ANNALES SCIENTIFIQUES DE L'É.N.S.

D. VAN DANTZIG

Nombres universels ou ν!-adiques avec une introduction sur l'algèbre topologique

Annales scientifiques de l'É.N.S. 3^e série, tome 53 (1936), p. 275-307

<http://www.numdam.org/item?id=ASENS_1936_3_53__275_0>

NOMBRES UNIVERSELS OU $\nu!$-ADIQUES [1]

AVEC

UNE INTRODUCTION SUR L'ALGÈBRE TOPOLOGIQUE

PAR M. D. VAN DANTZIG

(Delft).

Introduction [2].

La présente Note montre un aspect spécial d'une branche des mathématiques assez nouvelle : l'algèbre topologique. Le nom indique déjà qu'elle est une des deux filles hybrides, nées du mariage de l'algèbre avec la topologie. Tandis que sa sœur cadette, intimement liée avec elle, la *topologie algébrique*, ne se distingue que très faiblement de la *topologie* elle-même, et n'est que la topologie « combinatoire » ou « mixte », où l'on applique les méthodes et les résultats de l'algèbre abstraite, dans l'*algèbre topologique* les traits de l'*algèbre* prédominent, au moins partiellement, sur ceux de la topologie, et

(1) Cette Note est à considérer comme une application d'un Mémoire dans les *Mathematische Annalen* :

D. VAN DANTZIG, *Zur topologischen Algebra*, I, *Komplettierungstheorie* (*Math. Ann.*, 107, 1932, p. 587-626, abrégé par *T. A.*, *I*).

(2) Le lecteur verra que le point de vue pris dans cette Introduction diffère un peu de celui pris dans le reste de l'article. Qu'il m'en excuse, puisque je l'ai écrite plus de deux années après le reste, et bien en vertu de la prière de la rédaction « d'indiquer dans une Introduction la place que la question que j'ai traitée tient dans une théorie plus générale ».

Quant à la bibliographie sur l'algèbre topologique, le lecteur trouvera une liste des plus importantes publications jusqu'à l'année 1932 dans mon article [4] (*voir* la liste à la fin de l'article); une partie de la bibliographie plus récente se trouve dans le rapport [7] que j'ai présenté à la conférence topologique de Moscou.

même ceux de ses aïeuls, l'analyse et l'arithmétique, y peuvent être reconnus.

D'une manière générale on peut dire que le développement historique d'une partie au moins de l'analyse a abouti à une dissolution toujours plus profonde en ses éléments purement algébriques et purement topologiques, et d'un traitement de ces éléments au moyen des méthodes abstraites introduites pendant ce siècle dans la topologie (¹) par MM. M. Fréchet et F. Hausdorff, et dans l'algèbre par la regrettée Emmy Nœther. Or, l'algèbre topologique est née du désir de recombiner ces deux éléments en conservant les avantages que les méthodes abstraites y ont apportés.

Qu'il me soit permis d'illustrer cela au moyen de quelques exemples, qui d'ailleurs ne seront pas discutés en détail dans le présent Mémoire. Considérons d'abord l'ensemble de tous les nombres complexes. La construction classique de ces nombres au moyen du principe de permanence, en partant des nombres naturels, repose en une partie essentielle (*voir* l'introduction des nombres réels) sur la notion de *grandeur*, donc sur une notion caractéristique de l'*analyse*. Les deux propriétés les plus importantes de cet ensemble sont : A. il constitue un corps (ou domaine de rationalité) *algébriquement clos*, c'est-à-dire : on y peut effectuer toujours les quatre règles de l'arithmétique, sauf la division par zéro, et chaque équation algébrique d'un degré > 0, à coefficients contenus dans le corps, y admet au moins une solution ; B. il constitue un espace topologique *localement compact*, c'est-à-dire : il y existe une notion de continuité, par rapport à laquelle chaque suite infinie et bornée de nombres complexes admet au moins un point d'accumulation. Or, la propriété A, dont la partie principale est exprimée par le théorème fondamental de d'Alembert-Gauss, est d'une nature purement algébrique, tandis que la propriété B, dont la partie essentielle est exprimée par le théorème non moins fondamental de Bolzano-Weierstrass, est purement topologique. Eh bien, on peut introduire et étudier d'une manière axiomatique d'une part les ensembles ayant des propriétés du type A (c'est ce que fait l'algèbre), d'autre part les ensembles ayant des propriétés du type B (c'est ce que fait la topo-

(¹) Un point de vue un peu différent est pris par M. H. Weyl dans son discours [1].

logie) et enfin les ensembles ayant simultanément des propriétés des types A et B (c'est ce que fait l'algèbre topologique). On trouve alors que l'ensemble des nombres complexes est *uniquement caractérisé* par l'ensemble des deux propriétés A et B (¹).

Un second exemple est fourni par la théorie des groupes de Lie. Il est connu qu'ils furent introduits par S. Lie d'une manière purement analytique et que jusqu'à ce jour l'analyse est le moyen le plus utilisé à leur étude. Or, il s'est manifesté que dans cette théorie un rôle très essentiel est joué par les propriétés topologiques de la variété de groupe, dont la plus simple réside dans la différence importante entre les groupes clos et les groupes ouverts, et dont le lecteur trouvera une étude systématique dans le beau fascicule de M. E. Cartan sur les groupes continus et l'*Analysis situs*. D'autre part, dès 1899, M. D. Hilbert posa le problème d'édifier la théorie des groupes de Lie sans avoir recours à la propriété des fonctions qui définissent les transformations d'être *dérivables*. Ceci revient à remarquer qu'un groupe de Lie peut être considéré d'une part comme un groupe abstrait (notion algébrique) et d'autre part comme une variété particulière à n dimensions (notion topologique), et qu'en recombinant ces deux aspects on pourrait développer la théorie sans aucun recours à l'analyse (²). C'est pour cela que O. Schreier en 1925 introduit la notion de groupe topologique, ressortissant à l'algèbre topologique, et par là devint l'initiateur principal de cette science. C'est grâce aux idées de O. Schreier que M. A. Haar en 1933 parvint à démontrer un théorème important sur les groupes topologiques compacts, dont M. J. von Neumann put déduire la solution du problème de Hilbert, au moins en tant qu'il s'agit des groupes de Lie *clos*. Quoique l'analyse n'ait pas encore été éliminée entièrement de la théorie, puisqu'on ne peut pas encore se passer des théorèmes de MM. F. Peter et H. Weyl sur la représentation des groupes clos, on peut dire que les méthodes abstraites de l'algèbre topologique ont conduit à la solution du problème très concret, posé par M. Hilbert.

(¹) D. VAN DANTZIG [2], Chap. IV.

(²) Sans avoir recours aux méthodes abstraites, M. L. E. J. BROUWER [2] (*cf.* aussi [1]) déjà en 1909 parvint à résoudre le cinquième problème de M. Hilbert pour les groupes de transformations de la droite et du plan.

Une fois en possession de la notion générale de groupe topologique, on peut en étudier des types autres que les groupes de Lie. Une première espèce est fournie par les groupes cantoriens, découverts en 1910 par L. E. J. Brouwer, et qui portent leur nom puisqu'ils sont ou bien finis, ou bien homéomorphes avec l'ensemble linéaire parfait et nulle part dense de Cantor (*voir* § 3). Ces groupes, qui paraîtront plusieurs fois dans le présent Mémoire, ont une grande ressemblance avec les groupes discrets *finis*, qu'ils généralisent. On connaît maintenant plusieurs propriétés de ces groupes et de leur généralisation, les groupes brouweriens, qui sont aussi à dimension zéro (1). Le « missing link » entre les groupes de Lie clos et les groupes cantoriens, si différents de ceux-ci, est formé par les *groupes solénoïdaux* qui furent découverts en 1930 par l'auteur de ce Mémoire (2). Ces groupes sont typiques pour tous les groupes compacts, comme l'a démontré en 1934 M. L. Pontriagin. Ils sont un vrai carrefour des mathématiques, puisqu'ils se rencontrent ici, outre l'algèbre et la topologie : l'analyse, représentée par les fonctions presque périodiques, et l'arithmétique, représentée par les nombres p-adiques.

Arrivons maintenant par ces nombres, découverts par K. Hensel, au troisième exemple que je veux considérer : l'analogie entre la théorie des fonctions et la théorie des nombres, et par lui au sujet proprement dit de ce Mémoire.

Comme plusieurs autres sciences mathématiques, on peut considérer la théorie des fonctions algébriques (ou aussi analytiques) du point de vue ou bien *local* ou bien *global*. Une fonction (analytique) montre son aspect local lorsqu'on considère l'*élément* de fonction, représenté par son développement en série d'après les puissances de $z - a$. D'autre part le développement d'une fonction en un produit fini ou infini de facteurs premiers, qui met en évidence les zéros et les pôles de la fonction, montre l'aspect global.

Dans la théorie des *nombres* algébriques, l'aspect global a d'abord prévalu. On connaît depuis Kummer et Dedekind les propriétés princi-

(1) D. VAN DANTZIG, *Zur topologischen Algebra*, III, *Brouwersche und Cantorsche Gruppen*, *Compositio Mathematica*, 3, 1936, p. 408-426, abrégé par *T. A.*, III. *Voir* aussi D. VAN DANTZIG [1], [3].

(2) *Cf.* D. VAN DANTZIG [1].

pales de la décomposition d'un nombre algébrique en facteurs premiers; la seule différence avec la théorie des fonctions consiste en ce que ces facteurs ne sont pas des nombres ordinaires, mais des idéaux. La théorie de Galois se rapporte aussi aux propriétés globales des nombres algébriques et des corps de ces nombres. Or, guidé par cette analogie, c'est Hensel qui, dans la théorie des nombres aussi, a introduit le point de vue local. Il avait en effet remarqué qu'on peut développer un nombre algébrique (ou rationnel) suivant les puissances d'un idéal (ou d'un nombre) premier, de même qu'on peut développer une fonction algébrique (ou rationnelle) suivant les puissances d'un facteur premier, comme $(z-a)^{\frac{1}{n}}$ (ou $z-a$), et qu'on peut considérer aussi, tout comme dans la théorie des fonctions, des développements de ce genre en séries *infinies*, qui (à la différence de ce qui se passe dans la théorie des fonctions) *convergent toujours*. Ces séries infinies comme par exemple

$$\sum_{\nu=n}^{\infty} a_\nu p^\nu,$$

où p est un nombre premier $\geqq 2$, et $a_\nu = 0, 1, \ldots, p-1$, sont appelées les nombres p-adiques (fractionnaires ou entiers selon que $n < 0$ ou $n \geqq 0$) de Hensel. L'ensemble de ces nombres pour un p donné est un corps (ou un anneau lorsqu'on se restreint aux *entiers* p-adiques) et possède des propriétés tout à fait analogues à celles de l'ensemble de toutes les fonctions d'une variable complexe, développables d'après les puissances de $z-a$ au voisinage d'un nombre donné a. On peut donc comparer un corps de nombres p-adiques (ou aussi le nombre p correspondant) à un *point* du plan complexe. D'une manière analogue un idéal $\mathfrak{p}$ dans un corps de nombres algébriques ou aussi le corps de nombres $\mathfrak{p}$-adiques correspondant, est à comparer à un point d'une surface de Riemann.

Or, qu'est-ce qui correspond à la surface de Riemann elle-même? D'abord le corps de nombres algébriques donné, correspondant à la totalité des fonctions *algébriques* qui sont univoques sur la surface. Mais on peut aussi étudier des fonctions transcendantes définies sur la surface de Riemann, qui admettent un développement par rapport à chaque point (d'un certain domaine) de la surface. Ce qui correspond

à ces fonctions ce sont les *nombres universels*, introduits par H. Prüfer en 1925 sous le nom de nombres idéaux, et étudiés mais non épuisés par J. von Neumann. C'est à ces nombres ou plutôt au cas non trop particulier où le corps donné est le corps des nombres rationnels (donc à comparer au cas où la surface de Riemann est la sphère complexe) que le présent Mémoire sera dédié. On trouve que la « surface » consiste en une infinité *dénombrable* de points, qui peuvent être représentés par les « unités » e ou par les idéaux qu'ils engendrent (les ensembles d' « éléments de fonction »), ou enfin par les idéaux premiers auxquels ils correspondent (les ensembles de « fonctions » qui « s'annulent » en un « point » donné). Un nombre universel quelconque peut être représenté comme une somme (infinie) de tous ses « éléments » (décomposition additive) et aussi par un produit (infini) de ses facteurs premiers (décomposition multiplicative). La première décomposition n'a pas d'équivalent dans la théorie des fonctions analytiques (1).

