Algebra a theorie čísel

Časopis pro pěstování matematiky a fysiky, Vol. 74 (1949), No. 3, 156--177

Persistent URL: http://dml.cz/dmlcz/109431

2. sekce:

Algebra a theorie čísel.

PŘÍSPĚVEK K THEORII SIMULTANNÍCH DIOFANTICKÝCH APROXIMACÍ.

KAREL ČERNÝ, Praha.

Sdělení se týkalo práce, která byla uveřejněna ve Spisech vydávaných přírodovědeckou fakultou university Karlovy, **188** (1948).

*

Résumé. — Výtah.

Contribution à la théorie des approximations diophantiques simultanées.

KAREL ČERNÝ, Praha.

L'objet de la communication a été publié dans Spisy vydávané přírodovědeckou fakultou university Karlovy (Acta facultatis rerum naturalium universitatis Carolinae), **188** (1948).

LES AUTOMORPHISMES DES GROUPES CLASSIQUES.

JEAN DIEUDONNÉ, Nancy.

L'objet de la communication sera publié en détail dans les Memoirs of the American Mathematical Society en 1950 sous le titre „On the automorphismes of the classical groups".

*

Výtah. — Résumé.

Automorfismy klasických grup.

JEAN DIEUDONNÉ, Nancy.

Sdělení se týkalo autorovy práce, která bude uveřejněna v Memoirs of the American Mathematical Society, 1950 pod názvem „On the automorphismes of the classical groups".

SUR LA FACTORISATION DES GROUPES ABÉLIENS.

G. HAJÓS, Budapest.

Soient A et B deux sous-ensembles du groupe abélien G. Nous multiplions chaque couple d'éléments a et b de ces deux sous-ensembles, et considérons le cas où tous ces produits sont différents. Si C est le sous-ensemble de G formé par tous ces produits différents ab, nous écrivons

$$A \,.\, B = C. \tag{1}$$

Le problème de factorisation du groupe G consiste en ceci: il s'agit de trouver les facteurs A et B pour lesquels on a

$$A \,.\, B = G.$$

On pourrait formuler ce problème pour tous les groupes. Si nous ne parlons que des groupes abéliens c'est parce que le problème est déjà assez compliqué pour ceux-ci, même dans le cas des groupes abéliens finis les plus simples.

1. C'était *l'hypothèse de Minkowski* sur les formes homogènes linéaires qui conduisait au problème de factorisation. La formulation originale de cette conjecture est en termes de la théorie des nombres. Nous considérons un système de formes linéaires homogènes à n variables $L_i = a_{i1}x_1 + \ldots + a_{in}x_n \quad (i = 1, \ldots, n)$ unimodulaire, c'est à dire à déterminant $|a_{ik}| = 1$. La conjecture de Minkowski dit que si le système d'inégalités $|L_1| < 1, \ldots, |L_n| < 1$ n'a pas une solution non-triviale à valeurs $x_1, \ldots, x_n$ entières, il faut qeu tous les coefficients de l'une des formes L_i soient des nombres entiers.

Minkowski a donné une formulation géométrique à sa conjecture. Nous disons qu'un système de corps remplit l'espace simplement si tous les points de l'espace appartiennent au moins à un de ces corps et ceux-ci n'ont pas de points intérieurs communs. Nous disons qu'un système de points isolés forme un réseau si toute translation changeant un point du système en un autre point du système change tous les points du système en des points du même système. La conjecture de Minkowski dit en termes géométriques qu'en remplissant l'espace euclidien a n-dimensions

simplement par des cubes congruents dont les milieux forment un réseau, il est nécéssaire que chaque cube ait une face entière à $(n - 1)$ dimensions en commun avec un de ses voisins.

J'ai réussi a vérifier cette conjecture[1]) en donnant à elle une formulation en termes de la théorie des groupes.[2]) J'appelle un sous-ensemble $(1, a, a^2, \ldots, a^{k-1})$ du groupe une série. Je dis qu'un sous-ensemble A du groupe est périodique s'il existe un élément a du groupe pour lequel on a $aA = A$. Une série n'est alors périodique que si elle est un sous-groupe cyclique. La conjecture de Minkowski équivaut à la proposition suivante: Si pour le groupe abélien fini G et pour les séries $S_1, \ldots, S_n$, nous avons

$$S_1 . S_2 . \ldots . S_n = G,$$

il est nécessaire qu'au moins une des séries soit périodique.

Je ne veux donner ici que l'essentiel de la démonstration de l'équivalence de cette formulation. On démontre tout d'abord qu'il suffit de considérer les systèmes de cubes remplissant simplement l'espace dont les milieux ont des coordonnées rationnelles dans un système de coordonnées parallèle aux arêtes des cubes. Les plans à $(n - 1)$-dimensions contenant les faces des cubes découpent les cubes en parallélotopes congruents. Les translations changeant l'un de ces parallélotopes en un autre forment un groupe abélien P. Les translations changeant l'un des cubes en un autre forment un groupe C qui est un sous-groupe de P. Le groupe quotient $G = P/C$ est le groupe dont nous parlerons. Les translations minimales parallèles aux arêtes des cubes correspondent aux éléments $a_1, \ldots, a_n$ de G. Les translations dans la directions des arêtes et ayant leurs longueurs correspondent aux éléments $a_1^{k_1}, \ldots, a_n^{k_n}$. Nous considérons les séries

$$S_i = (1, a_i, a_i^2, \ldots, a_i^{k_i - 1}). \tag{2}$$

On forme un cube d'un parallélotope situé dans un coin du cube en le transformant par toutes les translations du produit $S_1 . S_2 . \ldots . S_n$. Le système des cubes remplit simplement l'espace, si ce produit est le groupe G entier. Les cubes ont des faces entières en commun si la série S_i correspondante est périodique. On en conclut l'équivalence de la formulation donnée.

2. O. H. KELLER a exprimé l'opinion[3]) que l'hypothèse de Minkowski reste vraie pour tous les remplissages de l'espace par des cubes con-

---

[1]) G. HAJÓS: Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter. Mathematische Zeitschrift **47** (1941), 427—467.

[2]) O. H. KELLER a affirmé dans son rapport sur mon travail dans le Zentralblatt für Mathematik, **25**, 254 que Ph. FURTWÄNGLER a connu cette formulation. Furtwängler n'a publié rien dans cette direction. Je n'ai pas réussi à trouver quelqu'un qui aurait pu donner des moindres indications précises sur cette assertion.

[3]) O. H. KELLER: Über lückenlose Erfüllung des Raumes mit Würfeln. Journal für r. u. a. Mathematik, **163** (1930), 231—248.

gruents, c'est à dire sans imposer aucune condition aux milieux des cubes. On démontre aisément en utilisant les résultats de O. PERRON[4]) sur ce sujet et par la méthode esquissée que cette conjecture, dont la vérité n'est prouvé que pour les dimensions ne dépassant pas 6[4]), équivaut à la proposition suivante: Si pour un groupe abélien fini G, son sous-ensemble H et des séries $S_1, \ldots, S_n$, on a

$$H \,.\, S_1 \,.\, S_2 \,.\,.\,.\,.\, S_n = G,$$

il faut que H contienne, pour une des séries S_i écrite dans la forme (2), deux éléments de G dont le quotient est $a_i^{k_i}$.

