Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Esayas George Kundert

On the Algebra Structure of the s-d-Ring over $\mathbf{Z}_p$. Nota II

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **52** (1972), n.1, p. 1–5.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1972_8_52_1_1_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1972.

RENDICONTI

DELLE SEDUTE

DELLA ACCADEMIA NAZIONALE DEI LINCEI

Classe di Scienze fisiche, matematiche e naturali

Seduta del 15 gennaio 1972

Presiede il Socio anziano MAURO PICONE

SEZIONE I

(Matematica, meccanica, astronomia, geodesia e geofisica)

Algebra. — *On the Algebra Structure of the s–d–Ring over* $\mathbf{Z}_p$. Nota II di ESAYAS GEORGE KUNDERT, presentata (*) dal Socio B. SEGRE.

RIASSUNTO. — Continuazione della precedente Nota I (apparsa a p. 466 di questi « Rendiconti », *51* (6), 1971), alla quale si rinvia sia per il Sunto che per la Bibliografia.

Let $\mathfrak{Z}_p = \sum_{i=0}^{\infty} \mathbf{Z}_p^{(i)}$ (complete direct sum where $\mathbf{Z}_p^{(i)} \approx \mathbf{Z}_p$) considered as a $\mathbf{Z}_p$–algebra.

DEFINITION. An element $(a_i) \in \mathfrak{Z}_p$ is called *periodic* with *period* s if $a_{i+s} = a_i$ for all i. Let $\overline{\mathfrak{A}}_p = \{(a_i) \mid (a_i) \in \mathfrak{Z}_p$ with period p^m for some $m = 0, 1, 2, \cdots\}$. $\overline{\mathfrak{A}}_p$ is a $\mathbf{Z}_p$–subalgebra of $\mathfrak{Z}_p$. Let $\bar{\mathrm{A}}_{p^m} = \{(a_i) \mid (a_i) \in \mathfrak{Z}_p$ with period p^m, m fixed$\}$. $\bar{\mathrm{A}}_{p^0}$ is the diagonal of $\overline{\mathfrak{A}}_p$ and $\bar{\mathrm{A}}_{p^0} \approx \mathbf{Z}_p$. In general $\bar{\mathrm{A}}_{p^m} \approx \sum_{i=0}^{p^m-1} \mathbf{Z}_p^{(i)}$. Let $\mathrm{A}_{p^m} = \{a \mid a \in \mathfrak{A}_p$, deg $a < p^m\}$. This is certainly a $\mathbf{Z}_p$–vector space and it is actually a subalgebra of $\mathfrak{A}_p$. This follows at once from the following Theorem.

THEOREM II. *There exists an isomorphism between the* $\mathbf{Z}_p$*–algebras* $\mathfrak{A}_p$ *and* $\overline{\mathfrak{A}}_p$ *which maps each* A_{p^m} *onto* $\bar{\mathrm{A}}_{p^m}$.

Proof. Let $h = \mathrm{E} - d$ where E is the identity map and d the semi-derivation of $\mathfrak{A}_p$. h is an *automorphism* for the $\mathbf{Z}_p$–algebra $\mathfrak{A}_p$ (See [6]). Let σ be the homomorphism which belongs to the definition of the notion *s–d–*ring (see [1] pg. 270). Let $\sigma_k = \sigma h^{(k)}$. This is a homomorphism from $\mathfrak{A}_p$ onto $\mathbf{Z}_p$ leaving $\mathbf{Z}_p$ fixed.

(*) Nella seduta dell'11 dicembre 1971.

LEMMA 1. *If* $k' \equiv k \bmod p^m$ *and* $a \in A_{p^m}$ *then* $\sigma_{k'}(a) = \sigma_k(a)$.

