ANNALES SCIENTIFIQUES DE L'É.N.S.

X. STOUFF

Les lois de réciprocité et les sous-groupes du groupe arithmétique

Annales scientifiques de l'É.N.S. 3^e série, tome 10 (1893), p. 295-314

<http://www.numdam.org/item?id=ASENS_1893_3_10__295_0>

LES LOIS DE RÉCIPROCITÉ

ET LES

SOUS-GROUPES DU GROUPE ARITHMÉTIQUE,

PAR M. X. STOUFF,

MAITRE DE CONFÉRENCES A LA FACULTÉ DES SCIENCES DE MONTPELLIER.

Il est évidemment d'un grand intérêt d'augmenter autant que possible le nombre des principes qui peuvent servir à définir des groupes de substitutions linéaires (1). Il arrive souvent que ces principes peuvent se ramener les uns aux autres; mais chacun d'eux permet du moins d'envisager la question à un point de vue spécial et de préciser les véritables difficultés. C'est ce qui m'a décidé à publier ces recherches.

L'idée qui m'a servi de guide se trouve en partie dans un Travail de M. Sylvester relatif à la loi de réciprocité ordinaire pour les nombres réels (2). Mais, à cause d'une circonstance qui sera approfondie dans la suite, cette loi de réciprocité ne permet pas de définir de sous-groupes, du moins d'une manière simple. Il faut avoir recours aux lois de réciprocité des nombres complexes, données déjà en partie par Gauss, mais surtout par Eisenstein (3). Dans le dernier de ses travaux sur ce sujet

(1) KLEIN, *Vorlesungen über die Theorie der elliptischen Modulfunctionen*, p. 418, 1890; Teubner. — Comparer aussi : FRICKE, *Ueber die ausgezeichneten Untergruppen, etc.* (*Mathematische Annalen*, t. XXX; 1887).

(2) SYLVESTER, *Sur la loi de réciprocité dans la théorie des nombres* (*Comptes rendus des séances de l'Académie des Sciences*, p. 1053; 1880). — Comparer aussi : GEGENBAUER, *Sitzungsberichte der k. k. Akademie der Wissenschaften von Wien;* 1885. — *Ueber das Legendre-Jacobische Symbol.*

(3) EISENSTEIN, *Reciprositätsgesetz für die cübischen Reste* (*Journal de Crelle*, t. XXVII, p. 289). — *Nachtrag zum cübischen Reciprocitätssatze* (*Ibid.*, t. XXVIII,

(*Journal de Crelle*, Bd. XXXIX), ce géomètre fait observer que l'intérêt des lois de réciprocité consiste surtout dans leurs démonstrations. Il n'est donc pas inutile de faire voir ici qu'elles se rattachent à une théorie importante, celle des substitutions linéaires.

1. Considérons d'abord les substitutions à coefficients entiers réels

$$\left(z, \frac{\alpha z + \beta}{\gamma z + \delta}\right), \qquad \alpha\delta - \beta\gamma = 1,$$
$$\alpha - 1 \equiv \delta - 1 \equiv \beta \equiv \gamma \equiv 0 \pmod 4;$$

elles forment un groupe bien connu G.

J'envisage le signe de Jacobi $\left(\frac{p}{q}\right)$ tel qu'il est défini dans la *Théorie des nombres de Dirichlet*, p. 104, et j'introduis un nouveau signe $\left[\frac{m}{n}\right]$ que je définis de la manière suivante. m est un nombre *pair* positif ou *négatif*, n est un nombre positif ou négatif et toujours *congru à* 1 (mod. 4).

Soient m' et n' les valeurs absolues de ces deux nombres, on aura, par définition,

$$\left[\frac{m}{n}\right] = \left(\frac{m'}{n'}\right),$$

si l'un au moins des deux nombres m ou n est positif, et

$$\left[\frac{m}{n}\right] = -\left(\frac{m'}{n'}\right),$$

si ces deux nombres sont négatifs. Faisons les remarques suivantes.

1° *Le groupe* G *est un sous-groupe du groupe* H *des substitutions*

$$\left(z, \frac{\alpha z + \beta}{\gamma z + \delta}\right), \qquad \alpha\delta - \beta\gamma = 1,$$
$$\beta \equiv \gamma \equiv 0 \pmod 2;$$

---

p. 28). — *Lois de réciprocité* (*Ibid.*, p. 53). — *Fundamentaltheorem für die biquadratischen Reste* (*Ibid.*, p. 223). — *Einfaches Mittel zur Auffindung der höheren Reciprocitätsgesetze* (*Ibid.*, t. XXXIX, p. 351). — *Voir* aussi Busche, *Arithmetischer Beweis des Reciprocitätsgesetzes für die biquadratischen Reste* (*Journal de Crelle*, t. XCIX, p. 261).

2° *Le groupe* H *admet comme substitutions génératrices*

$$T:(z,\ z+2),\quad U:\left(z,\ \frac{z}{2z+1}\right),$$

qui correspondent aux substitutions homogènes

$$T'\begin{cases} x \text{ in } x+2y, \\ y \text{ in } y, \end{cases}\qquad U'\begin{cases} x \text{ in } x, \\ y \text{ in } 2x+y. \end{cases}$$

Cette proposition est bien connue. Le groupe H n'est autre que le groupe du mod. k^2 de Legendre.

