
ATTI ACCADEMIA NAZIONALE DEI LINCEI
CLASSE SCIENZE FISICHE MATEMATICHE NATURALI
RENDICONTI

ESAYAS GEORGE KUNDERT

On the algebra structure of the s-d-ring over \mathbb{Z}_p .

Nota I

*Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche,
Matematiche e Naturali. Rendiconti, Serie 8, Vol. 51 (1971), n.6, p. 466–471.*

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1971_8_51_6_466_0>

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

*Articolo digitalizzato nel quadro del programma
bdim (Biblioteca Digitale Italiana di Matematica)
SIMAI & UMI*

<http://www.bdim.eu/>

Algebra. — *On the algebra structure of the s - d -ring over \mathbf{Z}_p .*
 Nota I di ESAYAS GEORGE KUNDERT, presentata (*) dal Socio B. SEGRE.

RIASSUNTO. — La teoria degli s - d -anelli, sviluppata in tre precedenti Note lincee [1], [2], [3], viene qui approfondita nel caso di s - d -anelli aventi \mathbf{Z}_p come anello delle costanti. Per essi, in questa Nota I ed in una successiva Nota II, vengono stabiliti i due Teoremi specificati nel preambolo, ottenendo anche estensioni mod p di alcuni risultati classici di teoria dei numeri elementare (fattorizzazioni di coefficienti multinomiali, piccolo Teorema di Fermat, criterio di Eulero per i residui quadratici).

Let \mathfrak{A}_p denote the s - d -ring with \mathbf{Z}_p as ring of constants. (All definitions used in this paper may be found in [1], [2], [3]). \mathfrak{A}_p is a certain type of \mathbf{Z}_p -Hopf algebra (see [2]). In this article we will however use only the fact that \mathfrak{A}_p is a free \mathbf{Z}_p -algebra with an infinite basis $\{x_i\}_{i=0,1,2,\dots}$ (see [1]).

We shall prove two Theorems concerning \mathfrak{A}_p . If we write $\prod_{v=1}^n x_{i_v} = \sum_{s \geq 0} \beta(s | i_v) x_s$, then the first Theorem deals with the dependence of $\beta(s | i_v) \in \mathbf{Z}_p$ on the indices $(s | i_v)$. We show that the index symbols $(s | i_v)$ may be collected into classes which form a commutative semi-group \mathfrak{S} with identity element and that $\beta(s | i_v)$ defines a homomorphism from \mathfrak{S} onto the multiplicative group of \mathbf{Z}_p together with the zero. A Corollary shows an intimate connection with a Theorem of L. E. Dickson concerning factorization of multinomial coefficients in \mathbf{Z}_p .

The second Theorem (to be proved in a following "Nota II") shows the existence of a \mathbf{Z}_p -algebra isomorphism from \mathfrak{A}_p onto a well-characterized subalgebra $\bar{\mathfrak{A}}_p$ of the direct sum of countably many copies of \mathbf{Z}_p and it is further shown that \mathfrak{A}_p is built up by a chain of subalgebras A_{p^m} each of which is mapped by the above mentioned isomorphism onto a subalgebra \bar{A}_{p^m} which in turn is isomorphic to a direct sum of p^m copies of \mathbf{Z}_p . This allows us to draw conclusions about factorization in \mathfrak{A}_p . We see for example that \mathfrak{A}_p — while not a field — consists of units and zerodivisors only and that there are no irreducible elements in \mathfrak{A}_p . Our explicit description of the isomorphism permits us also to test each given element for being a unit or zerodivisor.