Malgré ces analogies étroites, il y a d'importantes différences entre la théorie des nombres universels et celle des fonctions analytiques, des différences qui ont toutes la même cause :

1° Tandis que les surfaces de Riemann sont très intéressantes du point de vue topologique (et même ont mené à la création de la topologie), il n'en est pas de même dans la théorie des nombres, puisqu'ici les « surfaces » analogues sont toujours des ensembles dénombrables *discrets*. Même les anneaux de nombres universels eux-mêmes n'ont rien d'intéressant du point de vue topologique, puisqu'ils sont tous homéomorphes à l'ensemble de Cantor;

2° Il n'y a rien qui corresponde au « point à l'infini » du plan complexe;

3° Il n'existe pas de « prolongement analytique »; un nombre universel n'est *pas* déterminé par un de ses « éléments », au moins lorsqu'on considère les composants additifs d'un nombre comme ses « éléments »;

(1) Néanmoins il y a une certaine analogie, lorsqu'on compare les nombres universels aux *intégrales* sur une surface de Riemann, et les termes de la décomposition additive aux *différentielles* (locales) correspondantes.

4° Un produit peut être nul sans qu'aucun de ses facteurs le soit.

La cause commune de ces différences avec la théorie des fonctions réside en ce qu'il n'y a aucune *continuité* entre les différents éléments d'une fonction, l'ensemble des « lieux » étant *discret*. Cela entraîne que la notion de nombre universel est beaucoup plus générale que celle de fonction analytique : un nombre universel correspond plutôt à un ensemble d'éléments de fonctions *indépendants*, où un élément correspond à chaque point de la surface. Cela entraîne aussi que l'étude de cette partie de l'algèbre topologique a un caractère plutôt algébrique que topologique.

Remarquons enfin que la théorie des nombres universels (par rapport à un anneau de nombres *algébriques*, non nécessairement rationnels) permet des applications dans la théorie des corps de classes. En effet, cette dernière théorie présente aussi un aspect global et un aspect local (théorie des corps de classes « im Grossen » et « im Kleinen »), et c'est bien la théorie des nombres universels qui permet d'unifier ces deux aspects.

Aperçu historique et abrégé.

Comme introduction à la théorie générale des anneaux b_ν-adiques abstraits, que je traiterai dans un autre Mémoire (1), je démontrerai ici quelques propriétés des nombres universels ou ν!-adiques.

Les nombres universels (ou plutôt des nombres plus généraux se rapportant à un anneau algébrique) ont été introduits par H. Prüfer [1], [2] (2) sous le nom de « nombres idéaux » que je préfère remplacer par « nombres universels », le mot « idéal » ayant déjà tant de significations. Le nom « universel » a été choisi puisque l'ensemble des nombres universels, l'anneau universel (par rapport à l'anneau des nombres entiers et rationnels) joue un rôle analogue à la surface de recouvrement universelle d'une surface de Riemann et au

(1) D. VAN DANTZIG, *Zur topologischen Algebra*, II. *Abstrakte b_ν-adische Ringe*, *Compositio Mathematica*, 2, 1935, p. 201-223, abrégé par *T. A.*, II.

(2) Les numéros entre [ ] se rapportent à la liste de publications qui se trouve à la fin de l'article.

groupe de recouvrement universel d'un groupe de Lie (1). Ensuite J. von Neumann [1] (2) a repris leur étude; en particulier il a beaucoup éclairci le rapport entre les nombres idéaux de Prüfer et les nombres p-adiques et $\mathfrak{p}$-adiques de K. Hensel [2], [1].

Néanmoins, il me semble que ces nombres n'ont pas suscité le grand intérêt qu'ils méritent. En effet, ils ont une très grande ressemblance avec les nombres naturels (resp. algébriques entiers). Par exemple on peut élever les nombres d'une grande classe de nombres $\nu!$-adiques (ou plus généralement $\mathfrak{b}_\nu$-adiques, aussi par rapport aux anneaux de nombres algébriques), les nombres dits « subsistants », à une puissance $\nu!$-adique arbitraire. En particulier, pour un tel nombre a, on peut définir a^0, a^{-1}, etc., qui sont tous des *entiers* $\nu!$-adiques (ou $\mathfrak{b}_\nu$-adiques dans le cas plus général). On pourrait aussi, d'après Prüfer et von Neumann, introduire les fractions $\nu!$-adiques; je préfère ne pas faire cela, puisque toutes les propriétés importantes expriment des relations entre des *entiers*. D'ailleurs l'équation $ax = b$ n'est pas toujours soluble, ni chez Prüfer et von Neumann, où elle n'est soluble que si a n'est pas un diviseur de zéro, ni chez moi, où elle n'est soluble que si b est un multiple du « fondement » de a. Enfin, en introduisant les fractions $\frac{b}{a}$ où a n'est pas subsistant, on obtient des puissances non continues. En effet, par exemple en définissant π^0 (3) (à cause de $\lim \nu! = 0$) comme $\pi^0 = \lim \pi^{\nu!} = 0$, tandis que la suite $\pi^{-\nu!}$ doit être divergente (puisque autrement on aurait $\lim 1 = \lim \pi^{+\nu!} . \pi^{-\nu!} = 0$) on trouverait $\pi^{-0} = \lim \pi^{-\nu!} \neq \pi^0$, ce qui n'est pas désirable.

Or, la continuité de l'exponentielle est d'un très grand intérêt pour la théorie. En effet, c'est elle qui permet de lier la théorie des groupes cantoriens [à laquelle j'espère revenir dans une publication future (4)] à la théorie des anneaux cantoriens. Par exemple, l'*ordre* d'un groupe cantorien quelconque est toujours un idéal dans l'anneau des nombres universels. D'ailleurs c'est elle qui permet d'introduire la théorie

(1) *Cf.* par exemple E. CARTAN [1].

(2) Une suite à cet article, annoncée par l'auteur, n'a pas encore paru.

(3) π est un nombre universel qui est divisible par chaque nombre premier ordinaire.

(4) Cf. *T. A.*, III, p. 420 seq.

multiplicative des idéaux, comme je l'indiquerai dans les paragraphes 4 et 5. A présent je me bornerai à introduire l'indicatrice d'Euler d'un idéal dont je démontrerai les propriétés principales, et les équations binômes. L'indicatrice $\varphi(\mathfrak{b})$ est définie comme l'ordre du groupe de tous les diviseurs d'Un dans l'anneau factoriel $\mathfrak{A}/\mathfrak{b}$ et a des propriétés tout à fait analogues à celles de l'indicatrice ordinaire $\varphi(n)$.

Dans le paragraphe 5 je prouve que l'équation $x^{\mathfrak{a}} - 1 = 0$ est toujours soluble et qu'elle admet toujours des racines *primitives*. Tandis que dans un anneau de nombres algébriques ordinaires (assez extensif) le nombre de solutions de l'équation $x^n - 1 = 0$ est égal à son degré $\mathfrak{a} = (n)$, ceci n'est ici le cas que lorsque $\mathfrak{a}$ est *idempotent*, le « nombre de solutions » étant interprété comme l'ordre du groupe de toutes les solutions. D'ailleurs, cette interprétation offre aussi des avantages dans la théorie ordinaire. En effet, là aussi le nombre de solutions de l'équation $x^{-n} - 1 = 0$ ($n =$ nombre naturel) n'est *pas* égal au « degré » $- n$. De même le nombre de solutions de l'équation $x^0 - 1 = 0$, qui est infini, n'est pas égal au degré, qui est zéro. Néanmoins l'*idéal* qui est l'ordre du groupe est égal à l'*idéal* $(-n) = (n)$, resp. (0).

Il est curieux que le cas où l'ordre du groupe des solutions $\nu!$-adiques de l'équation $x^{\mathfrak{a}} - 1 = 0$ est égal à $\mathfrak{a}$ *exclut* le cas où $\mathfrak{a}$ est un idéal, engendré par un nombre *fini*. En effet, l'équation $x^n - 1 = 0$ a toujours une infinité de solutions $\nu!$-adiques, voire n dans chaque anneau p-adique, où $p \equiv 1 \,(n)$.

J'ai choisi ici une méthode assez élémentaire pour introduire les nombres $\nu!$-adiques (c'est même la raison pour laquelle je n'ai pas commencé immédiatement par les nombres b_ν-adiques algébriques généraux) et j'ai lardé le texte de quelques exemples numériques. Dans *T. A.*, II, je traiterai de ces questions d'un point de vue plus général et plus abstrait. D'ailleurs j'ai omis ici les démonstrations de quelques théorèmes, qui résultent immédiatement des théorèmes correspondants généraux, qui seront démontrés dans *T. A.*, III.

L'essentiel du contenu des paragraphes 1, 2 se trouve déjà chez Prüfer ou von Neumann (à l'exception des derniers théorèmes du paragraphe 2). Le reste est en majeure partie nouveau, quoique

quelques-uns des théorèmes soient analogues à des théorèmes de Hensel, se rapportant aux nombres p-adiques et $\mathfrak{p}$-adiques.

I. — Définition des nombres universels.

1. Un nombre $\nu!$-adique ou nombre *universel* peut être défini par exemple comme une série formelle

$$x = \xi_1 . 1! + \xi_2 . 2! + \xi_3 . 3! + \dots, \tag{1}$$

où les ξ_n parcourent indépendamment les nombres 0, 1, ..., n. Ils peuvent être considérés comme limites de nombres naturels :

$$x = \lim x_\nu \quad (^1), \qquad x_n = \xi_1 . 1! + \dots + \xi_n . n!$$

Les nombres naturels sont des nombres universels spéciaux, à savoir des nombres dont seulement un nombre fini de coefficients ξ_ν sont différents de zéro. On appelle $n^{\text{ième}}$ voisinage $U_n(x)$ d'un nombre x l'ensemble de tous les nombres y dont les $n-1$ premiers coefficients $\eta_1, \dots, \eta_{n-1}$ sont identiques avec ceux de x : $\xi_i = \eta_i \, (i = 1, \dots, n-1)$, ce que nous exprimons aussi par $x \equiv y \, (n!)$.

En particulier $U_n(0)$ contient tous les nombres universels qui sont divisibles par $n!$ (^{2}). Une suite $x_{(1)}, x_{(2)}, \dots$ de nombres $\nu!$-adiques convergera vers x lorsque $x_{(\nu)}$ et x ont les premiers μ termes communs, où μ tend vers ∞ avec ν. Cette définition est équivalente à la suivante : on a $\lim x_{(\nu)} = x$ lorsque pour chaque nombre naturel n il existe un ν_n, tel que $x - x_{(\nu)}$ est divisible par n pour chaque $\nu \geqq \nu_n$. D'une telle suite on peut toujours extraire une suite *réduite*, c'est-à-dire une suite partielle $x_{(m_\nu)}$, telle que $x_{(m_{\nu+1})} \equiv x_{(m_\nu)} \equiv x \; (\nu!)$.

La propriété topologique principale de l'ensemble des nombres universels est qu'il est un ensemble topologique (^{3}) homéomorphe à

(^{1}) Lorsque je veux exprimer explicitement qu'un indice est *variable* et qu'il parcourt tous ou presque tous (c'est-à-dire tous à l'exception d'un nombre fini) les nombres naturels, je le désignerai par une lettre *grecque* (par exemple μ, ν, ρ); des indices constants seront désignés toujours par des lettres latines (par exemple k, m, n, r).

(^{2}) Un nombre universel $y = \lim y_\nu$ est divisible par m, lorsque presque tous les y_ν sont divisibles par m.