Proof of Lemma 1. $h^{(k')}(a) = \sum_{i=0}^{p^m-1} (-1)^i \binom{k'}{i} d^{(i)} a$ because $d^{(i)} a = 0$ for $i \geq p^m$. By assumption $k' = s \cdot p^m + k$. Let $k = \sum_{\nu \geq 0} \varkappa_\nu p^\nu$ and $i = \sum_{\nu=0}^{p^m-1} \tau_\nu p^\nu$ then:

$\binom{k'}{i} = \prod_{\nu=0}^{p^m-1} \binom{\varkappa_\nu}{\tau_\nu} = \binom{k}{i}$ by Lucas's Theorem. (See remark to Corollary of Theorem I) $\Rightarrow h^{(k')}(a) = h^{(k)}(a)$ and therefore $\sigma_{k'}(a) = \sigma_k(a)$.

Remark. Let $\varkappa \in \mathbf{Z}_p$. Lemma 1 tells us that it would make sense to define the mapping

$$\begin{aligned} \sigma_\varkappa : A_{p^m} &\to \mathbf{Z}_p \\ a &\to \sigma_k a \end{aligned}$$

where k is an element of the residue class $\varkappa \bmod p^m$.

Now let $\bar{a} = (\sigma_i a)$. By Lemma 1 $\bar{a} \in \overline{\mathfrak{A}}_p$ and if $a \in A_{p^m} \Rightarrow \bar{a} \in \bar{A}_{p^m}$. Define:

$$\begin{aligned} \lambda : \mathfrak{A}_p &\to \overline{\mathfrak{A}}_p \\ a &\to \bar{a} \end{aligned}$$

$$\lambda(ab) = (\sigma_i(ab)) = (\sigma_i(a) \cdot \sigma_i(b)) = (\sigma_i(a)) \cdot (\sigma_i(b)) = \lambda(a) \cdot \lambda(b)$$

so λ is a *homomorphism*.

Let now $\bar{a} = (\bar{\alpha}_k) \in \overline{\mathfrak{A}}_p$ and define $\alpha_i = \sum_{k=0}^{i} (-1)^k \binom{i}{k} \bar{\alpha}_k$.

LEMMA 2. *If* $\bar{a} \in \bar{A}_{p^m}$ *then* $\alpha_i = 0$ *for* $i \geq p^m$.

Proof. Let $i = s \cdot p^m + j$, $s \neq 0$, $0 \leq j < p^m$.

We may write $\alpha_i = \sum_{k=0}^{j} \left(\sum_{k' \equiv k \bmod p^m} (-1)^{k'} \binom{i}{k'} \right) \bar{\alpha}_k$. Let $k' = tp^m + k$, $0 \leq k < p^m$. If $t = \sum_{\nu \geq 0} \tau_\nu p^\nu$, $k = \sum_{\nu \geq 0} \varkappa_\nu p^\nu$, $s = \sum_{\nu \geq 0} \sigma_\nu p^\nu$, $j = \sum_{\nu \geq 0} \rho_\nu p^\nu$ then $i = \sum_{\nu \geq 0} \rho_\nu p^\nu + \sum_{\nu \geq 0} \sigma_\nu p^{\nu+m}$ and $k' = \sum_{\nu \geq 0} \varkappa_\nu p^\nu + \sum_{\nu \geq 0} \tau_\nu p^{m+\nu}$. Therefore

$$\binom{i}{k'} = \prod_{\nu \geq 0} \binom{\rho_\nu}{\varkappa_\nu} \prod_{\nu \geq 0} \binom{\sigma_\nu}{\tau_\nu} = \binom{j}{k} \binom{s}{t}$$

by Lucas's Theorem and we have:

$$\alpha_i = \sum_{k=0}^{j} (-1)^k \binom{j}{k} \left[\sum_{t=0}^{s} (-1)^t \binom{s}{t} \right] \bar{\alpha}_k \qquad \text{but} \qquad \sum_{t=0}^{s} (-1)^t \binom{s}{t} = (1-1)^s = 0.$$

Therefore $\alpha_i = 0$ for $i \geq p^m$.

