JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

PAUL LÉVY

L'arithmétique des lois de probabilité

Journal de mathématiques pures et appliquées 9^e série, tome 17, n° 1-4 (1938), p. 17-39.
<http://www.numdam.org/item?id=JMPA_1938_9_17_1-4_17_0>

L'arithmétique des lois de probabilité;

PAR PAUL LÉVY.

Il ne saurait être déplacé de parler dans ce volume du séminaire de M. Hadamard. Les travaux du savant sont des monuments durables qui témoigneront toujours de son génie; c'est à ses élèves qu'il appartient de louer l'œuvre du maître. Je ne peux que noter ici un des aspects les plus caractéristiques de ce séminaire : la variété des sujets qui y sont traités. Parcourant les périodiques récents, M. Hadamard y choisit, il nous l'a dit lui-même, tout ce qui l'amuse, et c'est visiblement avec une curiosité toujours amusée qu'il écoute les exposés faits par ses collaborateurs, dont chacun, suivant sa compétence, contribue à l'instruction de tous. Mais la compétence du maître s'étend aussi bien à l'arithmétique qu'à la théorie des équations aux dérivées partielles, et à la géométrie la plus concrète aussi bien qu'aux parties les plus abstraites de l'analyse générale. Sans effort, il passe d'un de ces sujets à l'autre, et, en intervenant fréquemment pour faire préciser un point obscur ou souligner au passage une idée particulièrement importante, prouve que rien, dans le domaine des mathématiques, ne lui est étranger.

Le présent travail est le texte d'une conférence faite à ce séminaire le 12 janvier 1937. J'ai déjà, dans des travaux antérieurs, exposé l'arithmétique des lois infiniment divisibles (1). Un théorème général de M. Khintchine, et un grand nombre de résultats particuliers de ce savant ou de ses élèves m'ont fait penser que le moment était venu de

(1) P. LÉVY, *Théorie de l'addition des variables aléatoires*, § 55. Cet ouvrage sera désigné dans la suite par l'abréviation « variables aléatoires ».

tenter une esquisse de l'arithmétique générale des lois de probabilité; le lecteur verra que, si maintenant le cadre existe, il reste, au moment où j'écris, beaucoup de problèmes particuliers à résoudre.

1. REMARQUES PRÉLIMINAIRES. — On sait que la loi $\mathcal{L}$ dont dépend une variable aléatoire réelle X peut être définie, soit par sa *fonction de répartition* $F(x)$, soit par sa *fonction caractéristique*

$$\varphi(z)=\int_{-\infty}^{+\infty} e^{izx}\,dF(x), \tag{1}$$

toujours bien définie pour z réel. Si $\mathcal{L}_1$, $\mathcal{L}_2$ et $\mathcal{L}$ désignent les lois dont dépendent respectivement deux variables indépendantes U et V et leur somme X, leurs fonctions caractéristiques sont liées par la relation

$$\varphi_1(z)\,\varphi_2(z)=\varphi(z), \tag{2}$$

et il est naturel de considérer la loi *résultante* $\mathcal{L}$ comme le *produit* des lois *composantes* $\mathcal{L}_1$ et $\mathcal{L}_2$, et de dire que ces lois composantes sont les *diviseurs* de la loi $\mathcal{L}$.

L'ensemble de toutes les lois possibles constitue ainsi un corps $\mathcal{K}$ dans lequel la multiplication est toujours bien définie; elle est commutative. Le symbole 1 doit naturellement représenter une loi telle que $\mathcal{L}\times 1=\mathcal{L}$, c'est-à-dire qu'il correspond au cas où X n'a qu'une valeur possible, égale à zéro. Une loi $\mathcal{L}$ est une *unité du corps* si l'on peut lui associer une autre loi $\mathcal{L}'$ de manière que $\mathcal{L}\mathcal{L}'=1$; cela implique que la variable X dépendant de la loi $\mathcal{L}$ n'ait qu'une valeur possible m (car si elle en avait au moins deux, il en serait de même pour le produit $\mathcal{L}\mathcal{L}'$); sa fonction caractéristique est e^{miz}; nous désignerons une telle loi par $\mathcal{U}^m$, $\mathcal{U}$ étant la loi qui correspond à $m=1$.

En dehors du cas où $\mathcal{L}$ est une unité, $|\varphi(z)|$, toujours au plus égal à l'unité, ne peut atteindre ce maximum (toujours atteint pour $z=0$), que pour une infinité dénombrable de valeurs de m, formant une progression arithmétique; on a donc presque partout $|\varphi(z)|<1$. Il en résulte que $\varphi^\alpha(z)$ ne peut être une fonction caractéristique que pour $\alpha\geq 0$. Le symbole $\mathcal{L}^\alpha$, représentant par définition la loi de fonction caractéristique $\varphi^\alpha(z)$ (si elle existe), a donc toujours un sens pour α

entier positif, peut en avoir pour des valeurs positives non entières de α, mais en dehors du cas des lois unités, n'a pas de sens pour α négatif.

Rappelons que la *dispersion* $\omega(\alpha)$ de la variable aléatoire X (ou de la loi $\mathcal{L}$ dont elle dépend) est la longueur minima d'un intervalle fermé auquel corresponde pour X une probabilité au moins égale à α; il s'agit d'un minimum toujours effectivement atteint. La valeur moyenne de cette fonction peut être utile à considérer; mais il peut arriver qu'elle soit infinie. Pour définir une moyenne qui soit toujours finie, introduisons une fonction $\lambda(\omega)$, définie pour ω positif, continue, constamment croissante, et restant bornée quand ω tend vers une des valeurs limites zéro et l'infini; par exemple $\frac{\omega}{\sqrt{1+\omega^2}}$ ou $\frac{\omega}{1+\omega}$. Nous appellerons dispersion moyenne de la loi $\mathcal{L}$ relativement à $\lambda(\omega)$, ou, plus simplement *dispersion moyenne* de la loi $\mathcal{L}$ (ou de la variable qui dépend de cette loi), et désignerons par $\delta = \delta(\mathcal{L})$ le nombre δ défini par la formule

$$\lambda(\delta) = \int_0^1 \lambda[\omega(\alpha)]\, d\alpha. \tag{3}$$

Il est toujours bien défini, nul pour les lois unités, positif dans tous les autres cas. Si la loi $\mathcal{L}$ dépend d'un paramètre variable t, dire que δ augmente indéfiniment revient à dire que $\omega(\alpha)$ augmente indéfiniment pour tout α positif, c'est-à-dire qu'à la limite toute la probabilité se concentre à l'infini; à un intervalle fini correspond dans ce cas une probabilité qui tend vers zéro. Au contraire, dire que δ tend vers zéro revient à dire que $\omega(\delta)$ tend vers zéro pour tout α inférieur à 1, c'est-à-dire qu'il existe un nombre m, fonction de t, tel que la variable $X-m$ dépendant de la loi $\mathcal{L}\mathfrak{U}^{-m}$ tende en probabilité vers zéro. On peut donc considérer que δ définit l'*écart* de la loi $\mathcal{L}$ et du type de loi unité (c'est du moins une définition possible).

Une propriété importante de l'écart ainsi défini est la suivante (1):

(1) Cette propriété appartient aussi à l'écart quadratique moyen, s'il est fini; mais ce qui oblige à introduire une notion différente de celle d'écart quadratique moyen est que, indépendamment du fait qu'il ne soit pas toujours fini, cet écart ne donne pas une définition acceptable pour l'écart de la loi étudiée et du type de loi unité. Du moins, il correspondrait à la convergence en moyenne de X vers une constante, et non à la convergence en probabilité, que nous considérons ici.

si $\mathcal{L} = \mathcal{L}'\mathcal{L}''$, *et si* $\mathcal{L}''$ *n'est pas une loi unité*, $\delta(\mathcal{L})$ *est supérieur à* $\delta(\mathcal{L}')$ (l'égalité étant exclue); c'est une conséquence immédiate du théorème 29, 1 de mon livre cité plus haut, d'après lequel la fonction $\omega(\alpha)$ relative à la loi $\mathcal{L}$ est toujours au moins égale à la fonction analogue relative à $\mathcal{L}'$, et lui est effectivement supérieure pour au moins certaines valeurs de α, donc dans au moins un intervalle.