3° Si l'on considère un système de deux nombres, x pair et y congru à 1 (mod. 4), et si l'on applique à ce système les substitutions T′ et U′ et leurs inverses un nombre quelconque de fois et dans un ordre quelconque, x reste toujours pair et y congru à 1 (mod. 4).

En effet, T′ ou T'^{-1} ne changent pas la parité de x, et U′ ou U'^{-1} ne changent pas x; donc, si x est primitivement pair, il reste toujours pair, T′ ou T'^{-1} ne changent pas y, et x étant pair, U′ ne fait varier x que d'un multiple de 4. C. Q. F. D.

4° G étant un sous-groupe de H, toute substitution S de G peut s'exprimer par un produit de substitutions T et U; je dis que, dans ce produit, T figure un nombre pair de fois et que U figure aussi un nombre pair de fois.

En effet, soit $S\left(z,\ \frac{\alpha z+\beta}{\gamma z+\delta}\right)$ une substitution du groupe G et

$$S'\begin{cases} x \text{ in } \alpha x+\beta y, \\ y \text{ in } \gamma x+\delta y \end{cases}$$

la substitution homogène correspondante. La substitution S′ transforme évidemment un système de deux entiers p et q tels que

$$p \equiv q-1 \equiv 0 \pmod 4,$$

en un système de deux entiers qui jouissent des mêmes propriétés.

Or U′ ne change pas x; T′ ou T'^{-1} change la parité de $\frac{x}{2}$; donc, pour que p primitivement divisible par 4 redevienne divisible par 4, il faut que T′ soit employé en tout un nombre pair de fois.

On observera que S′ transforme aussi un système de deux entiers p et q, tels que

$$p - 1 \equiv q \equiv 0 \pmod 4,$$

en un système de deux entiers jouissant des mêmes propriétés. Or T′ ne change pas y, U′ change la parité de $\frac{y}{2}$; donc, pour que q, primitivement divisible par 4, redevienne divsible par 4, il faut que U′ soit employé un nombre pair de fois.

La réciproque est vraie. Ainsi, pour qu'une substitution de H soit une substitution de G, *il faut et il suffit qu'elle contienne un nombre pair de fois la substitution* T *et un nombre pair de fois la substitution* U.

Il est facile de reconnaître d'après cela que le groupe G admet pour substitutions génératrices

$$T^2, \quad U^2, \quad TU^2T, \quad UT^2U, \quad TUTU.$$

Observons, de plus, que si l'on transforme l'un des systèmes p, q

$$p \equiv q - 1 \equiv 0 \pmod 4,$$
$$p - 1 \equiv q \equiv 0 \pmod 4,$$

par les substitutions T′ et U′, les parités de $\frac{p}{2}$ et de $\frac{q}{2}$ sont respectivement égales aux parités des nombres de fois que les substitutions T′ et U′ ont été employées.

5° On a toujours

$$\left[\frac{m}{n}\right] = \left[\frac{m + 2kn}{n}\right].$$

D'après les propriétés bien connues du symbole de Jacobi, cela est évident dans tous les cas, sauf peut-être celui où n est négatif et m et $m + 2kn$ de signes contraires. Supposons donc m positif

$$m + 2kn = -m_1, \qquad n = -n_1,$$

m_1 et n_1 étant positifs. On a

$$\left[\frac{m}{n}\right] = \left(\frac{m}{n_1}\right),$$
$$\left[\frac{m + 2kn}{n}\right] = -\left(\frac{m_1}{n_1}\right) = -\left(\frac{m + 2kn}{n_1}\right)\left(-\frac{1}{n_1}\right);$$

or n_1 est de la forme $4h+3$; donc $\left(-\frac{1}{n_1}\right)$ égale -1. Donc

$$\left[\frac{m+2kn}{n}\right]=\left(\frac{m+2kn}{n_1}\right)=\left(\frac{m}{n_1}\right)=\left[\frac{m}{n}\right].$$

6° *Soit l un nombre impair positif ou négatif, on a*

$$\left[\frac{m}{n}\right]=-\left[\frac{m}{n+2lm}\right](^1),$$

si m est simplement pair et

$$\left[\frac{m}{n}\right]=\left[\frac{m}{n+2lm}\right],$$

si m est doublement pair. Il y a un cas d'exception : c'est celui où m est négatif et n et $n+2lm$ de signes contraires; alors on a

$$\left[\frac{m}{n}\right]=\left[\frac{m}{n+2lm}\right],$$

si m est simplement pair, et

$$\left[\frac{m}{n}\right]=-\left[\frac{m}{n+2lm}\right],$$

si m est doublement pair.

Représentons par $2^k m'$ la valeur absolue de m; m' étant un nombre impair.

Nous distinguerons plusieurs cas.

Premier cas : n et $n+2lm$ sont tous les deux positifs. On a, d'après une formule connue (²),

$$\left[\frac{m}{n}\right]=\left(\frac{m'}{n}\right)=\delta^{2^{\frac{1}{2}(n-1)}}\varepsilon^{\frac{1}{8}(n^2-1)}\left(\frac{n}{m'}\right);$$

(¹) Comparer spécialement ici les travaux déjà cités de MM. Sylvester et Gegenbauer.