Ph. FURTWÄNGLER a exprimé l'opinion[5]) que l'hypothèse de Minkowski reste vraie pour les remplissages multiples, c'est à dire pour le cas, où tous les points qui ne sont pas situés sur la surface d'un cube sont couverts par k cubes. Sa proposition est équivalente à la suivante: Si pour un groupe abélien fini G, des séries $S_1, \ldots, S_n$ et un nombre entier k, on a

$$S_1 \,.\, S_2 \,.\,.\,.\,.\, S_n = kG$$

dans le sens que les produits des éléments des séries donnent tous les éléments de G et chacun k fois, il faut qu'au moins une des séries soit périodique. J'ai démontré[1]) que cette conjecture n'est vraie que pour $n \leqq 3$.

3. D'après ce que nous venons d'esquisser, le problème de factorisation des groupes conduit à la question suivante:[6])

Faut-il qu'un de deux facteurs A, B dont le produit est le groupe G, soit périodique? (Q)

Une question simple par apparence, mais bien compliquée en réalité. Je n'ai réussi qu'à donner une réponse affirmative pour le cas des groupes cycliques dont l'ordre est une puissance d'un nombre premier, quoique je n'ai trouvé aucun exemple donnant une réponse négative pour un groupe cyclique fini.*)

Pour le cas mentionné soit p un nombre premier et $a^{p^n} = 1$ la relation

---

[4]) O. PERRON: Über lückenlose Ausfüllung des n-dimensionalen Raumes durch kongruente Würfel, Mathematische Zeitschrift, **46** (1940), 1—26, 161—180.

[5]) Ph. FURTWÄNGLER: Über Gitter konstanter Dichte, Monatshefte für Mathematik u. Physik, **43** (1936), 281—288.

[6]) L'exemple $A = (1, b, b^2)$, $B = (1, ab, b^3, ab^4)$ pour le groupe défini par $a^2 = 1$, $b^6 = 1$, montre qu'il n'est pas nécessaire que l'un des facteurs soit uns ousgroupe.

*) *Remarque pendant la correction des épreuves.* Depuis ma conférence au congrès à Prague 1949 j'ai réussi à démontrer que la réponse est négative même pour les groupes cycliques dont l'ordre est un produit de trois nombres premiers entre eux si deux de ces trois nombres ne sont pas premiers eux-mêmes. L. RÉDEI a démontré que la réponse est affirmative pour les groupes cycliques dont l'ordre est un produit de trois nombres premiers. Tous les deux résultats cités apparaîtront bientôt dans *l'Acta Mathematica* de l'Académie Scientifique Hongroise. *(18 septembre 1950.)*

définissante du groupe G. Nous faison correspondre aux sous-ensembles

$$A = (a^{\alpha_1}, a^{\alpha_2}, \ldots, a^{\alpha_m}), \quad B = (a^{\beta_1}, a^{\beta_2}, \ldots, a^{\beta_n})$$

les polynômes

$$A(x) = \sum_{i=1}^{m} x^{\alpha_i}, \qquad B(x) = \sum_{i=1}^{n} x^{\beta_i}.$$

La relation $A \,.\, B = G$ donne

$$A(x)B(x) \equiv 0 \pmod{x^{p^n} - 1}.$$

En y substituant une racine de l'équation cyclotomique

$$1 + x^{p^{n-1}} + x^{2p^{n-1}} + \ldots + x^{(p-1)p^{n-1}} = 0,$$

un au moins des facteurs $A(x)$ et $B(x)$ s'annulle, ce facteur est alors divisible par ce polynôme cyclotomique irréducible. Cela revient à dire que A resp. B est périodique parce que, multiplié par $a^{p^{n-1}}$, il reste invariable.

Cette démonstration n'est pas applicable aux groupes d'autre type. La question est ouverte même pour les groupes cycliques. (Voir la note*) au bas de la page précedente. L. RÉDEI a prouvé[7]) que la réponse est affirmative pour les groupes non-cycliques d'ordre p^2.

4. Pour les groupes infinis, ils existent des exemples donnant une réponse négative à notre question (Q). T. SZELE a donné l'exemple suivant pour le groupe cyclique d'ordre infini:

$$A(x) = (1 + x)(1 + x^4)(1 + x^{16}) \ldots$$
$$B(x) = (1 + x^{-2})(1 + x^{-8})(1 + x^{-32}) \ldots$$

N. G. DE BRUIJN a écrit dans une lettre qu'il a démontré pour le groupe cyclique d'ordre infini que si $A \,.\, B = G$ et A est fini, B doit être cyclique. Sans connaître sa démonstration, je démontre sa proposition en parlant du groupe additif des nombres entiers. On peut supposer que le plus petit des éléments de A est 0. Nous désignons par a le plus grand élément de A. Soit B_k le sous-ensemble de B contenant les éléments de B ne dépassant pas k. Le plus petit nombre entier ne figurant pas dans le produit $A \,.\, B_k$ est nécessairement un élément de B, le plus petit de ses éléments non-contenus dans B_k. De cette manière on reconstruit, pas à pas, de AB_k le sous-ensemble B entier. S'ils existent alors deux ensembles AB_k et AB_l ne différant que par une constante additive, notre proposition sera démontrée. Mais AB_k contient tous les nombres entiers $\leqq k$ et ne contient aucun nombre $> k + a$. Il n'y a dès lors qu'un nombre fini de possibilités qui distinguent les types des ensembles AB_k pour les dif-

[7]) L. RÉDEI: Zwei Lückensätze über Polynome in endlichen Primkörpern mit Anwendung auf die endlichen Abelschen Gruppen und die Gaussischen Summen, Acta Mathematica, **79** (1947), 273—290.

férents valeurs de k. On a, par conséquant, deux entre eux du même type, c'est à dire ne différant que par une constante additive.

En général, on ne peut pas appliquer cette démonstration aux groupes abéliens sans torsion (n'ayant aucun élément d'ordre fini). Même la proposition analogue n'y est pas valable, ce que nous montrons par l'exemple suivant: a, b, c sont les éléments générateurs,

$$A = (1, a, b, c, ab, ac, bc, abc),$$

$$B = \begin{cases} a^{2k+1}b^2, b^{2k+1}c^2, a^2c^{2k+1} & (k \text{ entier}) \\ a^{2\alpha}b^{2\beta}c^{2\gamma} & (\alpha, \beta, \gamma \text{ entier}, \alpha \neq 1 \text{ si } \beta = 0, \\ & \beta \neq 1 \text{ si } \gamma = 0, \ \gamma \neq 1 \text{ si } \alpha = 0). \end{cases}$$

Pour les groupes abéliens infinis de torsion (n'ayant aucun élément d'ordre infini) aucun exemple n'est connu qui donnerait une réponse à notre question (Q). T. SZELE a fait la conjecture[8]) pour ces groupes que $G = S_1 . S_2 \ldots .$ entraîne la périodicité de l'une des séries; c'est une généralisation de la conjecture de Minkowski.

5. Nous donnons une construction des types différents de factorisation d'un groupe abélien fini. Nous désignons par $A \circ B$ un sous-ensemble obtenu en multipliant chaque élément de A par un élément quelconque de B (différent ou non pour les différents éléments de A). $A \circ B$ n'est pas alors une notation univoque.