Un produit infini de lois de probabilité est le symbole qui correspond à une série ΣX_n à termes aléatoires indépendants les uns des autres. Une telle série est, ou bien *quasi-convergente* (1), ou bien *essentiellement divergente;* dans le premier cas, ou bien elle est presque sûrement convergente, ou bien peut le devenir par l'addition d'une constante convenable à chacun de ses termes; sa somme est une variable aléatoire définie à une constante près; dans le deuxième cas elle est presque sûrement divergente, et il en est de même de toutes les séries obtenues en ajoutant à chaque terme une constante quelconque. Le *produit infini* $\Pi\mathcal{L}_n$ sera dit de même *quasi-convergent* dans le premier cas et *essentiellement divergent* dans le second cas; un produit quasi-convergent représente une loi définie à un facteur unité près. Nous dirons de même qu'une *suite* de lois $\mathcal{L}'_n$ est *quasi-convergente* si l'on peut la rendre convergente en multipliant chacune de ces lois par une loi unité.

Pour que le produit $\Pi\mathcal{L}_n$ *soit quasi-convergent, il faut et il suffit que* $\delta(\mathcal{L}_1\mathcal{L}_2\ldots\mathcal{L}_n)$, qui croît constamment avec n si aucun des $\mathcal{L}_n$ n'est une loi unité, *reste borné*; cela résulte immédiatement de ce que la fonction $\omega(\alpha)$ relative à $\mathcal{L}_1\mathcal{L}_2\ldots\mathcal{L}_n$, pour n'importe quelle valeur de α fixe et inférieur à un, reste bornée dans le cas de quasi-convergence et augmente indéfiniment dans le cas de divergence essentielle (2). La condition indiquée étant remplie si tous les produits finis $\mathcal{L}_1\mathcal{L}_2\ldots\mathcal{L}_n$

(1) Je propose ce terme, après avoir hésité longtemps à introduire le mot « convergentable », qui correspond mieux à l'idée que je voudrais exprimer; mais il choque notre oreille, sans doute parce qu'on n'a pas encore introduit le verbe « convergenter ». J'ai d'ailleurs déjà, dans l'expression « loi quasi-stable » utilisé le préfixe « quasi » devant un adjectif pour indiquer que la propriété exprimée par cet adjectif est vraie à une constante additive près.

(2) Cf. *Variables aléatoires*, § 43. Mentionnons aussi qu'une condition nécessaire évidente est que $\delta(\mathcal{L}_n)$ tende vers zéro.

sont des diviseurs d'une loi $\mathcal{L}$ indépendante de n, on est assuré dans un tel cas de la quasi-convergence du produit infini $\Pi\mathcal{L}_n$. De même, si une suite de lois $\mathcal{L}'_n$ est telle que pour tout n assez grand $\mathcal{L}'_n$ soit un diviseur de $\mathcal{L}'_{n-1}$, on est assuré de la quasi-convergence de cette suite; ce résultat n'est autre que le précédent appliqué au produit $\Pi\mathcal{L}_n$, en posant $\mathcal{L}'_{n-1} = \mathcal{L}_n\mathcal{L}'_n$.

Si chaque loi $\mathcal{L}_n$ est définie par sa fonction caractéristique $\varphi_n(z)$, la quasi-convergence du produit infini $\Pi\mathcal{L}_n$ ne dépend que des modules $|\varphi_n(z)|$; la condition nécessaire et suffisante pour cette quasi-convergence est que, au moins dans un petit intervalle comprenant l'origine, le module du produit

$$\Phi_n(z) = \varphi_1(z)\,\varphi_2(z)\ldots\varphi_n(z)$$

tende uniformément vers une limite $|\Phi(z)|$ (1); cela suffit d'ailleurs pour être assuré que la limite $|\Phi(z)|$ est bien définie pour tout z réel, et que, dans tout intervalle fini, non seulement l'erreur $|\Phi(z)| - |\Phi_n(z)|$, mais l'erreur relative $\log\left|\frac{\Phi(z)}{\Phi_n(z)}\right|$ tend vers zéro pour n infini. La fonction $\Phi(z)$ elle-même est définie à un facteur près de la forme e^{miz}.

Il faut bien préciser que la suite des produits finis $\mathcal{L}_1\mathcal{L}_2\ldots\mathcal{L}_n$ n'est pas du tout une suite de lois quelconques; le résultat qui précède ne peut pas s'étendre au cas d'une suite de lois quelconques. Si d'ailleurs la convergence du produit $\Pi|\varphi_n(z)|$ entraîne la quasi-convergence du produit $\Pi\varphi_n(z)$, il ne suffit pas de connaître la limite $|\Phi(z)|$ du premier produit pour connaître $\Phi(z)$ à un facteur près de la forme e^{miz}. Ainsi on peut choisir une suite partielle d'entiers n pour lesquelles on remplacera X_n par $-X_n$, donc $\varphi_n(z)$ par $\varphi_n(-z)$; $|\varphi_n(z)|$, et par suite $|\Phi(z)|$, n'est pas changé, et l'on peut avoir pour $\Phi(z)$ une infinité de fonctions différentes, dont l'ensemble a la puissance du continu.

Il peut enfin être utile d'indiquer que, si $\delta(\mathcal{L}_1\mathcal{L}_2\ldots\mathcal{L}_n)$ est connu, on peut borner supérieurement le nombre n' des facteurs $\mathcal{L}_\nu$ pour lesquels $\delta(\mathcal{L}_\nu)$ dépasse une valeur donnée ε; si inversement on connaît ce nombre n', et $\delta(\mathcal{L}_1\mathcal{L}_2\ldots\mathcal{L}_n)$, n est supérieur à une fonction de ε

(1) Nous indiquons ici sans démonstration un résultat inutile pour la suite, mais qui semble n'avoir jamais été énoncé explicitement, et mériter de l'être.

qui augmente indéfiniment quand ε tend vers zéro. Ces énoncés correspondent à des propriétés connues de la fonction de dispersion $\omega(\alpha)$ (Cf. *Variables aléatoires*, § **48**).

2. LES LOIS INDÉCOMPOSABLES ET LES PRODUITS FINIS DE FACTEURS INDÉCOMPOSABLES. — Une loi $\mathcal{L}$ est dite *indécomposable* si elle ne peut être mise sous la forme $\mathcal{L}'\mathcal{L}''$ qu'en prenant un des facteurs égal à une loi unité. On ne connaît pas de méthode pour reconnaître sûrement si une loi est indécomposable. Nous allons seulement indiquer quelques conditions suffisantes.

Nous dirons que x est une *valeur possible* pour une variable aléatoire X si, quel que soit ε positif, l'inégalité $|X - x| < \varepsilon$ a sa probabilité positive. Il ne faut pas confondre cette notion avec celle de *valeur à probabilité positive*. C'est seulement si une valeur possible est isolée qu'on peut affirmer qu'elle est à probabilité positive.