(²) Dirichlet, *Zahlentheorie*, p. 127.

les unités δ et ε ne dépendent que de m; donc on a aussi

$$\left[\frac{m}{n+2lm}\right]=\left(\frac{m}{n+2lm}\right)=\delta^{\frac{1}{2}(n+2lm-1)}\,\varepsilon^{\frac{1}{8}[(n+2lm)^2-1]}\left(\frac{n+2lm}{m'}\right);$$

en réduisant et en comparant ces deux égalités, on a

$$\left[\frac{m}{n+2lm}\right]=\varepsilon^{\frac{lm}{2}}\left[\frac{m}{n}\right];$$

si m est doublement pair, $\varepsilon^{\frac{lm}{2}}$ égale 1; si m est simplement pair, ε égale -1, et l'exposant est impair; le théorème est donc démontré dans ce cas.

Deuxième cas : n et $n+2lm$ sont tous les deux négatifs. On ramènera les signes [ ] aux signes de Legendre ( ) et l'on suivra une marche absolument analogue à la précédente.

Troisième cas : n et $n+2lm$ sont de signes contraires. Supposons, par exemple, n positif et $n+2lm$ négatif et égal à $-n_1$. Ce cas se subdivisera en deux autres.

A. m est positif :

$$\left[\frac{m}{n}\right]=\left(\frac{m}{n}\right)=\delta^{\frac{1}{2}(n-1)}\,\varepsilon^{\frac{1}{8}(n^2-1)}\left(\frac{n}{m'}\right),$$

$$\left[\frac{m}{n+2lm}\right]=\left(\frac{m}{n_1}\right)=\delta^{\frac{1}{2}(n_1-1)}\,\varepsilon^{\frac{1}{8}(n_1^2-1)}\left(\frac{n_1}{m'}\right)$$

$$=\delta^{\frac{1}{2}(n-1)+1}\,\varepsilon^{\frac{1}{8}(n^2-1)+\frac{lm}{2}}\left(\frac{-n}{m'}\right)$$

$$=\delta^{\frac{1}{2}(n-1)+1}\,\varepsilon^{\frac{1}{8}(n^2-1)+\frac{lm}{2}}\left(\frac{-1}{m'}\right)\left(\frac{n}{m'}\right);$$

or,

$$\left(\frac{-1}{m'}\right)=\delta,$$

donc

$$\left[\frac{m}{n+2lm}\right]=\varepsilon^{\frac{lm}{2}}\left[\frac{m}{n}\right],$$

ce qu'il fallait démontrer.

B. m est négatif :

$$\left[\frac{m}{n}\right] = \left(\frac{2^k m'}{n}\right) = \delta^{\frac{1}{2}(n-1)}\,\varepsilon^{\frac{1}{8}(n^2-1)}\left(\frac{n}{m'}\right),$$

$$\left[\frac{m}{n+2lm}\right] = -\left(\frac{2^k m'}{n_1}\right) = -\delta^{\frac{1}{2}(n_1-1)}\,\varepsilon^{\frac{1}{8}(n_1^2-1)}\left(\frac{n_1}{m'}\right)$$

$$= -\delta^{\frac{1}{2}(n-1)+1}\,\varepsilon^{\frac{1}{8}(n^2-1)+\frac{lm}{2}}\left(\frac{-1}{m'}\right)\left(\frac{n}{m'}\right);$$

on suppose que δ et ε correspondent à $2^k m'$; donc

$$\delta = \left(\frac{-1}{m'}\right)$$

et

$$\left[\frac{m}{n+2lm}\right] = -\varepsilon^{\frac{lm}{2}}\left[\frac{m}{n}\right],$$

ce qu'il fallait démontrer.

Considérons une substitution du groupe G, et réduisons $\frac{\beta}{\delta}$ en fraction continue en ne prenant que des quotients pairs et des restes positifs ou négatifs, mais moindre en valeur absolue que le diviseur employé. En supposant, pour fixer les idées, que le nombre des quotients incomplets soit pair, nous aurons, en les désignant alternativement par les lettres a et b affectées d'indices,

$$(1)\qquad \frac{\beta}{\delta} = 2a_1 + \cfrac{1}{2b_1 + \cfrac{1}{2a_2 + \cfrac{1}{2b_2 + \cfrac{1}{2a_3 + \cfrac{1}{2b_3 + \cdots + \cfrac{1}{2a_n + \cfrac{1}{2b_n}}}}}}}$$

et, par suite,

$$(2)\qquad \frac{\beta + \alpha z}{\delta + \gamma z} = 2a_1 + \cfrac{1}{2b_1 + \cdots + \cfrac{1}{2a_n + \cfrac{1}{2b_n + \cfrac{1}{2t + \frac{1}{\ldots}}}}}.$$

La substitution considérée peut alors se représenter par le produit

$$U^{a_1}T^{b_1}\dots U^{a_n}T^{b_n}U^{t}; \tag{3}$$

on a

$$a_1+a_2+\dots+a_n+t\equiv b_1+\dots+b_n\equiv 0 \pmod 2.$$

Soient i_1, i_2, i_3, ..., i_k ceux des indices des a *impairs* tels que le nombre total des substitutions T qui se trouvent *à leur droite* dans le produit (3) soit *impair;* considérons un système de deux nombres p et q, tels que

$$p\equiv q-1\equiv 0 \pmod 4. \tag{4}$$

Soumettons ce système successivement aux substitutions

$$U^{t}, \quad T^{b_n}, \quad U^{a_n}, \quad \dots;$$

nous obtiendrons des systèmes

$$p', \quad q'; \quad p'', \quad q''; \quad p''', \quad q'''; \quad \dots; \quad p^{h}, \quad q^{h};$$

le dernier sera

$$\beta q+\alpha p, \quad \delta q+\gamma p.$$

Soit r le nombre de fois qu'une puissance de la substitution U′ fait changer de signe $q^{(h)}$; $p^{(h)}$ étant négatif (1).

