UNIVERSITATIS IAGELLONICAE ACTA MATHEMATICA, FASCICULUS XLVI
2008

NOTES ON STRUCTURE OF COMPLETE DISCRETE VALUATION RINGS

BY TOMASZ GRYSZTAR

Abstract. This note shows how the structure of a complete discrete valuation ring can be derived from some ring of formal Laurent series and its natural valuation. Later there are introduced infinite coordinate systems on such ring, and some properties of the operations on those coordinates are shown. In a special case of p-adic field there is shown how the sum of two p-adic numbers can be approximated with the elementary operations on the coordinates only.

1. Discrete valuations. Let K be any field. A discrete valuation on K is a mapping $v : K \setminus \{0\} \to \mathbb{Z}$ with additional value $v(0) = \infty$ such that for any $x, y \in K$:

$$v(x \cdot y) = v(x) + v(y)$$

and

$$v(x + y) \geq \min\{v(x), v(y)\},$$

with the rule that $a < \infty$ for any $a \in \mathbb{Z}$.

Given a field K with a valuation v, the set $R_v = \{x \in K : v(x) \geq 0\}$ is a ring with the unique maximal ideal $M_v = \{x \in K : v(x) > 0\}$. The R_v is called the valuation ring of v. The R_v/M_v is a field, which is called the residue field of the valuation ring R_v.

If we fix any $a \in (0, 1) \subset \mathbb{R}$, then the valuation v induces a norm on K, defined as $\| x \| = a^{v(x)}$ for an $x \in K \setminus \{0\}$ (with $\| 0 \|$ set to be 0). The metric induced by such norm makes K an ultrametric space and its topology is independent of the choice of a. Thus we will refer to this topology directly in the terms of v. For example, the sequence of elements $x_0, x_1, \ldots \in K$ converges to zero if and only if $v(x_n) \to \infty$.

We will call a sequence $x_0, x_1, \ldots \in K$ a Cauchy sequence iff for any $M \in \mathbb{Z}$ there exists $N \in \mathbb{N}$ such that for all $m, n > N$:

$$v(x_m - x_n) > M.$$

This is equivalent to the fact that the sequence is a Cauchy sequence in any metric induced by v. The field K with a discrete valuation v such that every Cauchy sequence has a limit in the topology induced by v will be called a complete discrete valuation field.

THEOREM 1.1. *Let K be a complete discrete valuation field with valuation v. For any sequence $x_0, x_1, \ldots \in K$, the series:*

$$\sum_{n=0}^{\infty} x_n$$

converges if and only if $x_n \to 0$.

The proof of this fact may be found in [**1**] (chapter II, 1).

2. Structure of a complete discrete valuation field. Let K be a field complete with respect to a valuation $v : K \to \mathbb{Z} \cup \{\infty\}$, let R_v and M_v be the valuation ring and its unique maximal ideal. Choose an $m \in K$ such that $v(m) = 1$. Then $M_v = (m)$ and m is called a uniformizing element of R_v.

Let A be any subring in the R_v and $A((X))$ a ring of formal Laurent series in one variable. Any element of $A((X))$ can be written in the form:

$$f = \sum_{n=0}^{\infty} a_n X^{n+ord_X(f)}.$$

Now for such Laurent series we may define $f(m) \in K$ as the sum of the series:

$$f(m) = \sum_{n=0}^{\infty} a_n m^{n+ord_X(f)},$$

which converges, since $v(a_n m^{n+ord_X(f)}) \to \infty$ (as $v(a_n) \geq 0$ for each n). The mapping

$$\Psi_m : A((X)) \ni f \mapsto f(m) \in K$$

is a homomorphism of the rings. Our objective is to show that if A has some additional property, then Ψ_m is an epimorphism, K is isomorphic to $A((X))/ker\Psi_m$, and the valuation v can be derived from ord_X.

