BULLETIN DES SCIENCES
MATHÉMATIQUES ET ASTRONOMIQUES

R. DEDEKIND

Sur la théorie des nombres entiers algébriques

Bulletin des sciences mathématiques et astronomiques 2^e *série*, tome 1, n° 1 (1877), p. 17-41

<http://www.numdam.org/item?id=BSMA_1877_2_1_1_17_1>

MÉLANGES.

SUR LA THÉORIE DES NOMBRES ENTIERS ALGÉBRIQUES (¹);

PAR M. R. DEDEKIND.

(Suite.)

I.

THÉORÈMES AUXILIAIRES DE LA THÉORIE DES MODULES.

Ainsi qu'il ressort de l'*Introduction*, nous aurons dans la suite à considérer très-souvent des systèmes de nombres qui se reproduisent par *addition* et *soustraction;* le développement des propriétés générales de pareils systèmes forme l'objet d'une théorie assez étendue, qui peut aussi être utilisée pour d'autres recherches, tandis que, pour notre but, les premiers éléments de cette théorie sont suffisants. Pour ne pas interrompre plus tard le cours de notre exposition, et en même temps pour faire apercevoir plus clairement la portée des divers concepts sur lesquels s'appuie notre théorie suivante des nombres algébriques entiers, il nous semble à propos d'établir préalablement un petit nombre de théorèmes très-simples, bien qu'ils ne puissent offrir un véritable intérêt que par leurs applications.

(¹) Voir *Bulletin*, t. XI, p. 278.

§ 1. — *Modules et leur divisibilité.*

1° Un système $\mathfrak{a}$ de nombres réels ou complexes sera dit un *module* quand toutes les sommes et les différences de ces nombres appartiendront à ce même système $\mathfrak{a}$.

Si donc α est un nombre déterminé du module $\mathfrak{a}$, tous les nombres

$$\alpha+\alpha=2\alpha, \quad 2\alpha+\alpha=3\alpha, \quad \ldots,$$
$$\alpha-\alpha=0, \quad 0-\alpha=-\alpha, \quad -\alpha-\alpha=-2\alpha, \quad \ldots,$$

et, par suite, tous les nombres de la forme $x\alpha$ appartiendront aussi au module $\mathfrak{a}$, x pouvant devenir égal à tous les nombres rationnels entiers, c'est-à-dire à tous les nombres

$$0, \quad \pm 1, \quad \pm 2, \quad \pm 3, \quad \ldots.$$

Un tel système de nombres $x\alpha$ forme à lui seul un module, que nous désignerons par $[\alpha]$; si, par conséquent, un module contient un nombre α différent de zéro, il contiendra aussi une infinité de nombres différents les uns des autres. Mais il est évident que le nombre zéro, contenu dans chaque module, forme aussi déjà à lui seul un module.

2° Un module $\mathfrak{a}$ sera dit *divisible* par le module $\mathfrak{b}$ ou un *multiple* de $\mathfrak{b}$, et $\mathfrak{b}$ un *diviseur* de $\mathfrak{a}$, quand tous les nombres du module $\mathfrak{a}$ seront contenus aussi dans le module $\mathfrak{b}$.

Le module zéro est donc un multiple commun de tous les modules; si, de plus, α est un nombre déterminé d'un module $\mathfrak{a}$, le module $[\alpha]$ sera divisible par $\mathfrak{a}$. Il est, en outre, évident que tout module est divisible par lui-même, et que deux modules $\mathfrak{a}$, $\mathfrak{b}$, dont chacun est divisible par l'autre, sont identiques, ce que nous indiquerons toujours par $\mathfrak{a}=\mathfrak{b}$. Si, de plus, chacun des modules $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$, ... est divisible par celui qui le suit immédiatement, il est clair que chacun d'eux sera divisible par tous ceux qui le suivront.

3° Soient $\mathfrak{a}$, $\mathfrak{b}$ deux modules quelconques; le système $\mathfrak{m}$ de tous les nombres qui appartiennent à la fois à ces deux modules sera lui-même un module; il sera dit le *plus petit commun multiple* de $\mathfrak{a}$, $\mathfrak{b}$, parce que tout multiple commun de $\mathfrak{a}$, $\mathfrak{b}$ est divisible par $\mathfrak{m}$.

Soient, en effet, μ, μ' deux nombres quelconques du système $\mathfrak{m}$,

et contenus par conséquent aussi bien dans $\mathfrak{a}$ que dans $\mathfrak{b}$; chacun des deux nombres $\mu \pm \mu'$ appartiendra (d'après 1°) aussi bien au module $\mathfrak{a}$ qu'au module $\mathfrak{b}$, et partant aussi au système $\mathfrak{m}$, d'où il s'ensuit que $\mathfrak{m}$ est un module. Puisque tous les nombres de ce module $\mathfrak{m}$ sont contenus dans $\mathfrak{a}$ et aussi dans $\mathfrak{b}$, $\mathfrak{m}$ est un multiple commun de $\mathfrak{a}$, $\mathfrak{b}$. Si, de plus, le module $\mathfrak{m}'$ est un multiple commun quelconque de $\mathfrak{a}$, $\mathfrak{b}$, et qu'ainsi $\mathfrak{m}'$ se compose entièrement de nombres contenus à la fois dans $\mathfrak{a}$ et dans $\mathfrak{b}$, ces nombres (en vertu de la définition du système $\mathfrak{m}$) seront aussi contenus dans $\mathfrak{m}$, c'est-à-dire que $\mathfrak{m}'$ est divisible par $\mathfrak{m}$.

4° Si α devient successivement égal à tous les nombres d'un module $\mathfrak{a}$, et de même β à tous les nombres d'un module $\mathfrak{b}$, le système $\mathfrak{d}$ de tous les nombres de la forme $\alpha + \beta$ formera un module; ce module sera dit le *plus grand commun diviseur* de $\mathfrak{a}$, $\mathfrak{b}$, parce que tout diviseur commun de $\mathfrak{a}$, $\mathfrak{b}$ est aussi un diviseur de $\mathfrak{d}$.

En effet, deux nombres quelconques δ, δ' du système $\mathfrak{d}$ pouvant se mettre sous la forme $\delta = \alpha + \beta$, $\delta' = \alpha' + \beta'$, où α, α' appartiennent au module $\mathfrak{a}$, et β, β' au module $\mathfrak{b}$, on en tire

$$\delta \pm \delta' = (\alpha \pm \alpha') + (\beta \pm \beta');$$

et, puisque les nombres $\alpha \pm \alpha'$ sont contenus dans $\mathfrak{a}$ et les nombres $\beta \pm \beta'$ dans $\mathfrak{b}$, les nombres $\delta \pm \delta'$ appartiendront également au système $\mathfrak{d}$, c'est-à-dire que $\mathfrak{d}$ est un module. Le nombre zéro étant contenu dans chaque module, tous les nombres $\alpha = \alpha + 0$ du module $\mathfrak{a}$ et tous les nombres $\beta = 0 + \beta$ du module $\mathfrak{b}$ appartiennent au module $\mathfrak{d}$, lequel est, par suite, un diviseur commun de $\mathfrak{a}$ et $\mathfrak{b}$. Si, de plus, le module $\mathfrak{d}'$ est un diviseur commun quelconque de $\mathfrak{a}$, $\mathfrak{b}$, et qu'ainsi tous les nombres α et tous les nombres β soient contenus dans $\mathfrak{d}'$, alors (en vertu de 1°) tous les nombres $\alpha + \beta$, c'est-à-dire tous les nombres du module $\mathfrak{d}$, appartiendront aussi au module $\mathfrak{d}'$; donc $\mathfrak{d}$ est divisible par $\mathfrak{d}'$.

Après avoir développé rigoureusement ces démonstrations, nous pourrons nous dispenser de faire voir comment les notions du plus petit commun multiple et du plus grand commun diviseur devront être entendues pour un nombre quelconque (même infini) de modules. Cependant il sera peut-être utile de justifier le mode d'expression choisi, par la remarque suivante : Si a, b sont deux nombres rationnels entiers déterminés, m leur plus petit commun

multiple, et d leur plus grand commun diviseur, il résulte des premiers éléments de la théorie des nombres que $[m]$ sera le plus petit commun multiple, et $[d]$ le plus grand commun diviseur des deux modules $[a]$ et $[b]$. D'ailleurs on reconnaîtra bientôt que les propositions de la théorie des nombres qui se rapportent à ce cas peuvent se déduire réciproquement de la théorie des modules.