Nous aurons en tenant compte de la sixième remarque

$$\left[\frac{\beta q+\alpha p}{\delta q+\gamma p}\right]=(-1)^{k+r}\left[\frac{p}{q}\right].$$

Ceci posé, considérons une substitution du groupe G. Elle sera de la forme (3), à cela près que le produit pourra commencer par des substitutions T et finir par des substitutions U. En parcourant le produit de droite à gauche, comptons le nombre σ de fois qu'un exposant impair de U a, à sa droite, un nombre total impair de substitutions T. *Les substitutions du groupe* G *pour lesquelles ce nombre est pair forment un sous-groupe* Γ. En effet, le nombre σ, relatif à la substitution SV, est la somme (mod. 2) des nombres σ relatifs aux deux substitutions S

(1) Cela revient à la considération de la *chaîne réductive* de M. Sylvester.

et V, parce que, en comptant le nombre σ de SV, on peut, lorsque l'on arrive aux substitutions qui proviennent de S, faire abstraction des substitutions U de V, dont le nombre total est pair.

Les substitutions du groupe Γ peuvent être caractérisées de la manière suivante :

On aura d'abord

$$\alpha - 1 \equiv \delta - 1 \equiv \beta \equiv \gamma \pmod 4.$$

Si, de plus, on considère un système quelconque satisfaisant aux conditions (4) *et si l'on forme le nombre r correspondant, en désignant par* $(-1)^m$ *le produit* $\left[\frac{\beta q + \alpha p}{\delta q + \alpha p}\right]\left[\frac{p}{q}\right]$, *il faut et il suffit que m et r soient de même parité.*

On peut encore faire sur ce sujet une autre remarque. Le nombre r dépend du signe de certaines quantités et, par conséquent, reste le même quand $\frac{p}{q}$ varie de telle sorte que ces quantités conservent un signe constant. Ainsi le nombre r reste constant tant que le signe des termes des fractions U^t, $T^{b_n}U^t$, $U^{a_n}T^{b_n}U^t$, ... ne change pas. Les zéros de ces fonctions linéaires déterminent sur l'axe réel des régions. Pour chacune de ces régions, la transformation que la substitution fait subir au symbole $\left[\frac{p}{q}\right]$ est parfaitement déterminée.

Un autre sous-groupe Γ' du groupe G peut être aussi défini de la manière suivante. Après avoir mis une substitution de G sous la forme (3), comptons le nombre de fois qu'un exposant impair de T a, à sa droite, un nombre total impair de substitutions U : si ce nombre est pair, la substitution considérée appartiendra au groupe Γ'. On pourra caractériser les substitutions du groupe Γ' d'une manière analogue à celles du groupe Γ.

Enfin des considérations analogues s'appliqueraient au groupe Γ'' formé des substitutions communes à Γ et à Γ'.

On voit que cette manière de définir de nouveaux groupes est loin d'être satisfaisante, puisqu'elle exige, pour reconnaître le caractère d'une substitution, un développement en fraction continue. On pourrait se demander si par un choix plus convenable de la définition

de $\left[\frac{m}{n}\right]$, pour les valeurs négatives de m et de n, on ne pourrait pas s'en dispenser; mais on reconnaît aisément que tout autre choix présente un désavantage équivalent.

Nous verrons, au contraire, que les lois de réciprocité des nombres complexes donnent des caractères tout à fait satisfaisants.

2. Considérons le groupe G des substitutions à coefficients entiers réels

$$\left(z, \frac{\alpha z + \beta}{\gamma z + \delta}\right), \qquad \alpha\delta - \beta\gamma = 1,$$
$$\beta \equiv 0 \pmod 3;$$

ce groupe admet pour substitutions génératrices

$$T(z, z+3), \qquad U\left(z, \frac{z}{z+1}\right).$$

Je ferai, dans ce paragraphe, usage de la loi de réciprocité cubique et j'entendrai le symbole $\left[\frac{}{}\right]$ dans le sens adopté par Eisenstein. Considérons $\left[\frac{3(a+b\rho)}{c+d\rho}\right]$ où le dénominateur est tel que

$$c \equiv 0 \pmod 3, \qquad d \equiv 1 \pmod 3, \tag{1}$$

on aura

$$c + d\rho \equiv -\rho(c' + d'\rho),$$

$c' + d'\rho$ étant un nombre primaire d'Eisenstein, c'est-à-dire tel que $c' + 1 \equiv d' \equiv 0 \pmod 3$. Ce symbole n'est appliqué par Eisenstein que lorsque le dénominateur est un nombre primaire. Nous ajouterons à la définition d'Eisenstein cette définition complémentaire bien naturelle

$$\left[\frac{3(a+b\rho)}{c+d\rho}\right] = \left[\frac{3(a+b\rho)}{c'+d'\rho}\right],$$

mais il ne faudra appliquer les règles d'Eisenstein (¹) qu'aux symboles où le dénominateur sera primaire.

(¹) *Journal de Crelle*, t. XXVIII, p. 28.

Quant au numérateur, nous examinerons seulement trois cas. Nous dirons que le caractère du numérateur est

(2) 0 pour $a \equiv 2$, $b \equiv 1$ (mod.3),

(3) 1 pour $a \equiv 2$, $b \equiv 2$ (mod.3),

(4) 2 pour $a \equiv 2$, $b \equiv 0$ (mod.3).