Let k be the residue field of R_v. A set $T \subset R_v$ is a set of representatives for K if it is mapped bijectively on k under the canonical map $R_v \to R_v/M_v = k$.

Let T be a set of representatives for K and $x = x_0$ be any element of R_v. There exists exactly one $a_0 \in T$ such that $x_0 - a_0 \in M_v$ (also note that if $x_0 \notin M_v$ then $a_0 \notin M_v$). Inductively, if $x_n \in R_v$, then there exists

exactly one $a_n \in T$ such that $x_n = a_n + x_{n+1}m$, where $x_{n+1} \in R_v$, and $x_0 = a_0 + a_1 m + \ldots + a_n m^n + x_{n+1}m^{n+1}$. From this follows:

$$x = \sum_{n=0}^{\infty} a_n m^n.$$

Now let y be any non-zero element of K. Let $x = y \cdot m^{-v(y)}$, then $v(x) = 0$ and x can be written as the sum of series as the one above, with $a_0 \notin M_v$. Thus:

$$y = \sum_{n=0}^{\infty} a_n m^{n+v(y)}.$$

THEOREM 2.1. *Let K be a complete discrete valuation field, with valuation v and the valuation ring R_v. Let A be a subring in R_v such that A contains a set of representatives for K, and let m be a uniformizing element of R_v. Then the mapping*

$$\Psi_m : A((X)) \ni f \mapsto f(m) \in K$$

is an epimorphism such that $v(x) = max\{ord_X(f) : f \in \Psi_m^{-1}(x)\}$ for each $x \in K$.

PROOF. We already know that Ψ_m is a homomorphism. Let $T \subset A$ be a set of representatives for K. Then, as we have already seen, each non-zero element $x \in K$ can be written as:

$$x = \sum_{n=0}^{\infty} a_n m^{n+v(x)},$$

where a_0 is a unit in R_v. Thus $x = \Psi_m(f_x)$, where:

$$f_x(X) = \sum_{n=0}^{\infty} a_n X^{n+v(x)},$$

and so Ψ_m is an epimorphism. Also, since $ord_X(f_x) = v(x)$, then

$$v(x) \leq max\{ord_X(f) : f \in \Psi_m^{-1}(x)\}.$$

Let $g \in A((X))$ be a series such that $ord_X(g) > v(x)$. Then:

$$(f - g)(X) = a_0 X^{v(x)} + \sum_{n=1}^{\infty} b_n X^{n+v(x)}$$

with some $b_n \in A$. From this follows that $v((f-g)(m)) = v(x)$, so $f - g \notin ker\Psi_m$, and thus $g \notin \Psi_m^{-1}(x)$. Therefore, $ord_X(g) \leq v(x)$ for each $g \in \Psi_m^{-1}(x)$ and so:

$$v(x) \geq max\{ord_X(f) : f \in \Psi_m^{-1}(x)\},$$

which completes the proof. □

From the formula for valuation v in the theorem above, for $x \in R_v$ there exists $f \in \Psi_m^{-1}(x)$ such that $v(x) = ord_X(f)$, and so $f \in A[[X]]$. Conversely, for any $f \in A[[X]]$:

$$v(\Psi_m(f)) \geq ord_X(f) \geq 0.$$

Therefore, $\Psi_m(A[[X]]) = R_v$, and for any $x \in R_v$ holds:

$$v(x) = max\{ord_X(f) : f \in \Psi_m^{-1}(x) \cap A[[X]]\}.$$

We will now apply this theorem to an example. Fix a prime p and let $K = \mathbb{Q}_p$ be the field of p-adic numbers and $v = ord_p$, the p-adic valuation (their detailed description may be found in [**1**]). The $R_v = \mathbb{Z}_p$ is called the ring of p-adic integers. The $T = \{0, 1, \ldots, p-1\}$ is the set of representatives for $\mathbb{Q}_p$, and so we can take $A = \mathbb{Z}$, a minimal subring of $\mathbb{Z}_p$ that contains T. The element p of the ring $\mathbb{Z}_p$ is an uniformizing element of this ring, so we can define Ψ_p that maps $\mathbb{Z}((X))$ onto $\mathbb{Q}_p$.