The previously discovered fact that Fermat's Theorem holds in \mathfrak{A}_p (see [4]) is now easily explained on ground of Fermat's Theorem in \mathbf{Z}_p . (The proof of Fermat's Theorem given in [4] does not assume Fermat's Theorem in \mathbf{Z}_p , the latter is then a consequence of the former). Other number theoretical Theorems of \mathbf{Z}_p may be lifted to \mathfrak{A}_p , we mention as another example Euler's Criterion for quadratic rests. Finally we show with help of Theorem II how $\beta(s | i_v)$ may be computed in terms of binomial coefficients and in parti-

(*) Nella seduta del 13 novembre 1971.

cular how it may be expressed in terms of the difference operator Δ (used in difference calculus). That $\beta(s | i_v)$ can be expressed in terms of binomial coefficients is clear also from the facts that $\beta(s' | i, j)$ for two indices i, j is computable in terms of binomial coefficients (see [3] page 477) and that $\beta(s | i_v)$ is a sum of products of such $\beta(s' | i, j)$ which follows at once from its definition; however the representation which we give is a different one. Comparison of the two representations gives certain identities between binomial coefficients. In the remark at the end of the announced "Nota II", we shall give the simplest example of such an identity. It should not be difficult to prove these identities directly or with help of difference calculus.

To be able to formulate Theorem I we make the following definitions:

1) We call ${}_s i = (s | i_v)$ an index symbol if s, i_v ($v = 1, 2, 3, \dots$) are non-negative integers and $i_v = 0$ for large v .

2) We expand s and i_v in terms of powers of p : $s = \sum_{\mu \geq 0} \sigma_\mu p^\mu$ and $i_v = \sum_{\mu \geq 0} \kappa_{v\mu} p^\mu$ where $0 \leq \sigma_\mu < p - 1$ and $0 \leq \kappa_{v\mu} < p - 1$ and define ${}_s I = (\sigma_\mu | \kappa_{v\mu})$ to be the associated (infinite) matrix to ${}_s i$ where the σ_μ form the first column and $\kappa_{v\mu}$ (v fixed) the v -th column.

Note: ${}_s i$ and ${}_s I$ determine each other uniquely.

3) We define: ${}_s I \sim {}_t J$ if and only if ${}_t J$ is obtained from ${}_s I$ by *a*). A finite number of permutations of rows and *b*). A finite number of permutations of elements $\kappa_{v\mu}$ in the μ -th row. This is clearly an equivalence relation. We define further: ${}_s i \sim {}_t j$ iff ${}_s I \sim {}_t J$ for the associated matrices. Let $(i) = ({}_s I)$ denote the equivalence class of ${}_s i$ or ${}_s I$ and \mathfrak{I} the set of these equivalence classes.

4) We introduce a multiplication in \mathfrak{I} : $({}_s I) \cdot ({}_t J) = \left(\begin{smallmatrix} s & I \\ t & J \end{smallmatrix} \right)$ where the symbol on the right denotes the class of the matrix formed by the rows of ${}_s I$ and ${}_t J$ together. (The order of the rows is of course irrelevant). It is clear that this multiplication is *well-defined*, *associative* and *commutative*. The class of the O -matrix plays the role of the *identity* element. \mathfrak{I} becomes therefore together with this multiplication a *commutative semi-group with an identity*. Besides the identity there are no units in \mathfrak{I} .

5) Let ${}_s q = (s | {}_v i)$ be an index symbol with $0 \leq s < p - 1$ and $0 \leq {}_v i < p - 1$ but ${}_s q \neq (0 | 0)$. It is clear that ${}_s q = {}_s Q$ and that $({}_s q)$ is an irreducible element in \mathfrak{I} . On the other hand any irreducible element in \mathfrak{I} must be of this form. Furthermore one checks at once that: *Every element of \mathfrak{I} is a finite product of irreducible elements and this representation is unique up to order of factors.*

6) We define a mapping from \mathfrak{I} into \mathbf{Z}_p : Let $(i) \in \mathfrak{I}$, ${}_s i = (s | {}_v i)$. Let $\{x_i\}$ be a basis for the \mathbf{Z}_p -algebra \mathfrak{A}_p and let $\prod_v x_{i_v} = \sum_s \beta(s | i_v) x_s$, then define:

$$\begin{aligned} \beta: \mathfrak{I} &\rightarrow \mathbf{Z}_p \\ (i) &\rightarrow \beta(s | i_v). \end{aligned}$$

THEOREM I. β is a well-defined homomorphism from the semigroup \mathfrak{S} onto the multiplicative group of \mathbb{Z}_p together with the zero element.