Dans le premier cas, le numérateur est de la forme

$$3(-1)^{\lambda}\rho^{\mu}(1-\rho)(a'+b'\rho);$$

dans le second cas

$$-3\rho^{2}(a'+b'\rho);$$

dans le troisième

$$3(a'+b'\rho),$$

où $a'+b'\rho$ est primaire.

Je désignerai par N(L) la norme d'un nombre complexe L.

Voici d'abord quelques remarques analogues à celles du premier paragraphe :

1° Si l'on soumet le système

$$3(a+b\rho), \quad c+d\rho$$

aux substitutions homogènes T', U' qui correspondent aux substitutions fractionnaires T et U un nombre quelconque de fois et dans un ordre quelconque, la nature du dénominateur ne change pas, c'est-à-dire que c reste toujours congru à zéro et d à 1 (mod.3).

Le caractère final du numérateur est congru au caractère primitif augmenté du nombre de fois que la substitution T' a été employée (mod. 3), en supposant, bien entendu, que le système primitif présente l'un des trois cas que nous avons examinés.

Afin d'éviter une confusion qui ne produit cependant pas d'inconvénient essentiel, il ne sera pas permis de changer simultanément les signes des quatre coefficients d'une substitution de G. On devra toujours supposer δ congru à 1 (mod.3).

2° Soit K le sous-groupe de G formé des substitutions pour lesquelles β est divisible par 9. Pour qu'une substitution de G appartienne à K, il faut et il suffit qu'en la décomposant en substitutions T et U le nombre total de fois qu'elle contient la substitution T soit divisible par 3.

3° Je compare le symbole

$$\left[\frac{3(a+b\rho)}{c+d\rho}\right]$$

et le symbole

$$\left[\frac{3(a+b\rho)}{c+d\rho+3l(a+b\rho)}\right]$$

qui résulte du premier par la substitution U'^{l}. Je distingue trois cas :

I. Le caractère de $3(a+b\rho)$ est o. On a

$$\left[\frac{3(a+b\rho)}{c+d\rho}\right]=\left[\frac{3(-1)^{\lambda}\rho^{\mu}(1-\rho)(a'+b'\rho)}{c'+d'\rho}\right]$$
$$=\left[\frac{(-1)^{\lambda+1}\rho^{\mu+2}(1-\rho)^{3}(a'+b'\rho)}{c'+d'\rho}\right];$$

$(1-\rho)^3$ étant un cube parfait, on peut le supprimer sans altérer le signe. Il reste

$$\left[\frac{(-1)^{\lambda+1}}{c'+d'\rho}\right]\left[\frac{\rho^{\mu+2}}{c'+d'\rho}\right]\left[\frac{a'+b'\rho}{c'+d'\rho}\right]$$
$$=\rho^{\frac{(\mu+2)[N(c'+d'\rho)-1]}{3}}\left(\frac{c'+d'\rho}{a'+b'\rho}\right)=\rho^{\frac{(\mu+2)[N(c+d\rho)-1]}{3}}\left(\frac{c'+d'\rho}{a'+b'\rho}\right).$$

Le nombre $c+3la+(d+3lb)\rho$ est de la forme $-\rho(c''+d''\rho)$, $c''+d''\rho$ étant aussi un nombre primaire, qui ne diffère de $c'+d'\rho$, que par un multiple de $a'+b'\rho$; donc

$$\left[\frac{3(a+b\rho)}{c+3la+(d+3lb)\rho}\right]=\rho^{\frac{1}{3}(\mu+2)\{N[c+3la+(d+3lb)\rho]-1\}}\left(\frac{c'+d'\rho}{a'+b'\rho}\right).$$

On a

$$N[c+3la+(d+3lb)\rho]=(c+3la)^2-(c+3la)(d+3lb)+(d+3lb)^2,$$
$$N(c+d\rho)=c^2-cd+d^2$$

et, par suite,

$$N[c+3la+(d+3lb)\rho]-N(c+d\rho)\equiv 3l(2b-a)\pmod 9.$$

Or $2b-a$ est congru à o (mod. 3). Donc

$$\left[\frac{3(a+b\rho)}{c+3la+(d+3lb)\rho}\right]=\left[\frac{3(a+b\rho)}{c+d\rho}\right].$$

II. Le caractère de $3(a+b\rho)$ est 1.

$$\left[\frac{3(a+b\rho)}{c+d\rho}\right]=\left[\frac{-3\rho^2(a'+b'\rho')}{c'+d'\rho}\right]=\rho^{\frac{2}{3}[d'+\mathrm{N}(c'+d'\rho)-1]}\left[\frac{c'+d'\rho}{a'+b'\rho}\right].$$

Or

$$c'=c-d,\qquad d'=c,\qquad \mathrm{N}(c'+d'\rho)=\mathrm{N}(c+d\rho),$$

donc

$$\left[\frac{3(a+b\rho)}{c+d\rho}\right]=\rho^{\frac{2}{3}[c+\mathrm{N}(c+d\rho)-1]}\left[\frac{c'+d'\rho}{a'+b'\rho}\right]; \tag{5}$$

on aura de même

$$\left[\frac{3(a+b\rho)}{c+3la+(d+3lb)\rho}\right]=\rho^{\frac{2}{3}\{c+3la+\mathrm{N}[(c+3la)+(d+3lb)\rho]-1\}}\left[\frac{c'+d'\rho}{a'+b'\rho}\right]. \tag{6}$$

