q, et qu'il en est de même de toute expression imaginaire de la forme $\beta\sqrt{-1}$.

§. 3.

Nous passons aux modules qui sont des nombres premiers de seconde espèce. Désignons par $A+B\sqrt{-1}$ un pareil nombre (B étant pair), par $\alpha+\beta\sqrt{-1}$ un nombre quelconque non-divisible par $A+B\sqrt{-1}$, et faisons pour abréger:

$$A^2+B^2 = P,$$

P désignant un nombre premier réel $4n+1$.

Comme d'après la définition même du résidu quadratique, $\alpha+\beta\sqrt{-1}$ est dit résidu ou non-résidu de $A+B\sqrt{-1}$, selon qu'il existe ou qu'il n'existe pas d'expression $t+u\sqrt{-1}$ telle que:

$$(t+u\sqrt{-1})^2 \equiv \alpha+\beta\sqrt{-1} \pmod{A+B\sqrt{-1}},$$

et comme, d'un autre côté, on peut toujours trouver un nombre réel s qui satisfasse à la congruence:

$$s \equiv t+u\sqrt{-1} \pmod{A+B\sqrt{-1}},$$

on voit que, pour décider si $\alpha+\beta\sqrt{-1}$ est ou n'est pas résidu de $A+B\sqrt{-1}$,

tout se réduit à savoir si la congruence:

$$s^2 \equiv \alpha+\beta\sqrt{-1} \pmod{A+B\sqrt{-1}},$$

admet ou n'admet pas de solution. Pour voir de quoi dépend sa possibilité, remplaçons-la par cette équation équivalente:

$$s^2-\alpha-\beta\sqrt{-1} = (A+B\sqrt{-1})(\varphi+\psi\sqrt{-1}),$$

ou ce qui revient au même, par celles-ci:

$$s^2-\alpha = A\varphi-B\psi, \quad -\beta = A\psi+B\varphi.$$

Multipliant ces dernières par A et B et ajoutant, il viendra:

$$As^2-A\alpha-B\beta = P\varphi$$

d'où l'on conclut:

$$\left(\frac{A\alpha+B\beta}{P}\right) = \left(\frac{A}{P}\right).$$

On peut démontrer réciproquement que, si la condition:

$$\left(\frac{A\alpha+B\beta}{P}\right) = \left(\frac{A}{P}\right)$$

a lieu, $\alpha+\beta\sqrt{-1}$ est nécessairement résidu de $A+B\sqrt{-1}$. En effet, il est facile de voir que la condition supposée entraîne cette équation:

$$As^2-A\alpha-B\beta = P\varphi = (A^2+B^2)\varphi^*).$$

Or cette équation pouvant être mise sous la forme:

$$A(s^2-A\varphi-\alpha) = B(B\varphi+\beta),$$

et les nombres A, B n'ayant pas de diviseur commun, il faut que $B\varphi+\beta$ soit divisible par A. Faisons donc:

$$B\varphi+\beta = -A\psi.$$

Mettant ensuite cette expression dans la dernière équation, il viendra:

$$s^2-\alpha = A\varphi-B\psi.$$

On voit par là que les deux équations nécessaires et suffisantes pour que $\alpha+\beta\sqrt{-1}$ soit résidu de $A+B\sqrt{-1}$, résultent de la condition:

$$\left(\frac{A\alpha+B\beta}{P}\right) = \left(\frac{A}{P}\right).$$

Ayant ainsi prouvé que, si $\alpha+\beta\sqrt{-1}$ est résidu de $A+B\sqrt{-1}$, on a:

$$\left(\frac{A\alpha+B\beta}{P}\right) = \left(\frac{A}{P}\right),$$

*) *Théorie des nombres* vol. I. pag. 240.

et que la réciproque a également lieu, nous pouvons en conclure que l'on a:

$$\left(\frac{A\alpha+B\beta}{P}\right)=+\left(\frac{A}{P}\right) \quad \text{ou} \quad \left(\frac{A\alpha+B\beta}{P}\right)=-\left(\frac{A}{P}\right)$$

selon que $\alpha+\beta\sqrt{-1}$ est ou n'est pas résidu de $A+B\sqrt{-1}$.