Si U et V sont deux variables aléatoires indépendantes, les valeurs possibles de $U + V$ s'obtiennent en ajoutant de toutes les manières possibles une valeur possible de U et une valeur possible de V. De même pour les valeurs à probabilités positives. On en déduit que la différence entre deux valeurs possibles de U doit se retrouver pour la somme $U + V$ au moins autant de fois qu'il y a de valeurs possibles pour V. De même la différence entre deux valeurs à probabilités positives pour U doit se retrouver pour $U + V$ au moins autant de fois que V a de valeurs à probabilités positives. D'ailleurs, si U a un nombre fini p de valeurs à probabilités positives, si V en a q, $U + V$ en a au moins $p + q - 1$ et au plus pq. De ces remarques résultent immédiatement les conséquences suivantes :

1° Si les valeurs possibles d'une variable aléatoire X ont des différences qui soient toutes distinctes, la loi $\mathcal{L}$ dont dépend X est indécomposable.

2° Si X a au moins n^2 valeurs à probabilités positives, et si l'on ne peut pas trouver n groupes de deux valeurs à probabilités positives x_h et $x'_h (h = 1, 2, \ldots, n)$ tels que

$$x'_1 - x_1 = x'_2 - x_2 = \ldots = x'_n - x_n,$$

la loi $\mathcal{L}$ dont dépend X est indécomposable.

Donnons-nous alors une suite infinie de valeurs $x_n (n = 1, 2, \ldots)$ telle que les différences $x_p - x_q$ soient toutes distinctes. Si toute la probabilité est répartie entre ces valeurs, et quelle que soit la loi de répartition, on obtient une loi indécomposable. Tel est le cas, par exemple, si $x_n = \log p_n$, tous les p_n étant des nombres premiers. Il est facile aussi de définir (précisons bien que nous voulons dire *nommer*, au sens de M. Lebesgue), un ensemble de valeurs x_n qui ait la propriété considérée et qui soit partout dense; on a ainsi facilement des exemples de lois indécomposables à fonctions de répartition constamment croissantes.

Mentionnons encore qu'une loi est indécomposable s'il y a deux valeurs à probabilités positives et deux seulement, et que ce soient les valeurs extrêmes. Il serait facile d'allonger la liste de ces exemples. Indiquons maintenant quelques cas où l'on peut limiter le nombre des facteurs dont la loi donnée est le produit (si l'on ne tient pas compte des facteurs unités).

D'abord on voit aisément que, si les valeurs possibles pour X sont toutes de la forme log N, N étant le produit d'au plus p nombres premiers, la loi $\mathcal{L}$ dont dépend X est le produit d'au plus p facteurs qui ne soient pas des unités. Si ces valeurs sont toutes de la forme $\log \frac{N}{N'}$, chacun des nombres N et N′ étant le produit d'au plus p nombres premiers, la loi $\mathcal{L}$ est le produit d'au plus $2p$ facteurs.

Si X a $p+1$ valeurs possibles, la loi $\mathcal{L}$ est le produit d'au plus p facteurs, et ce maximum ne peut être atteint que si les valeurs possibles sont $p+1$ termes consécutifs d'une progression arithmétique. En faisant au besoin un changement linéaire sur la variable, nous pouvons supposer que ces valeurs soient $0, 1, \ldots, p$; désignons leurs probabilités par $\alpha_0, \alpha_1, \ldots, \alpha_p$ et introduisons, au lieu de la fonction caractéristique $\varphi(z)$, la *fonction génératrice de Laplace*

$$f(u) = \alpha_0 + \alpha_1 u + \ldots + \alpha_1 u^p,$$

qui se réduit d'ailleurs à $\varphi(z)$ si l'on pose $u = e^{iz}$. Chaque décomposition de $\mathcal{L}$ en facteurs est liée à une décomposition du polynome $f(u)$ en un produit de polynomes à coefficients non négatifs. Si notamment il n'existe pas de telle décomposition, la loi $\mathcal{L}$ est indécomposable; si

l'équation $f(u) = 0$ a toutes ses racines réelles (elles sont alors nécessairement négatives), et dans ce cas seulement, elle est le produit de p facteurs.

Désignons par $f_p(u)$ la fonction génératrice

$$f_p(u) = \frac{1}{p}(1 + u + \ldots + u^{p-1}) = \frac{1 - u^p}{p(1-u)},$$

et par X_p, X'_p, des variables dépendant de la loi L_p définie par cette fonction, c'est-à-dire qu'elles ont p valeurs possibles et également probables, $0, 1, \ldots, p-1$. On a évidemment

$$f_{pq}(u) = f_p(u) f_q(u^p) = f_q(u) f_p(u^q), \tag{4}$$

ce qui peut s'écrire

$$X_{pq} \sim X_p + pX'_q \sim X_q + qX'_p, \tag{5}$$

le signe $\sim$ écrit entre deux expressions aléatoires indiquant qu'elles dépendent de la même loi de probabilité et les variables ajoutées dans un même membre étant indépendantes l'une de l'autre (1). Cette formule montre qu'une loi telle que L_6 est, de deux manières *essentiellement différentes* (2), le produit de deux facteurs indécomposables; cette circonstance est digne de remarque, car on aurait pu croire qu'une loi ne peut pas être représentée de plusieurs manières par un tel produit. Plus généralement, si la décomposition d'un nombre entier n en facteurs premiers est de la forme

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} \qquad (\alpha_1 + \alpha_2 + \ldots + \alpha_k = h),$$

l'application répétée de la formule (4) donne autant de décompositions

---

(1) Pour $p = 2$, $q = 3$, par exemple, cela revient à dire que

$$(0 \text{ ou } 1) + (0 \text{ ou } 2 \text{ ou } 4) \sim (0 \text{ ou } 1 \text{ ou } 2) + (0 \text{ ou } 3).$$

(2) Nous disons que deux décompositions sont *différentes* si l'on peut passer de l'une à l'autre en multipliant chaque facteur par une loi unité; bien entendu il n'est pas tenu compte de l'ordre des facteurs. Elles sont *essentiellement différentes*, si l'on ne peut pas les déduire d'une même décomposition par des groupements différents de facteurs. Si tous les facteurs mis en évidence sont indécomposables, ces deux notions coïncident.

différentes de la loi L_n en un produit de h facteurs qu'il y a de permutations différentes des facteurs premiers de n, c'est-à-dire $\frac{h!}{\alpha_1!\alpha_2!\dots\alpha_k!}$.

Il semble probable que L_n n'admet pas d'autres diviseurs que ceux qui résultent de ces décompositions, ce qui entraîne en particulier comme conséquence que L_n est indécomposable si n est premier, et que dans le cas général toutes les décompositions de D_n aboutissent à un produit du même nombre h de facteurs indécomposables. L'arithmétique des lois L_n aurait ainsi une structure assez simple (1).

Pour les lois indécomposables quelconques, les questions suivantes se posent naturellement : *peut-il arriver qu'un produit de h facteurs indécomposables ait plus de h! décompositions essentiellement différentes? Peut-il arriver que le produit de h lois indécomposables admette une décomposition comportant plus de h facteurs* (dont aucun ne soit une loi unité) (2)?

Si l'on passe du fini à l'infini, les remarques qui précèdent se rattachent à la numération généralisée, dans laquelle un nombre X

---

(1) Depuis que ces lignes ont été écrites, l'exactitude de cette hypothèse a été établie, dès le 15 janvier 1937 (trois jours après la conférence mentionnée plus haut au cours de laquelle j'ai exposé les résultats développés dans le présent travail) par M. Krasner. Pour le cas où n est premier, la solution a aussi été obtenue, indépendamment, d'une part par M. Liénard, d'autre part par M. Raikoff.

Il peut être utile d'observer que ce résultat résout complètement le problème de la décomposition en facteurs, non seulement de n'importe quelle loi L_n, mais plus généralement de toute loi pour laquelle n valeurs de X en progression arithmétique ont pour probabilités les valeurs correspondantes d'une progression géométrique. On passe en effet du cas traité dans le texte au cas plus général que nous indiquons en remplaçant $f(x)$ par $\frac{f(qx)}{f(q)}$, et faisant ensuite un changement de variable linéaire sur X, et le problème de la décomposition de $f(x)$ en facteurs à coefficients non négatifs ne change pas par le changement de x en qx.