(^{3}) Je préfère cette expression à l'expression usuelle « espace topologique ».

l'ensemble cantorien bien connu, qu'on peut obtenir par exemple comme suit : on considère l'intervalle $<0, 1>$, et on le considère comme intervalle de première marche; on divise chaque intervalle de $n^{\text{ième}}$ marche en $2n+1$ intervalles égaux; ceux de ces intervalles égaux dont le numéro d'ordre (à partir du commencement de l'intervalle de $n^{\text{ième}}$ marche) est *impair* seront des intervalles de $(n+1)^{\text{ième}}$ marche. L'ensemble cantorien est alors l'ensemble des points qui appartiennent à l'ensemble des intervalles de $n^{\text{ième}}$ marche pour chaque n. On obtient donc l'ensemble de tous les nombres d'abscisses

$$\xi = \frac{2\xi_1}{3} + \frac{2\xi_2}{3.5} + \frac{2\xi_3}{3.5.7} + \ldots = \sum_{n=1}^{\infty} \frac{2^{n+1} n!}{(2n+1)!} \xi_n \qquad (0 \leqq \xi_n \leqq n).$$

Un nombre universel x pourra être représenté par le nombre réel ξ qui a les mêmes coefficients ξ_ν, la relation entre les x et les ξ étant biunivoque et bicontinue (mais non isomorphe) (1). On peut aussi bien, en construisant l'ensemble cantorien, diviser chaque intervalle de $n^{\text{ième}}$ marche en $2a_n - 1$ parties égales, où les a_ν sont des nombres naturels $\geqq 1$ quelconques. On obtient ainsi l'ensemble des nombres réels

$$(2) \quad \xi = \frac{2\xi_0}{2a_1 - 1} + \frac{2\xi_1}{(2a_1-1)(2a_2-1)} + \frac{2\xi_2}{(2a_1-1)(2a_2-1)(2a_3-1)} + \ldots,$$

où $0 \leqq \xi_n \leqq a_{n+1} - 1$ (2). En posant $b_n = a_1 a_2 \ldots a_n$, $b_0 = 1$, on peut faire correspondre ces nombres réels avec les « nombres »

$$(3) \qquad x = \xi_0 b_0 + \xi_1 b_1 + \xi_2 b_2 + \ldots,$$

que nous appellerons des *nombres b_ν-adiques* généraux. Ici les b_ν forment une suite de nombres naturels, tels que

$$(4) \qquad b_{\nu+1} \equiv 0 \,(b_\nu).$$

Évidemment les nombres $\nu!$-adiques en forment un cas spécial : $b_n = n!$.

D'autre part, pour $b_n = p^n$ on obtient les *nombres p-adiques* (entiers)

---

(1) *Cf.* D. VAN DANTZIG [1].

(2) La construction classique de Cantor lui-même s'obtient pour $a_1 = a_2 = a_3 = \ldots = 2$ et correspond avec l'anneau des nombres dyadiques.

de Hensel, que nous appellerons, par raison d'analogie, plutôt des nombres p^ν-adiques.

Considérons enfin le cas spécial, où, dès un certain n, tous les b_ν sont égaux. Donc $b_\nu = b_n (\nu \geqq n)$, ou bien $a_\nu = 1 (\nu \geqq n+1)$. Alors dans la série (2) tous les $\xi_\nu (\nu \geqq n+1$ doivent être nuls, c'est-à-dire l'ensemble qui prend la place de l'ensemble cantorien est *fini*; il ne contient que b_n points. Dans ce cas nous conviendrons que b_n sera considéré comme égal à zéro, c'est-à-dire dans la série (3) x peut parcourir seulement les nombres différents mod. b_n.

Tous les ensembles qu'on obtient dans le cas général sont homéomorphes. Leurs propriétés topologiques principales sont les suivantes : 1° l'ensemble est *compact* (c'est-à-dire que chaque suite infinie contient au moins une suite partielle qui est *convergente*); 2° le nombre de dimensions de l'ensemble est *zéro*; les $U_n(x)$ sont à la fois ouverts et fermés; 3° l'ensemble est *dense en soi*. Dans le cas où $b_\nu = b_n$, les ensembles ne sont pas homéomorphes; ils possèdent les deux premières propriétés, mais non la troisième.

2. Par la somme, la différence et le produit de deux nombres b_ν-adiques nous entendrons :

$$x \pm y = \lim (x_\nu \pm y_\nu); \qquad xy = \lim x_\nu y_\nu,$$

où $x = \lim x_\nu$, $y = \lim y_\nu$. Par rapport à cette définition les nombres b_ν-adiques constituent *un anneau topologique* $\mathfrak{A}(b_\nu)$ (cf. *T.A.*, I, p. 617). Dans le cas spécial $b_\nu = \nu !$ nous l'appellerons l'anneau *universel* et nous le désignons par $\mathfrak{J}$. Dans le cas $b_\nu = b_n$ les définitions coïncident avec les définitions ordinaires pour les classes mod. b_n. En général l'ensemble $U_n(0)$ sera pour chaque n un *idéal* dans $\mathfrak{A}(b_\nu)$, et bien un *idéal principal*, engendré par b_n :

$U_n(0) = (b_n)$; les $U_n(x)$ sont des classes mod. b_n : $U_n(x) = x + (b_n)$ (1).

(1) M et N étant des ensembles, nous désignons par $M + N$ resp. MN l'ensemble de toutes les sommes resp. tous les produits d'un élément de M et d'un élément de N :

$$M + N = \{ x + y \}_{x \in M, y \in N},$$
$$MN = \{ xy \}_{x \in M, y \in N}.$$

D'une manière analogue nous définissons $a + M$, aM, ΣM_ν, ΠM_ν, etc. Lorsque $M = a$

3. En remplaçant les b_ν par d'autres nombres b'_ν, on obtient le même anneau b_ν-adique, à une transformation isomorphique près (1), lorsque pour chaque n il existe un μ_n tel que

$$b_{\mu_n} \equiv o(b'_n), \qquad b'_{\mu_n} \equiv o(b_n). \tag{5}$$

Donc on peut caractériser la suite des b_ν par un produit infini formel

$$p_0^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \dots, \tag{6}$$

où $p_0, p_1, \dots$ sont tous les nombres premiers, rangés par exemple par ordre de grandeur naturelle ($p_0 = 2, p_1 = 3, p_2 = 5, p_3 = 7, \dots$), tandis que $\alpha_r = k \geqq o$ lorsque presque tous les b_ν (c'est-à-dire tous les b_ν à l'exception d'un nombre fini) sont $\equiv o(p_r^k)$, mais $\not\equiv o(p_r^{k+1})$, tandis que $\alpha_r = \infty$ lorsque les b_ν sont asymptotiquement divisibles par chaque puissance de p_r (2).

Le produit (6) sera appelé l'*ordre formel* de $\mathfrak{A}(b_\nu)$. En particulier l'anneau universel a l'ordre formel $p_0^\infty p_1^\infty p_2^\infty \dots$ et peut être obtenu en vertu du théorème d'isomorphie [*cf.* (5)] non seulement en prenant $b_n = n!$, mais aussi en prenant par exemple

$$b_n = (p_0 p_1 \dots p_n)^n \qquad \text{ou} \qquad b_n = p_0^n p_1^{n-1} p_2^{n-2} \dots p_{n-2}^2 p_{n-1},$$

ou enfin

$$b_n = p_0^{k+1} p_1^k \dots p_{i-1}^{k+2-i} p_i^{k-i} \dots p_{k-2}^2 p_{k-1},$$

lorsque

$$n = \frac{1}{2} k(k+1) + i, \qquad o \leqq i \leqq k, \text{ etc.}$$

Le choix d'une suite particulière de b_ν comme « base de développement » n'est pas essentiel et n'est, pour ainsi dire, que le choix d'un « système de coordonnées » (3). Dans le cas où $b_\nu = b_n$ pour $\nu \geqq n$,

---

et $\mathfrak{N} = \mathfrak{b}$ sont des idéaux, $\mathfrak{a} + \mathfrak{b} = (\mathfrak{a}, \mathfrak{b})$ est le p. g. c. d.; $\mathfrak{ab}$ n'est pas un idéal lui-même, mais il *engendre* l'idéal produit que nous désignerons par conséquent par $(\mathfrak{ab})$.

(1) Nous employons le mot *isomorphie* pour désigner la relation *bi*-univoque, le mot *homomorphie* pour désigner la relation univoque («isomorphie mériédrique»), en concordance avec par exemple B. L. VAN DER WAERDEN, *Moderne Algebra*, et contrairement à par exemple Speiser et Cartan.

(2) C'est-à-dire pour chaque n il existe un ϱ_n, tel que $b_\nu \equiv o(p^n)$ pour $\nu \geqq \varrho_n$.

(3) Nous avons choisi (arbitrairement) la suite $b_\nu = \nu!$ puisqu'elle permet d'exprimer les propriétés générales des nombres universels d'une manière très courte. Néanmoins, pour beaucoup de calculs numériques, elle n'est pas très convenable, puisque la décomposition en facteurs indivisibles de $n!$ est très compliquée.

presque tous les α_r sont nuls, tandis que les autres sont tous finis. La valeur du produit (6) est alors b_n, c'est-à-dire l'ordre du groupe additif formé par les classes mod. b_n. Dans le cas $b_\nu = n^\nu$ le théorème d'isomorphie se réduit au théorème de Hensel d'après lequel les anneaux des nombres m-adiques et n-adiques sont isomorphes, lorsque m et n ont les mêmes facteurs premiers. En effet soit

$$m = p_1^{k_1} \dots p_h^{k_h}, \qquad n = p_1^{l_1} \dots p_h^{l_h} \qquad (0 < k_i,\ l_i < \infty),$$

et soit M le maximum des k_i et des l_i, alors

$$m^{M\nu} \equiv 0(n^\nu) \qquad \text{et} \qquad n^{M\nu} \equiv 0(m^\nu).$$

4. Pour chaque r il existe un nombre b_ν-adique $\underset{r}{e}$, déterminé sans ambiguïté, tel que

$$\underset{r}{e} \equiv 1(p_r^{\alpha_r}), \qquad \underset{r}{e} \equiv 0(p_s^{\alpha_s}) \quad (1) \tag{7}$$

pour chaque $s \neq r$ (2).

On aura

$$1 = \underset{0}{e} + \underset{1}{e} + \underset{2}{e} + \dots, \tag{8}$$

où la somme à droite est convergente (comme toutes les sommes et les produits infinis que nous rencontrerons). Les $\underset{r}{e}$ seront appelés les *unités* (3) de $\mathfrak{A}(b_\nu)$. x étant un nombre b_ν-adique quelconque, on aura

$$x = \underset{0}{x} + \underset{1}{x} + \underset{2}{x} + \dots, \qquad \underset{r}{x} = x\underset{r}{e}. \tag{9}$$

---

(1) Lorsqu'un nombre b_ν-adique x est divisible par *chaque* puissance d'un nombre p, nous dirons pour abréger que x est divisible par p^∞.

(2) Voir *T. A.*, II (TR. 39). La démonstration est d'ailleurs facile : soit $b_n = p_r^k q_r$, où $q_r \not\equiv 0(p_r)$ et $k = k_{n,r}$; alors les congruences $\underset{r}{e}_n \equiv 1(p_r^k)$, $\underset{r}{e}_n \equiv 0(q_r)$ ont une solution commune; $\underset{r}{e}$ est simplement la limite des $\underset{r}{e}_\nu$.

(3) Puisque le mot « unité » a plusieurs significations, nous conviendrons que :

1° l' « élément unité » d'un groupe et aussi de l'anneau le plus étendu qui sera considéré, sera appelé « l'Un »;

2° les composants (additifs) directs de l'Un d'un anneau seront appelés les « unités »;

3° les éléments d'un anneau qui possèdent un élément réciproque seront appelés les « diviseurs d'Un ».