Soit G un groupe abélien fini, $H_1, \ldots, H_n$ des sous-groupes pour lesquels on a

$$H_1 . H_2 . \ldots . H_n = G.$$

Nous obtenons des factorisations $A . B = G$ par les formules

$$\begin{aligned} A &= 1 . H_1 \circ H_2 . \circ \ldots \\ B &= 1 . H_1 . H_2 \circ . \ldots \end{aligned} \tag{3}$$

où nous avons supprimé les paranthèses de manière que $1 . H_1 \circ H_2 . H_3$ par exemple signifie $[(1 . H_1) \circ H_2] . H_3$. La vérification est facile en utilisant la relation

$$[(K \circ M) . (L . M)] . N = K . L . M . N$$

où N et $M . N$ sont des sous-groupes.

Nos formules (3) ne donnent que des factorisations ayant un facteur périodique. Elles donnent toutes les factorisations d'un groupe fini pour lequel la réponse à la question (Q) est affirmative.

6. Tout ce que nous avons dit aurait pu être formulé en termes de l'algèbre du groupe en écrivant des sommes d'éléments au lieu des sous-ensembles. Nous disons de même qu'un élément A de l'algèbre du groupe est périodique s'il existe un élément a du groupe pour lequel

[8]) T. SZELE: Neuer vereinfachter Beweis des gruppentheoretischen Satzes von Hajós, Publicationes Mathematicae, Debrecen, I (1949), 56—62.

on a $aA = A$. Si nous considérons l'égalité $A \,.\, B = G$ dans l'algèbre du groupe et si nous la multiplions par $(a - 1)$, en employant un élément a quelconque de G, nous recevons une égalité du type

$$CD = 0. \tag{4}$$

Cela montre que le problème de factorisation d'un groupe est étroitement lié au problème suivant: trouver les diviseurs de zéro de l'algèbre du groupe. Les factorisations du groupe ayant un facteur périodique fournissent par multiplication des solutions de (4) ayant un facteur périodique.

On peut demander si toutes les solutions de (4) ont un facteur périodique. La réponse à cette question pour les groupes cycliques n'est affirmative que s'ils sont d'ordre p^n. Pour ceux-ci la réponse peut être trouvée par la méthode qui nous a donné la réponse à la question (Q) pour les mêmes groupes. Pour le groupe défini par $a^6 = 1$ nous avons le contre-exemple

$$(a^3 - 2a^2 + 2a - 1)(a^3 + 2a^2 + 2a + 1) = 0.$$

On obtient cet exemple en factorisant le polynôme $a^6 - 1$, une méthode qui fournit un contre-exemple pour tous les groupes cycliques dont l'ordre a deux facteurs premiers différents. Pour le groupe cyclique infini l'exemple de T. SZELE donne par multiplication un exemple désiré.

*

Výtah. — Résumé.

O faktorisaci Abelových grup.

G. HAJÓS, Budapest.

Sdělení pojednává o známé domněnce Minkowského o lineárních formách: Mějme soustavu n lineárních forem o n proměnných $L_i = a_{i1}x_1 + \ldots + a_{in}x_n$ $(i = 1, \ldots, n)$ a o determinantu $|a_{ik}| = 1$. Nemá-li soustava nerovností $|L_1| < 1, \ldots, |L_n| < 1$ netriviální řešení celými čísly $x_1, \ldots, x_n$, pak aspoň u jedné formy L_i jsou všechny koeficienty čísla celá. Tuto domněnku dokázal autor prostředky theorie grup. Nato pojednává autor o některých řešených i neřešených problémech, týkajících se faktorisace Abelových grup, které se přirozeně vynořily v souvislosti s jeho důkazem Minkowského domněnky.

NOVÉ VÝSLEDKY O VĚTĚ JORDAN-HÖLDEROVĚ VE SVAZECH.

VLADIMÍR KOŘÍNEK, Praha.

Sdělení se týkalo práce, která vyjde v Rozpravách České akademie věd a umění, třída II, **59** (1949), čís. 23.

Résumé. — Výtah.

Résultats nouveaux concernant le théorème de Jordan-Hölder dans les treillis.

VLADIMÍR KOŘÍNEK, Praha.

L'objet de la communication était un travail qui sera publié dans le Bulletin international de l'Académie tchèque des sciences, Classe des sciences mathématiques, naturelle et de la médecine, **59** (1949), Nr. 23.

TOPOLOGICKÉ SVAZY.

KAREL KOUTSKÝ, Brno.

Sdělení vyšlo v Comptes rendus, tome **225**, 659—661 pod názvem Sur les lattices topologiques.

*

Résumé. — Výtah.

Les lattices topologiques.

KAREL KOUTSKÝ, Brno.

L'objet de la communication a été publié aux Comptes rendus, tome **225**, 659—661.

ROZKLADY DETERMINANTU JAKO POLYNOMU NAD KOMUTATIVNÍM OKRUHEM.

JAN MAŘÍK, Praha.

Sdělení se týkalo práce: La réductibilité du déterminant ayant des indéterminées pour éléments, si l'on le considère comme un polynôme sur un anneau commutatif, Spisy vydávané přírodovědeckou fakultou university Karlovy, **191** (1949).

*

Résumé. — Výtah.

La réductibilité du déterminant comme un polynôme sur un anneau commutatif.

JAN MAŘÍK, Praha.

L'objet de la communication a été publié dans la collection: Spisy vydávané přírodovědeckou fakultou university Karlovy (Acta facultatis rerum naturalium universitatis Carolinae), **191** (1949).

NUTNÁ A POSTAČUJÍCÍ PODMÍNKA, ABY V JISTÝCH OKRUZÍCH CELÝCH ČÍSEL NEREÁLNÝCH KVADRATICKÝCH TĚLES PLATIL JEDNOZNAČNÝ ROZKLAD V PRVOČINITELE.

JAN MAŘÍK, Praha.

Věta 1. Buď O komutativní okruh s jednotkovým prvkem 1. Nechť jsou splněny tyto předpoklady:

1. V O je definována ekvivalence $\sim$; třídy této ekvivalence jsou dobře uspořádány. $b < c$ značí, že třída prvku b je před třídou prvku c.

2. $a \neq 0$, $b < c \Leftrightarrow ab < ac$.

3. $b \sim 1 \Rightarrow$ existuje b', že $bb' = 1$.

4. Existuje pevný prvek $A \in O$, že ke každé dvojici a, b, pro niž platí $a \gtrsim Ab$, $b \neq 0$, existuje d, že $a > a - bd$.

5. Existuje pevný prvek $B \in O$, že ke každé dvojici a, b, kde $a \gtrsim b \neq 0$, existují c, d, že platí $0 \neq c \lesssim B$, $a > ac - bd$.

6. Je-li $a < A^2B^2$, má a nejvýš jeden rozklad v prvočinitele.

Za těchto předpokladů je O obor integrity s jednoznačným rozkladem v prvočinitele.

Důkaz věty 1 lze provést methodou, kterou Zermelo dokázal jednoznačnost rozkladu přirozených čísel v součin prvočísel.

Věta 2. Buď C okruh celých čísel. Buď s nereálný kořen rovnice $0 = x^2 + mx + n$, kde m, n jsou celá čísla. Pak existuje komplexní číslo t a čísla e, p, $e = 0$ nebo $e = -1$, p přirozené číslo, že platí

$$C[s] = C[t], \quad t^2 + te + p = 0.$$

Je-li $e = 0$, platí v $C[s]$ jednoznačný rozklad v prvočinitele, když a jen když $p = 1$ nebo $p = 2$.