(2) Depuis que ces lignes ont été écrites, j'ai montré qu'un produit de h facteurs indécomposables ($h > 1$) peut être indéfiniment divisible, ou admettre des diviseurs indéfiniment divisibles, ce qui donne à ces deux questions des réponses affirmatives. Mais les questions analogues, relatives au cas où l'on ne considère que des décompositions en facteurs indécomposables, restent posées.

compris entre o et 1 est représenté par la formule

$$X = \frac{a_1}{P_1} + \frac{a_2}{P_2} + \ldots + \frac{a_n}{P_n} + \ldots, \tag{6}$$

où $P_n = p_1 p_2 \ldots p_n$, les p_ν étant premiers, et où chaque a_n est un des nombres o, 1, ..., p_{n-1}. Cela revient au même de dire que chaque a_n est choisi indépendamment des autres, les p_n valeurs possibles étant également probables, ou que X est une variable aléatoire choisie entre o et 1 avec une répartition uniforme de la probabilité dans cet intervalle. Si S_n désigne la somme des n premiers termes de la série (6), $P_n S_n$ dépend de la loi $L_N(N = P_n)$, et un changement dans l'ordre des facteurs premiers $p_1 p_2 \ldots p_n$ est sans effet sur cette loi, pour laquelle on obtient des décompositions différentes dont le nombre peut atteindre $n!$. A la limite, la loi dont dépend X est indépendante du choix des p_n (le passage d'une suite à une autre pouvant même n'être pas une permutation); on a ainsi des décompositions différentes dont l'ensemble a la puissance du continu.

A propos des décompositions multiples, signalons encore une circonstance très curieuse, découverte par M. Khintchine : il est possible que l'on ait

$$\mathcal{L} = \mathcal{L}_1 \mathcal{L}_2 = \mathcal{L}_1 \mathcal{L}_3, \tag{7}$$

les lois $\mathcal{L}_2$ et $\mathcal{L}_3$ étant différentes, c'est-à-dire qu'*il existe des cas où, une loi $\mathcal{L}_n$ étant divisible par une loi $\mathcal{L}_1$, le quotient peut être défini de plusieurs manières.* En désignant respectivement par $\varphi_1(z)$, $\varphi_2(z)$, $\varphi_3(z)$ les fonctions caractéristiques de $\mathcal{L}_1$, $\mathcal{L}_2$, $\mathcal{L}_3$, la relation (7) équivaut à

$$\varphi_1(z)\,|\varphi_2(z) - \varphi_3(z)| = 0. \tag{8}$$

Prenons pour $\varphi_2(z)$ et $\varphi_3(z)$ les fonctions

$$\begin{cases} \varphi_2(z) = \dfrac{2}{\pi}\displaystyle\int_0^{-\infty} \frac{1-\cos x}{x^2}\cos zx\, dx, \\ \varphi_3(z) = \dfrac{1}{2} + \dfrac{4}{\pi^2}\left[\dfrac{\cos \pi x}{1^2} + \ldots + \dfrac{\cos(2n+1)\pi x}{(2n+1)^2} + \ldots\right], \end{cases} \tag{9}$$

qui sont évidemment des fonctions caractéristiques (les coefficients étant tous non négatifs). Pour $|z| < 1$, elles ont la valeur commune

$1-|z|$, mais la première est nulle pour $|z|\geqq 1$, tandis que la seconde est une fonction périodique. On vérifie alors l'équation (8) en prenant pour $\varphi_1(z)$ la détermination $\varphi_2(z)$, ou $\varphi_2(\lambda z)$, avec $\lambda > 1$; le second facteur est en effet nul de -1 à $+1$; le premier l'est en dehors de cet intervalle.

On remarque que, c et c' étant des constantes non négatives et de somme un, la loi $\mathcal{L}'$ de fonction caractéristique $c\varphi_2(z)+c'\varphi_3(z)$ peut, aussi bien que $\mathcal{L}_2$ et $\mathcal{L}_3$, être considérée comme étant le quotient de $\mathcal{L}$ par $\mathcal{L}_1$.

Il est facile de montrer que la loi $\mathcal{L}_3$ est indécomposable; il en est évidemment ainsi de toutes les lois ayant comme valeurs possibles tous les nombres d'une progression arithmétique (ici les multiples impairs de π), et une seule valeur n'appartenant pas à cette progression (ici zéro). On montre aussi aisément que, à l'exception peut-être de $\mathcal{L}_2$, les lois $\mathcal{L}'$ sont indécomposables; le produit $\mathcal{L}_1\mathcal{L}_2$ peut donc être représenté par des produits $\mathcal{L}_1\mathcal{L}'$ de deux facteurs indécomposables dépendant d'un paramètre qui varie d'une manière continue.

3. Les lois indéfiniment divisibles. — Il existe un autre mode de décomposition possible, qui est au précédent ce qu'une intégrale est à une série. Les lois susceptibles d'être ainsi décomposées sont appelées lois *indéfiniment divisibles*. En termes précis, une loi $\mathcal{L}$ est indéfiniment divisible si, quelque petit que soit ε positif, elle peut être représentée par un produit de facteurs ayant tous leur dispersion moyenne inférieure à ε.

J'ai montré en 1934 que la condition nécessaire et suffisante pour qu'une loi soit indéfiniment divisible est que le logarithme de sa fonction caractéristique soit de la forme

$$(10)\qquad \psi(z)=\mu i z-\lambda\frac{z^2}{2}+\left(\int_{-\infty}^{0}+\int_{0}^{+\infty}\right)\left(e^{izu}-1-\frac{izu}{1+u^2}\right)d\mathbf{n}(u),$$

λ étant non négatif, et $\mathbf{n}(u)$ étant non décroissant dans chacun des intervalles $(-\infty, 0)$ et $(0, +\infty)$; cette fonction doit naturellement être telle que l'expression écrite ait un sens pour toutes les valeurs réelles de z, ce qui revient à dire que la fonction

$$\int\frac{u^2}{1+u^2}d\mathbf{n}(u)$$

est à variation bornée de $-\infty$ à $+\infty$. M. Khintchine a observé que l'introduction de la fonction $g(u)$ définie par cette intégrale de $-\infty$ à zéro, et de zéro à $+\infty$, mais qui augmente brusquement de λ quand u franchit la valeur zéro, permet d'écrire plus simplement

$$(11) \qquad \psi(z) = \mu i z + \int_{-\infty}^{+\infty} \left(e^{izu} - 1 - \frac{izu}{1+u^2} \right) \frac{1+u^2}{u^2} \, dg(u).$$

Le terme linéaire en z correspond à l'addition d'une constante à la variable aléatoire étudiée; mais l'introduction d'un tel terme dans l'intégrale peut être nécessaire pour la convergence de cette intégrale; dans les cas où l'on peut le supprimer, ou remplacer $\frac{izu}{1+u^2}$ par l'expression plus simple izu, sans que l'intégrale cesse de converger, il n'y a aucun inconvénient à le faire. On peut en tout cas le supprimer si l'on accepte d'écrire des intégrales qui soient simplement *quasi-convergentes;* c'est ce que nous ferons. On voit ainsi que la loi indéfiniment divisible la plus générale est formée en partant de deux éléments constituants, la loi de Gauss $\mathcal{G}$, et la loi de Poisson $\mathcal{P}_u$ (qui dépend du paramètre u), dont les fonctions $\psi(z)$ sont respectivement

$$\frac{z^2}{2}, \quad e^{izu} - 1,$$

et la formule (10), en négligeant un facteur qui est une loi unité, peut s'écrire symboliquement

$$(12) \qquad \log \mathcal{L} = \lambda \log \mathcal{G} + \int_{-\infty}^{+\infty} \log \mathcal{P}_u \, d\mathbf{n}(u).$$

J'ai montré d'autre part que la représentation d'une loi $\mathcal{L}$ par cette formule est unique. On peut exprimer ce résultat en disant qu'à l'intérieur du corps $\mathcal{K}$ *les lois indéfiniment divisibles constituent un corps* $\mathcal{K}'$ *à l'intérieur duquel la décomposition d'une loi en facteurs élémentaires est unique.* C'est le théorème fondamental de l'arithmétique des lois indéfiniment divisibles.