§ 2. — *Congruences et classes de nombres.*

1° Soit $\mathfrak{a}$ un module; deux nombres quelconques ω, ω' seront dits *congrus* ou *incongrus* suivant $\mathfrak{a}$, selon que leur différence $\pm(\omega - \omega')$ sera contenue ou non dans $\mathfrak{a}$. La *congruence* des nombres ω, ω' par rapport au module $\mathfrak{a}$ sera indiquée par la notation

$$\omega \equiv \omega' \pmod{\mathfrak{a}}.$$

On tire de là immédiatement les propositions simples suivantes, dont nous pourrons nous dispenser de donner les démonstrations :

Si $\omega \equiv \omega' \pmod{\mathfrak{a}}$, et $\omega' \equiv \omega'' \pmod{\mathfrak{a}}$, on aura aussi $\omega \equiv \omega'' \pmod{\mathfrak{a}}$.

Si $\omega \equiv \omega' \pmod{\mathfrak{a}}$, et que x soit un nombre rationnel entier quelconque, on aura $x\omega \equiv x\omega' \pmod{\mathfrak{a}}$.

Si $\omega \equiv \omega' \pmod{\mathfrak{a}}$, et $\omega'' \equiv \omega''' \pmod{\mathfrak{a}}$, on aura aussi $\omega \pm \omega'' \equiv \omega' \pm \omega''' \pmod{\mathfrak{a}}$.

Si $\omega \equiv \omega' \pmod{\mathfrak{a}}$, et que le module $\mathfrak{b}$ soit un diviseur de $\mathfrak{a}$, on aura aussi $\omega \equiv \omega' \pmod{\mathfrak{b}}$.

Si $\omega \equiv \omega' \pmod{\mathfrak{a}}$, et $\omega \equiv \omega' \pmod{\mathfrak{b}}$, on aura aussi $\omega \equiv \omega' \pmod{\mathfrak{m}}$, $\mathfrak{m}$ étant le plus petit commun multiple de $\mathfrak{a}$, $\mathfrak{b}$.

2° Le premier des théorèmes précédents conduit à l'introduction de la notion d'une *classe de nombres* relativement au module $\mathfrak{a}$: nous entendrons par là l'ensemble de tous les nombres, et de ces nombres seulement qui sont congrus à un nombre déterminé et par suite aussi entre eux, suivant $\mathfrak{a}$. Une telle classe suivant $\mathfrak{a}$ est donc complétement déterminée quand on donne un seul des nombres qu'elle contient, et tout nombre peut être regardé comme *représentant* d'une classe tout entière. Les nombres du module $\mathfrak{a}$, par exemple, forment eux-mêmes une pareille classe, représentée par le nombre zéro.

Si maintenant $\mathfrak{b}$ est un second module, on pourra toujours choisir

dans ce module un nombre fini ou infini de nombres,

$$(\beta_1) \qquad \beta_1,\ \beta_2,\ \beta_3,\ \ldots,$$

de telle manière que tout nombre contenu dans $\mathfrak{b}$ soit congru suivant le module $\mathfrak{a}$ à un de ces nombres, et à un seul. Un tel système de nombres β_r du module $\mathfrak{b}$, qui sont tous incongrus par rapport à $\mathfrak{a}$, mais qui représentent aussi toutes les classes qui ont des nombres communs avec $\mathfrak{b}$, je le nommerai *un système complet de représentants du module* $\mathfrak{b}$ *suivant le module* $\mathfrak{a}$, et le nombre de ces nombres β_r ou des classes qu'ils représentent, lorsqu'il est fini, sera désigné par $(\mathfrak{b}, \mathfrak{a})$; si, au contraire, le nombre des représentants β_r est infini, il convient alors d'attribuer au symbole $(\mathfrak{b}, \mathfrak{a})$ la valeur zéro. L'examen plus approfondi d'un tel système de représentants (β_r) conduit maintenant au théorème suivant :

3° Soient $\mathfrak{a}$, $\mathfrak{b}$ deux modules quelconques, $\mathfrak{m}$ leur plus petit commun multiple, $\mathfrak{d}$ leur plus grand commun diviseur; tout système complet de représentants du module $\mathfrak{b}$ par rapport à $\mathfrak{a}$ sera en même temps un système complet de représentants du module $\mathfrak{b}$ par rapport à $\mathfrak{m}$, ainsi que du module $\mathfrak{d}$ par rapport à $\mathfrak{a}$, et par suite on aura

$$(\mathfrak{b}, \mathfrak{a}) = (\mathfrak{b}, \mathfrak{m}) = (\mathfrak{d}, \mathfrak{a}).$$

Il est d'abord évident que deux nombres quelconques β, β' du module $\mathfrak{b}$, congrus suivant $\mathfrak{a}$, sont congrus suivant $\mathfrak{m}$, puisque $\beta - \beta'$ est contenu aussi bien dans $\mathfrak{a}$ que dans $\mathfrak{b}$, et, par suite, aussi dans $\mathfrak{m}$. Maintenant, comme tout nombre β du module $\mathfrak{b}$ est congru avec un des représentants β_r suivant $\mathfrak{a}$ et par suite aussi suivant $\mathfrak{m}$, et que deux quelconques de ces représentants β_r, différents entre eux, sont incongrus suivant $\mathfrak{a}$ et par suite aussi suivant $\mathfrak{m}$, ces nombres β_r appartenant au module $\mathfrak{b}$ formeront un système complet de représentants du module $\mathfrak{b}$ suivant $\mathfrak{m}$. On démontrera absolument de même la seconde partie : les mêmes nombres β_r, puisque $\mathfrak{b}$ est divisible par $\mathfrak{d}$, sont contenus dans $\mathfrak{d}$, et, d'après l'hypothèse, incongrus suivant $\mathfrak{a}$; et, comme tout nombre δ contenu dans $\mathfrak{d}$ est de la forme $\alpha + \beta$, α étant contenu dans $\mathfrak{a}$ et β dans $\mathfrak{b}$, on aura

$$\delta = \alpha + \beta \equiv \beta \pmod{\mathfrak{a}};$$

et, comme β et par suite aussi δ sont congrus à l'un des nombres β_r suivant $\mathfrak{a}$, les nombres β_r formeront un système complet de représentants du module $\mathfrak{d}$ suivant $\mathfrak{a}$. C. Q. F. D.

Si $\mathfrak{b}$ est divisible par $\mathfrak{a}$, on aura $(\mathfrak{b}, \mathfrak{a}) = 1$, puisque tous les nombres contenus dans $\mathfrak{b}$ sont $\equiv 0 \pmod{\mathfrak{a}}$; réciproquement, si $(\mathfrak{b}, \mathfrak{a}) = 1$, $\mathfrak{b}$ sera divisible par $\mathfrak{a}$, puisque tous les nombres contenus dans $\mathfrak{b}$ sont congrus entre eux et par suite $\equiv 0 \pmod{\mathfrak{a}}$; on a évidemment en même temps $\mathfrak{m} = \mathfrak{b}$, $\mathfrak{b} = \mathfrak{a}$.

4° Si $\mathfrak{b}$ est un diviseur de $\mathfrak{a}$ et en même temps un multiple de $\mathfrak{c}$, si de plus β_r devient successivement égal à tous les représentants de $\mathfrak{b}$ suivant $\mathfrak{a}$, et de même γ_s égal à tous les représentants de $\mathfrak{c}$ suivant $\mathfrak{b}$, tous les nombres $\beta_r + \gamma_s$ formeront alors un système complet de représentants du module $\mathfrak{c}$ suivant $\mathfrak{a}$, et par suite on aura

$$(\mathfrak{c}, \mathfrak{a}) = (\mathfrak{c}, \mathfrak{b})(\mathfrak{b}, \mathfrak{a}).$$

Car, *en premier lieu,* tous ces nombres $\beta_r + \gamma_s$ appartiennent au module $\mathfrak{c}$, puisque β_r est contenu dans $\mathfrak{b}$ et par suite aussi dans $\mathfrak{c}$, et que γ_s est également contenu dans $\mathfrak{c}$. *En second lieu,* ils sont tous incongrus suivant $\mathfrak{a}$; si l'on désigne, en effet, par β', β'' des valeurs particulières de β_r, et par γ', γ'' des valeurs particulières de γ_s, alors de l'hypothèse $\beta' + \gamma' \equiv \beta'' + \gamma'' \pmod{\mathfrak{a}}$, puisque $\mathfrak{a}$ est divisible par $\mathfrak{b}$ et que $\beta' \equiv \beta'' \equiv 0 \pmod{\mathfrak{b}}$, il s'ensuivrait d'abord que $\gamma' \equiv \gamma'' \pmod{\mathfrak{b}}$; mais, comme γ', γ'' sont des termes particuliers de la série de nombres parcourue par γ_s, et que deux quelconques de ces nombres différents entre eux sont en même temps incongrus suivant $\mathfrak{b}$, il faudra que l'on ait $\gamma' = \gamma''$, et par conséquent la supposition précédente se changera en $\beta' \equiv \beta'' \pmod{\mathfrak{a}}$; maintenant, comme β', β'' sont pareillement des termes particuliers de la série de nombres parcourue par β_r, et que deux quelconques de ces nombres différents entre eux sont en même temps incongrus suivant $\mathfrak{a}$, il faudra que l'on ait $\beta' = \beta''$, ce qui démontre l'assertion ci-dessus. *En troisième lieu,* il faut faire voir que tout nombre γ contenu dans $\mathfrak{c}$ est congru à l'un des nombres $\beta_r + \gamma_s$ suivant $\mathfrak{a}$; en effet, chaque nombre γ étant congru à l'un des nombres γ_s suivant $\mathfrak{b}$, on peut poser $\gamma = \beta + \gamma_s$, β désignant un nombre du module $\mathfrak{b}$; de plus, chacun de ces nombres β étant congru à l'un des nombres β_r suivant $\mathfrak{a}$, on peut poser $\beta = \alpha + \beta_r$, α désignant un nombre du module $\mathfrak{a}$; on aura donc

$$\gamma = \beta + \gamma_s = \alpha + \beta_r + \gamma_s \equiv \beta_r + \gamma_s \pmod{\mathfrak{a}}.$$