Je-li $e = -1$, platí v $C[s]$ jednoznačný rozklad, když a jen když čísla $p + k(k+1)$ jsou prvočísla nebo 1 pro všechna celá nezáporná k, pro něž $k(k+1) \leqq \frac{p-1}{3}$. (Na př. pro $p = 1, 2, 3, 5, 11, 17, 41$.)

Důkaz: Abychom splnili předpoklady věty 1, klademe $a \sim b \Leftrightarrow |a| = |b|$, $a < b \Leftrightarrow |a| < |b|$. Dosti snadno najdeme A; abychom našli B, použijeme pomocné věty, podle níž ke každé dvojici komplexních čísel u, v, kde v není reálné, $|v| < \sqrt{3}$, existují celá čísla j, k tak, že platí $|u + j - kv| < 1$. Množina všech $x \in C[s]$, pro něž $|x| < |A^2B^2|$, má již jen konečný počet prvků; podrobné vyšetření je však dost složité.

Věta 3. Buď q přirozené číslo; buď $k^2 + k + q$ prvočíslo pro všechna celá nezáporná k, pro něž $k(k+1) \leqq \frac{q-1}{3}$. Buďte a, b celá nesoudělná čísla. Buď $c = a^2 + ab + b^2q < q^2$. Pak je c prvočíslo. Obecněji: Je-li $c < q^r$, je c součinem nejvýš $r - 1$ (stejných nebo různých) prvočísel.

Důkaz: Plyne snadno z věty 2.

La condition nécessaire et suffisante, pour que le théorème de la décomposition univoque en produit des facteurs premiers soit vrai dans certains anneaux des nombres entiers des corps quadratiques.

JAN MAŘÍK, Praha.

Théorème 1. Soit O un anneau commutatif avec l'élément un. Si les conditions 1.—6. sont satisfaites, O est un champ d'integrité avec la décomposition univoque en facteurs premiers.

Théorème 2 contient la condition nécessaire et suffisante, pour que le théorème de la décomposition univoque en facteurs premiers soit vrai dans l'anneau $C[s]$, où C est l'anneau des nombres entiers rationnels, s un nombre imaginaire, $s^2 + ms + n = 0$, m, n entiers rationnels.

Théorème 3. Soit q un nombre naturel; soit $k^2 + k + q$ un nombre premier pour tout entier non négatif k, satisfaisant la condition $k(k+1) \leqq \leqq \frac{q-1}{3}$. Soient a, b premiers entre eux. Soit $c = a^2 + ab + b^2q < q^r$. Si c est le produit de r' nombres premiers (égaux ou différents), on a $r' < r$.

O SYSTÉMECH S DVOJÍM NÁSOBENÍM S JEDNÍM DISTRIBUTIVNÍM ZÁKONEM.

MIROSLAV NOVOTNÝ, Brno.

Systém s dvojím násobením s levým distributivním zákonem (zkr. l-systém), je množina $\mathfrak{M}$, k jejíž každé uspořádané dvojici prvků a, b patří součet $a + b \in \mathfrak{M}$ a součin $a \,.\, b \in \mathfrak{M}$. Tyto dvě operace jsou k sobě vázány levým distributivním zákonem: $a \,.\, (b + c) = a \,.\, b + a \,.\, c$. Prvky systému tvoří vzhledem k sčítání grupoid sčítání, vzhledem k násobení grupoid násobení.

Základní problém zní: K danému grupoidu sčítání $\mathfrak{G}$ nalézti všechny l-systémy. Tyto l-systémy se naleznou takto: Buď f libovolné zobrazení grupoidu $\mathfrak{G}$ do množiny všech jeho endomorfismů. (Endomorfismem rozumíme deformaci grupoidu do sebe.) Označme $f(a) = A$, $f(b) = B$ atd. a definujme $a \,.\, x = A(x)$, $b \,.\, x = B(x)$ atd. Při tom symbolem $A(x)$ rozumíme obraz prvku x v endomorfismu A. Je-li grupoid sčítání konečný řádu n a jeho endomorfismů je m, existuje nad ním m^n l-systémů.

Hledejme nyní ke grupoidu sčítání $\mathfrak{G}$ takový l-systém, jehož násobení je vázáno k sčítání také pravým distributivním zákonem. Zde zní podmínka nutná a postačující k existenci takto: Na grupoidu $\mathfrak{G}$ existují dva systémy endomorfismů σ_1 a σ_2 takové, že l. $\mathfrak{G}$ se dá zobrazit

na σ_1 i σ_2; $f_1(\mathfrak{G}) = \sigma_1$, $f_2(\mathfrak{G}) = \sigma_2$. 2. Označíme-li $f_1(a) = A_1$, $f_2(a) = A_2$, $f_1(b) = B_1$, $f_2(b) = B_2$ atd., platí pro libovolný pár prvků a, b $A_1(b) = B_2(a)$. — Definujeme-li pak $a \,.\, b$ jako $A_1(b) = B_2(a)$, je tato definice jednoznačná a násobení je distributivní zprava i zleva. Pro abelovské násobení oba systémy i obě zobrazení splynou.

Žádáme-li, aby násobení nad daným grupoidem sčítání $\mathfrak{G}$ bylo asociativní, ukazuje se, že je zde úzká souvislost s grupoidem endomorfismů. Všechny endomorfismy grupoidu tvoří totiž pologrupu s jednotkou. Asociativní 1-systém pak existuje nad $\mathfrak{G}$ tehdy a jen tehdy, existuje-li zobrazení f grupoidu $\mathfrak{G}$ na nějaký podgrupoid σ v grupoidu endomorfismů, jež má tuto vlastnost: označíme-li $f(a) = A$, $f(b) = B$ atd. a definujeme-li $a \,.\, b = A(b)$, jest f deformace takto vzniklého grupoidu násobení na podgrupoid σ.

Má-li konečně nad daným grupoidem sčítání $\mathfrak{G}$ existovat 1-systém, jehož násobení má dělení, pak k tomu je nutno a stačí, existuje-li na $\mathfrak{G}$ systém endomorfismů σ s těmito vlastnostmi: 1. $\mathfrak{G}$ se dá zobrazit na σ, 2. každý endomorfismus $X \in \sigma$ deformuje $\mathfrak{G}$ na sebe, 3. ke každému páru prvků a, $b \in \mathfrak{G}$ existuje endomorfismus $X \in \sigma$ tak, že $X(a) = b$. Ukazuje se, že dělení konečného 1-systému je vždy jednoznačné.

Buď $\mathfrak{M}$ 1-systém, f deformace jeho grupoidu sčítání $\mathfrak{G}$ na jiný grupoid $\mathfrak{G}^*$. Jaké jsou podmínky nutné a dostatečné k tomu, aby se na $\mathfrak{G}^*$ dalo definovat násobení tvořící grupoid $\mathfrak{H}^*$ tak, že f je současně deformace grupoidu $\mathfrak{H}$ na $\mathfrak{H}^*$? Označíme-li $\overline{\mathfrak{G}}$ rozklad patřící k zobrazení $x \to f(x)$, ${}_a\overline{\mathfrak{G}}$ rozklad patřící k zobrazení $x \to f(a \,.\, x)$ a $\overline{\mathfrak{G}}_a$ rozklad patřící k zobrazení $x \to f(x \,.\, a)$ pro všechny prvky $a \in \mathfrak{G}$, pak podmínka jest tato: $\overline{\mathfrak{G}}$ jest zjemnění největšího společného zjemnění všech ${}_a\overline{\mathfrak{G}}$ i $\overline{\mathfrak{G}}_a$. V této úvaze jsme předpokládali, že $\mathfrak{G}^*$ a $\mathfrak{H}^*$ tvoří obecně jen systém s dvojím násobením $\mathfrak{M}^*$. Avšak deformace f přenáší jisté vlastnosti z $\mathfrak{M}$ i na $\mathfrak{M}^*$; totiž distributivnost, asociativnost i existenci dělení.