Now let $a = \sum_{i \geq 0} \alpha_i x_i$ and define

$$\begin{aligned} \mu : \overline{\mathfrak{A}}_p &\to \mathfrak{A}_p \\ \bar{a} &\to a. \end{aligned}$$

By Lemma 2 it is then clear that if $\bar{a} \in \bar{A}_{p^m}$ that $\mu(\bar{a}) \in A_{p^m}$ and since every $\bar{a}$ is in some $\bar{A}_{p^m} \Rightarrow \mu(\bar{a}) \in \mathfrak{A}_p$.

LEMMA 3. $\mu \circ \lambda =$ *identity and* $\lambda \circ \mu =$ *identity.*

Proof. First we observe that $\bar{\alpha}_k = \sigma_k a = \sum_{j=0}^{k} (-1)^j \binom{k}{j} \alpha_j$ if $a = \sum_{i \geq 0} \alpha_i x_i \in \mathfrak{A}_p$. Let $\mu \circ \lambda (a) = a' = \sum_{i \geq 0} \alpha'_i x_i$ then

$$\alpha'_i = \sum_{k=0}^{i} (-1)^k \binom{i}{k} \bar{\alpha}_k = \sum_{k=0}^{i} (-1)^k \binom{i}{k} \sum_{j=0}^{k} (-1)^j \binom{k}{j} \alpha_j$$

but

$$\binom{i}{k}\binom{k}{j} = \frac{i!\,k!}{k!\,(i-k)!\,j!\,(k-j)!} = \frac{i!\,(i-j)!}{(i-j)!\,(i-k)!\,j!\,(k-j)!} = \binom{i}{j}\binom{i-j}{i-k}$$

therefore $\alpha'_i = \sum_{j=0}^{k} \left[(-1)^j \binom{i}{j} \sum_{k=j}^{i} (-1)^k \binom{i-j}{i-k} \right] \alpha_j$. Now for $j < i$ we have $\sum_{k=j}^{i} (-1)^k \binom{i-j}{i-k} = \pm (1-1)^{i-j} = 0$ and for $j = i$ the expression in the bracket is 1, therefore $\alpha'_i = \alpha_i$. $\lambda \circ \mu =$ identity is shown dually.

The mapping λ is therefore an isomorphism from $\mathfrak{A}_p$ onto $\overline{\mathfrak{A}}_p$ which maps A_{p^m} onto $\bar{A}_{p^m}$ and μ is the inverse of λ mapping $\bar{A}_{p^m}$ onto A_{p^m}.

COROLLARY 1. A_{p^m} *is a* $\mathbf{Z}_p$*-subalgebra of* $\mathfrak{A}_p$ *and is isomorphic to* $\sum_{i=0}^{p^m-1} \mathbf{Z}_p^{(i)}$.

Proof. By Theorem II: $\mathfrak{A}_p \approx \overline{\mathfrak{A}}_p$ and $A_{p^m} \approx \bar{A}_{p^m}$ but $\bar{A}_{p^m}$ is a $\mathbf{Z}_p$-subalgebra of $\overline{\mathfrak{A}}_p$ and therefore A_{p^m} is a $\mathbf{Z}_p$-subalgebra of $\mathfrak{A}_p$.

Theorem II gives us information about factorization in $\mathfrak{A}_p$. We state some corollaries to this effect:

COROLLARY 2. *Let* $a \in \mathfrak{A}_p$ *with* $p^{m-1} \leq \deg a < p^m$. *a is a zerodivisor in* $\mathfrak{A}_p$ *iff* $\sigma_k a = 0$ *for at least one* $k = 0, 1, \cdots, p^m - 1$.

Proof. In the following we denote by $\bar{a}$ the image of a under the isomorphism λ between $\mathfrak{A}_p$ and $\overline{\mathfrak{A}}_p$ defined above.

1) If a is a zerodivisor in $\mathfrak{A}_p \Rightarrow \exists b \neq 0, b \in \mathfrak{A}_p$ such that $ab = 0 \Rightarrow \bar{a} \cdot \bar{b} = \bar{0}, \bar{b} \neq \bar{0} \Rightarrow \sigma_k a \cdot \sigma_k b = 0$ for $k = 0, 1, 2, \cdots$ and $\exists k_0$ such that $\sigma_{k_0} b \neq 0 \Rightarrow \sigma_{k_0} a = 0 \Rightarrow \exists\, 0 \leq k'_0 \leq p^m - 1$ such that $\sigma_{k'_0} a = 0$ (see Lemma 1 above).