C. Q. F. D.

5° Soient $\mathfrak{m}$ le plus petit commun multiple, $\mathfrak{b}$ le plus grand com-

mun diviseur des deux modules $\mathfrak{a}$, $\mathfrak{b}$, et soient ρ, σ deux nombres donnés; le système des deux congruences

$$\omega \equiv \rho \pmod{\mathfrak{a}}, \qquad \omega \equiv \sigma \pmod{\mathfrak{b}}$$

aura toujours une racine commune, lorsqu'on aura, et dans ce cas seulement,

$$\rho \equiv \sigma \pmod{\mathfrak{d}},$$

et tous les nombres ω formeront une classe déterminée de nombres suivant le module $\mathfrak{m}$.

S'il existe, en effet, un nombre ω satisfaisant aux deux congruences, les nombres $\omega - \rho$, $\omega - \sigma$ seront contenus respectivement dans $\mathfrak{a}$, $\mathfrak{b}$, et partant contenus tous les deux dans $\mathfrak{d}$, et par conséquent leur différence $\rho - \sigma$ sera contenue également dans $\mathfrak{d}$, c'est-à-dire que la condition indiquée $\rho \equiv \sigma \pmod{\mathfrak{d}}$ est nécessaire; réciproquement, si elle est remplie, il existera (en vertu de la définition de $\mathfrak{d}$ dans le § 1, 4°) un nombre α dans $\mathfrak{a}$ et un nombre β dans $\mathfrak{b}$, dont la somme $\alpha + \beta = \rho - \sigma$, et par suite le nombre $\omega = \rho - \alpha = \sigma + \beta$ satisfera aux deux congruences; donc la condition indiquée est aussi suffisante. Si, de plus, ω' est un nombre quelconque remplissant les mêmes conditions que ω, alors $\omega' - \omega$ sera contenu aussi bien dans $\mathfrak{a}$ que dans $\mathfrak{b}$, et par suite aussi dans $\mathfrak{m}$, c'est-à-dire qu'on aura $\omega' \equiv \omega \pmod{\mathfrak{m}}$, et réciproquement, tout nombre ω' de la classe représentée par ω suivant $\mathfrak{m}$ satisfera aux deux congruences. C. Q. F. D.

§ 3. — *Modules finis.*

1° Soient $\beta_1, \beta_2, \beta_3, \ldots, \beta_n$ des nombres déterminés; tous les nombres de la forme

$$\beta = y_1\beta_1 + y_2\beta_2 + y_3\beta_3 + \ldots + y_n\beta_n,$$

$y_1, y_2, y_3, \ldots, y_n$ désignant des nombres rationnels entiers arbitraires, constituent évidemment un module, que nous appellerons un module *fini,* et que nous désignerons par $[\beta_1, \beta_2, \beta_3, \ldots, \beta_n]$; le complexe des constantes $\beta_1, \beta_2, \beta_3, \ldots, \beta_n$ sera dit la *base* du module.

Ce module $[\beta_1, \beta_2, \ldots, \beta_n]$ est évidemment le plus grand com-

mun diviseur des n modules finis $[\beta_1]$, $[\beta_2]$, ..., $[\beta_n]$; il serait facile de faire voir que tout multiple d'un module fini est également un module fini; mais je me bornerai ici à démontrer le théorème fondamental suivant, dont on fera plus tard des applications importantes.

2° Si tous les nombres d'un module fini $\mathfrak{b} = [\beta_1, \beta_2, \ldots, \beta_n]$ peuvent, en les multipliant par des nombres rationnels différents de zéro, être transformés en des nombres d'un module $\mathfrak{a}$, le plus petit commun multiple $\mathfrak{m}$ de $\mathfrak{a}$, $\mathfrak{b}$ sera un module fini, et l'on pourra choisir un système de $\frac{1}{2}(n+1)n$ nombres rationnels entiers a, tel que les n nombres

$$\begin{aligned}
\mu_1 &= a'_1\,\beta_1,\\
\mu_2 &= a''_1\,\beta_1 + a''_2\,\beta_2,\\
\mu_3 &= a'''_1\,\beta_1 + a'''_2\,\beta_2 + a'''_3\,\beta_3,\\
&\cdots\cdots\cdots\cdots\cdots\cdots,\\
\mu_n &= a_1^{(n)}\beta_1 + a_2^{(n)}\beta_2 + a_3^{(n)}\beta_3 + \ldots + a_n^{(n)}\beta_n
\end{aligned}$$

forment une base de $\mathfrak{m}$, et que l'on ait en même temps

$$(\mathfrak{b}, \mathfrak{a}) = (\mathfrak{b}, \mathfrak{m}) = a'_1 a''_2 a'''_3 \ldots a_n^{(n)}.$$

Par hypothèse, il existe n fractions, différentes de zéro,

$$\frac{s_1}{t_1},\quad \frac{s_2}{t_2},\quad \frac{s_3}{t_3},\quad \ldots,\quad \frac{s_n}{t_n},$$

dont les numérateurs et les dénominateurs sont des nombres rationnels entiers, tels que les n produits

$$\frac{s_1}{t_1}\beta_1,\quad \frac{s_2}{t_2}\beta_2,\quad \frac{s_3}{t_3}\beta_3,\quad \ldots,\quad \frac{s_n}{t_n}\beta_n$$

appartiennent au module $\mathfrak{a}$; maintenant, puisque des nombres quelconques d'un module $\mathfrak{a}$, lorsqu'on les multiplie par des nombres rationnels entiers $t_1, t_2, t_3, \ldots, t_n$, se changent toujours en des nombres du même module $\mathfrak{a}$ (§ 1, 1°), pareillement les produits $s_1\beta_1, s_2\beta_2, s_3\beta_3, \ldots, s_n\beta_n$, et de même, en désignant par s la valeur absolue du produit $s_1 s_2 s_3 \ldots s_n$, les nombres $s\beta_1, s\beta_2, s\beta_3, \ldots, s\beta_n$, par suite aussi tous les produits $s\beta$ appartiendront au module $\mathfrak{a}$, β désignant un nombre arbitraire quelconque du module $\mathfrak{b}$.

Soit maintenant ν un indice déterminé, de la suite $1, 2, \ldots, n$; parmi les nombres du module $[\beta_1, \beta_2, \ldots, \beta_n]$ divisible par $\mathfrak{b}$, désignons par

$$\mu'_\nu = y_1\beta_1 + y_2\beta_2 + \ldots + y_\nu\beta_\nu$$

tous ceux qui, comme, par exemple, $s\beta_\nu$, appartiennent en même temps au module $\mathfrak{a}$ et par suite aussi au module $\mathfrak{b}$; parmi ces nombres μ'_ν, il doit y avoir au moins un nombre

$$\mu_\nu = a_1^{(\nu)}\beta_1 + a_2^{(\nu)}\beta_2 + \ldots + a_\nu^{(\nu)}\beta_\nu,$$

dans lequel y prend sa *plus petite* valeur *positive* $a_\nu^{(\nu)}$. On peut alors faire voir que, dans *tous* les nombres μ'_ν, le coefficient y_ν est divisible par $a_\nu^{(\nu)}$; car, puisqu'on peut toujours poser

$$y_\nu = x_\nu a_\nu^{(\nu)} + y'_\nu,$$

x_ν et y'_ν désignant des nombres rationnels entiers, dont le dernier satisfait à la condition (1)

$$0 \leqq y'_\nu < a_\nu^{(\nu)},$$

alors, si l'on pose

$$y'_1 = y_1 - x_\nu a_1^{(\nu)}, \quad y'_2 = y_2 - x_\nu a_2^{(\nu)}, \quad \ldots, \quad y'_{\nu-1} = y_{\nu-1} - x_\nu a_{\nu-1}^{(\nu)},$$

le nombre

$$\mu'_\nu - x_\nu\mu_\nu = y'_1\beta_1 + y'_2\beta_2 + \ldots + y'_{\nu-1}\beta_{\nu-1} + y'_\nu\beta_\nu$$

appartiendra à la fois au module $[\beta_1, \beta_2, \ldots, \beta_\nu]$, et aussi au module $\mathfrak{m}$, parce que μ'_ν et μ_ν sont contenus dans $\mathfrak{m}$. Mais, puisque (d'après la définition de μ_ν) dans aucun de ces nombres le coefficient de β_ν n'est moindre que $a_\nu^{(\nu)}$ et en même temps positif, il faut que l'on ait $y'_\nu = 0$, et partant que $y_\nu = x_\nu a_\nu^{(\nu)}$ soit divisible par $a_\nu^{(\nu)}$, ce qu'il s'agissait de montrer; en même temps,

$$\mu'_\nu - x_\nu\mu_\nu = \mu'_{\nu-1}$$

devient un nombre contenu dans $[\beta_1, \beta_2, \ldots, \beta_{\nu-1}]$ et dans $\mathfrak{m}$, ou devient égal à zéro, au cas où $\nu = 1$.