We know that any element $x \in \mathbb{Q}_p$ has a unique representation:

$$x = \sum_{n=0}^{\infty} a_n p^{n+ord_p(x)},$$

with $a_n \in T$ for all n. It means that x is the isomorphic image of the class of equivalence for the series in $\mathbb{Z}((X))$ with all the coefficients in T. Therefore, for any $f \in \mathbb{Z}((X))$ we may find such $f_p \in \mathbb{Z}((X))$, that $f - f_p \in ker\Psi_p$ and f_p has all coefficients in T. We will call such f_p a base p reduction of f. For example, if we take $x = (p-1) + (p-1)p$, $y = 1$ and sum their corresponding power series, the result is $p + (p-1)X$. The reduction of such power series is X^2, obtained by the substraction $p + (p-1)X - X^2 \in ker\Psi_p$.

3. Coordinate systems on discrete valuation rings. Let K, v, R_v and M_v be as in the previous section. Let us choose m – an uniformizing element of R_v and T – a set of representatives for K.

We have seen that each element $x \in R_v$ (including zero) may be obtained as a sum:

$$x = \sum_{n=0}^{\infty} a_n m^n,$$

where each a_n is an element of T and $a_n \in M_v$ for any $n < v(x)$. Thus if $0 \in T$, then $a_n = 0$ for $n < v(x)$, and if we represent x as in the proof of theorem 2.1 (with the assumption that x is non-zero):

$$x = \sum_{n=0}^{\infty} b_n m^{n+v(x)},$$

then $b_n = a_{n+v(x)}$, and so those two representations are equivalent.

The choice of T and m such that m is an uniformizing element of R_v and T is a set of representatives for K such that $0 \in T$ will be called a coordinate system on R_v. We will call the set T the set of coefficients for this system. Each element $x \in R_v$ is then uniquely determined by a sequence of elements of $a_n \in T$ such that:

$$x = \sum_{n=0}^{\infty} a_n m^n.$$

We will call the coefficients a_n the coordinates of x in the given coordinate system.

Because each element $a \in T$ corresponds to unique element $[a] \in k$ (where k is the residue field of K), the system of coordinates gives us also a bijection between elements of R_v and $k^{\mathbb{N}}$:

$$\Phi : R_v \ni \sum_{n=0}^{\infty} a_n m^n \mapsto ([a_0], [a_1], \ldots) \in k^{\mathbb{N}}.$$

On $k^{\mathbb{N}}$ we have a natural structure of a ring, with operations defined as:

$$(x_0, x_1, \ldots) + (y_0, y_1, \ldots) = (x_0 + y_0, x_1 + y_1, \ldots)$$

and

$$(x_0, x_1, \ldots) \cdot (y_0, y_1, \ldots) = (x_0 \cdot y_0, x_1 \cdot y_1, \ldots),$$

where $(x_0, x_1, \ldots)$ and $(y_0, y_1, \ldots)$ are any elements of $k^{\mathbb{N}}$. Therefore, through Φ we may define the additional operations on R_v, for any $x, y \in R_v$ defined as:

$$x \oplus y = \Phi^{-1}(\Phi(x) + \Phi(y))$$

and

$$x \odot y = \Phi^{-1}(\Phi(x) \cdot \Phi(y)).$$

The set R_v with operations $\oplus$ and $\odot$ – induced by the chosen coordinate system – forms a ring, with a characteristic equal to the characteristic of k. The unit of this ring is the element $\overline{1} = \Phi^{-1}(1, 1, 1, \ldots)$. We are going to denote $\overline{a} = \Phi^{-1}(a, a, a, \ldots)$ for any $a \in k$. It follows from the definitions that for any $a, b \in k$ there is $\overline{a + b} = \overline{a} \oplus \overline{b}$ and $\overline{a \cdot b} = \overline{a} \odot \overline{b}$.