Aussi il existe des nombres $\overset{r}{z}$, tels que

$$\overset{r}{z} \equiv 0 \,(p_r^{\alpha_r}), \qquad \overset{r}{z} \equiv 1 \,(p_s^{\alpha_s}), \tag{10}$$

pour $s \neq r$.

On aura

$$0 = \overset{0\,1\,2}{z z z} \ldots, \tag{11}$$

où le produit à droite aussi est convergent. En général, on aura

$$x = \overset{0\,1\,2}{x x x} \ldots, \qquad \overset{r}{x} = \underset{r}{x} + \overset{r}{z}. \tag{12}$$

Entre les $\underset{r}{e}$ et les $\overset{r}{z}$ plusieurs relations existent, par exemple :

$$\begin{cases} \underset{r}{e}^2 = \underset{r}{e}, & \underset{r}{e}\overset{r}{z} = 0, & \overset{r}{z}^2 = \overset{r}{z}, & \underset{r}{e} + \overset{r}{z} = 1, \\ \underset{rs}{ee} = 0, & \underset{r}{e}\overset{s}{z} = \underset{r}{e}, & \overset{rs}{z z} = \overset{r}{z} + \overset{s}{z} - 1 = 1 - \underset{r}{e} - \underset{s}{e}, \end{cases} \tag{13}$$

pour chaque $s \neq r$. Pour un r avec $\alpha_r = 0$ on aura $\underset{r}{e} = 0$, $\overset{r}{z} = 1$. x, y et u étant des nombres b_ν-adiques quelconques, on aura

$$\begin{aligned} &\underset{r}{x} + \underset{r}{y} = \underset{r}{u}, \qquad \overset{r}{x} + \overset{r}{y} = \overset{r}{u} + \overset{r}{z} \quad \text{pour} \quad x + y = u, \\ &\underset{r\,r}{xy} = \underset{r}{u}, \qquad \overset{r\,r}{x y} = \overset{r}{u} \quad \text{pour} \quad xy = u. \end{aligned}$$

Lorsque $\alpha_r = \infty$ l'ensemble de tous les $\underset{r}{x}$ (r fixe) est isomorphe à l'ensemble de tous les nombres p_r^ν-adiques entiers de Hensel. En effet,

$$x = \lim x_\nu = \Sigma \xi_\nu b_\nu$$

étant un nombre b_ν-adique, on peut le développer d'après les puissances de p_r :

$$\Sigma \xi_\nu b_\nu = \Sigma \eta_\nu p_r^\nu.$$

La somme à droite est convergente en vertu de

$$x_{\nu+1} - x_\nu \equiv 0 \,(b_\nu) \equiv 0 \,(p_r^{\mu_\nu}) \qquad (\mu_\nu \to \infty).$$

Donc on a

$$x = \underset{r}{x}\underset{r}{e} = \underset{r}{e} \Sigma \eta_r p_r^\nu.$$

Dans le cas des nombres universels nous considérons quelques exemples numériques, en choisissant la suite $b_\nu = \nu!$ comme base de développement. On aura par exemple

$$e_0 = 1.1! + 1.2! + 1.3! + 4.4! + 1.5! + 1.6! + 7.7! + 1.8! + 6.9! + \ldots$$

En supprimant les facteurs $\nu!$ et les $+$ on peut écrire d'une façon abrégée :

$$e_0 = 1114117\,16.$$

On obtient ainsi par exemple

	1!	2!	3!	4!	5!	6!	7!	8!	9!	....	
$e_0 =$	1	1	1	4	1	1	7	1	6	...	$(p_0 = 2)$
$e_1 =$	0	2	2	1	5	3	3	1	7	...	$(p_1 = 3)$
$e_2 =$	0	0	0	4	4	2	6	1	5	...	$(p_2 = 5)$
$e_3 =$	0	0	0	0	0	6	6	3	1	...	$(p_3 = 7)$
$e_4 =$	0	0	0	0	0	0	0	0	0	...	$(p_4 = 11)$
$\varepsilon_0 =$	0	2	2	0	4	5	0	7	3	...	
$\varepsilon_1 =$	1	1	1	3	0	3	4	7	2	...	
$\varepsilon_2 =$	1	0	0	1	1	4	1	7	4	...	
$\varepsilon_3 =$	1	0	0	0	0	1	1	5	8	...	
$2_0 =$	0	0	3	3	3	2	6	3	2	...	$= 2.e_0$
$2_1 =$	0	1	1	3	4	0	7	2	4	...	$= 2.e_1$
$2_2 =$	0	0	0	3	3	5	4	3	0	...	$= 2.e_2$
$2_3 =$	0	0	0	0	0	5	5	7	2	...	$= 2.e_3$

Remarquons enfin qu'on a

$$1234567\ldots = -1,$$

donc

$$2234567\ldots = 0334567\ldots = 0044567\ldots = \ldots = 0,$$
$$4134567\ldots = 0624567\ldots = 0083567\ldots = \ldots = 0,$$

Aussi on a par exemple :

$$-\underset{0}{e} = 1120450 73\ldots = \underset{0}{1} + \underset{0}{2} + \underset{0}{4} + \underset{0}{8} + \ldots = \underset{0}{e}(1 + 2 + 2^2 + \ldots) = \xi \underset{0}{e},$$

où ξ est le nombre 2^ν-adique $1111\ldots$, c'est-à-dire -1. De même on a

$$-\underset{2}{e} = 2230141 74\ldots = \underset{2}{e}(4 + 4.5 + 4.5^2 + \ldots) = \eta \underset{2}{e},$$

où η est le nombre 5^ν-adique $4444\ldots$, c'est-à-dire -1.

II. — Nombres premiers et idéaux b_ν-adiques.

5. Deux nombres b_ν-adiques x, y sont *associés* lorsque chacun d'eux est un multiple de l'autre : $x = uy$, $y = vx$, ou, autrement dit, lorsqu'ils ne se distinguent que par un facteur qui est un *diviseur d'Un* :

$$x = uy, \qquad 1 \equiv 0(u).$$

Introduisons le nombre universel

$$\pi = \Sigma p_r \underset{r}{e}. \tag{14}$$

On aura donc

$$\underset{r}{\pi} = \underset{r}{p_r}, \qquad \overset{r}{\pi} = \overset{r}{p_r} = p_r \underset{r}{e} + \overset{r}{z}. \tag{15}$$

Chaque nombre $\overset{r}{x}$ *est associé avec une puissance* (*dont l'exposant peut être zéro ou infini*) *de* $\overset{r}{\pi}$. Cela équivaut à dire qu'il existe un diviseur $\underset{r}{u}$ de $\underset{r}{e}$, tel que

$$\underset{r}{x} = \underset{r}{u}\,\underset{r}{\pi^k}, \qquad \underset{r}{e} \equiv 0\left(\underset{r}{u}\right),$$

car de ces relations il s'ensuit

$$\overset{r}{x} = \overset{r}{u}\,\overset{r}{\pi^k}, \qquad 1 \equiv 0\left(\overset{r}{u}\right).$$

Mais on a

$$\underset{r}{x} = (\Sigma \eta_\nu p_r^\nu)\underset{r}{e}.$$

Supposons d'abord que tous les η_ν soient nuls. Alors $\underset{r}{x} = 0$ est associé

avec $\overset{r}{\pi}^{\infty} = 0$, et $\overset{r}{x}$ avec $\overset{r}{\pi}^{\infty} = \overset{r}{z}$. Supposons alors qu'on ait

$$\eta_0 = \ldots = \eta_{k-1} = 0, \qquad \eta_k \not\equiv 0,$$

alors $x p_r^{-k}$ est $\not\equiv 0(p_r)$, donc un diviseur de e. [Car de $u \not\equiv 0(p_r)$ il s'ensuit qu'il existe des φ_ν avec $u\varphi_\nu \equiv 1(p_r^\nu)$, donc $u\varphi = e$, où $\varphi = \lim \varphi_\nu e$.] Donc x est associé avec $p_r^k e = \pi^k$. Nous appellerons ∞ ou k la *hauteur* de x (1).

Il s'ensuit immédiatement que *chaque nombre universel est associé avec un produit fini ou infini de puissances des* $\overset{r}{\pi}$. Car soit

$$x = \Pi \overset{r}{x}, \qquad \overset{r}{x} = u \overset{r}{\pi}^{k_r}, \qquad 1 \equiv 0\left(\overset{r}{u}\right),$$

alors

$$x = u \Pi \overset{r}{\pi}^{k_r}, \qquad u = \Pi \overset{r}{u}, \qquad \text{donc} \quad 1 \equiv 0(u).$$

En particulier chaque nombre naturel est associé avec un produit fini de puissances finies des $\overset{r}{\pi}$. Les associés des p_r sont les $\overset{r}{\pi}$ eux-mêmes. Donc soit $n = \prod_1^m p_i^{ki}$, alors $n = u \prod_1^m \overset{i}{\pi}_{k_i}$, $1 \equiv 0(u)$. Il est remarquable que les nombres premiers *universels* $\overset{r}{\pi}$ ont dans un certain sens des propriétés plus simples que les nombres premiers ordinaires p_r, qu'ils remplacent. Car outre $\overset{r}{\pi} = p_r$ on a $\overset{r}{\pi} = e(s \neq r)$, tandis que les p_r ne sont que des nombres associés à e sans aucune particularité.

Prenons comme exemples quelques-uns des nombres premiers universels :

$$\overset{0}{\pi} = 2\overset{0}{e} + \overset{0}{z} = 021411716\ldots, \qquad p_0 = 2 = 01000\ldots,$$

$$\overset{1}{\pi} = 3\overset{1}{e} + \overset{1}{z} = 111340724\ldots, \qquad p_1 = 3 = 11000\ldots,$$

$$\overset{2}{\pi} = 5\overset{2}{e} + \overset{2}{z} = 100114170\ldots, \qquad p_2 = 5 = 12000\ldots,$$

$$\overset{3}{\pi} = 7\overset{3}{e} + \overset{3}{z} = 100001058\ldots, \qquad p_3 = 7 = 10100\ldots.$$

(1) Afin d'éviter le mot « ordre » dont fait usage Hensel et que nous employons dans un autre sens.

En effet, on a :

$$\overset{0}{\pi}/2 = \underset{0}{e} + \frac{1}{2}\overset{0}{z} = 1224047\,08\ldots, \qquad 2/\overset{0}{\pi} = \underset{0}{e} + 2\overset{0}{z} = 1220450\,62\ldots;$$

$$\overset{1}{\pi}/3 = \underset{1}{e} + \frac{1}{3}\overset{1}{z} = 10325473\ldots., \qquad 3/\overset{1}{\pi} = \underset{1}{e} + 3\overset{1}{z} = 10311606\ldots.;$$

$$\overset{2}{\pi}/5 = \underset{2}{e} + \frac{1}{5}\overset{2}{z} = 12043331\ldots., \qquad 5/\overset{2}{\pi} = \underset{2}{e} + 5\overset{2}{z} = 12044263\ldots.;$$

$$\overset{3}{\pi}/7 = \underset{3}{e} + \frac{1}{7}\overset{3}{z} = 101400\ldots\ldots, \qquad 7/\overset{3}{\pi} = \underset{3}{e} + 7\overset{3}{z} = 10100663\ldots..$$

D'autant plus

$$\underset{0}{\pi} = \underset{0}{2} = 2\ 2\ 2\ 8\ 2\ 2\ 14\ 2\ 12\ \ldots = 0\ 0\ 3\ 3\ 3\ 2\ 6\ 3\ 2\ \ldots,$$

$$\underset{1}{\pi} = \underset{1}{3} = 0\ 6\ 6\ 3\ 15\ 9\ 9\ 3\ 21\ \ldots = 0\ 0\ 0\ 0\ 4\ 4\ 2\ 4\ 1\ \ldots,$$

$$\underset{2}{\pi} = \underset{2}{5} = 0\ 0\ 0\ 20\ 20\ 10\ 30\ 5\ 35\ \ldots = 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 6\ \ldots,$$

$$\underset{3}{\pi} = \underset{3}{7} = 0\ 0\ 0\ 0\ 0\ 42\ 42\ 21\ 7\ \ldots = 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ \ldots,$$

d'où

$$\pi = 0\ 0\ 3\ 3\ 1\ 0\ 1\ 8\ 9\ \ldots.$$

6. *Chaque idéal fermé dans* $\mathfrak{J}$ *est un idéal principal.* — En effet, soit $\mathfrak{b} = \bar{\mathfrak{b}}$ un idéal fermé quelconque, $\underset{r}{\mathfrak{b}} = \mathfrak{b}\underset{r}{e}$, et soit $\underset{r}{\pi}^{\beta_r}$ la puissance la plus grande de $\underset{r}{\pi}$ par laquelle chaque élément de $\underset{r}{\mathfrak{b}}$ est divisible ($0 \leqq \beta_r \leqq \infty$) ($\beta_r$ est dite la hauteur de $\underset{r}{\mathfrak{b}}$). Puisque chaque élément de $\underset{r}{\mathfrak{b}}$ d'une hauteur γ est divisible par $\underset{r}{\pi}^{\gamma}$ et puisque $\gamma \geqq \beta_r$, $\underset{r}{\mathfrak{b}} \equiv 0(\underset{r}{\pi}^{\beta_r})$.