Il importe de préciser un point. En nous bornant au cas où $\lambda = 0$, nous pouvons écrire

$$\log \mathcal{L} = \int_0^1 dt \int_{-\infty}^{+\infty} \log \mathcal{P}_u \, d\mathbf{n}(u),$$

et considérer cette expression comme une intégrale double. Toute division du champ d'intégration en plusieurs régions donne une représentation de $\mathfrak{L}$ par un produit; on peut avoir ainsi des décompositions d'aspects très différents; les décompositions *horizontales*, obtenues en fractionnant l'intervalle de variation de t (décompositions toujours possibles, et qu'on peut toujours continuer indéfiniment), et les décompositions *verticales*, obtenues en fractionnant l'intervalle de variation de u (ce qui n'est pas possible si $\mathfrak{L}$ se réduit à un seul élément $c\mathfrak{R}_u$), ont des caractères essentiellement différents. Mais si l'on a une décomposition de la forme

$$\mathfrak{L} = \mathfrak{L}_1 \mathfrak{L}_2 \dots \mathfrak{L}_n,$$

en décomposant verticalement chaque facteur, et en rapprochant tous les éléments correspondant à un même intervalle de variation pour u, on retrouve la décomposition verticale de $\mathfrak{L}$, qui est unique.

Si l'arithmétique du corps $\mathfrak{K}'$ semble ainsi définitivement constituée, il reste à la situer à l'intérieur de celle du corps $\mathfrak{K}$ et à cet effet étudier le problème suivant : une loi indéfiniment divisible admet-elle d'autres décompositions que celles que nous venons de définir? En d'autres termes : *une loi indéfiniment divisible peut-elle admettre des diviseurs indécomposables?* (1).

Nous allons montrer, par deux exemples simples, que : *la réponse à cette question est affirmative;* nous montrerons au prochain paragraphe que : *pour une loi $\mathfrak{L}$ réduite à un seul élément* (loi de Gauss, ou loi de Poisson pour une valeur donnée de u) *la réponse est négative.*

Le premier exemple est dû à M. Khintchine. La loi de fonction caractéristique $\frac{2+\cos z}{3}$ n'est pas indéfiniment divisible (elle est le produit de deux lois pour chacune desquelles il n'y a que deux valeurs possibles $\frac{1}{2}$ et $-\frac{1}{2}$, qui par suite sont indécomposables). En développant son logarithme en série de Fourier, observant qu'il s'annule avec z et que le développement obtenu est absolument convergent, et séparant les termes à coefficients positifs et les termes à coefficients

(1) Nous verrons plus loin qu'une loi qui n'est pas indéfiniment divisible admet toujours des facteurs indécomposables. Les deux manières de poser le problème sont donc bien équivalentes.

négatifs, on trouve une formule de la forme

$$\log\frac{2+\cos z}{3}=\sum_{1}^{\infty}a_n(\cos nz-1)-\sum_{1}^{\infty}a'_n(\cos nz-1), \tag{13}$$

a_n et a'_n étant toujours non négatifs, l'un ou l'autre étant nul pour chaque valeur de n. Ce logarithme étant ainsi la différence de deux expressions de la forme (10), la loi considérée $\mathcal{L}$ est le quotient de deux lois indéfiniment divisibles $\mathcal{L}'$ et $\mathcal{L}''$. On a donc $\mathcal{L}'=\mathcal{L}\mathcal{L}''$; la loi indéfiniment divisible $\mathcal{L}'$ est donc divisible par $\mathcal{L}$, et par suite par les deux lois indécomposables dont $\mathcal{L}$ est le produit.

En remplaçant dans cet exemple $\cos z$ par e^{iz}, et introduisant deux coefficients positifs, α et $\beta(\alpha>\beta)$, de somme égale à l'unité, on est de la même manière conduit à une formule de la forme

$$\log(\alpha+\beta e^{iz})=\sum_{-\infty}^{+\infty}a_n(e^{inz}-1)-\sum_{-\infty}^{+\infty}a'_n(e^{inz}-1), \tag{13'}$$

qui montre qu'une loi indécomposable peut être le quotient de deux lois indéfiniment divisibles; c'est le cas d'une loi n'ayant que deux valeurs possibles, si ces deux valeurs ne sont pas également probables. Bien entendu, une loi indéfiniment divisible ne peut pas admettre de diviseur qui soit une loi dont la fonction caractéristique ait des racines réelles; donc le résultat précédent ne s'étend pas à la loi du jeu de pile ou face.

Le second exemple, qui m'a aussi été communiqué par M. Khintchine, est dû à M. Raikoff. Il montre qu'une loi indéfiniment divisible peut être un produit de facteurs indécomposables. Les formules

$$\prod_{0}^{\infty}\frac{1+(ae^{iz})^{2^k}}{1+a^{2^k}}=\frac{1-a}{1-ae^{iz}}=\varphi_1(z), \tag{14}$$

$$\log\frac{1-a}{1-ae^{iz}}=\sum_{1}^{\infty}a^n(e^{inz}-1), \tag{15}$$

où $0<a<1$, montrent, l'une que la loi de fonction caractéristique $\varphi_1(z)$ est un produit de facteurs indécomposables, l'autre qu'elle est indéfiniment divisible.

On ne sait pas actuellement si une loi indéfiniment divisible peut être obtenue en multipliant des lois indécomposables en nombre fini (1); en tout cas il ne saurait s'agir, comme dans l'exemple précédent, de lois pour lesquelles il n'y a qu'un nombre fini de valeurs possibles. Pour une loi indéfiniment divisible mise sous la forme (12), ou bien $\lambda > 0$ et toutes les valeurs sont possibles, ou bien $\lambda = 0$ et il y a au moins un diviseur $\mathfrak{X}_u$ pour lequel il y a une infinité de valeurs possibles.

4. LES LOIS A FONCTIONS CARACTÉRISTIQUES ENTIÈRES. — Jusqu'ici, nous n'avons considéré que les valeurs réelles de z. Il peut arriver que l'intégrale (1) ait un sens pour des valeurs imaginaires de z, et même qu'elle soit convergente quel que soit z; $\varphi(z)$ est alors une fonction entière. Inversement, on montre aisément (2) que, si pour z réel $\varphi(z)$

---

(1) Depuis que ce mémoire a été écrit, j'ai pu montrer que la réponse à cette question est affirmative.