Proof. Let $s = (s | i_v)$ and $\sigma_\mu = (\sigma_\mu | \kappa_{v\mu})$ its associated matrix. We show first:

$$(A) \quad \beta(s | i_v) = \prod_{\mu \geq 0} \beta(\sigma_\mu | \kappa_{v\mu}).$$

We may assume that $i_v \geq i_{v+1}$ because the commutative law holds in \mathfrak{A}_p and therefore the value of $\beta(s | i_v)$ is independent of the order of the i_v . From the definition of $\beta(s | i_v)$ and the fact that $\beta(s | i_1, i_2) = (-1)^{i_1+i_2+s} \binom{i_1}{s-i_2} \binom{s}{i_1}$ (see [3] the Remark after Lemma I) it follows at once that $\beta(s | i_v) = 0$ if $s < i_1$, but from $s < i_1 \Rightarrow \sigma_{\mu_0} < \kappa_{1\mu_0}$ for some μ_0 and $\beta(\sigma_{\mu_0} | \kappa_{v\mu_0}) = 0$. Therefore if $s < i_1$ then (A) holds. (A) holds clearly for $(s | i_v) = (0 | 0)$. We assume now that $s \geq i_1$ and that (A) be true for $s' < s$. (A) is trivial for $s < p$. Let μ_1 be such that $\sigma_{\mu_1} \neq 0$ but $\sigma_\mu = 0$ for $\mu < \mu_1$. Now if d is the semi-derivation in \mathfrak{A}_p then $d^{(p^{\mu_1})}$ is also a semi-derivation (see [6]). Let $i_m \neq 0$ but $i_v = 0$ for $v > m$. We have then:

$$(B) \quad d^{(p^{\mu_1})} x_{i_1} x_{i_2} \cdots x_{i_m} = \sum_{s \geq p^{\mu_1}} \beta(s | i_v) x_{s-p^{\mu_1}} \\ = \sum_{(\rho_1, \rho_2, \dots, \rho_m) \neq (0, 0, \dots, 0)} (-1)^{1+\rho_1+\rho_2+\dots+\rho_m} x_{i_1-\rho_1 p^{\mu_1}} x_{i_2-\rho_2 p^{\mu_1}} \cdots x_{i_m-\rho_m p^{\mu_1}}$$

where $\rho_v = 0$ or 1 and x_j is to be put $= 0$ if $j < 0$.

If $i_1 < p^{\mu_1} \Rightarrow \beta(s | i_v) = 0$ and $\beta(\sigma_{\mu_1} | \kappa_{v\mu_1}) = 0$ also and therefore (A) holds. Assume $i_1 \geq p^{\mu_1}$. From (B) and the induction hypothesis follows then:

$$(C) \quad \beta(s | i_v) = \sum_{(\rho_1, \rho_2, \dots, \rho_m) \neq (0, 0, \dots, 0)} (-1)^{1+\rho_1+\dots+\rho_m} \beta(s - p^{\mu_1} | i_v - \rho_v p^{\mu_1}) \\ = \prod_{\mu \neq \mu_1} \beta(\sigma_\mu | \kappa_{v\mu}) \cdot \sum_{(\rho_1, \rho_2, \dots, \rho_m) \neq (0, 0, \dots, 0)} (-1)^{1+\rho_1+\rho_2+\dots+\rho_m} \beta(\sigma_{\mu_1} - 1 | \kappa_{v\mu_1} - \rho_v)$$

where we must put those β 's equal to zero, when at least one index becomes negative.