Práce se stejným názvem vyjde ve spisech přírodovědecké fakulty Masarykovy university v Brně.

*

Résumé. — Výtah.

Les systèmes à deux compositions avec une loi distributive.

MIROSLAV NOVOTNÝ, Brno.

Soit $\mathfrak{M}$ un ensemble, dans lequel une somme $a + b \in \mathfrak{M}$ et un produit $a \,.\, b \in \mathfrak{M}$ sont définis pour chaque couple ordonné d'éléments $a, b \in \mathfrak{M}$. Supposons que l'addition et la multiplication sont liées par la loi distributive gauche: $a \,.\, (b + c) = a \,.\, b + a \,.\, c$. J' appelle cet ensemble avec les deux opérations *système à deux compositions avec la loi distributive gauche* (abréviation: 1-système). Les éléments de l'ensemble $\mathfrak{M}$ forment le groupoïde additif par rapport à l'addition et le groupoïde multiplicatif par rapport à la multiplication.

Le problème principal est le suivant: trouver tous les l-systèmes appartenant au groupoïde additif donné $\mathfrak{G}$. — Soit f une application du groupoïde $\mathfrak{G}$ dans le système d'endomorphismes de ce groupoïde. (L'endomorphisme du groupoïde est la déformation du groupoïde dans lui-même.) Désignons $f(a) = A$, $f(b) = B$ etc. et définissons $a \,.\, x = A(x)$, $b \,.\, x = B(x)$ etc., où $A(x)$ est l'image de l'élément x dans l'endomorphisme A. La multiplication définie est distributive à gauche et chaque l-système peut être construit par ce procédé.

Par un procédé analogue, on peut donner les conditions nécessaires et suffisantes pour la construction d'un l-système, dans lequel même la loi distributive droite est valable, d'un l-système abélien, d'un l-système associatif, d'un l-système, dont la multiplication possède une division. Enfin, la solution de quelques problèmes concernant l'homomorphisme des l-systèmes est donnée.

Un travail intitulé Les systèmes à deux compositions avec une loi distributive apparaîtra dans les Publications de la Faculté des Sciences de l'Université Masaryk à Brno.

O VNOŘITELNOSTI SEMIGRUP.

VLASTIMIL PTÁK, Praha.

Sdělení se týkalo práce uveřejněné ve Spisech vydávaných přírodovědeckou fakultou university Karlovy, **192** (1949).

*

Summary. — Výtah.

Immersibility of Semigroups.

VLASTIMIL PTÁK, Praha.

The essential parts of the communication are contained in the author's paper published (in English) in Spisy vydávané přírodovědeckou fakultou university Karlovy (Acta facultatis rerum naturalium universitatis Carolinae), **192** (1949).

ОБ ОДНОЙ ОБЩЕЙ ТЕОРЕМЕ ТЕОРИИ ВЕРОЯТНОСТЕЙ И О ЕЕ ПРИМЕНЕНИИ В ТЕОРИИ ЧИСЕЛ.

АЛФРЕД РЕНЬИ, Будапешт.

Уже давно известно существование некоторой связи между понятиями теории вероятностей и теории чисел. Однако до сих пор в большинстве случаев речь шла только о том, что были установлены некоторые аналогии между обеими теориями.

Например известно; что распределения целых чисел в классах вычетов по взаимно простым модчлям являются в некотором смысле независимыми. Это замечание был источником многих попыток доказательства и нестрогих выводов, но число результатов, строго доказанных таким путем невелико. Мы должны в этом отношении упомянуть только исследования P. Erdös и M. Kac[1]) о распределении значений мултипликативных функций. Однако некоторые авторы применяли понятия теории вероятностей без критики, и это часто приводило к противоречиям.

В настоящее время, после того как акад. *А. Н. Колмогоровым*[2]) было дано строгое аксиоматическое обоснование теории вероятностей, устранены все неясности понятия вероятности. Теория *Колмогорова*, как всякая вполне аксиоматическая теория, допускает разные интерпретации, и поэтому может быть применена в различных областях. Итак открыт путь к плодотворному применению теории вероятностей также в теории чисел.

В настоящеи сообщении будет изложена новая теорема теории вероятностей, имеющая важные следствия для теории чисел. Эту теорему я нашел исходя из известного метода *Ю. В. Линника*, метода, который называется „большим решетом".[3]) Обобщая „большое решето", удалось доказать следующую теорему:[4]) всякое четное число $2N$ может быть представлено в виде суммы простого и „полу-простого" числа, т. е. в виде $2N = p + p_1 p_2 \dots p_k$ где $p, p_1, p_2, \dots p_k$ простые числа и k не превосходит абсолютную константу K. Изучение „большого решета" открыло, что оно принадлежит в сущности к теории вероятностей. Общая теорема, которая была найдена мною таким путем, и которую я хочу здесь изложить, содержит „большое решето" *Линника*, вместе с упомянутыми обобщениями в качестве частных случаев.

С точки зрения теории вероятностей в основе нашей теоремы лежит следующий очевидный факт: если x_1 и x_2 — независимые случайные величины и случайная величина y тесно связана с x_1 то y слабо связана с x_2. Для того чтобы формулировать нашу теорему во всей общности, прежде всего введем некоторые обозначения и определения.

Пусть E — некоторое множество и пусть через ξ означаются элементы множества E. Пусть F — борелевское тело подмножеств множества E, которое содержит также E в кажестве элемента. Элементы тела F будем обозначать через $A, B, \dots$ и называть событиями. Пусть $P(A)$ обозначает вполне аддитивную неотрицательную функцию множеств, определенную для $A \varepsilon F$; предположим $P(E) = 1$. Другими словами мы рассматриваем поле вероятностей $\{F, P\}$ в смысле *Колмогорова*.

P — измеримую функцию $x = x(\xi)$ определенную на E, принимающую вещественные значения, будем называть случайной величиной. Через

$$e(x) = \int_E x \, dP \tag{1}$$

обозначаем математическое ожидание величины x, и через $e_A(x)$ условное математическое ожидание величины x при гипотезе что событие A осуществлено, т. е. мы положим (для $P(A) \neq 0$)

$$e_A(x) = \frac{1}{P(A)} \int_A x \, dP \tag{2}$$

Через $\beta(x)$ обозначаем дисперсию величины x, т. е.

$$\beta(x) = e((x - e(x))^2) \tag{3}$$

Пусть $I = (a, b)$ обозначает полуинтервал $a \leqq t < b$ на вещественной оси, $(-\infty \leqq a < b \leqq +\infty)$, и пусть $A^x(I)$ означает множество таких ξ для которых значение $x(\xi)$ содержится в I. Положим $V^x(I) = P(A^x(I))$, значит $V^x(I)$ — функция распределения величины x; $V^x(I)$ — аддитивная функция полуинтервала. Как обычно, мы будем называть величины x и y независимыми, если

$$P(A^x(I_1)\, A^y(I_2)) = P(A^x(I_1))\, P(A^y(I_2)) \tag{4}$$

для всех полуинтервалов I_1 и I_2.