Ce résultat peut se simplifier, si l'on remarque que l'on a toujours:

$$\left(\frac{A}{P}\right)=1.$$

Pour s'en convaincre, on considérera l'équation:

$$P=A^2+B^2,$$

et l'on décomposera A en ses facteurs simples, en posant:

$$A=g.g'.g''\ldots,$$

les lettres g, g', g'', ... désignant des nombres premiers réels impairs, positifs ou négatifs. Il résulte immédiatement de l'équation précédente qu'on a:

$$\left(\frac{P}{g}\right)=1,$$

d'où l'on conclut, en appliquant un théorème connu et en se rappelant que P est de la forme $4n+1$:

$$\left(\frac{g}{P}\right)=1.$$

On a pareillement:

$$\left(\frac{g'}{P}\right)=1, \quad \left(\frac{g''}{P}\right)=1, \quad \ldots,$$

et l'on tire de là en multipliant:

$$\left(\frac{g.g'.g''\ldots}{P}\right)=\left(\frac{A}{P}\right)=1,$$

ce qu'il s'agissait de prouver. En profitant de cette remarque, on peut modifier le résultat obtenu plus haut comme il suit:

IV. „Le nombre $\alpha+\beta\sqrt{-1}$ étant supposé n'être pas divisible par le nombre premier de seconde espèce $A+B\sqrt{-1}$, si l'on pose:

$$A^2+B^2=P,$$

je dis que $\alpha+\beta\sqrt{-1}$ sera ou ne sera pas résidu de $A+B\sqrt{-1}$, selon que l'on a:

$$\left(\frac{A\alpha+B\beta}{P}\right)=+1 \quad \text{ou} \quad \left(\frac{A\alpha+B\beta}{P}\right)=-1.$$"

Si l'on pose:

$$\left(\frac{A\alpha+B\beta}{P}\right)=\varepsilon, \quad \left(\frac{A\alpha'+B\beta'}{P}\right)=\varepsilon',$$

ε sera d'après ce théorème $+1$ ou -1, selon que $\alpha+\beta\sqrt{-1}$ est ou n'est pas résidu de $A+B\sqrt{-1}$, et ε' aura la même signification par rapport à $\alpha'+\beta'\sqrt{-1}$. Multipliant ces expressions entre elles, remplaçant B^2 par $P-A^2$ et faisant attention qu'on a:

$$\left(\frac{A}{P}\right)=1,$$

il viendra:

$$\varepsilon\varepsilon'=\left(\frac{A(\alpha\alpha'-\beta\beta')+B(\alpha\beta'+\beta\alpha')}{P}\right).$$

Or cette dernière expression correspondant au produit:

$$(\alpha+\beta\sqrt{-1})(\alpha'+\beta'\sqrt{-1})=\alpha\alpha'-\beta\beta'+(\alpha\beta'+\beta\alpha')\sqrt{-1},$$

on voit facilement que le théorème II subsiste également pour les nombres premiers de seconde espèce.

§. 4.

Après avoir fixé, dans ce qui précède, les conditions qui doivent avoir lieu pour qu'un nombre complexe soit ou ne soit pas résidu quadratique d'un nombre premier quelconque, nous allons faire voir comment on peut en déduire l'expression la plus simple des caractères distinctifs des nombres premiers dont un nombre complexe donné est résidu. Mais auparavant nous ferons remarquer qu'il est permis de se borner au cas où le nombre donné est premier; car s'il est composé, il résulte du théorème II démontré plus haut que sa relation à un nombre premier quelconque, dépend de celles de ses facteurs simples à ce même nombre premier.

Nous commençons par le nombre premier $1+\sqrt{-1}$. D'après le théorème III, ce nombre sera ou ne sera pas résidu d'un nombre premier de première espèce q, selon que l'on a:

$$\left(\frac{2}{q}\right)=1 \quad \text{ou} \quad \left(\frac{2}{q}\right)=-1.$$

On sait d'un autre côté que le premier ou le second de ces cas aura lieu, selon que q, pris positivement, a la forme $8n+7$ ou celle-ci: $8n+3$. Donc $1+\sqrt{-1}$

sera résidu de tout nombre premier de la forme $8n+7$, non-résidu au contraire des nombres premiers de la forme $8n+3$. Passons aux nombres premiers de seconde espèce. Pour décider si $1+\sqrt{-1}$ est ou n'est pas résidu d'un pareil nombre $A+B\sqrt{-1}$, il suffit, d'après le théorème IV, de savoir si l'on a:

$$\left(\frac{A+B}{P}\right)=+1 \quad \text{ou} \quad \left(\frac{A+B}{P}\right)=-1,$$

où l'on a fait, comme plus haut:

$$P=A^2+B^2.$$

Multipliant par 2 les deux membres de cette équation, il viendra celle-ci:

$$2P=(A+B)^2+(A-B)^2.$$

Décomposons le nombre impair $A+B$ en facteurs simples positifs ou négatifs $g, g', g'', \ldots$ de sorte que:

$$A+B=g.g'.g''\ldots.$$

On aura évidemment:

$$\left(\frac{2}{g}\right)=\left(\frac{P}{g}\right)$$

et par suite, en vertu de la loi de réciprocité:

$$\left(\frac{2}{g}\right)=\left(\frac{g}{P}\right).$$

D'un autre côté, il résulte d'un théorème connu que le premier membre est $+1$ ou -1, selon que g a la forme $8n\pm1$ ou celle-ci: $8n\pm3$. On a pareillement:

$$\left(\frac{2}{g'}\right)=\left(\frac{g'}{P}\right), \quad \left(\frac{2}{g''}\right)=\left(\frac{g''}{P}\right), \quad \ldots.$$

Faisant le produit, on obtient l'équation:

$$\left(\frac{g.g'.g''\ldots}{P}\right)=\left(\frac{A+B}{P}\right)=\pm1,$$

où le signe supérieur ou inférieur doit être pris selon que parmi les facteurs $g, g', g'', \ldots$ il y en a un nombre pair ou impair de la forme $8n\pm3$. Or il est évident que le produit:

$$A+B=g.g'.g''\ldots$$

aura la forme $8n\pm1$ ou celle-ci: $8n\pm3$, selon que ce nombre est pair ou impair. De là et de ce qu'on a vu plus haut, résulte ce théorème:

„$1+\sqrt{-1}$ est résidu ou non-résidu quadratique du nombre premier $A+B\sqrt{-1}$ selon que l'on a $A+B\equiv\pm1$ ou $A+B\equiv\pm3$ (mod. 8).“

On peut remarquer que cet énoncé comprend ce que nous avons trouvé plus haut sur la relation de $1+\sqrt{-1}$ aux nombres premiers de première espèce. Quant à la relation de $1-\sqrt{-1}$ aux différents nombres premiers, elle se déduit immédiatement du théorème précédent.

Après avoir terminé ce qui regarde le nombre $1\pm\sqrt{-1}$, nous allons nous occuper des autres nombres premiers. Désignons par $\alpha+\beta\sqrt{-1}$ un nombre premier de seconde espèce (β étant pair) et par $A+B\sqrt{-1}$ un autre nombre premier de la même espèce (B étant également pair), et proposons-nous de fixer la relation que le premier a au second.

Cette relation se détermine par un théorème très simple et qui consiste en ce que le premier est ou n'est pas résidu du second, selon que le second est ou n'est pas résidu du premier. Pour démontrer ce théorème, faisons pour abréger:

$$\alpha^2+\beta^2=p, \quad A^2+B^2=P.$$

Il résulte du théorème IV que $\alpha+\beta\sqrt{-1}$ est ou n'est pas résidu de $A+B\sqrt{-1}$, selon que l'on a:

$$\left(\frac{A\alpha+B\beta}{P}\right)=+1 \quad \text{ou} \quad \left(\frac{A\alpha+B\beta}{P}\right)=-1.$$

En échangeant les nombres $\alpha+\beta\sqrt{-1}$ et $A+B\sqrt{-1}$ entre eux, ce qui ne change pas l'expression $A\alpha+B\beta$, on conclut de la même proposition que $A+B\sqrt{-1}$ est ou n'est pas résidu de $\alpha+\beta\sqrt{-1}$, selon que l'on a:

$$\left(\frac{A\alpha+B\beta}{p}\right)=+1 \quad \text{ou} \quad \left(\frac{A\alpha+B\beta}{P}\right)=-1.$$

On voit par là que la démonstration du théorème énoncé plus haut se réduit à faire voir que l'équation:

$$\left(\frac{A\alpha+B\beta}{P}\right)=\left(\frac{A\alpha+B\beta}{p}\right)$$

a toujours lieu. Pour cela on fait le produit de p et de P, on trouve ainsi:

$$(A\alpha+B\beta)^2+(A\beta-B\alpha)^2=pP.$$

Comme, par hypothèse, A et α sont impairs, B et β pairs, $A\alpha+B\beta$ sera un nombre impair. Désignant par $g, g', g'', \ldots$ ses facteurs simples, on a:

$$A\alpha+B\beta=g.g'.g''\ldots$$

et l'équation précédente donne immédiatement:

$$\left(\frac{p}{g}\right)=\left(\frac{P}{g}\right),$$

d'où l'on conclut, en vertu d'un théorème connu:

$$\left(\frac{q}{p}\right) = \left(\frac{q}{P}\right).$$

On a pareillement:

$$\left(\frac{q'}{p}\right) = \left(\frac{q'}{P}\right), \quad \left(\frac{q''}{p}\right) = \left(\frac{q''}{P}\right), \quad \ldots,$$

d'où l'on tire en multipliant:

$$\left(\frac{q.q'.q''\ldots}{p}\right) = \left(\frac{q.q'.q''\ldots}{P}\right) \quad \text{ou} \quad \left(\frac{A\alpha+B\beta}{p}\right) = \left(\frac{A\alpha+B\beta}{P}\right),$$

ce qu'il s'agissait de prouver.

Il existe une réciprocité analogue, lorsque les deux nombres premiers n'appartiennent pas l'un et l'autre à la seconde espèce. Pour le faire voir, soient q et $A+B\sqrt{-1}$ deux nombres premiers qui sont respectivement de première et de seconde espèce. D'après le théorème III le second sera ou ne sera pas résidu du premier, selon que l'on a:

$$\left(\frac{A^2+B^2}{q}\right) = \left(\frac{P}{q}\right) = +1 \quad \text{ou} \quad \left(\frac{A^2+B^2}{q}\right) = \left(\frac{P}{q}\right) = -1.$$

Il résulte, d'un autre côté, du théorème IV que le premier sera ou ne sera pas résidu du second, selon que:

$$\left(\frac{qA}{P}\right) = \left(\frac{q}{P}\right) = +1 \quad \text{ou} \quad \left(\frac{qA}{P}\right) = \left(\frac{q}{P}\right) = -1.$$

Ces deux résultats combinés avec l'égalité:

$$\left(\frac{P}{q}\right) = \left(\frac{q}{P}\right)$$

qui dérive d'un théorème connu, suffisent pour établir la réciprocité énoncée plus haut. Il ne reste plus à considérer que le cas de deux nombres premiers de première espèce. Dans ce troisième cas, la réciprocité est évidente puisque nous avons vu plus haut qu'un nombre réel quelconque est toujours résidu de tout nombre premier de première espèce. Les trois cas que nous venons d'examiner conduisant au même résultat, nous pouvons énoncer le théorème suivant qui est celui dont il a été question dans le préambule de ce mémoire.

„Désignant par $\alpha+\beta\sqrt{-1}$ et $A+B\sqrt{-1}$ (β et B étant pairs et pouvant se réduire à zéro) deux nombres premiers complexes, le premier sera ou ne sera pas résidu quadratique du second, selon que le second est ou n'est pas résidu quadratique du premier."

Berlin, au mois de septembre 1832.

DÉMONSTRATION DU THÉORÈME DE FERMAT POUR LE CAS DES 14IÈMES PUISSANCES.

PAR

M. G. LEJEUNE DIRICHLET,
PROF. DE MATH. A BERLIN.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 9 p. 390—393.

DÉMONSTRATION DU THÉORÈME DE FERMAT POUR LE CAS DES 14IÈMES PUISSANCES.

S'il existe des nombres entiers t, u, v propres à satisfaire à l'équation:

(1) $$t^{14} = u^{14}+v^{14},$$

il est manifeste que tout facteur commun δ de deux d'entre eux, divisera nécessairement aussi le troisième. On pourra donc diviser chacun d'eux par δ, ce qui ne changera en rien la forme de l'équation: d'où l'on conclut, qu'il est permis, pour prouver l'impossibilité de l'équation (1), d'y considérer les entiers t, u, v, pris deux à deux, comme libres de tout facteur commun. Cela posé, ces entiers devront évidemment être supposés l'un pair, les autres impairs, et le nombre pair sera l'un de ceux que renferme le second membre. On voit aussi que si parmi ces nombres il y en a un divisible par 7, ce ne saurait être t, puisque 7 ne peut jamais diviser la somme de deux carrés premiers entre eux. L'équation étant symétrique par rapport à u et à v, nous pourrons supposer que, si parmi ces nombres il y a un multiple de 7, v se trouve dans ce cas. Transposant le terme en u, l'équation se changera en celle-ci:

(2) $$t^{14}-u^{14} = v^{14}$$

qu'on peut mettre sous cette autre forme:

(3) $$(t^2-u^2)[(t^2-u^2)^6+7t^2u^2(t^4-t^2u^2+u^4)^2] = v^{14}.$$

Les nombres t, u ayant été supposés premiers entre eux, t^2-u^2 et tu sont aussi sans diviseur commun; il en est de même de t^2-u^2 et $t^4-t^2u^2+u^4$, car tout nombre premier diviseur commun de ceux-ci diviserait:

$$t^4-t^2u^2+u^4-(t^2-u^2)^2 = t^2u^2,$$

et par conséquent aussi tu. Les nombres tu et t^2-u^2 auraient donc ce même diviseur commun, ce qui ne s'accorde pas avec ce qu'on vient de prouver. Il résulte de là, si l'on fait pour abréger:

$$t^2-u^2 = \varphi, \quad tu(t^4-t^2u^2+u^4) = \psi,$$

que φ et ψ, qui sont évidemment l'un pair, l'autre impair, n'ont pas de diviseur commun, et l'on aura:

$$\varphi((\varphi^3)^2+7\psi^2) = v^{14}. \tag{4}$$

Nous distinguons maintenant deux cas, selon que v est ou n'est pas divisible par 7. Si l'on suppose en premier lieu v non-divisible par 7, φ ne le sera pas non plus. Il suit de là et de ce que φ et ψ sont premiers entre eux, que les deux facteurs du premier membre sont aussi premiers entre eux et par conséquent égaux l'un et l'autre à des $14^{\text{ièmes}}$ puissances. D'un autre côté, l'on conclut d'un théorème connu que la racine de la $14^{\text{ième}}$ puissance impaire $(\varphi^3)^2+7\psi^2$ a la même forme, g^2+7h^2, et l'on prouve facilement*) que les entiers g, h satisfont à l'équation:

$$\varphi^3+\psi\sqrt{-7} = (g+h\sqrt{-7})^{14}$$

où il faut égaler séparément les parties réelles et les coefficients de $\sqrt{-7}$. Sans développer cette expression, il est évident que la valeur qu'elle donne pour ψ est divisible par 7. Mais ψ étant égal à:

$$tu(t^4-t^2u^2+u^4) = tu((t^2-u^2)^2+t^2u^2)$$

ne peut être divisible par 7, à moins que t ou u ne le soit, ce qui serait contraire à la supposition faite plus haut. Il est donc prouvé que le cas où l'on suppose v non-divisible par 7, en même temps que t et u, ne saurait avoir lieu. Reste à faire voir que l'équation (2) ne peut pas subsister non plus, si l'on considère v comme un multiple de 7. En y faisant:

$$v = 7w$$

elle deviendra:

$$t^{14}-u^{14} = 7^{14}w^{14}.$$

C'est l'équation dont il s'agit de prouver l'impossibilité. Sans compliquer la marche de la démonstration, nous pouvons, au lieu de l'équation précédente, traiter l'équation plus générale:

$$t^{14}-u^{14} = 2^m7^{1+n}w^{14} \tag{5}$$

*) Pour prouver ce dont il s'agit, on peut s'y prendre à peu près de la même manière dont nous avons démontré un théorème analogue (Vol. III de ce Journal, page 359, 360). Les théorèmes I (page 355) et III (page 358) ainsi que leurs démonstrations subsistent également, lorsque a est négatif. Supposant donc $a = -7$, la démonstration s'achève comme à l'endroit cité; elle est même plus simple en ce qu'elle n'est pas compliquée de la considération des solutions, en nombre infini, de l'équation $t^2-au^2 = 1$ qui n'en a qu'une lorsque a est négatif.[1])

[1]) Von den citirten Stellen findet sich die erste auf S. 28, 29, die zweite auf S. 24, die dritte auf S. 27 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

les nombres t, u étant toujours supposés sans diviseur commun, et m, n désignant des entiers positifs (sans excepter zéro).

En conservant toutes les dénominations précédentes, l'équation pourra être mise sous cette forme:

$$\varphi((\varphi^3)^2+7\psi^2) = 2^m7^{1+n}w^{14}.$$

Comme elle exige évidemment que φ soit divisible par 7, faisons $\varphi = 7\chi$; nous aurons ainsi:

$$7^2\chi(\psi^2+7(7^2\chi^3)^2) = 2^m7^{1+n}w^{14}.$$

Il est facile de voir que les deux facteurs $7^2\chi$ et $\psi^2+7(7^2\chi^3)^2$, dont le second est impair, n'ont pas de diviseur commun. Il résulte de là que l'équation précédente ne peut subsister à moins que $\psi^2+7(7^2\chi^3)^2$ et $7^2\chi$ ne soient le premier une $14^{\text{ième}}$ puissance, le second le produit d'une pareille puissance par 2^m7^{1+n}. Quant à la première de ces conditions, elle exige, d'après ce qu'on a vu plus haut, qu'on ait:

$$\psi+7^2\chi^3\sqrt{-7} = (r+s\sqrt{-7})^{14},$$

c'est-à-dire:

$$7^2\chi^3 = \frac{(r+s\sqrt{-7})^{14}-(r-s\sqrt{-7})^{14}}{2\sqrt{-7}},$$

où les entiers r, s sont premiers entre eux, l'un pair, l'autre impair et le premier de plus non-divisible par 7. On peut faire subir à cette expression une transformation semblable à celle que nous avons effectuée sur le premier membre de l'équation (2). Il suffit pour cela de remplacer dans le premier membre de l'équation (3), t et u respectivement par $r+s\sqrt{-7}$ et $r-s\sqrt{-7}$. En opérant ainsi et en faisant pour abréger:

$$(r^2+7s^2)(r^4-2.7^2r^2s^2+7^2s^4) = R,$$

on obtient:

$$7^2\chi^3 = 2.7.rs[R^2-(7.4^2r^2s^2)^2]$$

ou, ce qui revient au même, en multipliant les deux membres par 7^4:

$$7^6\chi^3 = 2.7^5rs(R+7(4rs)^2)(R-7(4rs)^2).$$

Il est facile de faire voir que les trois facteurs 2.7^5rs, $R+7(4rs)^2$, $R-7(4rs)^2$, pris deux à deux, n'ont pas de diviseur commun. Il est d'abord évident que s'il y a un diviseur commun, ce ne peut être ni 2 ni 7, car les deux derniers des nombres en question sont impairs et non-divisibles par 7. Soit en second lieu p un nombre premier impair différent de 7, et supposons qu'il soit divi-

seur commun de deux des expressions dont il s'agit. On s'aperçoit, à leur seule inspection, que p sera facteur commun de rs et R, et en faisant ensuite attention à la manière dont l'expression R est composée en r et s, il est évident qu'il est nécessaire que p divise à la fois r et s, ce qui est absurde, r et s étant premiers entre eux. Nous avons vu plus haut que $7^2\chi$ devait être une $14^{\text{ième}}$ puissance multipliée par $2^m 7^{1+n}$; le premier membre $7^6\chi^3$ de la dernière équation sera donc le produit d'une puissance du même degré et de $2^{3m}7^{3+3n}$. Il résulte de là et de ce que les trois facteurs du second membre sont premiers entre eux, que les deux derniers sont des $14^{\text{ièmes}}$ puissances, et que le premier est le produit d'une pareille puissance et de $2^{3m}7^{3+3n}$. On aura donc:

$$2.7^5 rs = 2^{3m}7^{3+3n}v'^{14}, \quad R+7(4rs)^3 = t'^{14}, \quad R-7(4rs)^3 = u'^{14}.$$

Il est facile de voir qu'on peut mettre le second membre de la première de ces équations sous la forme $2^{3m}7^{6+n'}v'^{14}$, où n' désigne un entier positif ou zéro. Lorsque n diffère de zéro, la chose est évidente; dans le cas où $n=0$, il faut, pour que le second membre puisse être égal au premier membre, qui est divisible par 7^5, que v' soit un multiple de 7. Mettant en conséquence $7v'$ à la place de v', le second membre prendra encore la forme supposée. Nous pouvons donc remplacer la première des équations précédentes par celle-ci:

$$4rs = 2^{3m+1}7^{1+n'}v'^{14}.$$

Prenant ensuite la différence des deux dernières, comparant et posant pour abréger $v'^3 = w'$, il viendra:

$$t'^{14} - u'^{14} = 2^{9m+4}7^{3n'+4}w'^{14}.$$

Cette équation dans laquelle t' et u' n'ont pas de diviseur commun, est entièrement semblable à l'équation (5) dont elle dérive. Seulement, les entiers t', u' qui y entrent, sont beaucoup plus petits que leurs analogues t, u dans l'équation (5). On est en droit de conclure de là, à la manière ordinaire, que l'équation (5), et par conséquent aussi l'équation (1) ne saurait avoir lieu.

Berlin, au mois d'octobre 1832.

UNTERSUCHUNGEN ÜBER DIE THEORIE DER QUADRATISCHEN FORMEN.

VON

G. LEJEUNE DIRICHLET.

Abhandlungen der Königlich Preussischen Akademie der Wissenschaften 1833, S. 101—121.