---

(1) C'est là-dessus que repose la théorie de la divisibilité des nombres rationnels entiers.

On déduit de là facilement que les n nombres μ_ν, que l'on obtient en posant successivement $\nu = n, n-1, \ldots, 2, 1$, jouissent des propriétés énoncées dans le théorème à démontrer; car tout nombre μ du module $\mathfrak{m}$, c'est-à-dire tout nombre μ'_n contenu à la fois dans $\mathfrak{a}$ et dans $\mathfrak{b} = [\beta_1, \beta_2, \ldots, \beta_n]$, est de la forme

$$\mu = \mu'_{n-1} + x_n \mu_n,$$

où x_n désigne un nombre rationnel entier, et μ'_{n-1} un nombre appartenant aux deux modules $\mathfrak{a}$ et $[\beta_1, \beta_2, \ldots, \beta_{n-1}]$, et par suite aussi au module $\mathfrak{m}$; tout nombre μ'_{n-1} de cette nature est de la forme

$$\mu'_{n-1} = \mu'_{n-2} + x_{n-1} \mu_{n-1},$$

où x_{n-1} désigne un nombre rationnel entier, et μ'_{n-2} un nombre appartenant aux deux modules $\mathfrak{a}$ et $[\beta_1, \beta_2, \ldots, \beta_{n-2}]$, et ainsi de suite; enfin tout nombre μ'_1, appartenant aux deux modules $\mathfrak{a}$ et $[\beta_1]$ est de la forme

$$\mu'_1 = x_1 \mu_1,$$

où x_1 désigne un nombre rationnel entier. Il est donc démontré que tout nombre μ du module $\mathfrak{m}$ peut être représenté sous la forme

$$\mu = x_1 \mu_1 + x_2 \mu_2 + \ldots + x_n \mu_n,$$

$x_1, x_2, \ldots, x_n$ étant des nombres rationnels entiers; et comme, réciproquement, tout système choisi arbitrairement de nombres rationnels entiers $x_1, x_2, \ldots, x_n$ produit certainement un nombre μ appartenant au module $\mathfrak{m}$, puisque $\mu_1, \mu_2, \ldots, \mu_n$ sont eux-mêmes contenus dans $\mathfrak{m}$, ces n nombres $\mu_1, \mu_2, \ldots, \mu_n$ formeront une base du module $\mathfrak{m}$.

Pour démontrer enfin la dernière partie du théorème, nous allons considérer tous les nombres

$$\beta' = z'_1 \beta_1 + z'_2 \beta_2 + \ldots + z'_n \beta_n$$

du module $\mathfrak{b}$, dans lesquels les nombres rationnels entiers z'_1, $z'_2, \ldots, z'_n$ remplissent les n conditions

$$0 \leqq z'_\nu < a'^{(\nu)}_\nu,$$

et nous démontrerons que ces nombres β', dont le nombre est évidemment égal à $a'_1 a''_2 \ldots a'^{(n)}_n$, forment un système complet de repré-

sentants du module $\mathfrak{b}$ suivant $\mathfrak{m}$ (ou $\mathfrak{a}$). En effet, *premièrement,* tous ces nombres β' appartenant au module $\mathfrak{b}$ sont incongrus suivant $\mathfrak{m}$; car soit

$$z'_1\beta_1 + \ldots + z'_n\beta_n \equiv z''_1\beta_1 + \ldots + z''_n\beta_n \pmod{\mathfrak{a}},$$

les nombres $z''_1, z''_2, \ldots, z''_n$ remplissant les n mêmes conditions que les nombres $z'_1, z'_2, \ldots, z'_n$; si les n différences

$$z'_n - z''_n, \quad z'_{n-1} - z''_{n-1}, \quad \ldots, \quad z'_2 - z''_2, \quad z'_1 - z''_1$$

ne s'annulent pas toutes, soit $z'_\nu - z''_\nu$ la première d'entre elles qui ait une valeur différente de zéro, valeur que, à cause de la symétrie, nous supposerons positive, et qui en outre est $< a_\nu^{(\nu)}$, puisque les deux nombres z'_ν et z''_ν sont $> a_\nu^{(\nu)}$; alors la différence

$$(z'_1 - z''_1)\beta_1 + \ldots + (z'_\nu - z''_\nu)\beta_\nu$$

serait évidemment un nombre μ_ν, contenu dans $\mathfrak{a}$ et dans $[\beta_1, \beta_2, \ldots, \beta_n]$, et dans lequel le coefficient de β_ν serait positif et $< a_\nu^{(\nu)}$, ce qui est contraire à la définition du nombre μ_ν; donc deux systèmes différents quelconques de n nombres $z'_1, z'_2, \ldots, z'_n$, qui satisfont aux conditions ci-dessus, produisent aussi deux nombres β' du module $\mathfrak{b}$, incongrus suivant $\mathfrak{a}$. *En second lieu,* il est aisé de voir que tout nombre arbitraire

$$\beta = z_1\beta_1 + z_2\beta_2 + \ldots + z_n\beta_n$$

du module $\mathfrak{b}$ est congru suivant $\mathfrak{a}$ (ou $\mathfrak{m}$) à l'un de ces nombres β'; car, si $z_1, z_2, \ldots, z_n$ sont donnés, il est clair que l'on pourra choisir successivement les n nombres rationnels entiers

$$x_n, \quad x_{n-1}, \quad \ldots, \quad x_2, \quad x_1,$$

de manière que les n nombres

$$\begin{aligned}
z'_n &= z_n + a_n^{(n)} x_n, \\
z'_{n-1} &= z_{n-1} + a_{n-1}^{(n)} x_n + a_{n-1}^{(n-1)} x_{n-1}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots, \\
z'_2 &= z_2 + a_2^{(n)} x_n + a_2^{(n-1)} x_{n-1} + \ldots + a''_2 x_2, \\
z'_1 &= z_1 + a_1^{(n)} x_n + a_1^{(n-1)} x_{n-1} + \ldots + a''_1 x_2 + a'_1 x_1
\end{aligned}$$

remplissent les n conditions ci-dessus $0 \leqq z'_\nu < a_\nu^{(\nu)}$; si l'on pose

maintenant

$$\beta' = z'_1\beta_1 + z'_2\beta_2 + \ldots + z'_n\beta_n,$$

on aura

$$\beta' = \beta + x_1\mu_1 + x_2\mu_2 + \ldots + x_n\mu_n,$$

et partant $\beta \equiv \beta' \pmod{\mathfrak{m}}$. C. Q. F. D.

§ 4. — *Systèmes irréductibles.*

1° Un système de n nombres $\alpha_1, \alpha_2, \ldots, \alpha_n$ sera dit un *système irréductible,* et ces nombres seront dits *indépendants* entre eux, quand la somme

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n,$$

pour tout système de nombres rationnels entiers (ou fractionnaires) $x_1, x_2, \ldots, x_n$, qui ne seront pas tous nuls, prendra une valeur différente de zéro; alors deux systèmes différents quelconques de nombres rationnels $x_1, x_2, \ldots, x_n$ produiront évidemment aussi deux sommes α inégales. Dans le cas contraire, c'est-à-dire quand il existe un système de nombres rationnels $x_1, x_2, \ldots, x_n$, qui ne s'annulent pas tous et pour lesquels la somme α devient égale à zéro, le système des nombres $\alpha_1, \alpha_2, \ldots, \alpha_n$ sera dit *réductible,* et ces nombres eux-mêmes seront *dépendants* entre eux. Si l'on veut conserver encore cette terminologie pour le cas de $n = 1$, un nombre unique formera évidemment un système réductible ou un système irréductible, suivant qu'il sera égal à zéro ou non. De la définition précédente découlent aisément les théorèmes suivants, dont le nombre pourrait être extraordinairement accru, sur les *déterminants* de nombres rationnels.