Or, dans les formules (5) et (6), la différence des multiplicateurs de $\frac{2}{3}$ dans les exposants de ρ est, en tenant compte des congruences (1), congrue à $6lb\,(\mathrm{mod.}\,9)$. Mais, b étant congru à $2\,(\mathrm{mod.}\,3)$ on a

$$\left[\frac{3(a+b\rho)}{c+3la+(d+3lb)\rho}\right]=\rho^{2l}\left[\frac{3(a+b\rho)}{c+d\rho}\right].$$

III. Le caractère de $3(a+b\rho)$ est 2 :

$$\left[\frac{3(a+b\rho)}{c+d\rho}\right]=\left[\frac{3(a'+b'\rho)}{c'+d'\rho}\right]=\rho^{\frac{2}{3}d'}\left[\frac{c'+d'\rho}{a'+b'\rho}\right]=\rho^{\frac{2}{3}c}\left[\frac{c'+d'\rho}{a'+b'\rho}\right];$$

de même

$$\left[\frac{3(a+b\rho)}{c+3la+(d+3lb)\rho}\right]=\rho^{\frac{2}{3}(c+3la)}\left[\frac{c'+d'\rho}{a'+b'\rho}\right];$$

donc

$$\left[\frac{3(a+b\rho)}{c+3la+(d+3lb)\rho}\right]=\rho^{l}\left[\frac{3(a+b\rho)}{c+d\rho}\right].$$

Ceci posé, considérons une substitution S du groupe K, et supposons-la exprimée par les substitutions T et U

$$\mathrm{S}=\mathrm{T}^{a_1}\mathrm{U}^{b_1}\mathrm{T}^{a_2}\mathrm{U}^{b_2}\ldots\mathrm{T}^{a_n}\mathrm{U}^{b_n},$$

on aura

$$a_1+a_2+\ldots+a_n\equiv 0\pmod 3.$$

Désignons par $r_1, r_2, \ldots, r_n$ le nombre total des substitutions T qui se trouvent respectivement à *la droite* des exposants $b_1, b_2, \ldots, b_n$ de U. Considérons un système

$$[3(a+b\rho),\ c+d\rho).$$

La substitution homogène S′, qui correspond à la substitution S, transforme ce système en un autre

$$3(e+f\rho),\quad g+h\rho,$$

et comme le nombre total des substitutions T employées est congru par rapport au module 3, le caractère de $3(e+f\rho)$ est le même que le caractère primitif.

D'après la troisième remarque, une substitution U′ multiplie le symbole de Jacobi par ρ^{2r_i}, r_i étant le nombre total des substitutions T qui sont à sa droite; on a donc

$$\left[\frac{3(e+f\rho)}{g+h\rho}\right] = \rho^{2(b_1r_1+b_2r_2+\ldots+b_nr_n)}\left[\frac{3(a+b\rho)}{c+d\rho}\right]. \tag{5}$$

Les substitutions S, pour lesquelles

$$\sigma = b_1r_1+b_2r_2+\ldots+b_nr_n \tag{6}$$

est congru (mod. 3), forment un groupe R, parce que, dans la substitution SV, S et V étant deux substitutions du groupe K qui jouissent de la propriété (6) pour déterminer σ, on peut faire abstraction, chaque fois que l'on considère une substitution U des substitutions T, dont V est composée, puisque V appartient au groupe K et que le nombre des substitutions T qu'elle contient est congru (mod. 3). Le σ de SV est donc congru à la somme des σ de S et de V.

C'est précisément le groupe R que j'avais en vue et dont je me proposais de donner le caractère arithmétique.

Pour qu'une substitution à coefficients entiers réels de déterminant 1 *appartienne au groupe* R, *il faut et il suffit que*

$$\beta \equiv 0 \pmod 9,$$

et que, en prenant au hasard un système de deux nombres complexes

$$[3(a+b\rho),\quad c+d\rho],$$

$$a\equiv 2,\qquad b\equiv 1,\qquad c\equiv 0,\qquad d\equiv 1\pmod 3,$$

on ait

$$\left[\frac{3\alpha(a+b\rho)+\beta(c+d\rho)}{3\gamma(a+b\rho)+\delta(c+d\rho)}\right]=\left[\frac{3(a+b\rho)}{c+d\rho}\right].$$

Signalons encore une circonstance extrêmement remarquable. La possibilité de définir un sous-groupe R, à l'aide des deux nombres complexes $3(a+b\rho)$, $c+d\rho$, tient essentiellement aux congruences imposées au second des deux nombres; en effet, si, au lieu de supposer c divisible par 3, nous prenions, par exemple pour $c+d\rho$, un nombre primaire d'Eisenstein, nous verrions facilement que les substitutions du groupe G laissent le symbole $\left[\frac{3(a+b\rho)}{c+d\rho}\right]$ absolument invariable.

3. La théorie des restes biquadratiques fournit des résultats analogues. Revenons au groupe G du premier paragraphe. J'emploie, pour représenter le caractère biquadratique, le symbole d'Eisenstein (1) [,], et je l'applique à un système de deux nombres entiers complexes

$$2(a+bi),\quad c+di, \tag{1}$$

où

$$d-1\equiv c\equiv 0\pmod 4, \tag{2}$$

de sorte que

$$c+di=i(c'+d'i),$$

$c'+d'i$ étant un nombre primaire d'Eisenstein. Il faut encore faire une remarque analogue à celle de tout à l'heure. Eisenstein n'applique son symbole que dans le cas où le second nombre est primaire. Nous conviendrons que

$$[2(a+bi),\ c+di]=[2(a+bi),\ c'+d'i].$$

(1) *Journal de Crelle*, t. XXVIII, p. 223. Comparer le Mémoire de Busche déjà cité (*Crelle*, 99).