But we have also:

$$(D) \quad d(x_{\kappa_{1\mu_1}} \cdot x_{\kappa_{2\mu_1}} \cdots x_{\kappa_{m\mu_1}}) = \sum_{\sigma \geq 1} \beta(\sigma | \kappa_{v\mu_1}) x_{\sigma-1} \\ = \sum_{(\rho_1, \rho_2, \dots, \rho_m) \neq (0, 0, \dots, 0)} (-1)^{1+\rho_1+\dots+\rho_m} x_{\kappa_{1\mu_1}-\rho_1} x_{\kappa_{2\mu_1}-\rho_2} \cdots x_{\kappa_{m\mu_1}-\rho_m}.$$

From which follows:

$$(E) \quad \beta(\sigma_{\mu_1} | \kappa_{\nu\mu_1}) = \sum_{(\rho_1, \rho_2, \dots, \rho_m) \neq (0, 0, \dots, 0)} (-1)^{1+\rho_1+\dots+\rho_m} \beta(\sigma_{\mu_1-1} | \kappa_{\nu\mu_1-\rho_\nu}).$$

From (C) & (E) \Rightarrow (A).

Now let ${}_i j \sim {}_s i$ and apply (A) also for $\beta(t | {}_s j)$ the only changes on the right side of formula (A) which will occur consist in a permutation of factors $\beta(\sigma_\mu | \kappa_{\nu\mu})$ (which of course does not change the value of the right side) and a permutation of indices $\kappa_{\nu\mu}$ in $\beta(\sigma_\mu | \kappa_{\nu\mu})$ for μ fixed. $\beta(\sigma_\mu | \kappa_{\nu\mu})$ is the coefficient of x_{σ_μ} in the expansion of $\prod_\nu x_{\kappa_{\nu\mu}}$ in terms of the basis $\{x_i\}$ and is therefore independent of such a permutation since the multiplication in \mathfrak{A}_p is commutative. β is therefore well-defined on \mathfrak{J} .

If $({}_s i) = \prod_k ({}_k q)$ is the factorization of $({}_s i)$ into irreducible elements then formula (A) tells us exactly that $\beta({}_s i) = \prod_k \beta({}_k q)$.

From this and the fact that the factorization into irreducible elements is unique in \mathfrak{J} follows at once that β is a homomorphism.

To show that β is *onto* we observe that $x_1 \cdot x_{n-1} = n \cdot x_n - (n-1)x_{n-1}$ and therefore $\beta(n | n-1, 1) \equiv n \pmod p$ for $n \geq 1$ and $\beta(0 | 1) \equiv 0 \pmod p$.

COROLLARY. Let m_i be natural numbers ($i = 1, 2, \dots, r$). Put ${}_j m = \sum_{i=1}^j m_i$ and $[m_1, m_2, \dots, m_r] = \frac{r!}{m_1! m_2! \dots m_r!}$ (r -nomial coefficient). We have the following formulae:

$$(I) \quad [m_1, m_2, \dots, m_r] \equiv (-1)^{\sum_{i=1}^{r-1} i m_i} \beta\left(\prod_{i=2}^r ({}_i m | {}_i m, {}_{i-1} m)\right) \pmod p.$$

Let $m_i = \sum_{\mu \geq 0} \kappa_{i\mu} p^\mu$ then:

$$(II) \quad [m_1, m_2, \dots, m_r] \equiv \prod_{\mu \geq 0} [\kappa_{1\mu}, \kappa_{2\mu}, \dots, \kappa_{r\mu}] \pmod p.$$

Let ${}_j m = \sum_{\mu \geq 0} {}_j \kappa_\mu p^\mu$ then:

$$(III) \quad [m_1, m_2, \dots, m_r] \equiv 0 \pmod p \quad \text{iff} \quad {}_r \kappa_\mu \neq \sum_{j=1}^r \kappa_{j\mu}$$

for some μ .

Remarks: (II) & (III) are well-known formulae of L. E. Dickson. See [5] pg. 273 for references. For $r = 2$ (II) turns into Lucas's formula for binomial coefficients:

$$\binom{{}_2 m}{m_2} \equiv \prod_{\mu \geq 0} \binom{{}_2 \kappa_\mu}{\kappa_{2\mu}} \pmod p. \quad (\text{See [5] pg. 271}).$$

Proof of the corollary:

$$\begin{aligned}
 \text{(I)} \quad [m_1, m_2, \dots, m_r] &= \frac{r-1m!}{m_1! m_2! \dots m_{r-1}!} \cdot \frac{r m!}{r-1m! m_r!} \\
 &= [m_1, m_2, \dots, m_{r-1}] \cdot (-1)^{r-1m} \beta(rm | rm, r-1m) \\
 &= (-1)^{\sum_{i=1}^{r-1} i^m} \prod_{j=0}^{r-2} \beta(r-jm | r-jm, r-j-1m) = (-1)^{\sum_{i=1}^{r-1} i^m} \beta\left(\prod_{i=2}^r (im | im, i-1m)\right)
 \end{aligned}$$

by Theorem I.