2° Si les n nombres $\alpha_1, \alpha_2, \ldots, \alpha_n$ sont indépendants entre eux, les n nombres

$$\begin{aligned}
\alpha'_1 &= c'_1\alpha_1 + c'_2\alpha_2 + \ldots + c'_n\alpha_n,\\
\alpha'_2 &= c''_1\alpha_1 + c''_2\alpha_2 + \ldots + c''_n\alpha_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
\alpha'_n &= c^{(n)}_1\alpha_1 + c^{(n)}_2\alpha_2 + \ldots + c^{(n)}_n\alpha_n,
\end{aligned}$$

les n^2 coefficients c désignant des nombres rationnels entiers ou fractionnaires, formeront un système irréductible ou réductible,

suivant que le déterminant

$$C = \Sigma \pm c'_1 c''_2 \dots c^{(n)}_n$$

sera ou non différent de zéro.

Car, si $x_1, x_2, \dots, x_n$ désignent des nombres rationnels arbitraires, ne s'annulant pas tous, la somme

$$x_1 \alpha'_1 + x_2 \alpha'_2 + \dots + x_n \alpha'_n = \alpha',$$

puisque $\alpha_1, \alpha_2, \dots, \alpha_n$ sont indépendants entre eux, ne pourra s'annuler que si l'on a à la fois

$$\begin{aligned} c'_1 x_1 + c''_1 x_2 + \dots + c^{(n)}_1 x_n &= 0, \\ c'_2 x_1 + c''_2 x_2 + \dots + c^{(n)}_2 x_n &= 0, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots &, \\ c'_n x_1 + c''_n x_2 + \dots + c^{(n)}_n x_n &= 0, \end{aligned}$$

ce qui est impossible lorsque C a une valeur différente de zéro, et par suite, dans ce cas, les nombres $\alpha'_1, \alpha'_2, \dots, \alpha'_n$ sont indépendants entre eux. Mais, si l'on a $C = 0$, il existera toujours un système de nombres rationnels $x_1, x_2, \dots, x_n$ qui satisferont aux équations précédentes, sans toutefois être tous nuls; cela se voit immédiatement, lorsque tous les n^2 coefficients c s'annulent; s'il n'en est pas ainsi, alors, parmi ceux des déterminants mineurs de C qui ne s'annulent pas, il y en aura un, par exemple le déterminant

$$\Sigma \pm c'_1 c''_2 \dots c^{(r)}_r,$$

qui sera du degré *le plus élevé* $r < n$, de sorte que tous les déterminants mineurs de degré plus élevé s'annulent; dans ce cas, comme on sait, les $n - r$ dernières des équations ci-dessus seront des conséquences identiques des r précédentes, et l'on pourra donner à celles-ci la forme

$$\begin{aligned} x_1 &= p'_{r+1} x_{r+1} + \dots + p'_n x_n, \\ \dots\dots\dots\dots\dots\dots\dots\dots &, \\ x_r &= p^{(r)}_{r+1} x_{r+1} + \dots + p^{(r)}_n x_n, \end{aligned}$$

où les $r(n - r)$ coefficients p sont des nombres rationnels; en attribuant maintenant aux quantités $x_{r+1}, \dots, x_n$, au nombre de $n - r \geqq 1$, des valeurs rationnelles arbitraires, pourvu seulement qu'elles ne soient pas toutes nulles, les quantités $x_1, \dots, x_r$ pren-

dront également des valeurs rationnelles, et l'on aura par suite un système de n nombres rationnels $x_1, x_2, \ldots, x_n$, qui ne s'annuleront pas tous, et pour lesquels la somme α' sera égale à zéro; donc, dans ce cas, les n nombres $\alpha'_1, \alpha'_2, \ldots, \alpha'_n$ seront dépendants entre eux.

C. Q. F. D.

3° Si les n nombres indépendants entre eux $\alpha_1, \alpha_2, \ldots, \alpha_n$, d'une part, et d'autre part les n nombres $\alpha'_1, \alpha'_2, \ldots, \alpha'_n$ forment les uns et les autres une base d'un seul et même module $\mathfrak{a}$, on aura alors

$$\alpha'_\nu = c_1^{(\nu)}\alpha_1 + c_2^{(\nu)}\alpha_2 + \ldots + c_n^{(\nu)}\alpha_n,$$

où les n^2 coefficients c désignent des nombres rationnels entiers, dont le déterminant $= \pm 1$, et par suite les nombres $\alpha'_1, \alpha'_2, \ldots, \alpha'_n$ seront aussi indépendants entre eux.

En effet, puisque les nombres α'_ν sont contenus dans le module $\mathfrak{a} = [\alpha_1, \alpha_2, \ldots, \alpha_n]$, il existera dans tous les cas n équations de la forme précédente, dans lesquelles les coefficients c seront des nombres rationnels entiers. Puisque réciproquement les n nombres α_ν sont contenus dans le module $\mathfrak{a} = [\alpha'_1, \alpha'_2, \ldots, \alpha'_n]$, il existera aussi n équations de la forme

$$\alpha_\nu = e_1^{(\nu)}\alpha'_1 + e_2^{(\nu)}\alpha'_2 + \ldots + e_n^{(\nu)}\alpha'_n,$$

à coefficients e pareillement rationnels et entiers. En y substituant les n premières équations pour les n nombres α'_ν, et considérant que les n nombres α_ν forment un système irréductible, il s'ensuit que la somme

$$e_1^{(\nu)}c'_{\nu'} + e_2^{(\nu)}c''_{\nu'} + \ldots + e_n^{(\nu)}c_{\nu'}^{(n)} = 1 \quad \text{ou} \quad = 0,$$

selon que les indices ν, ν' seront égaux ou inégaux. Donc le produit de déterminants

$$\Sigma \pm c'_1 c''_2 \ldots c_n^{(n)} . \Sigma \pm e'_1 e''_2 \ldots e_n^{(n)} = 1,$$

et par suite, puisque les deux facteurs sont des nombres rationnels entiers,

$$\Sigma \pm c'_1 c''_2 \ldots c_n^{(n)} = \Sigma e'_1 e''_2 \ldots e_n^{(n)} = \pm 1.$$

C. Q. F. D.

Réciproquement, il est clair que $[\alpha'_1, \alpha'_2, \ldots, \alpha'_n] = [\alpha_1, \alpha_2, \ldots, \alpha_n]$,

quand il existe n équations de la forme

$$\alpha'_\nu = c_1^{(\nu)}\alpha_1 + \ldots + c_n^{(\nu)}\alpha_n,$$

où les coefficients c sont des nombres rationnels entiers, dont le déterminant $= \pm 1$.

4° Si les n nombres indépendants entre eux $\beta_1, \ldots, \beta_n$ forment la base d'un module $\mathfrak{b}$, et que de ces nombres dépendent les n nombres $\alpha_1, \alpha_2, \ldots, \alpha_n$ de la base d'un module $\mathfrak{a}$, au moyen de n équations de la forme

$$\alpha_\nu = b_1^{(\nu)}\beta_1 + \ldots + b_n^{(\nu)}\beta_n,$$

les coefficients b désignant des nombres rationnels entiers, dont le déterminant B est différent de zéro, le nombre des classes sera

$$(\mathfrak{b}, \mathfrak{a}) = \pm B.$$

En effet, puisque chacun des nombres $\beta_1, \ldots, \beta_n$, et par suite tout nombre β du module $[\beta_1, \beta_2, \ldots, \beta_n]$ peut, en le multipliant par le nombre rationnel B différent de zéro, être changé en un nombre du module $\mathfrak{a}$, qui est divisible par $\mathfrak{b}$, et qui par suite aussi est le plus petit commun multiple de $\mathfrak{a}$ et $\mathfrak{b}$, $\mathfrak{a}$ possédera (d'après le § 3, 2°) n nombres de base de la forme

$$\alpha'_\nu = a_1^{(\nu)}\beta_1 + a_2^{(\nu)}\beta_2 + \ldots + a_\nu^{(\nu)}\beta_\nu,$$

où les coefficients a sont des nombres rationnels entiers et choisis, de telle manière que l'on ait

$$(\mathfrak{b}, \mathfrak{a}) = a'_1 a''_2 \ldots a_n^{(n)} = \Sigma \pm a'_1 a''_2 \ldots a_n^{(n)}.$$

Comme, de plus, les n nombres $\alpha_1, \ldots, \alpha_n$ forment également une base du module $\mathfrak{a}$, et que (d'après 2°) chacun de ces deux systèmes de n nombres est irréductible, puisqu'on a supposé que le système $\beta_1, \ldots, \beta_n$ l'était, on aura alors (d'après 3°) n équations de la forme

$$\alpha'_\nu = c_1^{(\nu)}\alpha_1 + \ldots + c_n^{(\nu)}\alpha_n,$$

ayant des coefficients rationnels entiers c, dont le déterminant

$$\Sigma \pm c'_1 c''_2 \ldots c_n^{(n)} = \pm 1.$$

En y substituant, à la place des nombres $\alpha_1, \ldots, \alpha_n$, leurs expressions ci-dessus au moyen des n nombres indépendants entre eux

$\beta_1, \ldots, \beta_n$, on voit, par la comparaison avec les expressions précédentes des nombres α'_ν au moyen des mêmes nombres $\beta_1, \ldots, \beta_n$, que

$$a_\nu^{(\nu)} = c_1^{(\nu)} b'_\nu + c_2^{(\nu)} b''_\nu + \ldots + c_n^{(\nu)} b_\nu^{(n)},$$

et par suite

$$\Sigma \pm a'_1 \ldots a_n^{(n)} = \Sigma \pm c'_1 \ldots c_n^{(n)} . \Sigma \pm b'_1 \ldots b_n^{(n)};$$

on a donc bien $(\mathfrak{b}, \mathfrak{a}) = \pm B$. C. Q. F. D.