Since v has a simple interpretation in term of the coordinates, it is a straightforward conclusion from the definitions, that $v(x \oplus y) \geq min(v(x), v(y))$ and $v(x \odot y) \geq max(v(x), v(y))$ for any $x, y \in R_v$.

If $x = \sum_{n=0}^{\infty} a_n m^n$ then it is easy to verify that $x \odot m^n = a_n m^n$. This allows to recover the coordinates of a particular element of R_v given the $\odot$ operation, and any element $x \in R_v$ may be represented in the following form:

$$x = \sum_{n=0}^{\infty} x \odot m^n.$$

This example shows that operations induced by a coordinate system may provide some insight into the algebraic structure of R_v itself. Because of their relatively easy computability, it may be interesting to find out whether it may be possible to find formulas that would allow to compute the results of standard operations on R_v using only the elementary operations on the coordinates of those values. This would not be possible if we exclusively considered $\oplus$ and $\odot$ as such elementary operations, since with those operations the result has the coefficient at any given position dependent on the coefficients on the same positions in the operands only. For this reason we are going to use one more operation as an elementary one – the shift of coefficients.

Shifting the coefficients of any element $x \in R_v$ one position to the right is exactly the same operation as multiplying (in the standard sense) this element by m. For this reason we will use the mx symbol to represent x shifted one position to the right, and $m^n x$ to represent the result of applying such shift n times (which results in x shifted right by n positions).

To make some of later formulas simpler, we are going to give the $\oplus$ and $\odot$ operator a priority over $+$ and $\cdot$, so $x \oplus y + z = (x \oplus y) + z$. However, we are going to use shift operator as having priority over $\oplus$ and $\odot$, and to avoid the resulting ambiguity we will always explicitly state the $\cdot$ operator when it is used and is not a shift operation. So, for example, $mx \oplus y = (mx) \oplus y$, but $m \cdot x \oplus y = m \cdot (x \oplus y)$.

Since both $\oplus$ and $\odot$ break down to the operations on the coefficients on parallel positions, and the shift just moves the coefficients one position to the right, it is easy to see that $mx \oplus my = m(x \oplus y)$ and $mx \odot my = m(x \odot y)$ for any $x, y \in R_v$. Also, for any $a \in k$, there is $\overline{a} \odot mx = m(\overline{a} \odot x)$.

4. Approximating the sum of p-adic numbers. Let us go back to the example of the field of p-adic numbers. There is a canonical coordinate system on $\mathbb{Z}_p$ given by the set of coefficients $T = \{0, 1, \ldots, p-1\}$ and uniformizing element p, and we are going to use this coordinate system throughout this section. We will also often call the coefficients of this system the p-adic digits. The residue field of Z_p is F_p, the field of numbers modulo p. We are also going to denote the ring $(\mathbb{Z}_p, \oplus, \odot)$ with the symbol $\mathbb{Z}_p^{\oplus,\odot}$, as opposed to simple $\mathbb{Z}_p$ meaning the ring $(\mathbb{Z}_p, +, \cdot)$ with $\oplus$ and $\odot$ as additional operations.

In this section our goal is to provide formulas for calculating any given number of digits of sum of two p-adic numbers, using the three elementary operations: $\oplus$, $\odot$ and the shift (multiplication by p) only.