(2) Il peut être utile de rappeler brièvement la démonstration de ce fait. D'abord, s'il existe un entier p positif ou nul tel que le moment E_{2p} d'ordre $2p$ soit fini, et E_{2p+1} infini, la fonction caractéristique $\varphi(z)$ admet, pour z réel, des dérivées continues jusqu'à l'ordre $2p$, et la dérivée d'ordre $2p$ de la partie paire $\varphi_0(z)$ de $\varphi(z)$ est

$$(-1)^p \int_{-\infty}^{+\infty} x^{2p} \cos zx \, dF(x) = (-1)^p E_{2p} - (-1)^p \frac{z^2}{2} \int_{-\infty}^{+\infty} x^{2p+2} \theta(zx) \, dx,$$

$\theta(zx)$ étant non négatif et tendant vers 1 quand z tend vers zéro; alors le coefficient de z^2 au second membre augmente indéfiniment. Comme cette circonstance est incompatible avec l'hypothèse que $\varphi(z)$ soit une fonction entière, si $\varphi(z)$ est une fonction entière, tous les moments pairs de X sont finis; les moments d'ordres impairs (tant de $|X|$ que de X) le sont aussi, d'après l'inégalité de Schwarz, et, d'après leurs relations avec les dérivées de $\varphi(z)$ pour $z = 0$, la série entière qui représente $\varphi(z)$ s'écrit

$$\varphi(z) = 1 + iE_1 z + \ldots + i^n E_n \frac{z^n}{n!} + \ldots;$$

elle est toujours convergente. Pour $z = iy$ (y réel), on a alors

$$\varphi_0(iy) = \sum_0^\infty \frac{y^{2p}}{(2p)!} \int_{-\infty}^{+\infty} x^{2p} \, dF(x) = \int_{-\infty}^{+\infty} \operatorname{ch} yx \, dF(x),$$

est une fonction entière, cette fonction entière est, pour toutes les valeurs complexes de z, représentable par la formule (1). On a alors, pour r réel,

$$\frac{\varphi(ir)+\varphi(-ir)}{2}=\int_{-\infty}^{+\infty}\operatorname{ch} rx\, d\,\mathrm{F}(x)\geq\frac{\alpha}{2}e^{\varepsilon r}, \tag{16}$$

α désignant la probabilité des valeurs de $|\,\mathrm{X}\,|$ au moins égales à ε. Il en résulte que : *si une fonction caractéristique $\varphi(z)$ est entière, en dehors du seul cas où elle est constamment égale à* 1, *elle est d'ordre au moins égal à* 1.

Si les valeurs possibles de X sont bornées, la formule (1) montre que $\varphi(z)$ est une fonction entière de module au plus égal à e^{ar}, où a est le module maximum de X, et où $r=|z|$; elle est donc, en dehors du cas déjà mentionné où $\varphi(z)=1$, d'ordre exactement égal à 1. Elle est d'autre part bornée pour z réel, ce qui ne peut pas être le cas pour une fonction de la forme $\mathrm{P}(z)\,e^{(a+ib)z}$ [$\mathrm{P}(z)$ étant un polynome], en dehors du cas où $\mathrm{P}(z)$ est constant et où $a=0$. Donc, *en excluant seulement le cas des lois unités, les lois pour lesquelles* X *est borné ont pour fonctions caractéristiques des fonctions entières d'ordre* 1 *ayant une infinité de racines.*

D'autre part la formule (10) montre que : *la fonction caractéristique d'une loi indéfiniment divisible peut être une fonction entière sans racine*, ce qui revient à dire que $\psi(z)$ peut être une fonction entière. Il est pour cela nécessaire et suffisant que l'intégrale qui figure dans la formule (10) soit définie pour toutes les valeurs de z (réelles ou complexes), et cela dépend seulement des valeurs de $\mathrm{n}(u)$ pour u très grand; si en particulier $\mathrm{n}(u)$ ne varie que dans un intervalle fini, $\psi(z)$

---

cette intégrale étant finie. Comme, pour $z=\zeta+iy$ (ζ et y réel), on a

$$|\,e^{iz.x}\,|=e^{-xy}<2\operatorname{ch}xy,$$

l'intégrale (1) est toujours convergente, et représente $\varphi(z)$, puisque c'est une fonction entière égale à $\varphi(z)$ pour z réel.

Signalons qu'on montre de même que, s'il existe une fonction représentable par une série de Taylor ayant un rayon de convergence fini R, et égale à $\varphi(z)$ pour z réel, au moins dans un petit intervalle entourant l'origine, on peut affirmer que l'intégrale (1) définit une fonction holomorphe pour $|\,y\,|<\mathrm{R}$ et admettant au moins un des points $i\mathrm{R}$ et $-i\mathrm{R}$ comme points singuliers.

est une fonction entière; en particulier pour la loi de Gauss et pour la loi de Poisson, $\psi(z)$ est une fonction entière. On peut observer que, pour z réel et très grand, l'intégrale qui figure dans la formule (10) est $o(z^2)$; d'ailleurs $\psi(z)$ ne peut être un polynome du second degré (au plus) que dans le cas de la loi de Gauss [non réduite; c'est-à-dire celle définie par $\psi(z) = \mu i z - \lambda \frac{z^2}{2}$]. Donc, en dehors de ce cas, si la fonction $\psi(z)$ définie par la formule (10) est entière, elle ne se réduit pas à un polynome, de sorte que $\varphi(z)$ est une fonction entière sans racine et d'ordre infini.

On peut se demander si réciproquement une loi dont la fonction caractéristique est une fonction entière sans racine peut n'être pas indéfiniment divisible. Cette question n'est pas actuellement résolue (1).

La possibilité d'appliquer ces remarques à la décomposition des lois de probabilité provient du théorème suivant, que j'ai obtenu en généralisant un lemme de M. Cramer (Cf. *Variables aléatoires*, §**31**).

THÉORÈME. — *Si le produit de deux fonctions caractéristiques est une fonction entière, chacun des facteurs est une fonction entière.*

Pour le montrer, observons d'abord que le fait que l'intégrale (1) ait un sens pour $z = ir$, quelque grand que soit r, prouve que

$$\Pr.\{|X| > x\} = F(-x-0) + 1 - F(x+0)$$

tend vers zéro, pour x infini, plus rapidement que n'importe quelle exponentielle e^{-rx}. On déduit alors de (16), par une intégration par parties

$$(17) \qquad \frac{\varphi(ir) + \varphi(-ir)}{2} = 1 + r\int_0^\infty \operatorname{sh} rx \Pr.\{|X| > x\}\, dx = P(r).$$

D'autre part, si X est la somme de deux variables indépendantes U et V, nous pouvons, en ajoutant une même constante à V et à — U, ou

(1) Depuis que ces lignes ont été écrites, j'ai, à la séance du 10 février 1937 de la Société Mathématique de France, résolu ce problème en montrant que $\varphi(z) = \exp.[P(e^{iz}) - P(1)]$, où $P(x)$ est un polynome à coefficients non tous positifs, peut être une fonction caractéristique.

à V et à X (ce qui ne change pas la nature des fonctions caractéristiques de ces variables : elles restent fonctions entières, si elles le sont et ne peuvent pas le devenir, si elles ne le sont pas), supposer que zéro soit valeur médiane pour V; alors

$$\Pr.\{X>x\}\geqq\frac{1}{2}\Pr.\{U>x\},\qquad \Pr.\{X<-x\}\geqq\frac{1}{2}\Pr.\{U<-x\},$$

et, par suite,

$$\Pr.\{|U|>x\}\leqq 2\Pr.\{|X|>x\}. \tag{18}$$

Il résulte d'abord de cette formule que le premier membre tend vers zéro pour x infini plus rapidement que n'importe quelle exponentielle e^{-rx}, ce qui suffit pour démontrer notre théorème. D'une manière plus précise, $\varphi_1(z)$ désignant la fonction caractéristique relative à la variable U, on déduit de (17) et (18)

$$P_1(r)=\frac{\varphi_1(ir)+\varphi_1(-ir)}{2}\leqq 2P(r)-1. \tag{19}$$

Or, $P(r)$ est du même ordre de grandeur que

$$M(r)=\operatorname*{Max}_{|z|=r}|\varphi(z)|.$$

Si, en effet, $z=\zeta+i\zeta'$ (ζ et ζ' étant réels), $|\varphi(z)|$ est majoré par $\varphi(i\zeta')$. Cette fonction étant convexe est majorée, pour $|\zeta'|\leqq r$, par le plus grand des nombres $\varphi(ir)$ et $\varphi(-ir)$, et *a fortiori* par leur somme $2P(r)$. On en déduit que, pour $|z|=r$, $|\varphi(z)|$ est majoré par $2P(r)$. Donc

$$P(r)\leqq M(r)\leqq 2P(r). \tag{20}$$

On peut donc introduire cette fonction $P(r)$ aussi bien que $M(r)$ pour définir l'ordre de grandeur d'une fonction caractéristique, et la formule (19) montre que, non seulement $\varphi_1(z)$ est une fonction entière, mais qu'au facteur 2 près cet ordre est limité par celui de $\varphi(z)$ (1).