D'autre part, x étant un élément de hauteur β_r, appartenant à $\underset{r}{\mathfrak{b}}$, x est associé à $\underset{r}{\pi}^{\beta_r}$, donc $\underset{r}{\pi}^{\beta_r} \equiv 0(x) \equiv 0(\underset{r}{\mathfrak{b}})$, donc $\underset{r}{\mathfrak{b}} = (\underset{r}{\pi}^{\beta_r})$. Donc, en posant $y = \sum_{\rho} \overset{\rho}{\pi}^{\beta_\rho}$, on a $\mathfrak{b} = (y)$ (1). Puisqu'on a aussi $y = \prod_{\rho} \overset{\rho}{\pi}^{\beta_\rho}$, on peut caractériser un idéal (fermé) quelconque par son produit convergent $\overset{0}{\pi}^{\beta_0}\overset{1}{\pi}^{\beta_1}\overset{2}{\pi}^{\beta_2}\ldots$ ou aussi par le produit formel $p_0^{\beta_0}p_1^{\beta_1}p_2^{\beta_2}\ldots$.

(1) C'est ici qu'intervient la condition que $\mathfrak{b}$ soit fermé. Autrement la somme d'une infinité de termes π^{β_r} appartenant à $\mathfrak{b}$ n'appartiendrait pas nécessairement à $\mathfrak{b}$.

Les seuls idéaux premiers $\neq(1)$ *sont* $\overset{r}{\mathfrak{p}}=(\overset{r}{\pi})$ *et* $(\overset{r}{\mathfrak{z}})=(\overset{r}{z})$. On démontre facilement que $(\overset{r}{\pi})=(p_r)$ reste premier dans $\mathfrak{J}$. Aussi il est clair que $\overset{r}{\mathfrak{z}}=\overset{r}{\mathfrak{p}}^{\infty}$ doit être premier, car xy étant divisible par p_r^{∞}, ou bien x ou bien y doit contenir une puissance infinie de p_r. La preuve qu'il n'y a pas d'autres éléments premiers est immédiate. Il est à remarquer que $\overset{r}{\mathfrak{z}}$, quoique premier, n'est pas indivisible. En effet, on a $\overset{r}{\mathfrak{z}}\equiv o(\overset{r}{\mathfrak{p}})$. Tous les idéaux primaires, appartenant à $\overset{r}{\mathfrak{p}}$, c'est-à-dire les $\overset{r}{\mathfrak{p}}^{\nu}$ sont des diviseurs de $\overset{r}{\mathfrak{z}}$. Donc le théorème des chaînes multiplicatives (« Vielfachenkettensatz ») n'est pas valable en $\mathfrak{J}$ (1). Le seul idéal primaire appartenant à $\overset{r}{\mathfrak{z}}$ est $\overset{r}{\mathfrak{z}}$ lui-même.

Chaque anneau b_ν*-adique est isomorphe à un anneau factoriel* $\mathfrak{J}/\mathfrak{b}$ où $\mathfrak{b}$ *est l'idéal engendré par* $\overset{0}{\pi}^{\beta_0}\overset{1}{\pi}^{\beta_1}\ldots$, *correspondant à l'ordre formel* $p_0^{\beta_0}p_1^{\beta_1}\ldots$ de $\mathfrak{A}(b_\nu)$. Cet idéal sera appelé l'*ordre idéal* ou simplement l'*ordre* de $\mathfrak{A}(b_\nu)$. En effet, du théorème d'homomorphie (2) il s'ensuit que $\mathfrak{A}(b_\nu)$ est homomorphe de $\mathfrak{J}$. Donc il existe un idéal $\mathfrak{b}\subset\mathfrak{J}$ avec $\mathfrak{A}(b_\nu)\cong\mathfrak{J}/\mathfrak{b}$. $\mathfrak{b}$ doit être fermé, puisqu'il est l'ensemble de tous les éléments qui correspondent à o, la correspondance étant univoque et continue. Puisqu'en $\mathfrak{A}(b_\nu)$, $(o)=[(b_1),(b_2),\ldots]$, on a $\mathfrak{b}=[(b_1),(b_2)\ldots]$ en $\mathfrak{J}$. Donc

$$\mathfrak{b}=\left(\overset{0}{\pi}^{\beta_0}\overset{1}{\pi}^{\beta_1}\ldots\right)=(p_0^{\beta_0}p_1^{\beta_1}\ldots),$$

c'est-à-dire $\mathfrak{b}$ est engendré par l'ordre formel de $\mathfrak{A}(b_\nu)$. De ce théorème fondamental il s'ensuit qu'il n'est plus nécessaire de considérer d'autres anneaux b_ν-adiques que $\mathfrak{J}$. Car un élément x d'un anneau b_ν-adique peut être remplacé par la classe $x+\mathfrak{b}$ des éléments congrus à x mod. $\mathfrak{b}$. En particulier les nombres p_n^{ν}-adiques sont les classes mod. $\overset{r}{\mathfrak{z}}$: $\mathfrak{A}(p_r^{\nu})\cong\underset{r}{\mathfrak{e}}\cong\mathfrak{J}/\overset{r}{\mathfrak{z}}$.

III. — Puissances ν!-adiques.

7. Un nombre universel x sera appelé *subsistant* lorsque l'idéal

(1) Ni aussi le théorème des chaînes additives (« Teilerkettensatz », théorème de base), puisque par exemple l'idéal formé de toutes les sommes *finies* $\underset{1}{x}+\ldots+\underset{n}{x}$ (n arbitraire) n'a pas de base finie.

(2) *T. A.*, II, TR. 28, p. 204.

$\mathfrak{x} = (x)$ qu'il engendre est *idempotent* (c'est-à-dire $\mathfrak{x}^2 = \mathfrak{x}$). On peut aussi dire : lorsque tous ses composants additifs sont ou bien des diviseurs des unités correspondantes, ou bien zéro ; or, aussi : lorsqu'il est un diviseur d'un *élément* idempotent. Car soit $\overset{r}{\mathfrak{x}} = \overset{r}{\mathfrak{p}}^{\alpha_r}$; alors $\overset{r}{\mathfrak{x}}^2 = \overset{r}{\mathfrak{x}}$, donc $2\alpha_r = \alpha_r$, donc $\alpha_r = 0$ ou $\alpha_r = \infty$. On a donc : ou bien $(\underset{r}{x}) = \underset{r}{\mathfrak{x}} = (\underset{r}{e})$, ou bien $\underset{r}{x} = 0$. Autrement dit : ou bien $(\overset{r}{x}) = (1)$ ou bien $(\overset{r}{x}) = \overset{r}{\mathfrak{z}}$ (1). En particulier chaque diviseur d'Un est un nombre subsistant.

x (ou $\mathfrak{x}$) étant un nombre (idéal) quelconque, le nombre $\eta = \hat{\Sigma}\underset{r}{e}$, où la somme s'étend à tous les $\underset{r}{e}$ pour lesquels $(\underset{r}{x}) = \underset{r}{\mathfrak{x}}$ (respectivement $\underset{r}{\mathfrak{x}} = \underset{r}{\mathfrak{e}}$), sera appelé le *fondement* de x (respectivement de $\mathfrak{x}$). On peut aussi définir un nombre subsistant comme un nombre qui se reproduit par multiplication avec son fondement : $x = x\eta$. Deux nombres, subsistants ou non, seront appelés *équistants* lorsqu'ils ont le même fondement.

8. *Pour chaque nombre subsistant a et chaque nombre universel x il existe la puissance a^x.* — Nous la définissons comme $\lim a^{x_\nu}$, où les x_ν sont des nombres naturels $\geqq 0$, convergents vers x, et nous allons démontrer que la limite existe (2). On a

$$a^{x_n} = \sum_r \underset{r}{a}^{x_n}.$$

Soit d'abord $\underset{r}{a} \not\equiv 0$, donc $a \not\equiv 0 (p_r)$. Alors $a^{\varphi(p_r^n)} \equiv 1 (p_r^n)$, $\varphi(p_r^n) = p_r^{n-1}(p_r - 1)$ étant l'indicatrice d'Euler. En effet, soit $a = \lim a_\mu$,

(1) Donc x est subsistant lorsqu'il ne contient aucun facteur premier p_r dans une puissance *finie* $\neq 0$.

(2) On pourrait définir a^x aussi lorsque a n'est pas subsistant, en requérant que les x_ν soient les segments initiaux de x. Alors on aurait par exemple pour un a fini

$$a^\star = \lim a^{\nu!} = a^0 \neq 1.$$

En élevant un tel nombre d'abord à la puissance lim $\nu!$ et alors à une puissance quelconque, la seule partie qui subsiste est formée des puissances de $a^\star a$, nombre qui est donc la partie subsistante de a. Il y aurait des difficultés lorsque x est un nombre naturel, puisque $a^n \neq a^0 a^n$. En général a^{x+y} serait $\neq a^x . a^y$.

donc $a_\mu \not\equiv o(p_r), \ldots a_\mu^{\varphi(p_r^n)} \equiv 1(p_r^n), \ldots a^{\varphi(p_r^n)} \equiv 1(p_r^n)$. Mais pour $\nu \geqq \varphi(p_r^\mu)$ on a $\nu! \equiv o[\varphi(p_r^\mu)]$. Donc (la suite x_ν étant supposée réduite)

$$x_{\nu+1} - x_\nu \equiv o(\nu!) \equiv o[\varphi(p_r^\mu)],$$

donc

$$a^{x_{\nu+1}} - a^{x_\nu} \equiv o(a^{x_{\nu+1}-x_\nu} - 1) \equiv o(a^{\varphi(p_r^\mu)} - 1) \equiv o(p_r^\mu).$$

[Remarquons que de $u \equiv o(v)$, (u et v des nombres naturels) il s'ensuit $a^u - 1 \equiv o(a^v - 1)$ pour un a quelconque!]. Mais cette relation subsiste encore pour $\underset{r}{a} = o$, c'est-à-dire $a \equiv o(p_r^\varkappa)$, en supposant que les x_ν soient $> o$. D'autre part, pour $x = x_\nu = o$, elle est triviale. Donc elle existe pour chaque r. Donc aussi

$$a^{x_{\nu+1}} - a^{x_\nu} \equiv o(p_1^{\varrho_1} \ldots p_k^{\varrho_k}) = (\mu!) \qquad \text{pour} \quad \nu \geqq \varphi(\mu!).$$

Donc la suite des a^{x_ν} est fondamentale, c'est-à-dire $a^x = \lim a^{x_\nu}$ existe.