First we are going to construct $C \in F_p[X, Y]$, such a polynomial that for any $x, y \in \{0, 1, \ldots, p-1\}$ it has value $C([x], [y]) = [1]$ if $x + y \geq p$ and $C([x], [y]) = [0]$ otherwise. We start with defining for any $a, b \in \{0, 1, \ldots, p-1\}$

the polynomial:

$$D_{a,b}(X,Y) = \prod_{\substack{0\le i\le p-1\\ i\neq p-a}} (X+[i]) \cdot \prod_{\substack{0\le i\le p-1\\ i\neq p-b}} (Y+[i]).$$

Obviously, $D_{a,b}([x],[y]) = [0]$ for any $x, y \in \{0,1,\ldots,p-1\}$ unless $x = a$ and $y = b$. The value of $D_{a,b}([a],[b])$ is the product of two values, each being the product of all non-zero values of F_p. Since F_p is a field, such product has to be the unit, as for any element in the first product, there is exactly one element in second product being the inverse element of the former. Thus $D_{a,b}([a],[b]) = [1]$.

Now, in order to construct the required polynomial C it is enough to sum the polynomials $D_{a,b}$ for any $a, b \in \{0,1,\ldots,p-1\}$ such that $a + b \geq p$. Therefore, we may define C as:

$$C(X,Y) = \sum_{i=1}^{p-1} \sum_{j=1}^{i} D_{i,p-j}(X,Y).$$

For example, for $p = 2$, $C(X,Y) = XY$ and for $p = 3$, $C(X,Y) = X(X + [1])Y(Y+[2]) + X(X+[2])Y(Y+[2]) + X(X+[2])Y(Y+[1])$, which upon the reduction becomes $C(X,Y) = [2]XY(X+Y+[1])$.

Consider now the polynomial $\overline{C} \in \mathbb{Z}_p^{\oplus,\odot}[X,Y]$ being the polynomial C transformed through the mapping which maps each coefficient a of polynomial from $F_p[X,Y]$ into the coefficient $\overline{a}$ of polynomial in $\mathbb{Z}_p^{\oplus,\odot}[X,Y]$. For instance, for $p = 2$, $\overline{C}(X,Y) = X \odot Y$, and for $p = 3$, $\overline{C}(X,Y) = \overline{[2]} \odot X \odot Y \odot (X \oplus Y \oplus \overline{[1]})$.

Directly from definitions it follows that for $a, b \in \{0,1,\ldots,p-1\}$ there is $\overline{C}(a,b) = 0$ when $a + b < p$ and $\overline{C}(a,b) = 1$ otherwise. Because polynomial $\overline{C}$ has no constant term, and all of its coefficients are of the form $[a]$ for some $a \in F_p$, we may use the formulas given at the end of previous section to prove that $\overline{C}(px,py) = p\overline{C}(x,y)$ for any $x, y \in \mathbb{Z}_p$. It is also true for all such x, y that $\overline{C}(p \odot x, p \odot y) = p \odot \overline{C}(x,y)$, since $p \odot p = p$ and $\overline{C}$ has no constant term.

THEOREM 4.1. *Let $\mathbb{Z}_p$ be the ring of p-adic integers with operations $\oplus$ and $\odot$ induced by the canonical coordinate system, and the polynomial $\overline{C} \in \mathbb{Z}_p^{\oplus,\odot}[X,Y]$ defined as above. For any $x, y \in \mathbb{Z}_p$ there holds:*

$$x + y = x \oplus y + p\overline{C}(x,y).$$

PROOF. For any given n, let us take $x_n = x \odot p^n = a_n \cdot p^n$, $y_n = y \odot p^n = b_n \cdot p^n$, where $a_n, b_n \in \{0,1,\ldots,p-1\}$. $a_n + b_n = (c_n \cdot p + d_n)$, with $0 \leq d_n < p$ and c_n being either zero when $a_n + b_n < p$, or 1 otherwise, which gives $c_n = \overline{C}(a_n, b_n)$. In F_p, then $[a_n] + [b_n] = [d_n]$; therefore, $x_n \oplus y_n = d_n \cdot p^n$.