(1) On arrive aisément au même résultat en introduisant les moments. Les moments d'ordres pairs de U, si zéro est valeur médiane pour V, sont au plus égaux aux doubles des moments correspondants de X. D'autre part l'inégalité de

Il résulte immédiatement du théorème précédent que :

COROLLAIRE. — *Si le produit de deux fonctions caractéristiques est une fonction entière qui ne s'annule pas, il en est de même de chaque facteur.*

On déduit aisément des résultats précédents que la loi de Gauss ne peut pas avoir d'autres décompositions en facteurs que celles qui résultent de l'arithmétique du corps $\mathcal{K}'$ étudiée au paragraphe 3. En effet, chacun des facteurs $\varphi_1(z)$ et $\varphi_2(z)$ est une fonction entière, sans racine, d'ordre au plus égal à 2. Compte tenu en outre de ce qu'il est borné pour z réel et égal à 1 pour $z = 0$, son logarithme est de la forme $\mu iz - \lambda \frac{z^2}{2}$, ce qui démontre le résultat énoncé. C'est un théorème de M. Cramer; nous l'obtenons comme corollaire immédiat d'un théorème plus général, mais il convient de rappeler que nous avons déduit ce théorème des idées de M. Cramer.

Un théorème analogue s'applique à la loi de Poisson $\mathcal{P}_1$. Sa fonction caractéristique est $e^{\zeta-1}$, en posant $e^{iz} = \zeta$. Nous avons déjà rappelé que d'une manière générale la fonction caractéristique $\varphi(z) = f(\zeta)$, considérée comme fonction de ζ, est la fonction génératrice de Laplace. Elle est utile à considérer dans le cas des lois pour lesquelles toutes les valeurs possibles sont des entiers non négatifs, ce qui est le cas pour la loi de Poisson, et ce qui sera aussi le cas pour les lois $\mathcal{L}_1$ et $\mathcal{L}_2$ dont le produit est égal à $\mathcal{P}_1$, si nous déterminons convenablement la constante additive dont nous pouvons disposer pour l'ajouter à U et la retrancher de V. Si alors nous posons

$$\Pr.\{U = p\} = \alpha_p, \qquad \Pr.\{V = p\} = \beta_p,$$

les fonctions génératrices de U et V sont respectivement

$$f_1(\zeta) = \sum_0^\infty \alpha_p \zeta^p, \qquad f_2(\zeta) = \sum_0^\infty \beta_p \zeta^p,$$

Schwarz montre que la connaissance de ces moments permet de majorer les moments d'ordres impairs, ce qui revient à dire que l'ordre de grandeur de $M(r)$ est déterminé par la partie paire de $\varphi(z)$.

et leur produit est $f(\zeta)$. Si $f(\zeta)$ est une fonction entière, le fait que

$$\Pr.\{X=p\}=\alpha_0\beta_p+\alpha_1\beta_{p-1}+\ldots+\alpha_p\beta_0\geq\alpha_p\beta_0,$$

compte tenu de ce que $\alpha_0\beta_0$, qui est la probabilité de $X=0$, n'est pas nul, montre que, au facteur β_0 près, la série $f_1(\zeta)$ est majorée par celle qui représente $f(\zeta)$. Dans le cas de la loi de Poisson, où $f(\zeta)=e^{\zeta-1}$, c'est donc une fonction entière d'ordre 1 au plus, et sans zéro, de même que $f_2(\zeta)$, puisque les résultats obtenus pour $f_1(\zeta)$ doivent s'appliquer aussi à $f_1(\zeta)$ et que le produit de ces fonctions ne s'annule pas. Compte tenu de $f_1(1)=\varphi_1(0)=1$, on voit qu'on a nécessairement

$$\log f_1(\zeta)=\log\varphi_1(z)=c_1(\zeta-1)=c_1(e^{iz}-1),$$
$$\log f_2(\zeta)=\log\varphi_2(z)=c_2(\zeta-1)=c_2(e^{iz}-1),$$

avec $c_1+c_2=1$. D'ailleurs $\varphi_1(z)$ et $\varphi_2(z)$ ne sont évidemment des fonctions caractéristiques que si c_1 et c_2 sont non négatifs. On a ainsi la forme de décomposition annoncée.

Ce théorème est dû à M. Raikoff; la démonstration très simple qui précède est due à M. Khintchine.

5. LA STRUCTURE DU CORPS $\mathfrak{H}$; LE THÉORÈME FONDAMENTAL DE M. KHINTCHNE. — Ce théorème est le suivant : *toute loi $\mathfrak{L}$ peut être mise sous la forme $\mathfrak{L}'$, $\mathfrak{L}''$, $\mathfrak{L}'$ étant un produit fini ou infini de facteurs indécomposables, $\mathfrak{L}''$ étant indéfiniment divisible.*

Bien entendu, il peut arriver que l'un ou l'autre des facteurs $\mathfrak{L}'$ et $\mathfrak{L}''$ se réduise à l'unité; il peut arriver que $\mathfrak{L}'$, sans se réduire à l'unité, ne comprenne qu'un facteur indécomposable. Il peut arriver que la décomposition soit possible de plusieurs manières *essentiellement* différentes; les exemples indiqués plus haut le prouvent surabondamment. Il s'agit maintenant de montrer qu'elle est toujours possible. Cela peut paraître presque évident, car en décomposant $\mathfrak{L}$ en un produit de deux facteurs, et en recommençant indéfiniment et transfiniment tant que cela est possible, on doit aboutir à mettre en évidence le résultat énoncé. Mais il faut un peu d'attention pour arriver à un raisonnement rigoureux (1).

(1) La démonstration qui suit n'est pas celle de M. Khintchine.

A cet effet, nous désignerons par $\zeta(\mathcal{L})$ la borne supérieure de $\delta(L)$, quand on prend successivement pour $\mathcal{L}$ tous les diviseurs indécomposables de $\mathcal{L}$; $\zeta(\mathcal{L}) = 0$ caractérise des lois sans diviseurs indécomposables. Il faut noter que $\zeta(\mathcal{L})$ peut être une borne supérieure non atteinte. Si l'hypothèse énoncée au sujet des lois L_p du paragraphe **2** est exacte (1), il en est ainsi dans le cas où $\mathcal{L}$ est la loi correspondant à une répartition uniforme de la probabilité dans l'intervalle $(0, 1)$; car si p est un nombre premier suffisamment grand, en donnant la probabilité $\frac{1}{p}$ à chacune des valeurs $0, \frac{1}{p}, \frac{2}{p}, \ldots, \frac{p-1}{p}$, on définit une loi indécomposable L, divisant $\mathcal{L}$, et arbitrairement voisine de $\mathcal{L}$; $\delta(\mathcal{L})$ est alors pour $\delta(L)$ une borne supérieure non atteinte.