Теперь мы введем новое понятие: понятие *коэффициента родства* случайной величины x к случайной величине y. Коэффициент родства обозначим через $\varrho_y(x)$ и определим посредством формулы (предположим $\beta(y) \neq 0$)

$$\varrho_y(x) = \left[\frac{1}{\beta(y)} \int_{-\infty}^{+\infty} (e_{A^x(I)}(y) - e(y))^2 \, V^x(I)\right]^{\frac{1}{2}} \tag{5}$$

где интеграл означает интеграл Burkill-a функции полуинтервала которая стоит под знаком интеграла. Заметим следующие свойства коэффициента родства: если x и y независимы, то $\varrho_y(x) = 0$; если $y = x$, то $\varrho_x(x) = 1$; вообще $0 \leqq \varrho_y(x) \leqq 1$; $\varrho_y(x)$ не изменяется если заменяем x на $f(x)$ где $f(t)$ — одноэначная измеримая функция действительного переменного, т. е. $f(t_1) \neq f(t_2)$ если $t_1 \neq t_2$. Так например $\varrho_y(\lambda x + \mu) = \varrho_y(x)$ если $\lambda \neq 0$. Далее $\varrho_y(x)$ не изменяется если заменить y на $y - a$, где a — постоянное. Таким образом можем всегда заменить y на $Y = y - e(y)$, и поэтому имеем

$$\varrho_y(x) = \left[\frac{1}{e(Y^2)}\int_{-\infty}^{+\infty} e^2_{A^x(I)}(Y)\, V^x(I)\right]^{\frac{1}{2}} \tag{6}$$

Если x — характеристическая величина события A (т. е. $x(\xi) = 1$ если $\xi \varepsilon A$ и $x(\xi) = 0$ в противном случае), дальше y — характеристическая величина события B, то $\varrho_y(x) = \varrho_x(y)$ равен коэффициенту корреляции между событиями A и B, т. е.

$$\varrho_y(x) = \frac{P(AB) - P(A)\,P(B)}{\sqrt{P(A)\,(1 - P(A)\,)P(B)\,(1 - P(B))}} \tag{7}$$

Введем еще одно понятие. Обозначим

$$d(x, y) = \sup_{(I_1, I_2)} \left| \frac{P(A^x(I_1)\, A^y(I_2))}{P(A^x(I_1)\, P(A^y(I_2))} - 1 \right| \tag{8}$$

где I_1 и I_2 пробегают все полуинтервалы вещественной оси, и назовем $d(x, y)$ *коэффициентом зависимости* между x и y. Бесконечную последовательность случайных величин $x_1, x_2, \ldots, x_n, \ldots$ будем называть *ограниченно связанной* если квадратичная форма $\Sigma\Sigma d_{nm}t_nt_m$, где $d_{nm} = d(x_n, x_m)$, будет ограниченной, т. е. если имеем

$$\left| \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} d_{nm}t_nt_m \right| \leqq \Delta \tag{9}$$

для

$$\sum_{n=1}^{\infty} t_n^2 = 1.$$

Число Δ называем *модулем* ограниченно связанной последовательности. Очевидно, что $\Delta = 0$, если величины x_n попарно независимы.

Теперь можем формулировать нашу

Теорему: *Пусть $x_1, x_2, \ldots, x_n, \ldots$ означает ограниченно связанную последовательность случайных величин с модулем Δ, и пусть y — какое-либо случайная величина; предположим $\beta(y) > 0$. Тогда имеет место неравенство*

$$\sum_{n=1}^{\infty} \varrho_y{}^2(x_n) \leqq (1 + \Delta)\frac{e(y^2)}{\beta(y)}. \tag{10}$$

Для доказательства нам нужна следующая лемма, выражающая тот факт что неравенства Bessel-я в обобщенном виде справедлива для *почти ортогональных* систем случайных величин. Систему $\varphi_1, \varphi_2, \ldots, \varphi_n, \ldots$ случайных величин называем *почти ортогональной*, если квадратичная форма $\sum_{n=1}^{\infty}\sum_{m=1}^{\infty} c_{nm}t_nt_m$, где $c_{nm} =$

$= e(\varphi_n, \varphi_m)$, ограничена, т. е. если $\left|\sum_{n=1}^{\infty}\sum_{m=1}^{\infty} c_{nm}t_nt_m\right| \leqq K$ для $\sum_{n=1}^{\infty} t_n^2 = 1$
Константу K будем называть *гранью* системы $\{\varphi_n\}$. Имеет место

Лемма: *Если* $\{\varphi_n\}$ — *почти ортогональная система случайных величин с гранью* K, *и* y — *любая случайная величина, положим* $\gamma_n = e(y\varphi_n)$ для $n = 1, 2, \ldots$ Тогда имеет место неравенство

$$\sum_{n=1}^{\infty} \gamma^2{}_n \leqq Ke(y^2) \tag{11}$$

Эта лемма — для почти ортогональных систем функций действительного переменного — была доказана R. P. Boas-ом.[5])

Доказательство этой леммы очень просто. В самом деле, для всякого целого $N \geqq 1$ имеем

$$e\left((y - \frac{1}{K}\sum_{n=1}^{N}\gamma_n\varphi_n)^2\right) = e(y^2) - \frac{2}{K}\sum_{n=1}^{N}\gamma_n{}^2 + \frac{1}{K^2}\sum_{n=1}^{N}\sum_{m=1}^{N} c_{nm}\gamma_n\gamma_m \geqq 0.$$

Так как

$$\left|\sum_{n=1}^{N}\sum_{m=1}^{N} c_{nm}\gamma_n\gamma_m\right| \leqq K \cdot \sum_{n=1}^{N}\gamma_n{}^2$$

получаем

$$e(y^2) \geqq \frac{1}{K}\sum_{n=1}^{N}\gamma_n{}^2$$

что доказывает лемму.

Перейдем теперь к доказательству теоремы. Для всякого $n = 1, 2, 3, \ldots$ возьмем некоторое разложение действительной осьи на конечное число не пересекающихся полуинтервалов: $\{I_{nk}\}$ $k = 1, 2, \ldots, N(n)$. Пусть $A_k^{x_n}$ означает событие $x_n \varepsilon I_{nk}$ и положим $P(A_k^{x_n}) = p_{nk}$; очевидно что $\sum_{k=1}^{N(n)} p_{nk} = 1$. Пусть Φ_{nk} означает характеристическую величину события $A_k^{x_n}$ и пусть будет

$$\varphi_{nk} = \frac{\Phi_{nk} - p_{nk}}{\sqrt{P_{nk}}}. \tag{12}$$

(Ясно, что можно предположить $p_{nk} \neq 0$). Положим

$$c_{nn'kk'} = e(\varphi_{nk}\varphi_{n'k'}) \tag{13}$$

В силу определения коэффициента зависимости имеем для $n \neq n'$

$$|\, c_{nn'kk'} \,| \leqq \sqrt{P_{nk}P_{n'k'}} \cdot d(x_n, x_{n'}), \tag{14}$$