Ce théorème important peut aisément (et de la manière la plus simple au moyen du théorème suivant) s'étendre au cas plus général où les coefficients b sont des nombres rationnels *fractionnaires;* on obtient ainsi ce théorème

$$(\mathfrak{b}, \mathfrak{a}) = \pm B(\mathfrak{a}, \mathfrak{b}),$$

et chacun des deux nombres de classes $(\mathfrak{a}, \mathfrak{b})$ et $(\mathfrak{b}, \mathfrak{a})$ peut se déterminer d'après une règle simple, au moyen du déterminant B et de tous ses déterminants mineurs.

5° Si, parmi les m nombres $\alpha_1, \alpha_2, \ldots, \alpha_m$, qui forment une base du module $\mathfrak{a}$, il n'y en a que n qui soient indépendants entre eux, il existera une base du même module $\mathfrak{a}$ composée de n nombres indépendants entre eux $\alpha'_1, \alpha'_2, \ldots, \alpha'_n$.

L'hypothèse de ce théorème sera évidemment toujours vérifiée, quand tous les m nombres $\alpha_1, \ldots, \alpha_m$ seront représentés au moyen de n nombres indépendants entre eux $\omega_1, \ldots, \omega_n$, sous la forme

$$\alpha_\mu = r_1^{(\mu)} \omega_1 + r_2^{(\mu)} \omega_2 + \ldots + r_n^{(\mu)} \omega_n,$$

le système de coefficients

$$(r) \qquad \begin{cases} r'_1, & r'_2, & \ldots, & r'_n, \\ r''_1, & r''_2, & \ldots, & r''_n, \\ \ldots & \ldots & \ldots, & \ldots, \\ r_1^{(m)}, & r_2^{(m)}, & \ldots, & r_n^{(m)} \end{cases}$$

se composant uniquement de nombres rationnels, et l'un au moins des déterminants partiels R du degré n, que l'on peut former avec ce système et qui sont au nombre de

$$\frac{m(m-1)\ldots(m-n+1)}{1.2\ldots n},$$

ayant une valeur différente de zéro, puisque sans cela n quelconques des m nombres α_μ seraient dépendants entre eux. Réciproquement, il résulte de l'hypothèse du théorème que les m nombres α_μ pourront toujours être représentés au moyen de n nombres ω_ν indépendants entre eux; car, si l'on choisit pour ces derniers, par exemple, les n nombres, parmi les m nombres α_μ qui forment réellement un système irréductible, alors, puisque les $n+1$ nombres $\alpha_\mu, \omega_1, \ldots, \omega_n$ sont dépendants entre eux, il existera, pour chaque indice μ, une équation correspondante, de la forme

$$x_0\alpha_\mu + x_1\omega_1 + x_2\omega_2 + \ldots + x_n\omega_n = 0,$$

dont les coefficients x sont rationnels et ne s'évanouissent pas tous; comme, de plus, les nombres $\omega_1, \omega_2, \ldots, \omega_n$ sont indépendants entre eux, x_0 devra différer de zéro, et par suite α_μ pourra être représenté de la manière indiquée, au moyen des n nombres ω_ν; comme enfin parmi les m nombres α_μ se trouvent aussi les n nombres ω_ν, l'un au moins des déterminants R sera différent de zéro.

Je vais partir, en conséquence, de l'hypothèse que les m nombres α_μ sont représentés de la manière indiquée au moyen de n nombres ω_ν indépendants entre eux, et je vais démontrer que, de quelque manière que l'on choisisse ces nombres ω_ν, il existera toujours n nombres α'_ν de la forme

$$\alpha'_\nu = c_1^{(\nu)}\omega_1 + c_2^{(\nu)}\omega_2 + \ldots + c_\nu^{(\nu)}\omega_\nu,$$

à coefficients rationnels c, qui formeront une base du même module $\mathfrak{a} = [\alpha_1, \alpha_2, \ldots, \alpha_m]$. Pour cela, je remarque d'abord qu'évidemment on peut toujours choisir un nombre rationnel, entier et positif k, de telle manière que tous les mn produits $kr_\nu^{(\mu)}$ deviennent des nombres entiers; si l'on pose maintenant

$$\omega_1 = k\beta_1, \quad \omega_2 = k\beta_2, \quad \ldots, \quad \omega_n = k\beta_n,$$

et que l'on exprime les nombres α_μ au moyen des nombres β_ν, il en résultera que le module $\mathfrak{a} = [\alpha_1, \alpha_2, \ldots, \alpha_m]$ est divisible par le module $\mathfrak{b} = [\beta_1, \beta_2, \ldots, \beta_n]$, et par suite qu'il est le plus petit commun multiple de $\mathfrak{a}$, $\mathfrak{b}$. Comme, de plus, les n nombres β_ν, étant multipliés par k, se changent dans les n nombres ω_ν, et que ceux-ci, étant multipliés par un déterminant R différent de zéro, se chan-

gent en des nombres de la forme

$$x_1\alpha_1 + x_2\alpha_2 + \ldots + x_m\alpha_m,$$

les coefficients x désignant des nombres rationnels entiers ou fractionnaires, il est clair que tout nombre β du module $\mathfrak{b}$, multiplié par un nombre rationnel différent de zéro, peut se changer lui-même en un nombre du module $\mathfrak{a}$, et il résulte de là (d'après le § 3, 2°) que le plus petit commun multiple $\mathfrak{a}$ des deux modules $\mathfrak{a}$, $\mathfrak{b}$ possède une base composée de n nombres de la forme

$$\alpha'_\nu = a_1^{(\nu)}\beta_1 + a_2^{(\nu)}\beta_2 + \ldots + a_\nu^{(\nu)}\beta_\nu,$$

les coefficients a désignant des nombres rationnels entiers, et le produit $a'_1 a''_2 \ldots a_n^{(n)}$ étant différent de zéro. Si l'on y exprime de nouveau les n nombres β_ν au moyen des n nombres ω_ν, on en conclut la vérité de l'assertion ci-dessus, ce qui démontre en même temps le théorème.

6° A la démonstration précédente j'ajouterai encore les remarques suivantes. Comme les m nombres α_μ forment, aussi bien que les n nombres α'_ν, une base du même module $\mathfrak{a}$, il existera m équations de la forme

$$\alpha_\mu = p_1^{(\mu)}\alpha'_1 + p_2^{(\mu)}\alpha'_2 + \ldots + p_n^{(\mu)}\alpha'_n,$$

et n équations de la forme

$$\alpha'_\nu = q'_\nu\alpha_1 + q''_\nu\alpha_2 + \ldots + q_\nu^{(m)}\alpha_m,$$

où les $2mn$ coefficients p et q sont tous des nombres rationnels *entiers;* en substituant les premières expressions dans les secondes, et considérant que les n nombres α'_ν sont indépendants entre eux, on en déduit que la somme

$$q'_\nu p'_{\nu'} + q''_\nu p''_{\nu'} + \ldots + q_\nu^{(m)} p_{\nu'}^{(m)} = 1 \quad \text{ou} \quad = 0,$$

suivant que les deux indices ν, ν', contenus dans la série $1, 2, \ldots, n$, sont égaux ou inégaux. En désignant donc par P respectivement tous les déterminants partiels du $n^{\text{ième}}$ degré formés avec le système de coefficients (p), et par Q les déterminants correspondants formés de la même manière avec le système de coefficients (q), on sait que la somme

$$\Sigma PQ,$$

étendue à toutes les combinaisons différentes de n indices supérieurs, est égale à l'unité, et, par suite, tous les déterminants P n'ont point de commun diviseur; et réciproquement, cette propriété des déterminants P est essentielle pour que les n nombres α'_ν, aussi bien que les m nombres

$$\alpha_\mu = p_1^{(\mu)}\alpha'_1 + \ldots + p_n^{(\mu)}\alpha'_n,$$

forment des bases du même module $\mathfrak{a}$.