Relativement à $a + bi$ j'examine quatre cas : je dis que le caractère de $a + bi$ est

(3) $\quad 0$ pour $a \equiv 1, \quad b \equiv 1 \pmod 4$,

(4) $\quad 1$ pour $a \equiv 1, \quad b \equiv 2 \pmod 4$,

(5) $\quad 2$ pour $a \equiv 1, \quad b \equiv 3 \pmod 4$,

(6) $\quad 3$ pour $a \equiv 1, \quad b \equiv 0 \pmod 4$.

Dans le premier cas, le nombre $2(a + bi)$ est de la forme

$$i^3(1 + i)^3(a' + b'i);$$

dans le second, de la forme

$$i(1 + i)^7(a' + b'i);$$

dans le troisième,

$$i^2(1 + i)^3(a' + b'i);$$

dans le quatrième,

$$i^3(1 + i)^2(a' + b'i),$$

$a' + b'i$ désignant partout un nombre primaire.

Remarquons que la nature du dénominateur ne change jamais, lorsque l'on soumet le système (1) aux substitutions T′ et U′ du premier paragraphe. Quant au numérateur, la différence entre son caractère final et le caractère primitif est congrue (mod. 4) au nombre de fois que la substitution T′ a été employée.

Je rappelle les formules d'Eisenstein : on a

$$(7) \qquad [i, c' + d'i] = i^{\frac{3}{2}(c'-1)},$$

$$(8) \qquad [1 + i, c' + d'i] = i^{\frac{1}{4}(c'-d'-d'^2-1)},$$

$$(9) \qquad [a' + b'i, c' + d'i] = (-1)^{\frac{1}{2}(a'-1)(c'-1)}[c' + d'i, a' + b'i];$$

$a' + b'i$ et $c' + d'i$ désignent partout des nombres primaires, c'est-à-dire pour lesquels la partie réelle est congrue à 1 et la partie imaginaire congrue à 0, ou la partie réelle congrue à -1 et la partie imaginaire congrue à 2 (mod. 4). De plus, par suite des hypothèses antérieures, nous n'aurons, comme on le verra dans les calculs suivants, à employer la formule (9) que lorsque le second nombre appar-

tiendra à la première espèce de nombres primaires, c'est-à-dire c' étant congru à 1. Nous aurons donc, dans tous les cas où nous emploierons la formule (9),

$$[a'+b'i,\ c'+d'i]=[c'+d'i,\ a'+b'i].$$

Nous nous proposons de comparer les symboles

$$[2(a+bi),\ c+di] \quad \text{et} \quad [2(a+bi),\ c+4la+(d+4lb)i]$$

dans les quatre cas (3), (4), (5), (6).

I. Le caractère de $2(a+bi)$ est 0. On a

$$\begin{aligned}[2(a+bi),\ c+di] &= [i^3(1+i)^3(a'+b'i),\ c'+d'i]\\ &= [i,\ c'+d'i]^3[1+i,\ c'+d'i]^3[a'+b'i,\ c'+d'i]\\ &= i^{\frac{9}{2}(c'-1)+\frac{3}{4}(c'-d'-d'^2-1)}[c'+d'i,\ a'+b'i].\end{aligned}$$

Or

$$c'=d, \qquad d'=-c. \tag{10}$$

Donc

$$[2(a+bi),\ c+di]=i^{\frac{9}{2}(d-1)+\frac{3}{4}(d+c-c^2-1)}[c'+d'i,\ a'+b'i];$$

on aura de même

$$\begin{aligned}&[2(a+bi),\ c+4la+(d+4lb)i]\\ &\quad=i^{\frac{9}{2}(d+4lb-1)+\frac{3}{4}[d+4lb+c+4la-(c+4la)^2-1]}[c'+d'i,\ a'+b'i]\end{aligned}$$

et, par suite,

$$[2(a+bi),\ c+4la+(d+4lb)i]=[2(a+bi),\ c+di].$$

II. Le caractère de $c+di$ est 1, on a

$$\begin{aligned}[2(a+bi),\ c+di] &= [i,\ c'+d'i][1+i,\ c'+d'i]^2[c'+d'i,\ a'+b'i]\\ &= i^{\frac{3}{2}(c'-1)+\frac{1}{2}(c'-d'-d'^2-1)}[c'+d'i,\ a'+b'i],\end{aligned}$$

et, d'après les valeurs (10) de c' et de d',

$$[2(a+bi),\ c+di]=i^{\frac{3}{2}(d-1)+\frac{1}{2}(d+c-c^2-1)}[c'+d'i,\ a'+b'i],$$

on aura de même

$$[2(a+bi),\ c+4la+(d+4lb)i]$$
$$=i^{\frac{3}{2}(d+4lb-1)+\frac{1}{2}[d+4lb+c+4la-(c+4la)^2-1]}[c'+d'i,\ a'+b'i].$$