дальше для $k \neq k'$

$$c_{nnkk'} = -\sqrt{p_{nk}p_{nk'}}, \tag{15}$$

и наконец

$$c_{nnkk} = 1 - p_{nk} \tag{16}$$

Пользуясь этими формулами, докажем, что случайные величины $\{\varphi_{nk}\}$ $(n = 1, 2, \ldots;\ k = 1, 2, \ldots, N(n))$ образуют почти ортогональную систему с гранью равной $1 + \Delta$, где Δ — модуль ограниченно связанной последовательности $x_1, x_2, \ldots, x_n, \ldots$ В самом деле, пусть $\{t_{nk}\}$ — любая двойная последовательность $(n = 1, 2, \ldots;\ k = 1, 2, \ldots, N(n))$ для которого $\sum_{n=1}^{\infty}\sum_{k=1}^{N(n)} t_{nk}^2 < \infty$. Пользуясь формулами (14), (15) и (16), и полагая

$$S = \sum_{n=1}^{\infty}\sum_{n'=1}^{\infty}\sum_{k=1}^{N(n)}\sum_{k'=1}^{N(n')} c_{nn'kk'}t_{nk}t_{n'k'}, \tag{17}$$

полагая далее

$$T_n = \sum_{k=1}^{N(n)} t_{nk}^2, \tag{18}$$

применяя неравенство Cauchy и имея в виду, что $\sum_{k=1}^{N(n)} p_{nk} = 1$, найдем

$$|S| \leqq \sum_{n=1}^{\infty}\sum_{n'=1}^{\infty} d(x_n, x_{n'})\, T_n^{\frac{1}{2}} T_{n'}^{\frac{1}{2}} + \sum_{n=1}^{\infty} T_n. \tag{19}$$

Таким образом, в силу определения модуля зависимости, получаем

$$|S| \leqq (1 + \Delta) \sum_{n=1}^{\infty} T_n \tag{20}$$

Итак доказано, что система $\{\varphi_{nk}\}$ является почти ортогональной с гранью $K = 1 + \Delta$. Следовательно, с помощью доказанной леммы, и полагая $\gamma_{nk} = e(y\varphi_{nk})$ получаем неравенство

$$\sum_{n=1}^{\infty}\sum_{k=1}^{N(n)} \gamma_{nk}^2 \leqq (1 + \Delta)\, e(y^2) \tag{21}$$

Однако, пользуясь определением величины φ_{nk}, мы видим, что

$$\gamma_{nk}^2 = (e_{A_k^{x_n}}(y) - e(y)^2\, V^{x_n}(I_{nk}) \tag{22}$$

Поэтому, если для краткости положим

$$D_n = \sum_{k=1}^{N(n)} \gamma_{nk}^2, \tag{23}$$

то только что доказанное неравенство дает

$$\sum_{n=1}^{\infty} D_n \leqq (1 + \Delta)\, e(y^2) \tag{24}$$

С другой стороны, значение D_n зависит только от выбора разложения $\{I_{nk}\}$, и легко видеть что верхняя грань величины D_n — для всех возможных разложений — равна $\beta(y)\, \varrho_y{}^2(x_n)$. В самом деле, интеграл Burkill-а $\int_{-\infty}^{+\infty} F(I)$, как известно, равен верхной грани сумм $\sum F(I_k)$ — (где $\{I_k\}$ пробегает все возможные разложения действительной оси в конечное число непересекающих полуинтервалов), если только функция полуинтервала $F(I)$ *субаддитивна*, т. е. $F(I_1 + I_2) \equiv F(I_1) + F(I_2)$ при $I_1 I_2 = 0$. Таким образом, если мы покажем, что

$$F(I) = (e_{A^{x_{n(I)}}}(y) - e(y))^2\, V^{x_n}(I) \tag{25}$$

субаддитивна, то утверждение

$$\sup .\, D_n = \beta(y)\, \varrho_y{}^2(x_n) \tag{26}$$

будет доказано.

Доказательство субаддитивности функции (25) состоит из двух шагов. Во-первых, $F(I)$ может быть представлено в виде $\frac{G^2(I)}{H(I)}$, где $G(I)$ и $H(I)$ — аддитивные функции. В самом деле имеем

$$F(I) = e^2_{A^{x_{n(I)}}}(Y)\, V^{x_n}(I) = \frac{e^2(Y\, .\, Z(x_n, I))}{V^{x_n}(I)} \tag{27}$$

где $Z(x_n, I)$ — характеристическая величина события $A^{x_n}(I)$. Во-вторых, каждая функция вида $\frac{G^2(I)}{H(I)}$ где $G(I)$ и $H(I)$ аддитивны, является субаддитивной, как это видно из элементарного неравенства $\frac{(a+b)^2}{c+d} \leqq \frac{a^2}{c} + \frac{b^1}{d}$, где $c > 0$, $d > 0$, a и b вещественны. Таким образом (26) доказана. Имея в виду что разложения $\{I_{nk}\}$ $n = 1, 2, \ldots$ выбираются независимо одно от других, мы получаем таким образом

$$\beta(y) \sum_{n=1}^{\infty} \varrho_y{}^2(x_n) \leqq e(y^2) \tag{28}$$

и составляет утверждение нашей теоремы.

Наконец, отметим лишь одно из следствий нашей теоремы, касающееся распределения простых чисел в прогрессиях. Для множества E возьмем конечную последовательность целых чисель: 1, 2, 3, ..., N. Пусть F — множество всех подмножеств

$A = (n_1, n_2, \ldots, n_k)$ множества E; положим $P(A) = \frac{k}{N}$. Пусть p означает некоторое простое число $< N^\alpha$; определим случайную величину $x_p = x_p(n)$ $(n = 1, 2, \ldots N)$ следующим образом: $Xp(n) = r$ для $n \equiv r$ модp; $(r = 0, 1, \ldots, p-1)$. Через $\Lambda(n)$ обозначим функцию v. Mangoldt-a; $\Lambda(n) = \log p$ для $n = p^k$ (p простое) и $\Lambda(n) = 0$ для $n \neq p^k$. Пусть

$$\psi(N) = \sum_{n=1}^{N} \Lambda(n) \text{ и } \psi(N; p, r) = \sum_{\substack{n \leqq N \\ n \equiv r \bmod p}} \Lambda(n).$$

Если возьмем $y = \Lambda(n)$, получим, применяя нашу теорему, что

$$\sum_{p < N^\alpha} p \sum_{r=1}^{p-1} \left(\Psi(N; p, r) - \frac{\Psi(N)}{p} \right)^2 \leqq CN^{3\alpha - 1}, \tag{29}$$

где C — постоянное, $\frac{1}{3} \leqq \alpha < \frac{1}{2}$. Пусть β, γ и δ положительные числа, $\beta + \gamma + \delta < \frac{1}{\alpha} - 2$; из (29) получается следующее утверждение:

Для всех простых $p < N^\alpha$, за исключением не более чем $(N^{\alpha(1-\delta)}$ из них, и для всех $r = 1, 2, \ldots, p-1$ за исключением не более чем $p^{1-\gamma}$ из них, имеем

$$\Psi(N; p, x) = \frac{\Psi(N)}{p} + \frac{\vartheta \psi(N)}{p^{1+\beta}} \tag{30}$$

где $|\vartheta| \leqq 1$. Результат такого рода нужен для доказательства упомянутой теоремы о представлении четных чисел в виде суммы простого и полу-простого числа, и для других применений.