2) If $\sigma_{k_0} a = 0$ for $0 \leq k_0 \leq p^m - 1$. Take $\bar{b} = (\bar{\beta}_i) \in \overline{\mathfrak{A}}_p$ with $\bar{\beta}_i = 0$ if $i \not\equiv k_0 \bmod p^m$ and $\bar{\beta}_{k'_0} = 1$ if $k'_0 \equiv k_0 \bmod p^m$.

Let $b = \mu(\bar{b})$. Since $\bar{a} \cdot \bar{b} = 0 \Rightarrow a \cdot b = 0$ and since $\bar{b} \neq 0 \Rightarrow b \neq 0$.

It follows that a is a zerodivisor in $\mathfrak{A}_p$. (Note that b may be chosen in A_{p^m}).

COROLLARY 3. *$a \in \mathfrak{A}_p$ with $p^{m-1} \leq \deg a < p^m$. a is a unit in $\mathfrak{A}_p$ iff $\sigma_k a \neq 0$ for all $k = 0, 1, \cdots, p^m - 1$ and a^{p-2} is then the inverse of a.*

Proof. a is a unit in $\mathfrak{A}_p \iff \bar{a}$ is a unit in $\overline{\mathfrak{A}}_p \iff \sigma_k a$ is a unit in $\mathbf{Z}_p$ (which is a field) $\iff \sigma_k a \neq 0 \iff \sigma_k a \neq 0$ for $0 \leq k \leq p^m - 1$.

If $\sigma_k a \neq 0 \Rightarrow (\sigma_k a)^{p-2}$ is the inverse of $\sigma_k a$ in $\mathbf{Z}_p$ but $(\sigma_k a)^{p-2} = \sigma_k (a^{p-2}) \Rightarrow \bar{a}^{p-2}$ is the inverse of $\bar{a}$ in $\overline{\mathfrak{A}}_p \Rightarrow a^{p-2}$ is the inverse of a in $\mathfrak{A}_p$ if a is a unit.

COROLLARY 4. *Every non-zero element of $\mathfrak{A}_p$ which is not a unit is a zerodivisor. There are no irreducible elements in $\mathfrak{A}_p$.*

Proof. The first part of Corollary 4 follows at once from Corollary 3 and Corollary 2. Suppose next that a is not a unit in $\mathfrak{A}_p$. By Corollary 3 there exists a $k_0, 0 \leq k_0 \leq p^m - 1$, if $p^{m-1} \leq \deg a < p^m$, such that $\sigma_{k_0} a = 0$. Factor $\sigma_k a = \bar{\beta}_k \bar{\gamma}_k$ arbitrarily in $\mathbf{Z}_p$ if $0 \leq k \leq p^m - 1$ and $k \neq k_0$ and put $\bar{\beta}_{k'} = \bar{\beta}_k$ and $\bar{\gamma}_{k'} = \bar{\gamma}_k$ if $k' \equiv k \bmod p$. Furthermore let $\bar{\beta}_k = \bar{\gamma}_k = 0$ if $k \equiv k_0 \bmod p^m$. Put $\bar{b} = (\bar{\beta}_k)$, $\bar{c} = (\bar{\gamma}_k)$ then $\bar{b}, \bar{c} \in \overline{\mathfrak{A}}_p$ and $\bar{a} = \bar{b} \cdot \bar{c}$ where $\bar{b}$ and $\bar{c}$ are not units by Corollary 3. It follows that $a = b \cdot c$ with $b = \mu(\bar{b})$ and $c = \mu(\bar{c})$ and b, c are not units $\Rightarrow a$ is reducible.

Some properties of $\mathbf{Z}_p$ may be lifted to $\mathfrak{A}_p$. We give two such examples, but many more such examples might be given.