On démontre facilement que a^x est une fonction continue aussi bien de a que de x (à condition que a reste toujours subsistant) et que les relations usuelles

$$\text{(16)} \qquad \begin{cases} a^x . a^y = a^{x+y}, \\ (a^x)^y = a^{xy}, \\ a^x . b^x = (ab)^x \end{cases}$$

sont remplies. Il est à remarquer que a^x est subsistant lorsque a est subsistant et que ab est subsistant lorsque a et b sont subsistants. En particulier on a

$$\text{(17)} \qquad \begin{cases} a^1 = a, \\ a^0 = \hat{\Sigma}_r a^0 = \hat{\Sigma}_r e, \end{cases}$$

où l'accent circonflexe indique que la sommation ne s'étend qu'à des r pour lesquels $\underset{r}{a} \not\equiv o$(1). Donc a^0 est le fondement de a. Puisque $-1 = \lim(\nu! - 1)$ est une limite de nombres naturels, a^{-1} existe

(1) En général le signe $\hat{\Sigma}$ désignera une sommation étendue à une suite partielle (finie ou infinie) bien définie des r; le signe $\check{\Sigma}$ désignera une sommation, étendue à tous les autres r. Donc par exemple :

$$\hat{\Sigma}_r e + \check{\Sigma}_s e = 1, \qquad \hat{\Sigma}_r e . \check{\Sigma}_s e = o$$

aussi, et l'on a

$$a^{-1} = \sum_r a_r^{-1}, \tag{18}$$

où a_r^{-1} est le nombre satisfaisant à la relation

$$a_r \cdot a_r^{-1} = a_r^{-1} \cdot a_r = e_r.$$

(Celui-ci existe puisque a_r est un diviseur de l'unité) (1).

Remarquons enfin que non seulement 1, mais aussi 0 est un nombre subsistant. Outre la relation triviale

$$1^x = 1 \tag{19}$$

pour chaque nombre x, on a aussi

$$0^x = 0 \tag{20}$$

pour chaque x; en particulier on a les relations remarquables

$$0^1 = 0^0 = 0^{-1} = 0. \tag{21}$$

Un nombre universel *arbitraire* a est la somme d'un nombre subsistant $a' = a\eta$, où $\eta = a^0 = \lim a\nu!$, et d'un multiple

$$a'' = a - a' = a(1 - \eta)$$

de π (2). Évidemment $a'a'' = 0$. Dans ce cas aussi η est le fondement de a.

IV. — L'indicatrice d'Euler.

9. M étant un ensemble quelconque dans $\mathfrak{J}$, nous désignerons par a^M (a = nombre subsistant) l'ensemble de tous les nombres a^x, $x \varepsilon M$. En particulier $a^{\mathfrak{b}}$ est un groupe multiplicatif lorsque $\mathfrak{b}$ est un groupe additif, par exemple un idéal. L'Un du groupe $a^{\mathfrak{b}}$ est évidemment a^0. Le plus grand idéal $\mathfrak{b}$ (c'est-à-dire le p. g. c. d. de tous les idéaux)

(1) Chez Hensel, Prüfer et von Neumann a^{-1} n'est défini que dans le cas où *aucun* a_r n'est nul, c'est-à-dire où a n'est pas un diviseur de zéro.

(2) Donc a'' est divisible par tous les nombres premiers naturels p_r.

pour lequel $a^b = a^0$ sera appelé *l'ordre* de l'élément a (par rapport à la multiplication)(1).

Considérons un groupe multiplicatif fermé arbitraire $\mathfrak{G}$, contenu en $\mathfrak{J}$; soit η son élément unité. Évidemment un élément arbitraire x de $\mathfrak{G}$ doit être un nombre subsistant (puisque x^{-1} doit exister). En particulier, η étant idempotent, il doit être une somme d'un nombre fini ou infini d'unités : $\eta = \hat{\Sigma} e$. Puisque $x.x^{-1} = x^0$ doit être égal à η, tous les x ont le même fondement η. D'autre part l'ensemble de *tous* les nombres subsistants x, ayant le même fondement $x^0 = \eta$ est un groupe multiplicatif fermé $\mathfrak{G}$, ayant $\mathfrak{G}$ comme sous-groupe. Un cas spécial est celui où $\mathfrak{G}$ est « vide », c'est-à-dire ne contient que son élément unité η. Un cas encore plus spécial se présente lorsque $\mathfrak{G}$ aussi est vide, voir lorsque $\eta = 0$. Un autre cas spécial est présenté par le groupe $\hat{\mathfrak{G}}$ de tous les diviseurs d'Un, se rapportant à $\eta = 1$.

10. Chaque groupe $\mathfrak{G}$ (multiplicatif, fermé et contenu dans $\mathfrak{J}$) est un *groupe cantorien*, c'est-à-dire qu'il est ou bien homéomorphe avec l'ensemble cantorien, ou bien fini. Or, dans la théorie des groupes cantoriens, on démontre qu'un tel groupe est un *groupe $\mathfrak{G}_\nu$-adique*. Cela veut dire qu'il possède une suite de sous-groupes (invariants) $\mathfrak{G}_\nu$, tels que 1° $\mathfrak{G}_{\nu+1} \subset \mathfrak{G}_\nu$, 2° $\mathfrak{G}_n$ est ouvert, donc aussi fermé (2) dans $\mathfrak{G}$, 3° l'intersection de tous les $\mathfrak{G}_\nu$ est l'élément unité de $\mathfrak{G}$ (3).

Dans le cas spécial $\mathfrak{G} \subset \mathfrak{J}$ que nous considérons, on peut prendre pour $\mathfrak{G}_n$ l'ensemble de tous les x de $\mathfrak{G}$ tels que $x \equiv \eta\,(n!)$.

$\mathfrak{G}_n = \eta + (n!)$. Ils forment un groupe, car de $x \equiv \eta(n!)$, $y \equiv \eta(n!)$ il suit

$$xy \equiv \eta(n!) \qquad \text{et} \qquad \eta = xx^{-1} \equiv \eta x^{-1} = x^{-1}(n!).$$

$\mathfrak{G}$ étant commutatif, ce sous-groupe est invariant. Il est évident que les propriétés 1° et 3° sont remplies. Quant à 2°, soit x_ν une suite (que nous pouvons supposer réduite) dans $\mathfrak{G}$ avec $x_\nu \to \eta$; alors $x_\nu \equiv \eta(\nu!)$

(1) Par contre l'ordre *additif* de a est le plus grand idéal $\mathfrak{c}$ pour lequel $\mathfrak{c}a = 0$, donc $\mathfrak{c} = (0) : (a)$. (*Voir* n° 10.)

(2) Chaque sous-groupe ouvert d'un groupe topologique est fermé. Comp. *T. A.*, I, TG. 17).

(3) De tels groupes ont été introduits pour la première fois (abstraction faite du cas spécial des groupes de nombres p-adiques) par L. E. J. Brouwer [3].

pour presque tous les ν, c'est-à-dire x_ν est situé dans $\mathfrak{G}_\nu$, donc $\mathfrak{G}_\nu$ est ouvert, donc aussi fermé. Puisque $\mathfrak{G}$ est compact, chaque $\mathfrak{G}_n$ doit avoir un index fini g_n dans $\mathfrak{G}$; puisque $g_{n+1} \equiv o(g_n)$, la suite des g_ν définit un produit formel $p_0^{\gamma_0} p_0^{\gamma_1} \ldots$, donc aussi un idéal $\mathfrak{g} \subset \mathfrak{J}$, que nous appelons l'*ordre* $\mathfrak{o}(\mathfrak{G})$ de $\mathfrak{G}$ (1). L'ordre de chaque sous-groupe de $\mathfrak{G}$, et en particulier de chaque élément, est un diviseur de $\mathfrak{g}$. Donc, pour chaque élément x de $\mathfrak{g}$, on a la relation

$$x^{\mathfrak{g}} = \eta_1. \tag{22}$$

Chaque élément x de $\mathfrak{g}$ est relativement premier avec $1 - \eta_1$, c'est-à-dire que x est un diviseur d'Un mod. $(1 - \eta_1)$, $(x, 1 - \eta_1) = (1)$, puisque x est associé avec η_1.

11. Considérons maintenant un idéal $\mathfrak{b}$ (fermé) quelconque dans $\mathfrak{J}$. *Chaque nombre y qui est relativement premier avec $\mathfrak{b}$ est congru* mod. $\mathfrak{b}$ *à un nombre x ayant la même propriété, et qui est d'ailleurs subsistant.* En effet, soit $\mathfrak{b} = \hat{\sum}_r \mathfrak{p}^{\alpha_r} + \check{\sum}_r \mathfrak{e}$, où la première somme s'étend à tous les r pour lesquels $\alpha_r > o$ [y compris ceux-ci pour lesquels $\alpha_r = \infty$, c'est-à-dire $\mathfrak{b}_r = (o)$] et la seconde somme à tous les autres r. Posons $\eta_1 = \hat{\sum}_r e_r$. Alors $\varepsilon = \check{\sum}_r e_r = 1 - \eta_1 \equiv o(\mathfrak{b})$. Posons $x = y\eta_1 = y - y\varepsilon$, $\therefore x \equiv y(\mathfrak{b})$. Il reste à démontrer que x est subsistant. Puisque y (donc aussi x) est relativement premier avec $\mathfrak{b}$, il existe une relation $1 = ux + b$, $b \equiv o(\mathfrak{b})$. Soit maintenant e_r un des termes de η_1. Donc $\mathfrak{b} \equiv o(p_r)$, $e_r \eta_1 = e_r$. On a

$$e_r = u_r x + b_r.$$

Mais b_r étant un multiple de p_r, il s'ensuit que x_r est $\not\equiv o(p_r)$, donc x_r est associé avec e_r. Ceci est le cas pour tous les termes de η_1, donc $x = x\eta_1$ est associé avec η_1. Donc x est un nombre subsistant.

On peut donc représenter tous les diviseurs d'Un dans l'anneau $\mathfrak{J}/\mathfrak{b}$ par des nombres subsistants de $\mathfrak{J}$. Or, *les nombres subsistants, qui sont*

(1) En particulier, en considérant un idéal $\mathfrak{a}$ comme un groupe *additif*, son ordre additif $\mathfrak{g} = \mathfrak{o}(\mathfrak{a})$ satisfait à la relation $\mathfrak{g}\mathfrak{a} = (o)$. On a même $\mathfrak{g} = (o) : \mathfrak{a}$, c'est-à-dire $\mathfrak{g}$ est le p. g. c. d. de tous les x tels que $x\mathfrak{a} = (o)$, ou aussi : $\mathfrak{g}$ est l'*annulateur* de $\mathfrak{a}$. Évidemment $\mathfrak{g} = \mathfrak{o}(\mathfrak{a}) = (\eta)$, où $(1 - \eta) = \mathfrak{a}^0 = \lim_{\nu \to \infty} \mathfrak{a}^{\nu!}$.

relativement premiers avec $\mathfrak{b}$ *forment un groupe* $\mathfrak{G}$. En effet, soit $(x, \mathfrak{b}) = (1)$, $x^0 = \eta$, $x = x\eta$. Donc il existe un u avec $1 \equiv ux(\mathfrak{b})$. Donc u aussi est relativement premier avec $\mathfrak{b}$ et peut en vertu de $\eta \equiv 1(b)$ être supposé subsistant aussi avec $u^0 = \eta$. Mais alors $x^{-1}u^{-1} = (ux)^{-1} \equiv ux = \eta\,(\mathfrak{b})$, c'est-à-dire x^{-1} appartient à $\mathfrak{G}$. Soit aussi $(y, \mathfrak{b}) = (1)$, etc., donc $1 \equiv \eta y\,(\mathfrak{b})$, alors $1 \equiv uxy\eta y\,(\mathfrak{b})$, donc xy appartient à $\mathfrak{G}$. En effet $\mathfrak{G}$ se compose de tous les nombres universels associés à η. Deux nombres différents de $\mathfrak{G}$ peuvent être congrus mod $\mathfrak{b}$; par $\mathfrak{G}_\mathfrak{b}$ nous désignerons le groupe des diviseurs d'Un dans $\mathfrak{J}/\mathfrak{b}$. $\mathfrak{G}_\mathfrak{b}$ est isomorphe au groupe quotient $\mathfrak{G}/\mathfrak{B}$ suivant le sous-groupe $\mathfrak{B}$, se composant de tous les éléments de $\mathfrak{G}$, congrus à 1 (ou à η) mod $\mathfrak{b}$. Évidemment

$$\mathfrak{B} = \eta + \mathfrak{b}\eta \cong \varepsilon + \mathfrak{B} = 1 + \mathfrak{b}. \tag{23}$$