Литература:

1. См. M. Kac: Probability methods in some problems of analysis and number theory, Bulletin Amer. Math. Soc., **55** (1949), 641—665, где дается обзор результатов и подробный список литературы.
2. См. А. Н. Колмогоров: Основные понятия теории вероятностей. Москва-Ленинград, ОНТИ (1936), 1—80.
3. Ю.В. Линник: Большое решето, Доклады Академии Наук СССР, **30** (1941), 290—292.
4. А. Реньи: О представлении четных чисел в виде суммы простого и почти простого числа, Известия Академии Наук СССР, Серия Мат., **12** (1948), 57—78.
5. R. P. Boas, Jr: A general moment problem, American Journal of Mathematics, **63** (1941), 361—370.

*

Výtah. — Резюме.

O jedné obecné větě počtu pravděpodobnosti a jejím použití v theorii čísel.

ALFRED RÉNYI, Budapest.

V článku je dokázána následující věta z počtu pravděpodobnosti, jež má významné aplikace v theorii čísel.

Nechť posloupnost náhodových veličin $x_1, x_2, \ldots$ je omezeně vázaná s modulem vázanosti Δ a nechť y je náhodová veličina s dispersí $\beta(y) > 0$.

Potom

$$\sum_{n=1}^{\infty} \varrho_y^2(x_n) \leqq (1 + \Delta) \frac{e(y^2)}{\beta(y)}.$$

O USPOŘÁDANÝCH A CYKLICKY USPOŘÁDANÝCH GRUPÁCH.

LADISLAV RIEGER, Praha.

Sdělení se týkalo práce, uveřejněné ve třech pojednáních ve Věstníku Královské české společnosti nauk, 1946, čís. 6, 1—31; 1947, čís. 1, 1—33; 1948, čís. 1, 1—26.

*

Summary. — Výtah.

On the ordered and cyclically ordered groups.

LADISLAV RIEGER, Praha.

The communication was a rapport about author's three papers published in the Věstník Královské české společnosti nauk (Mémoires de la Société Royale des Sciences de Bohême) 1946, nr. 6, 1—31; 1947, nr. 1, 1—33; 1948, nr. 1, 1—26.

O ROVNICIACH TVARU $c_1x_1^{k_1} + c_2x_2^{k_2} + \ldots + c_sx_s^{k_s} = c$ V KONEČNÝCH TELESIACH.

ŠTEFAN SCHWARZ, Bratislava.

Prednášajúci ukázal najprv, ako možno dokázať jednoducho túto vetu:

Nech je daná kongruencia

$$c_1x_1^{k_1} + c_2x_2^{k_2} + \ldots + c_sx_s^{k_s} \equiv c \pmod{p}, \qquad (1)$$

kde $c_1 . c_2 \ldots c_s \not\equiv 0 \pmod{p}$. *Označme* $\delta_i = (k_i, p - 1)$. *Keď*

$$\frac{1}{\delta_1} + \frac{1}{\delta_2} + \ldots + \frac{1}{\delta_s} \geqq 1,$$

potom má kongruencia (1) *riešenie celými číslami a to pre každé c.*

Potom referoval o obsahu svojich troch prác, z ktorých dve vyšly v Quarterly Journal of Mathematics (Oxford Series), **19** (1948), 123—128 a **19** (1948), 160—163 a tretia výjde v Časopise pro pěstování matematiky a fysiky, **75** (1950). Naznačil obzvlášť dôkaz tejto vety:

Nech $GF(p^n)$ *je konečné teleso charakteristiky* p. *Nech* $c_1, c_2, \ldots, c_k$ *sú samé nenulové elementy telesa* $GF(p^n)$. *Nech konečne* $(p^n - 1, k) \leqq \leqq p - 1$. *Potom má rovnica* $c_1 x_1^k + c_2 x_2^k + \ldots + c_k x_k^k = c$ *pre každé* $c \in GF(p^n)$ *riešenie s* $x_1, x_2, \ldots, x_k \in GF(p^n)$.

Napokon sa prednášajúci zaoberal výsledkami, ktoré dostal L. K. Hua-H. S. Vandiver (Proc. Nat. Acad. Sci., **34** (1948), 258—263) a A. Weil (Bull. Amer. Math. Soc., **55** (1949), 497—508) a ktoré sa týkajú asymptotických vzorcov pre počet riešení rovníc uvedených v nadpise.

*

Summary. — Výtah.

On the equation $c_1x_1^{k_1} + c_2x_2^{k_2} + \ldots + c_sx_s^{k_s} = c$ in finite fields.

ŠTEFAN SCHWARZ, Bratislava.

The author gave some theorems concerning the existence of solutions of the equations considered in the title.

He gave an exposition of the results of his three papers. Two of them have been published in Quart. J. Math., Oxford Ser., **19** (1948), 123—128 and **19** (1948), 160—163. The third will appear in Časopis pro pěst. mat. fys., **75** (1950).

Finally he discusse l some results of L. K. Hua — H. S. Vandiver and A. Weil concerning the number of solutions of the equations which were considered.

O PIERWIASTKACH I KIERUNKACH CHARAKTERYSTYCZNYCH PEWNYCH MACIERZY.*)

ZOFIA SZMYDTÓWNA, Kraków.

Niech

$$A = \|a_{ij}\| \quad (i = 1, \ldots, n;\ j = 1, \ldots, n)$$

będzie macierzą rzeczywistą, której wszystkie elementy położone poza

*) Referowana praca ukazała się w Annales de la Société Polonaise de Mathématique, **22**, 235—240 p. t. „Sur les racines caractéristiques et sur les directions caractéristiques de certaines matrices".

przekątnią główną są nieujemne, to jest

$$a_{ij} \geqq 0 \text{ gdy } i \neq j. \tag{1}$$

Dla macierzy tego typu zachodzi twierdzenie następujące:

Twierdzenie. *Każdy pierwiastek charakterystyczny macierzy A mający największą część rzeczywistą jest rzeczywisty. Jeżeli ponadto założymy, że*

$$a_{ij} > 0 \text{ dla } i \neq j \tag{2}$$

wówczas największy pierwiastek rzeczywisty jest pojedynczy.

Dowód opiera się na twierdzeniu Frobeniusa odnoszącym się do macierzy A, której wszystkie elementy są dodatnie względnie nieujemne. Również i inne twierdzenia Frobeniusa tyczące tych ostatnich typów macierzy dają się przenieść z odpowiednimi zmianami na wypadek macierzy typu (1) i (2).

*

Résumé. — Streszczenie.

Sur les racines caractéristiques et sur les directions caractéristiques de certaines matrices.*)

ZOFIA SZMYDTÓWNA, Kraków.

Soit

$$A = \|a_{ij}\| \quad (i, j = 1, \ldots, n)$$

une matrice réelle dont tous les éléments situés à l'extérieur de la diagonale principale sont non négatifs, c'est-à-dire que

$$a_{ij} \geqq 0 \text{ lorsque } i \neq j. \tag{1}$$

Dans cette hypothèse, on a le théorème suivant:

Chaque racine caractéristique de la matrice A, dont la partie réelle est maxima, est forcément réelle. Si en plus

$$a_{ij} > 0 \text{ lorsque } i \neq j, \tag{2}$$

la racine caractéristique réelle la plus grande est simple.

La démonstration s'appuie sur un théorème de Frobenius concernant une matrice dont ou *tous* les éléments sont positifs ou *tous* non négatifs.

Plusieurs théorèmes de Frobenius (à une modification convenable près) subsistent pour les matrices du type (1) et (2).

*) Annales de la Société Polonaise de Mathématiques, **22**, 235—240.