Finally:

$$x_n + y_n = (c_n \cdot p + d_n) \cdot p^n = x_n \oplus y_n + p \cdot (p^n \cdot c_n) = x_n \oplus y_n + p(p^n \overline{C}(a_n, b_n))$$
$$= x_n \oplus y_n + p\overline{C}(p^n a_n, p^n b_n) = x_n \oplus y_n + p\overline{C}(x_n, y_n).$$

Now let us go back to the complete values of x and y:

$$\begin{aligned} x + y &= \sum_{n=0}^{\infty} x \odot p^n + \sum_{n=0}^{\infty} y \odot p^n = \sum_{n=0}^{\infty} (x \odot p^n + y \odot p^n) \\ &= \sum_{n=0}^{\infty} (x_n + y_n) = \sum_{n=0}^{\infty} (x_n \oplus y_n + p\overline{C}(x_n, y_n)) \\ &= \sum_{n=0}^{\infty} x_n \oplus y_n + \sum_{n=0}^{\infty} p\overline{C}(x_n, y_n) \\ &= \sum_{n=0}^{\infty} (x \odot p^n) \oplus (y \odot p^n) + p \sum_{n=0}^{\infty} \overline{C}(x \odot p^n, y \odot p^n) \\ &= \sum_{n=0}^{\infty} (x \oplus y) \odot p^n + p \sum_{n=0}^{\infty} \overline{C}(x, y) \odot p^n \\ &= x \oplus y + p\overline{C}(x, y). \end{aligned}$$

All the operations on infinite sums performed above are allowed, since all the series here converge, as in each one the elements are divisible by linearly progressing powers of p with n rising. This completes the proof of the theorem. □

The formula proved above gives us the first approximation of the sum $x+y$, as it shows that $v(x + y - x \oplus y) = v(p\overline{C}(x, y)) \geq 1$. This means that $x \oplus y$ is an approximation of at least one digit of $x + y$, which is an quite obvious fact. However, since every term in the polynomial $\overline{C}$ is a multiple of both X and Y, it is always true that $v(\overline{C}(x, y)) \geq v(y)$ and thus if we have any formula of the form $x + y = A_n(x, y) + R_n(x, y)$ with $v(R_n(x, y)) \geq n$, then by applying the formula from the theorem above once more to the right-hand side of the equation, we get $x + y = A_n(x, y) \oplus R_n(x, y) + p\overline{C}(A_n(x, y), R_n(x, y))$, and $v(p\overline{C}(A_n(x, y), R_n(x, y))) \geq n + 1$. This allows us to recursively get the approximation of any required accurateness. We start from $A_1(x, y) = x \oplus y$ and $R_1(x, y) = p\overline{C}(x, y)$, and continue inductively with $A_{n+1}(x, y) = A_n(x, y) \oplus R_n(x, y)$ and $R_{n+1}(x, y) = p\overline{C}(A_n(x, y), R_n(x, y))$. By induction, $x + y = A_n(x, y) + R_n(x, y)$ and $v(R_n(x, y)) \geq n$ for all n. Because $A_n(x, y)$ is obtained solely through combinations of the $\oplus$ operation, polynomial $\overline{C}$ and shift, it fulfils the goal stated for this section.

$A_n(x,y)$ approaches $x+y$ as n approaches infinity, and since

$$A_n(x,y) = x \oplus y \oplus \bigoplus_{i=1}^{n} R_i(x,y),$$

we may conclude that:

$$x + y = x \oplus y \oplus \bigoplus_{i=1}^{\infty} R_i(x,y).$$

We are now going to fix $p = 2$ and show how it works in this simple case. As F_2 is a boolean ring, so is the $\mathbb{Z}_2^{\oplus,\odot}$; thus, $x \odot x = x$ and $x \oplus x = 0$ for any $x \in \mathbb{Z}_2$.