Considérons d'autre part une représentation de $\mathcal{L}$ par un produit, fini ou infini, $\Pi\mathcal{L}_n$; les nombres $\delta(\mathcal{L}_n)$ ont un maximum $\bar{\delta}$ (effectivement atteint), et, quand on considère toutes les représentations possibles de $\mathcal{L}$ par un produit, $\bar{\delta}$ a une borne inférieure bien déterminée $\eta(\mathcal{L})$ (on peut remarquer que cette borne reste la même si l'on ne considère que les représentations de $\mathcal{L}$ par des produits finis). D'après cette définition, $\eta(\mathcal{L}) = 0$ caractérise les lois indéfiniment divisibles, et $\eta(\mathcal{L}) = \delta(\mathcal{L})$ caractérise les lois indécomposables; dans tous les autres cas $\eta(\mathcal{L})$ est compris entre zéro et $\delta(\mathcal{L})$.

Montrons maintenant que, si $\eta(\mathcal{L})$ est positif, *on peut toujours définir une loi indécomposable* L, *qui divise* $\mathcal{L}$, *et tel que* $\delta(L) \geq \eta(\mathcal{L})$. Donnons-nous, à cet effet, une suite de nombres ε_n, décroissants et tendant vers zéro, et, en partant de $\mathcal{L} = \mathcal{L}_0$, choisissons une suite de lois $\mathcal{L}_n$ de la manière suivante : $\mathcal{L}_{n-1}$ étant défini, il existe, par définition de $\eta(\mathcal{L}_{n-1})$, au moins une décomposition de $\mathcal{L}_{n-1}$ en facteurs ayant tous leur dispersion moyenne inférieure à $\eta(\mathcal{L}_{n-1}) + \varepsilon_n$, et dans cette décomposition il existe au moins un facteur, que nous prendrons pour $\mathcal{L}_n$, tel non seulement que $\delta(\mathcal{L}_n) \geq \eta(\mathcal{L}_{n-1})$, mais que $\mathcal{L}_n$ ne soit pas décomposable en facteurs ayant tous leurs dispersions moyennes inférieures à $\eta(\mathcal{L}_{n-1})$; autrement on aurait en effet une décomposition analogue pour $\mathcal{L}_{n-1}$, ce qui est en contradiction avec la définition

(1) Rappelons que l'exactitude de cette hypothèse est maintenant démontrée.

de $\eta(\mathcal{L}_{n-1})$. On a donc

$$\eta(\mathcal{L}_{n-1}) \leqq \eta(\mathcal{L}_n) \leqq \delta(\mathcal{L}_n) \leqq \eta(\mathcal{L}_{n-1}) + \varepsilon_n.$$

Si après un nombre fini d'opérations on arrive à une loi indécomposable $\mathcal{L}_n$, c'est la loi L cherchée. Dans le cas contraire, la suite des lois $\mathcal{L}_n$, dont chacune divise la précédente, est quasi-convergente; en multipliant chacune de ces lois par une loi unité, on obtient une suite qui converge vers une limite L. D'ailleurs la suite décroissante des $\delta(\mathcal{L}_n)$ et la suite non décroissante des $\eta(\mathcal{L}_n)$ convergent vers une limite η, dont nous allons montrer qu'elle est égale à la fois à $\delta(L)$ et à $\eta(L)$. En effet, L divisant $\mathcal{L}_n$, on a $\delta(L) < \delta(\mathcal{L}_n)$; d'autre part, s'il existait un nombre n pour lequel on ait $\eta(L) < \eta(\mathcal{L}_n)$, cette inégalité resterait vraie pour n arbitrairement grand; or $\delta\left(\frac{\mathcal{L}_n}{L}\right)$ tend vers zéro pour n infini, et est à partir d'un certain moment inférieur à $\eta(\mathcal{L}_n)$; alors la formule $\mathcal{L}_n = L\frac{\mathcal{L}_n}{L}$ montrerait la possibilité de décomposer $\mathcal{L}_n$ en facteurs ayant tous leur dispersion moyenne inférieure à $\eta(\mathcal{L}_n)$, ce qui est en contradiction avec la définition de cette expression. On a donc

$$\eta(\mathcal{L}_n) \leqq \eta(L) \leqq \delta(L) < \delta(\mathcal{L}_n).$$

Donc $\eta(L)$ et $\delta(L)$ sont égaux à la limite commune η des deux membres extrêmes, donc égaux entre eux. Donc L est une loi indécomposable, qui divise $\mathcal{L}$, et dont la dispersion moyenne est $\eta \geqq \eta(\mathcal{L})$.

C. Q. F. D.

Si alors $\mathcal{L}$ n'est pas une loi indéfiniment divisible, c'est-à-dire si $\eta(\mathcal{L})$ est positif, elle admet au moins un diviseur indécomposable, c'est-à-dire que $\zeta(\mathcal{L})$ est positif. Considérons alors une suite de lois indécomposables L_n définies comme suit : prenons pour L_1 un diviseur indécomposable de $\mathcal{L} = \mathcal{L}''_0$ tel que $\delta(L_1) > \zeta(\mathcal{L}) - \varepsilon_1$, et posons $\mathcal{L} = L_1\mathcal{L}''_1$; prenons pour L_2 un diviseur indécomposable de $\mathcal{L}''_1$ tel que $\delta(L_2) > \zeta(\mathcal{L}''_1) - \varepsilon_2$, et posons $\mathcal{L}''_1 = L_2\mathcal{L}''_2$; et ainsi de suite. On ne peut être arrêté que si l'on arrive à une loi $\mathcal{L}''_n$ indéfiniment divisible, et alors la formule

$$\mathcal{L} = L_1 L_2 \ldots L_n \mathcal{L}''_n$$

établit le théorème de M. Khintchine. Dans le cas où l'on peut continuer indéfiniment, le produit infini ΠL_n, divisant $\mathfrak{L}$ est quasi-convergent, et définit, à un facteur unité près, une loi $\mathfrak{L}'$, produit de facteurs indécomposables, et qui divise $\mathfrak{L}$. On peut poser $\mathfrak{L} = \mathfrak{L}'\mathfrak{L}''$. La loi $\mathfrak{L}''$ divise tous les $\mathfrak{L}''_n$. Or, puisque le produit ΠL_n est quasi-convergent, $\delta(L_n)$ tend vers zéro, et il en est de même de $\zeta(\mathfrak{L}''_n) < \delta(L_{n+1}) + \varepsilon_{n+1}$. Il en résulte que la loi $\mathfrak{L}''$ est indéfiniment divisible; en effet, s'il n'en était pas ainsi, elle aurait un diviseur indécomposable L'', non réduit à une unité, et qui devrait diviser tous les $\mathfrak{L}''_n$; donc $\delta(L'')$ serait inférieur à $\zeta(\mathfrak{L}''_n)$, donc égal à zéro et L'' serait une unité, contrairement à l'hypothèse. La loi $\mathfrak{L}$ est donc représentée par le produit $\mathfrak{L}'\mathfrak{L}''$ qui a bien la forme voulue, et le théorème de M. Khintchine est démontré dans tous les cas.

On remarque que nous avons même un résultat plus précis, $\mathfrak{L}''$ étant une loi indéfiniment divisible *sans diviseur indécomposable*. On peut se demander si, *avec cette condition restrictive imposée à* $\mathfrak{L}''$, il peut arriver que $\mathfrak{L}$ soit représentable de deux manières différentes par un produit tel que $\mathfrak{L}'\mathfrak{L}''$(1).

(1) Depuis que ce mémoire a été écrit, j'ai pu montrer que cela est en effet possible. M. Khintchine m'a d'autre part écrit qu'il avait aussi obtenu de son côté le résultat que je viens d'indiquer, qui précise le théorème qu'il m'avait d'abord communiqué. Sa démonstration repose sur l'introduction d'une fonction de la loi $\mathfrak{L}$, qui n'est pas $\delta(\mathfrak{L})$, mais qui joue un rôle analogue à celui que joue $\delta(\mathfrak{L})$ dans la démonstration que je viens d'indiquer.