COROLLARY 5. (Fermat's Theorem) *For each $a \in \mathfrak{A}_p \Rightarrow a^p = a$* (If a is a unit $\Rightarrow a^{p-1} = 1$).

Proof. $(\sigma_k a)^p = \sigma_k a^p = \sigma_k a$ by Fermat's Th. in $\mathbf{Z}_p$.

$\Rightarrow \bar{a}^p = \bar{a} \Rightarrow a^p = a$ by Theorem II.

Remark. A proof of Fermat's Theorem in $\mathfrak{A}_p$ independent of Fermat's Theorem in $\mathbf{Z}_p$ was given in [4].

COROLLARY 6. (Euler's Criterion) *If $a \in \mathfrak{A}_p$ then a is a square in $\mathfrak{A}_p \iff a^{(p+1)/2} = a$ (or $a^{(p-1)/2} = 1$ if a is a unit).*

Proof. $\sigma_k a$ is quadratic rest in $\mathbf{Z}_p$ iff $(\sigma_k a)^{(p+1)/2} = \sigma_k a$ by Euler's Criterion in $\mathbf{Z}_p \Rightarrow$ Euler's Criterion in $\overline{\mathfrak{A}}_p \Rightarrow$ Euler's Criterion in $\mathfrak{A}_p$.

COROLLARY 7.

$$\text{(A)} \qquad \beta(s \mid i_\nu) = \sum_{k=i_1}^{s} (-1)^{k+\sum_\nu i_\nu} \binom{s}{k} \prod_\nu \binom{k}{i_\nu}$$

$$\text{(B)} \qquad \beta(s \mid i_\nu) = (-1)^s \left[\Delta^s \prod_\nu \binom{k}{i_\nu} \right]_{k=0}$$

where Δ is the difference operator from difference calculus.

Proof. (A) Let $a = \sum_{i \geq 0} \alpha_i x_i$, $\bar{a} = \sum_{k \geq 0} \bar{\alpha}_k x_k$ then from the proof of Theorem II we know that $\bar{\alpha}_k = \sum_{i=0}^{k} (-1)^i \binom{k}{i} \alpha_i$ and $\alpha_i = \sum_{k \geq 0} (-1)^k \binom{k}{i} \bar{\alpha}_k$.

For $a = x_i \Rightarrow \bar{\alpha}_k = (-1)^{i_\nu}\binom{k}{i_\nu}$ and for $a = \prod_\nu x_{i_\nu} = \sum_s \beta(s \mid i_\nu)\, x_s \Rightarrow \bar{\alpha}_k =$
$= \prod_\nu (-1)^{\sum_\nu i_\nu}\binom{k}{i_\nu}$ and therefore $\beta(s \mid i_\nu) = \sum_{k=i_1}^{s} (-1)^{k+\sum_\nu i_\nu}\binom{s}{k}\prod_\nu \binom{k}{i_\nu}$.

(B) In the difference calculus one proves the formula (see [7] pg. 132 formula (1)) $\sum_{k=0}^{s}(-1)^k\binom{s}{k} f(k) = (-1)^s \Delta^s f(0)$. Take $f(k) = (-1)^{\sum_\nu i_\nu}\prod_\nu \binom{k}{i_\nu}$ and the left side becomes $\beta(s \mid i_\nu)$ according to (A).

Remark. By (A) $\beta(s \mid i, j) = (-1)^{s+i+j}\binom{s}{i}\binom{i}{s-j} = \sum_{k=i}^{s}(-1)^{k+i+j}\binom{s}{k}\binom{k}{i}\binom{k}{j}$
and we get the identity: $(-1)^s\binom{s}{i}\binom{i}{s-j} = \sum_{k=i}^{s}(-1)^k\binom{s}{k}\binom{k}{i}\binom{k}{j}$ for $s \geq i \geq j$.

LITERATURE

[1]–[5] see Nota I.
[6] TH. GIEBUTOWSKI, Thesis. University of Massachusetts 1971.
[7] CH. JORDAN, *Calculus of Finite Differences*, Chelsea Publ. Co. 1965.