Un système de coefficients, tel que (p), n'est évidemment qu'un cas particulier du système de coefficients précédent (r). Maintenant, les n nombres α'_ν pouvant également se représenter sous la forme

$$\alpha'_\nu = e_1^{(\nu)}\omega_1 + e_2^{(\nu)}\omega_2 + \ldots + e_n^{(\nu)}\omega_n,$$

à n^2 coefficients rationnels e, dont le déterminant

$$\mathrm{E} = \Sigma \pm e'_1 e''_2 \ldots e_n^{(n)}$$

est différent de zéro, il vient

$$r_\nu^{(\mu)} = p_1^{(\mu)} e'_\nu + p_2^{(\mu)} e''_\nu + \ldots + p_n^{(\mu)} e_\nu^{(n)},$$

et, par suite, deux déterminants correspondants quelconques R, P, formés avec les systèmes de coefficients (r), (p), ont entre eux la relation

$$\mathrm{R} = \mathrm{PE}.$$

Le problème de trouver, au moyen d'un système donné (r), tous les systèmes (p) correspondants peut se résoudre de la manière la plus compréhensive et la plus élégante par la généralisation d'une méthode appliquée par Gauss [1] dans des cas spéciaux, et dans laquelle on utilise les relations identiques qui ont lieu entre les déterminants partiels; cependant cela nous conduirait ici beaucoup trop loin, et je me contenterai d'avoir démontré l'*existence* d'un tel système (p), duquel, comme on le voit immédiatement (d'après 3°), on peut tirer tous les autres systèmes (p) par la composition avec tous les systèmes possibles de n^2 nombres rationnels entiers dont le déterminant $= \pm 1$.

Dans la pratique, c'est-à-dire dans tous les cas où l'on donne

[1] *Disquisitiones arithmeticæ*, art. 234, 236, 279.

numériquement les coefficients r, que l'on peut, sans diminuer la généralité, supposer être des nombres *entiers*, on arrivera au but, de la manière la plus prompte, par un enchaînement de transformations élémentaires, en s'appuyant sur cette proposition évidente, qu'un module $[\alpha_1, \alpha_2, \ldots, \alpha_m]$ n'est pas altéré quand on remplace, par exemple, le nombre α_1 par $\alpha_1 + x\alpha_2$, x étant un nombre rationnel entier quelconque. Les déterminants partiels R^0, correspondants à toutes les combinaisons de n nombres de la nouvelle base

$$\alpha_1^0 = \alpha_1 + x\alpha_2, \quad \alpha_2^0 = \alpha_2, \quad \alpha_3^0 = \alpha_3, \quad \ldots, \quad \alpha_m^0 = \alpha_m,$$

et au nouveau système de coefficients (r^0), coïncideront en partie avec les déterminants R correspondants à l'ancienne base

$$\alpha_1 = \alpha_1^0 - x\alpha_2^0, \quad \alpha_2 = \alpha_2^0, \quad \alpha_3 = \alpha_3^0, \quad \ldots, \quad \alpha_m = \alpha_m^0;$$

ils seront en partie de la forme $R_1^0 = R_1 + xR_2$, et de là on déduit facilement que le plus grand commun diviseur E des déterminants R est en même temps celui des déterminants R^0; donc les déterminants R^0 ne peuvent pas non plus s'annuler tous à la fois. De ces transformations de la base du module $\mathfrak{a}$, on fera maintenant l'usage suivant :

Les m coefficients $r_n^{(\mu)}$ du nombre ω_n ne peuvent pas s'annuler tous, car alors tous les déterminants R seraient nuls. Si maintenant *deux* au moins de ces coefficients, par exemple r'_n et r''_n, sont différents de zéro, et si l'on a, en valeur absolue, $r'_n \geq r''_n$, on pourra choisir le nombre rationnel entier x de manière que l'on ait, en valeur absolue, $r'_n + xr''_n < r''_n$ [1]; on obtient alors, par la transformation élémentaire ci-dessus, une nouvelle base, dans laquelle tous les m coefficients $r_n^{(\mu)}$, à l'exception du premier r'_n, sont restés invariables, et ce coefficient unique est remplacé par un autre de *moindre* valeur. Par une répétition successive de ce procédé, on arrivera donc nécessairement à une base, dans laquelle tous les m coefficients de ω_n, à l'exception d'un seul, seront nuls. Désignons le nombre de la base, dans lequel entre ce coefficient $a_n^{(n)}$ différent

[1] C'est encore ici le même principe qui sert de fondement à la théorie des nombres rationnels entiers.

de zéro, par

$$\alpha'_n = a_1^{(n)}\omega_1 + a_2^{(n)}\omega_2 + \ldots + a_n^{(n)}\omega_n,$$

et conservons-le invariable dans toutes les transformations suivantes de la base. Les déterminants partiels correspondants à la base actuelle ou s'évanouissent, ou sont de la forme $Sa_n^{(n)}$, S étant un déterminant partiel du $(n-1)^{\text{ième}}$ degré qui correspond à une combinaison arbitraire de $n-1$ des $m-1$ nombres de la base autres que α'_n, et qui est formé avec les $(n-1)^2$ coefficients correspondants de $\omega_1, \omega_2, \ldots, \omega_{n-1}$. Les déterminants S ne pouvant pas s'annuler tous, on procédera maintenant, avec ces $m-1$ nombres de la base actuelle, par rapport à ω_{n-1}, comme on l'a fait tout à l'heure avec les m nombres α_μ de la base primitive, par rapport à ω_n, et, si l'on continue toujours ces transformations, on finira par obtenir une base de $\mathfrak{a}$, composée de n nombres $\alpha'_1, \alpha'_2, \ldots, \alpha'_{n-1}, \alpha'_n$, de la forme

$$\alpha'_\nu = a_1^{(\nu)}\omega_1 + a_2^{(\nu)}\omega_2 + \ldots + a_\nu^{(\nu)}\omega_\nu,$$

et de $m - n = s$ nombres $\alpha''_1, \alpha''_2, \ldots, \alpha''_s$, qui s'annuleront tous, et par suite pourront être supprimés; les n coefficients $a_\nu^{(\nu)}$ différents de zéro pourront être choisis positifs, puisque α'_ν peut être remplacé, sans altération du module, par $-\alpha'_\nu$, et leur produit $a'_1 a''_2 \ldots a_n^{(n)}$ est évidemment le plus grand commun diviseur E de tous les déterminants partiels R.

Par là nous obtenons une seconde démonstration de l'important théorème (5°), et il est évident en même temps que, par la composition des transformations successives et par leur inversion, on trouve aussi bien le système de coefficients (p) qu'un système de coefficients (q). En effet, on obtient d'abord de cette manière m équations de la forme

$$\alpha_\mu = \sum^{\nu} p_\nu^{(\mu)}\alpha'_\nu + \sum^{\sigma} h_\sigma^{(\mu)}\alpha''_\sigma,$$

ou, les s nombres α''_σ étant nuls,

$$\alpha_\mu = \sum^{\nu} p_\nu^{(\mu)}\alpha'_\nu;$$

et, comme le déterminant de chacune des substitutions ou transfor-

mations est égal à 1, alors le déterminant du $m^{\text{ième}}$ degré

$$\begin{vmatrix} p'_1 & \dots & p'_n, & h'_1 & \dots & h'_s \\ \dots & \dots & \dots, & \dots & \dots & \dots \\ p_1^{(m)} & \dots & p_n^{(m)}, & h_1^{(m)} & \dots & h_s^{(m)} \end{vmatrix} = \Sigma PH = 1,$$

les quantités H étant les déterminants du $s^{\text{ième}}$ degré complémentaires des déterminants P, et formés avec le système de coefficients (h). Par inversion, on obtient le déterminant adjoint

$$\begin{vmatrix} q'_1 & \dots & q'_n, & k'_1 & \dots & k'_s \\ \dots & \dots & \dots & \dots & \dots & \dots \\ q_1^{(m)} & \dots & q_n^{(m)}, & k_1^{(m)} & \dots & k_s^{(m)} \end{vmatrix} = \Sigma QK = 1,$$

K désignant le déterminant complémentaire de Q; et, si P, Q sont deux déterminants correspondants, on a, comme on sait, H = Q, K = P; en même temps on obtient n équations de la forme

$$\alpha'_\nu = \sum^{\mu} q_\nu^{(\mu)} \alpha_\mu$$

et s équations de la forme

$$\alpha''_\sigma = \sum^{\mu} k_\nu^{(\mu)} \alpha_\mu = 0.$$

Ces dernières équations expriment de nouveau sous une autre forme la supposition primitive, que n seulement des m nombres α_μ sont indépendants entre eux, et l'on aurait pu fonder toute cette étude sur un pareil système de s équations.