En réduisant les exposants de i (mod. 4), on trouve ainsi

$$[2(a+bi),\ c+4la+(d+4lb)i]=(-1)^l[2(a+bi),\ c+di].$$

III. Le caractère de $c+di$ est 2, on a

$$[2(a+bi),\ c+di]=[i,\ c'+d'i]^2[1+i,\ c'+d'i]^3[c'+d'i,\ a'+b'i]$$
$$=i^{3(c'-1)+\frac{3}{4}(c'-d'-d'^2-1)}[c'+d'i,\ a'+b'i]$$
$$=i^{3(d-1)+\frac{3}{4}(d+c-c^2-1)}[c'+d'i,\ a'+b'i];$$

on aura de même

$$[2(a+bi),\ c+4la+(d+4lb)i]$$
$$=i^{3[(d+4la)-1]+\frac{3}{4}[d+4la+c+4lb-(c+4lb)^2-1]}[c'+d'i,\ a'+b'i]$$

et, en tenant compte des congruences (5),

$$[2(a+bi),\ c+4la+(d+4lb)i]=[2(a+bi),\ c+di].$$

IV. Le caractère de $c+di$ est 3.

$$[2(a+bi),\ c+di]=[i,\ c'+d'i]^3[1+i,\ c'+d'i]^2[c'+d'i,\ a'+b'i]$$
$$=i^{\frac{9}{2}(c'-1)+\frac{1}{2}(c'-d'-d'^2-1)}[c'+d'i,\ a'+b'i]$$
$$=i^{\frac{9}{2}(d-1)+\frac{1}{2}(d+c-c^2-1)}[c'+d'i,\ a'+b'i],$$

de même

$$[2(a+bi),\ c+4la+(d+4lb)i]$$
$$=i^{\frac{9}{2}[(d+4lb)-1]+\frac{1}{2}[d+4lb+c+4la-(c+4la)^2-1]}[c'+d'i,\ a'+b'i]$$

et, en tenant compte des congruences (6),

$$2(a+bi),\ c+4la+(d+4lb)i]=(-1)^l[2(a+bi),\ c+di].$$

En résumé, le caractère biquadratique de $2(a+bi)$ par rapport à $c+di$ ne change pas, quand le caractère de $2(a+bi)$ est 0 ou 2. Le caractère biquadratique est multiplié par $(-1)^t$ lorsque le caractère de $2(a+bi)$ est 1 ou 3.

En revenant aux considérations du n° 1, envisageons une substitution homogène S′ décomposée en substitutions T′ et U′. Je suppose que la substitution fractionnaire S qui correspond à la substitution S′ appartient au groupe G. Si l'on suppose S′ décomposée en substitutions T′ et U′ et si l'on soumet le système

$$2(a+bi), \quad c+di,$$

successivement, à ces substitutions, à partir de la droite, le premier nombre du système final

$$2(e+fi), \quad g+hi,$$

possède le même caractère que $2(a+bi)$; soit σ la somme (mod. 2) des exposants des substitutions U qui ont à leur droite un nombre impair de substitutions T, nous aurons

$$[2(e+fi),\ g+hi] \equiv (-1)^{\sigma}[2(a+bi),\ c+di].$$

Les substitutions, pour lesquelles σ est pair, forment un groupe Γ, et, en abrégeant un peu des raisonnements que l'analogie permet de rétablir facilement, nous pouvons donner un caractère arithmétique des substitutions du groupe Γ″ du n° 1.

Pour qu'une substitution S *appartienne au groupe* Γ″, *il faut et il suffit que*

$$\alpha - 1 \equiv \delta - 1 \equiv \beta \equiv \gamma \pmod 4,$$

et, de plus, qu'en choisissant arbitrairement un système de deux entiers complexes

$$2(a+bi), \quad c+di,$$

tel que

$$a \equiv 1, \quad b \equiv 1, \quad c \equiv 0, \quad d \equiv 1 \pmod 4,$$

on ait

$$[2\alpha(a+bi)+\beta(c+di),\ 2\gamma(a+bi)+\delta(c+di)] \equiv [2(a+bi),\ c+di],$$
$$[2\gamma(c+di)+2\alpha(a+di),\ a(c+di)+2\beta(a+bi)] \equiv [2(a+bi),\ c+di].$$

Voici une remarque analogue à celle qui termine le n° 3.

Si, au lieu de choisir dans $c + di$, d congru (mod. 3) on prend pour $c + di$ un nombre primaire, les substitutions du groupe G laissent absolument invariable le symbole

$$[2(a + bi),\ c + di].$$

4. Les lois de réciprocités d'ordre supérieur se prêteraient évidemment à des développements analogues. Les groupes que nous venons de définir forment donc le point de départ d'une théorie très générale et très entendue. Un simple aperçu paraît d'ailleurs indiquer que la généralisation présentera des circonstances spéciales, ce qui augmentera sans doute l'intérêt de la question.

Les sous-groupes précédents sont à congruences; par exemple, celui qui est défini dans le n° 2 satisfait aux relations

$$\delta - 1 \equiv \beta \pmod{9},$$
$$\alpha \equiv 0 \pmod{3}.$$

Il y aurait un grand intérêt à trouver des groupes qui ne fussent pas à congruences, et il paraît probable que la solution de ce problème pourrait être obtenue par des recherches dans le sens que je viens d'indiquer. Par exemple, les substitutions S du n° 2 telles que

$$\tau \equiv b_1^2 r_1^2 + b_2^2 r_2^2 + \ldots + b_n^2 r_n^2 \equiv 0 \pmod{3},$$

forment un groupe, mais je n'ai pu trouver de caractère arithmétique simple pour ses substitutions.