(II) Suppose first that $r\mathcal{X}_\mu = \sum_{j=1}^r \mathcal{X}_{j\mu}$ for all μ . It is clear that then also $i\mathcal{X}_\mu = \sum_{j=1}^i \mathcal{X}_{j\mu}$ for all μ . Since then $(im | im, i-1m) = \prod_{\mu \geq 0} (i\mathcal{X}_\mu | i\mathcal{X}_\mu, i-1\mathcal{X}_\mu)$ and observing that $(-1)^{im} = (-1)^{\sum_{\mu \geq 0} i\mathcal{X}_\mu}$ we get by (I):

$$[m_1, m_2, \dots, m_r] \equiv \prod_{\mu \geq 0} (-1)^{i\mathcal{X}_\mu} \beta(i\mathcal{X}_\mu | i\mathcal{X}_\mu, i-1\mathcal{X}_\mu) \equiv \prod_{\mu \geq 0} [\mathcal{X}_{1\mu}, \mathcal{X}_{2\mu}, \dots, \mathcal{X}_{r\mu}] \pmod{p}.$$

Since $[\mathcal{X}_{1\mu}, \mathcal{X}_{2\mu}, \dots, \mathcal{X}_{r\mu}] = \frac{r\mathcal{X}_\mu!}{\mathcal{X}_{1\mu}! \dots \mathcal{X}_{r\mu}!}$ and $p \nmid$ numerator since $r\mathcal{X}_\mu < p$ because of our assumption $\Rightarrow [\mathcal{X}_{1\mu}, \mathcal{X}_{2\mu}, \dots, \mathcal{X}_{r\mu}] \not\equiv 0 \pmod{p} \Rightarrow [m_1, m_2, \dots, m_r] \not\equiv 0 \pmod{p}$ by (II). This shows that the condition given in (III) is necessary.

Next suppose that there exists a μ_0 such that $r\mathcal{X}_\mu = \sum_{j=1}^r \mathcal{X}_{j\mu}$ for $\mu < \mu_0$ but $r\mathcal{X}_{\mu_0} \neq \sum_{j=1}^r \mathcal{X}_{j\mu_0}$. We have then $r\mathcal{X}_{\mu_0} = \sum_{j=1}^r \mathcal{X}_{j\mu_0} - \varepsilon_1 p$; $1 \leq \varepsilon_1 < r$.

For $r = 2$: $[m_1, m_2] = (-1)^{im} \beta(2m | 2m, 1m)$

$$\equiv (-1)^{im} \prod_{\mu \geq 0} \beta(2\mathcal{X}_\mu | 2\mathcal{X}_\mu, 1\mathcal{X}_\mu) \text{ by (I)}$$