On peut généralement abréger le calcul lui-même, en opérant à la fois plusieurs transformations élémentaires. Soit, par exemple, $m = 4$, $n = 2$, d'où $s = 2$, et

$$\alpha_1 = 21\,\omega_1, \quad \alpha_2 = 7\,\omega_1 + 7\,\omega_2, \quad \alpha_3 = 9\,\omega_2 - 3\,\omega_2, \quad \alpha_4 = 8\,\omega_1 + 2\,\omega_2,$$

partant

$$(r) \qquad \begin{cases} r'_1 = 21, & r''_1 = 7, & r'''_1 = 9, & r^{\text{IV}}_1 = 8, \\ r'_2 = 0, & r''_2 = 7, & r'''_2 = -3, & r^{\text{IV}}_2 = 2; \end{cases}$$

on obtient les six déterminants partiels

$$(R)\qquad \begin{cases} R_{1,2}=147, & R_{1,3}=-63, & R_{1,4}=42, \\ R_{3,4}=42, & R_{2,4}=-42, & R_{2,3}=-84, \end{cases}$$

où l'on a posé, pour abréger

$$r_1^{(\mu)}r_2^{(\mu')}-r_1^{(\mu')}r_2^{(\mu)}=R_{\mu,\mu'};$$

entre ces déterminants on a la relation identique

$$R_{1,2}R_{3,4}-R_{1,3}R_{2,4}+R_{1,4}R_{2,3}=0.$$

Comme maintenant ω_2 a dans α_4 le plus petit coefficient différent de zéro, on formera la nouvelle base

$$\beta_1=\alpha_1=21\omega_1, \qquad \beta_2=\alpha_2-3\alpha_4=-17\omega_1+\omega_2,$$
$$\beta_3=\alpha_3+2\alpha_4=25\omega_1+\omega_2, \qquad \beta_4=\alpha_4=8\omega_1+2\omega_2,$$

d'où s'ensuit, inversement,

$$\alpha_1=\beta_1, \quad \alpha_2=\beta_2+3\beta_4, \quad \alpha_3=\beta_3-2\beta_4, \quad \alpha_4=\beta_4.$$

Maintenant, comme ω_2, par exemple, dans β_2 a le plus petit coefficient 1 différent de zéro, on formera la troisième base

$$\gamma_1=\beta_1=21\omega_1, \qquad \gamma_2=\beta_2=-17\omega_1+\omega_2,$$
$$\gamma_3=-\beta_2+\beta_3=42\omega_1, \qquad \gamma_4=-2\beta_2+\beta_4=42\omega_1,$$

d'où s'ensuit, inversement,

$$\beta_1=\gamma_1, \quad \beta_2=\gamma_2, \quad \beta_3=\gamma_2+\gamma_3, \quad \beta_4=2\gamma_2+\gamma_4.$$

Actuellement γ_2 étant le seul nombre dans lequel ω_2 a un coefficient différent de zéro, et γ_1 étant, parmi les trois autres nombres, celui dans lequel ω_1 a le plus petit coefficient 21, on formera la quatrième base

$$\delta_1=\gamma_1=21\omega_1, \qquad \delta_2=\gamma_2=-17\omega_1+\omega_2,$$
$$\delta_3=-2\gamma_1+\gamma_3=0, \qquad \delta_4=-2\gamma_1+\gamma_4=0,$$

d'où l'on tire, inversement,

$$\gamma_1=\delta_1, \quad \gamma_2=\delta_2, \quad \gamma_3=2\delta_1+\delta_3, \quad \gamma_4=2\delta_1+\delta_4.$$

Comme $\delta_3=\delta_4=0$, la transformation est terminée, et les substi-

tutions successives donnent

$$\begin{aligned}
\alpha_1 &= \delta_1 &&&&= \delta_1,\\
\alpha_2 &= 6\delta_1 + 7\delta_2 &&+ 3\delta_4 &&= 6\delta_1 + 7\delta_2,\\
\alpha_3 &= -2\delta_1 - 3\delta_2 + \delta_3 &&- 2\delta_4 &&= -2\delta_1 - 3\delta_2,\\
\alpha_4 &= 2\delta_1 + 2\delta_2 &&+ \delta_4 &&= 2\delta_1 + 2\delta_2,
\end{aligned}$$

et inversement

$$\begin{aligned}
\delta_1 &= \alpha_1 &&&&= 21\omega_1,\\
\delta_2 &= \alpha_2 &&- 3\alpha_1 &&= -17\omega_1 + \omega_2,\\
\delta_3 &= -2\alpha_1 - \alpha_2 + \alpha_3 &&+ 5\alpha_4 &&= 0,\\
\delta_4 &= -2\alpha_1 - 2\alpha_2 &&+ 7\alpha_4 &&= 0.
\end{aligned}$$

Comme $\delta_1, \delta_2, \delta_3, \delta_4$ sont les quantités qui, dans la théorie générale, ont été désignées par $\alpha'_1, \alpha'_2, \alpha''_1, \alpha''_2$, on aura

$$(p)\qquad \begin{cases} p'_1 = 1, & p''_1 = 6, & p'''_1 = -2, & p^{IV}_1 = 2,\\ p'_2 = 0, & p''_2 = 7, & p'''_2 = -3, & p^{IV}_2 = 2; \end{cases}$$

on obtient donc, pour les déterminants proportionnels aux R,

$$(\mathrm{P})\qquad \begin{cases} \mathrm{P}_{1,2} = 7, & \mathrm{P}_{1,3} = -3, & \mathrm{P}_{1,4} = 2,\\ \mathrm{P}_{3,4} = 2, & \mathrm{P}_{2,4} = -2, & \mathrm{P}_{2,3} = -4; \end{cases}$$

on a de même

$$(q)\qquad \begin{cases} q_1 = 1, & q''_1 = 0, & q'''_1 = 0, & q^{IV}_1 = 0,\\ q'_2 = 0, & q''_2 = 1, & q'''_2 = 0, & q^{IV}_2 = -3, \end{cases}$$

et

$$(\mathrm{Q})\qquad \begin{cases} \mathrm{Q}_{1,2} = 1, & \mathrm{Q}_{1,3} = 0, & \mathrm{Q}_{1,4} = -3,\\ \mathrm{Q}_{3,4} = 0, & \mathrm{Q}_{2,4} = 0, & \mathrm{Q}_{2,3} = 0. \end{cases}$$

Ensuite, des systèmes de coefficients

$$(h)\qquad \begin{cases} h'_1 = 0, & h''_1 = 0, & h'''_1 = 1, & h^{IV}_1 = 0,\\ h'_2 = 0, & h''_2 = 3, & h'''_2 = -2, & h^{IV}_2 = 1, \end{cases}$$

et

$$(k)\qquad \begin{cases} k'_1 = -2, & k''_1 = -1, & k'''_1 = 1, & k^{IV}_1 = 5,\\ k'_2 = -2, & k''_2 = -2, & k'''_2 = 0, & k^{IV}_2 = 7, \end{cases}$$

on tire les déterminants $H_{\mu,\mu'} = Q_{\mu,\mu'}$ et $K_{\mu,\mu'} = P_{\mu,\mu'}$, qui sont respectivement complémentaires de $P_{\mu,\mu'}$ et $Q_{\mu,\mu'}$,

$$(H)\quad \begin{cases} H_{1,2} = h'''_1 h^{IV}_2 - h^{IV}_1 h'''_2, & H_{1,3} = h^{IV}_1 h''_2 - h''_1 h^{IV}_2, & H_{1,4} = h''_1 h'''_2 - h'''_1 h''_2, \\ H_{3,4} = h'_1 h''_2 - h''_1 h'_2, & H_{2,4} = h'''_1 h'_2 - h'_1 h'''_2, & H_{2,3} = h'_1 h^{IV}_2 - h^{IV}_1 h'_2, \end{cases}$$

$$(K)\quad \begin{cases} K_{1,2} = h'''_1 h^{IV}_2 - h^{IV}_1 h'''_2, & K_{1,3} = h^{IV}_1 h''_2 - h''_1 h^{IV}_2, & K_{1,4} = h''_1 h'''_2 - h'''_1 h''_2, \\ K_{3,4} = h'_1 h''_2 - h''_1 h'_2, & K_{2,4} = h'''_1 h'_2 - h'_1 h'''_2, & K_{2,3} = h'_2 h^{IV}_2 - h^{IV}_1 h'_2, \end{cases}$$

et ainsi l'exemple se trouve complétement traité.

Pour conclure, je remarquerai que l'application au cas de $n = 1$ conduit au théorème fondamental sur le plus grand commun diviseur d'un nombre quelconque de nombres rationnels entiers, théorème sur lequel repose toute la théorie de divisibilité de ces nombres.

Les recherches dans cette première Section ont été exposées sous la forme spéciale qui répond à notre but; mais il est clair qu'elles ne cessent en rien d'être vraies, quand les lettres grecques désignent, non plus des *nombres,* mais des éléments quelconques, objets de l'étude que l'on poursuit, dont deux quelconques α, β, par une opération commutative et uniformément inversible (composition), tenant la place de l'addition, produiront un élément déterminé $\gamma = \alpha + \beta$ de la même espèce; les modules $\mathfrak{a}$ se changent en *groupes* d'éléments, dont les résultats (les *composés*) appartiennent toujours au même groupe; les coefficients rationnels entiers indiquent combien de fois un élément contribue à la génération d'un autre.

(*A suivre.*)