THEOREM 4.2. *Let $\mathbb{Z}_2$ be the ring of 2-adic integers with operations $\oplus$ and $\odot$ induced by the canonical coordinate system. For any $x, y \in \mathbb{Z}_2$ there holds:*

$$x + y = x \oplus y \oplus \bigoplus_{n=1}^{\infty} R_n(x,y),$$

where:

$$R_n(x,y) = 2^n(x \odot y) \odot \bigodot_{i=1}^{n-1} 2^i(x \oplus y).$$

PROOF. Note that $v(R_n(x,y)) \geq n$ for any $x, y \in \mathbb{Z}_2$. We are going to prove that for any N:

$$x + y = x \oplus y \oplus \bigoplus_{n=1}^{N-1} R_n(x,y) + R_N(x,y) \tag{1}$$

and this will be enough to prove the theorem, as it shows that the difference between the $x + y$ and the partial sum of the series from the statement of the theorem has the valuation at least N, and thus approaches zero.

Since in the case $p = 2$ the polynomial $\overline{C}$ has form $\overline{C}(X,Y) = X \odot Y$, applying Theorem 4.1, we obtain the formula:

$$x + y = x \oplus y + 2(x \odot y) \tag{2}$$

for any $x, y \in \mathbb{Z}_2$. This formula is identical to (1) for the case of $N = 1$, because $R_1(x,y) = 2(x \odot y)$. We will now prove (1) by induction for all other values of N. Assume that we have established the formula:

$$x + y = x \oplus y \oplus \bigoplus_{n=1}^{N-2} R_n(x,y) + R_{N-1}(x,y)$$

and let us apply formula (2) to the right-hand side of this equation:

$$\begin{aligned} x+y &= x\oplus y\oplus \bigoplus_{n=1}^{N-2} R_n(x,y)\oplus R_{N-1}(x,y) \\ &\quad + 2\left(\left(x\oplus y\oplus \bigoplus_{n=1}^{N-2} R_n(x,y)\right)\odot R_{N-1}(x,y)\right) \\ &= x\oplus y\oplus \bigoplus_{n=1}^{N-1} R_n(x,y) \\ &\quad + 2\left((x\oplus y)\odot R_{N-1}(x,y)\right)\oplus 2\bigoplus_{n=1}^{N-2} R_n(x,y)\odot R_{N-1}(x,y). \end{aligned}$$

Now:

$$\begin{aligned} 2\left((x\oplus y)\odot R_{N-1}(x,y)\right) &= 2(x\oplus y)\odot 2\left(2^{N-1}(x\odot y)\right)\odot \bigodot_{i=1}^{N-2} 2\left(2^i(x\oplus y)\right) \\ &= 2^N(x\odot y)\odot\left(\bigodot_{i=1}^{N-2} 2^{i+1}(x\oplus y)\right)\odot 2(x\oplus y) = R_N(x,y), \end{aligned}$$

so in order to finish the proof, it suffices to show that:

$$\bigoplus_{n=1}^{N-2} R_n(x,y)\odot R_{N-1}(x,y) = 0.$$

Notice that for any $x, y \in \mathbb{Z}_2$:

$$x\odot y\odot(x\oplus y) = x\odot x\odot y\oplus x\odot y\odot y = x\odot y\oplus x\odot y = 0.$$

Therefore, for any n and m such that $m < n$:

$$2^m(x\odot y)\odot R_n(x,y) = 2^m(x\odot y)\odot 2^n(x\odot y)\odot \bigodot_{i=1}^{n-1} 2^i(x\oplus y) = 0,$$

because $2^m(x\odot y)$ multiplies to zero with the $2^i(x\oplus y)$ for $i = m$. And thanks to this, we obtain:

$$R_m(x,y)\odot R_n(x,y) = 0$$

for any n and m such that $m \neq n$. This completes the proof. □

References

1. Bachman G., *Introduction to p-adic numbers and valuation theory*, Academic Press, 1964.
2. Engler A. J., Prestel A., *Valued fields*, Springer-Verlag, 2005.
3. Nagata M., *Theory of Commutative Fields*, American Math. Soc., 1993.

Received May 30, 2007

Institute of Mathematics
Jagiellonian University
ul. Łojasiewicza 6
30-348 Kraków, Poland