and Theorem I, but $1m = m_1$ and $1\mathcal{X}_\mu = \mathcal{X}_{1\mu}$. Also $2\mathcal{X}_{\mu_0} = \mathcal{X}_{1\mu_0} + \mathcal{X}_{2\mu_0} - p = \mathcal{X}_{1\mu_0} - (p - \mathcal{X}_{2\mu_0}) < \mathcal{X}_{1\mu_0}$ since $p - \mathcal{X}_{2\mu_0} > 0$. Therefore $\beta(2\mathcal{X}_{\mu_0} | 2\mathcal{X}_{\mu_0}, 1\mathcal{X}_{\mu_0}) = 0 \Rightarrow [m_1, m_2] \equiv 0 \pmod{p}$ and (III) holds for $r = 2$. Now $[\mathcal{X}_{1\mu_0}, \mathcal{X}_{2\mu_0}] = \frac{(\mathcal{X}_{1\mu_0} + \mathcal{X}_{2\mu_0})!}{\mathcal{X}_{1\mu_0}! \mathcal{X}_{2\mu_0}!}$ and by our assumption $\mathcal{X}_{1\mu_0} + \mathcal{X}_{2\mu_0} > p \Rightarrow p \mid (\mathcal{X}_{1\mu_0} + \mathcal{X}_{2\mu_0})!$ but $p \nmid \mathcal{X}_{1\mu_0}!$ and $p \nmid \mathcal{X}_{2\mu_0}! \Rightarrow [\mathcal{X}_{1\mu_0}, \mathcal{X}_{2\mu_0}] \equiv 0 \pmod{p} \Rightarrow$ (II) holds for $r = 2$. Assume next that (II) & (III) hold for $r - 1$.

$$\begin{aligned}
 [m_1, m_2, \dots, m_r] &= [m_1, m_2, \dots, m_{r-1}] \cdot (-1)^{r-1m} \beta(rm | rm, r-1m) \\
 &\equiv [m_1, m_2, \dots, m_{r-1}] \cdot (-1)^{r-1m} \prod_{\mu \geq 0} \beta(r\mathcal{X}_\mu | r\mathcal{X}_\mu, r-1\mathcal{X}_\mu).
 \end{aligned}$$

Now either $r-1\mathcal{X}_{\mu_0} = \sum_{j=1}^{r-1} \mathcal{X}_{j\mu_0} - \varepsilon_1 p$ in which case $[m_1, m_2, \dots, m_{r-1}] \equiv 0 \pmod{p}$

by induction hypothesis and therefore (III) holds for r or

$${}_{r-1}\mathfrak{x}_{\mu_0} = \sum_{j=1}^{r-1} \mathfrak{x}_{j\mu_0} - \varepsilon_2 p \quad \text{with} \quad \varepsilon_2 < \varepsilon_1$$

then ${}_{r-1}\mathfrak{x}_{\mu_0} = {}_{r-1}\mathfrak{x}_{\mu_0} - (\varepsilon_1 - \varepsilon_2)p < {}_{r-1}\mathfrak{x}_{\mu_0}$ and $\beta({}_{r-1}\mathfrak{x}_{\mu_0} | {}_{r-1}\mathfrak{x}_{\mu_0}, {}_{r-1}\mathfrak{x}_{\mu_0}) \equiv 0 \pmod p \Rightarrow$ (III) holds for r . Since $[\mathfrak{x}_{1\mu_0}, \dots, \mathfrak{x}_{r\mu_0}] = \frac{{}_{r-1}\mathfrak{x}_{\mu_0}!}{\mathfrak{x}_{1\mu_0}! \dots \mathfrak{x}_{r\mu_0}!}$ and ${}_{r-1}\mathfrak{x}_{\mu_0} > p$ by our assumption, it follows again that p divides the numerator but not the denominator and (II) holds for r .

LITERATURE

- [1] E. G. KUNDERT, *Structure Theory in s-d-Rings. Note I*, « Accademia Nazionale dei Lincei », ser. VIII, 41, fasc. 5, November, 1966.
- [2] E. G. KUNDERT, *Structure Theory in s-d-Rings. Note II*, « Accademia Nazionale dei Lincei », ser. VIII, 43, fasc. 5, November, 1967.
- [3] E. G. KUNDERT, *Structure Theory in s-d-Rings. Note III*, « Accademia Nazionale dei Lincei », ser. VIII, 43, fasc. 6, December, 1967.
- [4] E. G. KUNDERT, *The Inteat Structure in the s-d-Ring over the Integers*, « Rendiconti di Matematica », (VI) 4, 533-546 (1971).
- [5] L. E. DICKSON, *History of the Theory of Numbers*, Vol. I.
- [6] TH. GIEBUTOWSKI, *Ph. D. Thesis*, Univ. of Mass. 1971.