L'ordre de $\mathfrak{G}_\mathfrak{b}$ *sera appelé l'indicatrice d'Euler de* $\mathfrak{b}$ *et sera dénoté par* $\varphi(\mathfrak{b})$. Il est à remarquer que cette indicatrice est un *idéal*. Il résulte immédiatement de (22) que le théorème d'Euler est valable ici :

Chaque nombre x *qui est relativement premier avec* $\mathfrak{b}$ *satisfait à l'équation*

$$x^{\varphi(\mathfrak{b})} - 1 \equiv 0(\mathfrak{b}). \tag{24}$$

12. Il reste à calculer $\varphi(\mathfrak{b})$. Nous démontrerons

$$\varphi(\mathfrak{b}) = \hat{\Pi}\,\overset{r}{\mathfrak{p}}{}^{\alpha_r - 1}(p_r - 1), \tag{25}$$

où par $\overset{r}{\mathfrak{p}}{}^{\alpha-1}$ il faut entendre l'idéal $\overset{r}{\mathfrak{p}}{}^{\alpha} = \overset{r}{\mathfrak{z}}$ lui-même, tandis que $\mathfrak{b} = \hat{\Pi}\overset{r}{\mathfrak{p}}{}^{\alpha_r}$ et que les produits s'étendent à tous les r avec $\alpha_r > 0$. En particulier on a donc comme d'ordinaire

$$\varphi(\mathfrak{b}) = \hat{\Pi}\,\varphi\left(\overset{r}{\mathfrak{b}}\right) = \Pi\,\varphi\left(\overset{r}{\mathfrak{b}}\right),$$
$$\varphi(\mathfrak{p}^\alpha) = \mathfrak{p}^{\alpha-1}(p-1) \qquad \text{pour} \quad \alpha > 0.$$

En effet, soit $\mathfrak{G}_n$ l'ensemble de tous les nombres de $\mathfrak{G}$, congrus à η mod $(p_{r_1}\ldots p_{r_n})^n$, où $p_{r_1}, p_{r_2}, \ldots$ sont *tous* les diviseurs premiers ordinaires de $\mathfrak{b}$. Tout comme ci-dessus on démontre que $\mathfrak{G}_n$ est un sous-groupe

de $\mathfrak{G}$, donc $\mathfrak{G}_{n,\mathfrak{b}}$ de $\mathfrak{G}_{\mathfrak{b}}$, où $\mathfrak{G}_{n,\mathfrak{b}} = \mathfrak{G}_n \mathfrak{B}/\mathfrak{B}$. Or l'index g_n de $\mathfrak{G}_{n,\mathfrak{b}}$ dans $\mathfrak{G}_{\mathfrak{b}}$ est égal au nombre d'éléments de $\mathfrak{G}$ qui sont différents mod. $(p_{r_1} \dots p_{r_n})^n$ et aussi mod. $\mathfrak{b}$, donc mod. $p_{r_1}^{\beta_{n,1}} \dots p_{r_n}^{\beta_{n,n}}$, où $\beta_{n,i}$ est le minimum des nombres α_{r_i} et n. Ce nombre est donc

$$g_n = \varphi(p_{r_1}^{\beta_{n,1}} \dots p_{r_n}^{\beta_{n,n}}) = \prod_1^n p_{r_i}^{\beta_{n,i}-1}(p_{r_i} - 1).$$

Ceux des α_r qui sont finis donneront donc pour chaque n qui est assez grand $\beta_{n,r} = \alpha_r$; ceux des α_r qui sont infinis donneront cependant $\beta_{n,r} = n$, donc $\lim \beta_{\nu,r} = \infty = \alpha_r$. L'ordre formel de $\mathfrak{G}_{\mathfrak{b}}$ étant la limite des (g_ν), on trouve par conséquent

$$\lim(g_\nu) = \hat{\Pi} p_{r_\nu}^{\alpha_{r_\nu}-1}(p_{r_\nu} - 1),$$

d'où suit la formule indiquée pour $\varphi(\mathfrak{b})$.

Notons quelques cas particuliers :

1° Tous les $\alpha_r = 0$: $\varphi(1) = (1)$.

2° Tous les $\alpha_r = \infty$: $\varphi(0) = (0)$.

3° Tous les $\alpha_r = 0$ ou $= \infty$:

$$\varphi(\varepsilon) = \varepsilon \hat{\Pi}(p_r - 1), \qquad \varepsilon = 1 - \hat{\Sigma} e_r.$$

Dans ce cas $\varphi(\mathfrak{b})$ est donc un *vrai multiple* de $\mathfrak{b} = (\varepsilon)$, excepté pour $\varepsilon = 1$, pour $\varepsilon = 0$ et pour $\varepsilon = \overset{0}{z}$, $(\overset{0}{z}) = \varphi(\overset{0}{z}) = \overset{0}{3} = (2^\infty)$.

En particulier

$$(27) \qquad \begin{cases} \varphi\left(\begin{smallmatrix} r \\ 3 \end{smallmatrix}\right) = (p_r - 1)\overset{r}{3}. \\ \varphi\left(\begin{smallmatrix} \varepsilon \\ r \end{smallmatrix}\right) = \varepsilon \prod_{r\, s \neq r} (p_s - 1) = (0) \qquad (\text{comp. } 4^\circ, 5^\circ). \end{cases}$$

4° Tous les $\alpha_r = 1$:

$$(28) \qquad \varphi(\pi) = \Pi(p_r - 1) = (0).$$

En effet, d'après le théorème célèbre de Dirichlet, chaque progression arithmétique dont la raison est un nombre relativement premier avec le terme initial contient une infinité de nombres premiers. Donc pour chaque p il existe une infinité de nombres premiers p_{n_ν} de la

forme $k_\nu p + 1$; donc

$$\varphi(p_{n_\nu}) \equiv o(p), \qquad \therefore \varphi\left(\prod_{\nu=1}^{\infty} p_{n_\nu}\right) \equiv o(p^\infty), \qquad \therefore \varphi(\pi) \equiv o\binom{r}{3}$$

pour chaque r, $\therefore \varphi(\pi) = (o)$

5° Plus généralement on a $\varphi(x) = (o)$ pour chaque élément x dont le fondement consiste en une somme *finie* de $\underset{r}{e}$.

V. — Équations binomes.

13. Supposons donné un idéal fermé quelconque $\mathfrak{a}$ dans $\mathfrak{J}$. Nous démontrerons que l'équation binome

$$x^{\mathfrak{a}} - 1 = o \tag{29}$$

est toujours soluble, qu'elle admet des racines *primitives*, c'est-à-dire des racines x telles que chaque relation de la forme $x^c = 1$ entraîne la relation $c \equiv o(\mathfrak{a})$, et nous déterminerons le « nombre » de toutes les solutions de (29), c'est-à-dire l'ordre du groupe (multiplicatif) qu'elles constituent.

Remarquons d'abord que chaque nombre $\underset{r}{x}$ peut être écrit dans la forme

$$\underset{r}{x} = \underset{r}{\pi}^{k_r} \underset{r}{w}^{l_r} \left(\underset{r}{e} + \underset{r}{y}\,\underset{r}{\pi}\right), \tag{30}$$

où $\underset{r}{w}$ est une racine primitive de l'équation $x^{p^{n_r}-1} = \underset{r}{e}$, pour $r > o$, tandis que $\underset{0}{w} = -\underset{0}{e}$ et $\underset{0}{y} \equiv o(\underset{0}{\pi}) \equiv o(2)$. L'existence des $\underset{r}{w}$ a été démontrée par Hensel (1); de même l'existence du développement (30), où seulement il fait usage du nombre $e^{m_r} = \sum_{0}^{\infty} \frac{(m_r)^\nu}{\nu\,!}$, au lieu de $\underset{r}{e} + \underset{r}{y}\,\underset{r}{\pi}$.

Pour $r \not\equiv o$ on peut toujours écrire $\underset{r}{e} + \underset{r}{y}\,\underset{r}{\pi}$ dans la forme $\underset{r}{\varepsilon}^{\underset{r}{z}}$, où

$$\varepsilon = 1 + \pi, \qquad \text{donc} \qquad \underset{r}{\varepsilon} = \underset{r}{e} + \underset{r}{\pi}, \tag{31}$$

pour $r = o$ seulement si $\underset{r}{y} - \underset{r}{y}^0 \equiv o$ (4). Mais nous nous bornerons à

(1) K. HENSEL [1].

la forme (30), puisque l'introduction de la fonction exponentielle n'a pas un grand avantage (¹).

Or, l'équation (29) est équivalente au système d'équations

$$x_r^{\mathfrak{a}} - e_r = 0.$$

Puisque x doit être un diviseur d'Un, il sera un nombre subsistant, donc on aura $k_r = 0$. Donc les équations deviennent :

$$\left\{ \omega_r^{l_r} \left(e_r + y_r \pi_r \right) \right\}^{\mathfrak{a}} = e_r.$$

Donc on aura d'abord $l_r \mathfrak{a} \equiv 0 \ (p_r - 1)$ pour $r > 0$, et $l_0 \mathfrak{a} \equiv 0 (2)$. Posons donc

$$(32) \quad (h_r) = \left(\frac{p_r - 1}{(\mathfrak{a}, p_r - 1)} \right) = (p_r - 1) : \mathfrak{a} \quad (r > 0), \qquad (h_0) = \frac{2}{(\mathfrak{a}, 2)} = (2) : \mathfrak{a};$$

la première condition sera

$$(33) \qquad l_r \equiv 0 (h_r);$$

elle est nécessaire et suffisante afin que $x_r^{\mathfrak{a}}$ soit une puissance de $e_r + y_r \pi_r$ seulement. Or, une telle puissance est elle-même de la forme $e_r + u_r \pi_r$. D'autant plus

$$\left(e_r + y_r \pi_r \right)^{p_r'} - e_r \equiv 0 \left(\pi_r^{\nu+1} \right).$$

(¹) La démonstration de (30) est aisée. En effet, k_r étant la hauteur de x, on a

$$x_r = \pi_r^{k_r} \rho_r,$$

où ρ_r est subsistant. Alors, l'existence de ω_r ayant été démontrée et l_r ayant été déterminé par la condition $\rho_r \equiv \omega_r^{l_r} (\pi_r)$, on a $\rho_r \omega_r^{-l_r} = e_r + y_r \pi_r$.

Il reste à démontrer l'existence de ω (nous omettons l'index r). Il existe une racine primitive ω_0, satisfaisante à la congruence $\omega_0^{p-1} \equiv e_r (p)$.

Soit $\omega_0^{p-1} - e_r = u_r \pi_r$, et posons $\omega_n = \omega_0^{p^n}$.

Alors

$$\omega_n^{p-1} = (e_r + u_r \pi_r)^{p^n} \equiv e_r (\pi_r^{n+1}) \qquad \text{et} \qquad \omega_{n+1} = \omega_n^p \equiv \omega_n (\pi_r^{n+1}).$$

Donc $\omega = \lim \omega_\nu$ satisfait à l'équation $\omega^{p-1} = e_r$.

Donc

$$\left(\underset{r}{e}+\underset{r}{y}\underset{r}{\pi}\right)^{\underset{z}{r}}=\lim\left(\underset{r}{e}+\underset{r}{y}\underset{r}{\pi}\right)^{p^{\nu}_{r}}=\underset{r}{e}\quad(^{1}).$$

Donc les équations deviennent

$$\left(\underset{r}{e}+\underset{r}{y}\underset{r}{\pi}\right)^{\mathfrak{a}}=\left(\underset{r}{e}+\underset{r}{y}\underset{r}{\pi}\right)^{\underset{r}{\mathfrak{a}}}=\underset{r}{e}.$$

Pour $\underset{r}{\mathfrak{a}}=(0)$, $\therefore\ \mathfrak{a}\equiv 0(z)$ cette condition est remplie indépendamment de $\underset{r}{y}$ (quoique nous puissions évidemment supposer $\underset{r}{y}\equiv 0(\underset{r}{e})$ sans aucune restriction. Soit donc $\underset{r}{\mathfrak{a}}=(\underset{r}{\pi}^{\alpha_r})\not\equiv(0)$, donc α_r *fini*. Mais on démontre aisément par induction pour $\underset{r}{y}\not\equiv 0$ que

$$\left(\underset{r}{e}+\underset{r}{y}\underset{r}{\pi}\right)^{\underset{r}{\pi}^{\alpha_r}}-\underset{r}{e}\equiv 0\left(\underset{r}{y}\underset{r}{\pi}^{\alpha_r+1}\right)\not\equiv 0\left(\underset{r}{y}\underset{r}{\pi}^{\alpha_r+2}\right),$$

excepté pour $r=0$, c'est-à-dire $p_r=2$, où cette relation ne doit être remplie que pour $\underset{0}{y}\equiv 0(\underset{0}{\pi})$, condition que nous avons supposé être remplie. Or, l'expression à gauche devant être égale à zéro, donc divisible par $\underset{r}{z}$, on doit avoir $\underset{r}{y}=0$, $\underset{r}{y}$ devant contenir une puissance infinie de $\underset{r}{\pi}$. Nous pouvons réunir les deux cas sous la seule condition $\underset{r}{y}\underset{r}{\mathfrak{a}}=(0)$. Puisqu'elle doit être remplie pour chaque r, on aura

$$y\mathfrak{a}=(0). \tag{34}$$

Ou aussi $y\equiv 0\,[(0):\mathfrak{a}]$, c'est-à-dire y doit être divisible par l'ordre de l'idéal $\mathfrak{a}$ (considéré comme groupe additif). En résumant nos résultats nous obtenons le théorème :

L'équation (29) *a pour racines tous les nombres* x *de la forme*

$$x=(1+y\pi)\prod_{r}\underset{r}{w}^{l_r},$$

où $l_r\equiv 0(h_r)$, $(h_r)=(p_r-1):\mathfrak{a}$, $(r>0)$, $(h_0)=2:\mathfrak{a}$, $y_0\equiv 0(2)$ (²) *et* $y\equiv 0\,[(0):\mathfrak{a}]$, *et point d'autres.*

(¹) Cette relation est un cas spécial de l'identité $x^{a}=\underset{r}{x}^{\underset{r}{a}}\underset{r}{u}^{a}$, où $u=\underset{r}{x}^{\underset{r}{z}}$ est la solution de l'équation $\underset{r}{u}^{p_r}=\underset{r}{u}$, laquelle est $\equiv\underset{r}{x}\ (p_r)$; cette identité est valable pour $\underset{r}{x}\not\equiv 0\ (p_r)$.

(²) Puisque pour chaque $r>0$ $(2\underset{r}{l})=(\underset{r}{l})$, cette dernière condition peut être remplacée par $y\equiv 0\ (2)$.

On voit immédiatement que x sera une racine primitive de l'équation (29), lorsque la condition suivante est remplie pour chaque r : si α_r est fini, ou bien il existe au moins un s avec

$$l_s \not\equiv 0 \left(\frac{\left(p_s - 1, \overset{r}{z}\right)}{(p_s - 1, p_r^{\alpha_r - 1})} \right) \quad (1), \qquad \text{ou bien} \qquad \alpha_0 = 1 \qquad \text{et} \qquad l_0 \equiv 1 \,(2);$$

si α_r est infini, ou bien il existe une suite infinie de nombres s_ν, tels que

$$l_{s_\nu} \not\equiv 0 \left(\frac{\left(p_{s_\nu} - 1, \overset{r}{z}\right)}{(p_{s_\nu} - 1, p_r^{\nu})} \right),$$

ou bien $\underset{r}{\gamma} \not\equiv 0$ (2). Puisque pour chaque r et chaque ν il existe des s tels que $p_s - 1 \equiv 0 \,(p_r^{\nu})$, on voit que chaque équation de la forme (29) possède des racines primitives. En particulier,

$$x = \prod_r \overset{r}{\omega}^{h_r} \tag{35}$$

est toujours une racine primitive de (29).

14. Enfin calculons l'ordre du groupe de toutes les racines $\mathfrak{a}$-ièmes d'Un. Ce groupe est le produit direct (infini) du groupe des $(1 + \gamma\pi)$ et des groupes $\overset{r}{\omega}^{\lambda_r h_r}$. Nous pouvons ici dévoir de la condition $\gamma_0 \equiv 0 \,(2)$ en faisant $\overset{0}{\omega} = 1$, $h_0 = 0$. Le premier groupe est la classe congrue à 1 suivant l'idéal $(\omega\pi)$, où ω est le fondement de $(0) : \mathfrak{a}$. Son ordre multiplicatif est donc égal à l'ordre additif de cet idéal (3), donc

$$(0) : (\omega\pi) = (0) : (\omega) = (1 - \omega).$$

L'ordre du groupe $\overset{r}{\omega}^{\lambda_r h_r}$, $r \geqq 1$ est $(\mathfrak{a}, p_r - 1)$. Donc l'ordre du groupe

(1) Cette condition est équivalente avec $p_s \equiv 1 \,(p_r^{\alpha_r})$, $\frac{l_s}{h_s} \not\equiv 0 \,(p_r)$.

(2) Cette condition est *nécessaire* et suffisante.

(3) Tandis que l'ordre du groupe des nombres *relativement premiers* avec $\omega\pi$ est $\varphi(\omega\pi) = (0)$. *Cf.* page 302, 5°.

de tous les produits $\prod_s \overset{r}{\omega}^{\lambda_r h_r}$ est

$$\prod_r (\mathfrak{a},\ p_s - 1) = \prod_r \prod_s \left(\overset{r}{\pi}^{\alpha_r},\ p_s - 1\right) \qquad (s \geqq 1,\ r \geqq 0). \tag{36}$$

Or, soit r tel que $\mathfrak{a} \equiv 0\ (\overset{r}{\pi})$. Alors il existe une infinité de s, tels que $p_s - 1 \equiv 0\ (\overset{r}{\pi})$, donc $(\overset{r}{\pi}^{\alpha_r},\ p_s - 1) \equiv 0\ (\overset{r}{\pi})$. Donc on aura

$$\prod_s \left(\overset{r}{\pi}^{\alpha_r},\ p_s - 1\right) \equiv 0\left(\overset{r}{\pi}^{\infty}\right) = \overset{r}{\mathfrak{z}}.$$

Soit d'autre part $\mathfrak{a} \not\equiv 0\ (\overset{r}{\pi})$, donc $\alpha_r = 0$. Alors

$$\left(\overset{r}{\pi}^{\alpha_r},\ p_s - 1\right) = (1), \qquad \text{donc} \qquad \prod_s \left(\overset{r}{\pi}^{\alpha_r},\ p_s - 1\right) = (1).$$

Ainsi on trouve que le produit (36) est égal au produit de tous les $\mathfrak{z}$, tels que $\mathfrak{a} \equiv 0\ (\overset{r}{\pi})$, c'est-à-dire à la somme de tous les $\overset{r}{\mathfrak{e}}$, tels que $\mathfrak{a} \not\equiv 0\ (\overset{r}{\pi})$, c'est-à-dire au fondement de $\mathfrak{a}$, que nous pouvons désigner par $\mathfrak{a}^0 = \lim \mathfrak{a}^{\nu}$! Or, puisque ω et $\mathfrak{a}^0$ s'annulent,

$$\mathfrak{a}^0 (1 - \omega) = \mathfrak{a}^0.$$

Donc nous trouvons :

L'ordre du groupe de toutes les racines $\mathfrak{a}$*-ièmes d'Un est égal au fondement* $\mathfrak{a}^0$ *de* $\mathfrak{a}$. *En particulier il est égal à* $\mathfrak{a}$ *lorsque* $\mathfrak{a}$ *est subsistant* (= *idempotent*). *Dans tout autre cas il est un vrai multiple de* $\mathfrak{a}$

Notons enfin quelques cas spéciaux.

1° L'équation $x^2 = 1$ a pour racines

$$x = \pm \prod_1^{\infty} \overset{r-1}{\omega}^{\lambda_r (p_r - 1)} \qquad (\lambda_r = 0,\ 1);$$

l'ordre du groupe des solutions est donc $(2^{\infty}) = \overset{0}{\mathfrak{z}}$.

2° L'équation $x^{2e_r} = 1$ a pour racines

$$x = \left(1 + y^{\overset{r}{z}} \overset{r}{\pi}\right) \prod_{s>0} \overset{s}{\omega}^{\lambda_s h_s}, \qquad h_s = \left(\frac{\frac{1}{2}(p_s - 1)}{\left(\frac{1}{2}(p_s - 1),\ p_r^{\infty}\right)} \right);$$

l'ordre du groupe est donc $2^{r}(1-\frac{r}{z})$, c'est-à-dire (o) ou $\mathfrak{e}_r$, selon que p_r est égal à 2 ou non.

3° L'équation $x^{\mathfrak{a}}=1$ est équivalente à l'équation $x^{\eta}=1$, lorsque $\mathfrak{a}$ est subsistant, $\eta=\mathfrak{a}^0$ étant son fondement. L'ordre est donc $\mathfrak{a}$. En particulier, a étant un diviseur d'Un, $x^{a}=1$ est équivalente à $x=1$; l'ordre du groupe est donc 1; $x^0=1$ est valable pour chaque diviseur d'Un; l'ordre est donc (o).

Wassenaar (Pay-Bas), janvier 1934 (mai 1936).

Bibliographie.

BROUWER (L. E. J.). — [1] Over de grondslagen der Wiskunde (Amsterdam-Leipzig, Maas et van Suchtelen, 1907).

— [2] Die Theorie der endlichen kontinuierlichen Gruppen, unabhängig von den Axiomen von Lie (*Math. Ann.*, 67, 1909, p. 246-267; 69, 1910, p. 181-203).

— [3] On the structure of perfect sets of points (*Proc. Kon. Akad.*, 12, Amsterdam, 1910, p. 785-794).

CARTAN (E). — La théorie des groupes finis et continus et l'*Analysis situs* (*Mém. des Sc. Math.*, 42, 1930).

DANTZIG (D. VAN). — [1] Ueber topologisch homogene Kontinua (*Fund. Math.*, 14, 1930, p. 102-125).

— [2] Studiën over topologische algebra (Amsterdam, H. J., Paris, 1931).

— [3] Einige Sätze über topologische Gruppen (*Jahresber. der D. M. V.*, 41, 1932, p. 42-44).

— [4, 5, 6] *T. A.*, I, II, III. *Zur topologischen Algebra* : I. Komplettierungstheorie (*Math. Ann.*, 107, 1932, p. 587-626). — II. Abstrakte $\mathfrak{b}_\nu$-adische Ringe (*Compositio Math.*, 2, 1935, p. 201-223). — III. Brouwersche und Cantorsche Gruppen (*Comp. Math.*, 3, 1936, p. 408-426).

— [7] *Neuere Ergebnisse der topologischen Algebra* (Rapport délivré à la Réunion Topologique internationale de Moscou, 1935).

HENSEL (K.). — [1] *Theorie der algebraischen Zahlen*, I (Leipzig, Teubner, 1908).

— [2] *Zahlentheorie* (Leipzig, Göschen, 1913).

NEUMANN (J. VON). — [1] Zur Prüferschen Theorie der idealen Zahlen (Szégéd, *Acta litt. sc.*, 2, 1927, p. 193-227).

PRÜFER (H). — [1] Theorie der Abelschen Gruppen (I, *Math. Zeits.*, 20, 1924, p. 165-187; II, *ibid.*, 22, 1925, p. 222-249).

— [2] Neue Begründung der algebraischen Zahlentheorie (*Math. Ann.*, 94, 1925, p. 198-243).

WEYL (H.). — [1] Topologie und Algebra als zwei Wege mathematischen Verständnisses (*Unterrichtsblätter f. Math. u. Naturw.*, 38, 1932, p. 177-188).